CS 2000 Management Tools Fault Management

The procedures available in the fault management section are listed under the following categories:

- Alarms
- Audit
- Line maintenance
- Trunk maintenance
- Logs
- CS 2000 Management Tools server
- Hardware
- Communications

Alarms

The table below lists the available procedures related to alarms.

Alarms procedures

Procedure	Page
CS 2000 Management Tools fault management overview	7
Accessing the Alarm Manager	11
Retrieving details about an alarm	17
Accessing the Alarm History	21
Acknowledging alarms	23
De-acknowledging alarms	25
Viewing acknowledged alarms	27

Alarms procedures

Audit

The table below lists the available procedures related to the audit.

Audit procedures

Line maintenance

The table below lists the available procedures related to line maintenance using the Line Maintenance Manager (LMM).

Line maintenance procedures

Trunk maintenance

The table below lists the available procedures related to trunk maintenance using the Trunk Maintenance Manager (TMM).

Trunk maintenance procedures

Logs

The table below lists the available procedures and information related to logs.

Logs procedures

Logs procedures

CS 2000 Management Tools server

The table below lists the available procedures related to the CS 2000 Management Tool server.

CS 2000 Management Tools server procedures

Procedure	Page
Performing a manual failover on a Sun Netra 240 in a two-server configuration	157

Hardware

The table below lists the available procedures related to hardware.

Hardware procedures

Procedure	Page
Replacing a failed disk drive in-service	159
Cleaning the DAT drive on the Netra T1400	167

Communications

The table below lists the available procedures related to communications.

Communications procedures

Procedure	Page
Restoring SSH communication between the CS 2000 Management Tools server and the CS 2000 Core Manager	169
Correcting a CORBA configuration issue between the CS 2000 Management Tools server and the MG 9000 Manager server	173

CS 2000 Management Tools fault management overview

Fault management strategy

The Succession Server Platform Foundation Software (SSPFS) on the CS 2000 Management Tools server consists of several common components, including a fault management sub-system. The network elements forward their alarms to the fault management sub-system using standard SNMP traps. The alarm sub-system consolidates the alarms from the network elements and provides the user with the ability to monitor both active and historical alarms.

User interface

A user can perform fault management using one of two interfaces:

- A user can view, filter, and acknowledge alarms through the CS2000 Management Tools GUI.
- A user can scan all SNMP-based traps that are sent by its managed network elements (NEs) through the command line syslog sub-system.

CS2000 Management Tools GUI

The CS2000 Management Tools GUI provides both an Alarm Manager and an Alarm History window for viewing alarms. Active alarms are typically viewed with the Alarm Manager, while the Alarm History window provides both active and inactive alarms. Both provide information on alarms in a tabular format. There are methods for filtering alarms to show only alarms for a particular network element, of a particular severity or alarm category.

Alarm severity color codes

Based on alarm severity, each alarm has an associated color code as shown in the Alarm Severity Color Codes figure.

- Critical and major - red
- Minor - amber
- Warning - yellow

Alarm Severity Color Codes

	UAS-S	Processing Error	2001-08-31 18:17:11	Minor	Software Error
	UAS-S	Processing Error	2001-09-11 08:31:33	Critical	Software Error
	UAS-S	Processing Error	2001-09-11 08:31:33	Major	File Error
	UAS-S	Processing Error	2001-09-11 08:31:33	Minor	Software Error
	UAS-S	Processing Error	2001-09-11 08:31:33	Warning	Software Error

Alarm totals

The Alarm Manager browser provides an alarm summary of the total number of active alarms, as well as the specific number of alarms for each severity (for example, Critical, Major, Minor, and Warning). This summary is located in the lower left-hand corner of the alarm manager below the “Active Alarm List”. The Alarm History browser provides the total number of alarms, but does not show the number of alarms for any severity. In addition, both the Alarm Manager and the Alarm History windows include the time the display was last updated.

Syslog traplogger interface

The SESM server application on the CS 2000 Management Tools server uses UNIX syslog to store SNMP traps that arrive from network elements into the CS 2000 Management Tools server. The CS 2000 Management Tools server sends messages to the UNIX daemon syslogd, which logs messages into a set of files described by the configuration file /etc/syslog.conf. The file containing SNMP traps is /var/log/ptmlog.

Note: Log entries in the ptmlog file are not forwarded to any external systems, such as the OSS. These logs are intended as a local tool to maintain a record of all incoming traps from devices managed by the SESM server application.

The syslog traplogger interface is automatically set up by scripts and is started when the SESM server application is started or restarted. There are currently three configuration parameters for the syslog traplogger interface:

- the maximum file size
- the hour when file rotation backup occurs
- the minute when file rotation backup occurs

The parameters mentioned above can be configured using the “configure” tool on the CS 2000 Management Tools server. Refer to procedure “Configuring log reporting” in this document.

SESM server application debug logs

These are debug log files residing on the CS 2000 Management Tools server that are produced by the SESM server application. Optionally, the maximum size, maximum number of files, default debug levels, log file name, and other options can be configured using the “ configure” tool on the CS 2000 Management Tools server. Refer to procedure “Configuring log reporting” in this document.

There are three debug log file name extensions: mi2, misc, and pa. The “mi2” log files (for example, ptmdebuglog1.mi2) contains logs from the SESM server application. This is typically the largest and most significant log file. The “pa” logs files (for example, ptmdebuglog1.pa) are produced by the Proxy Agent which is a different application that is also part of the SESM server application. The “misc” log files (for example, ptmdebuglog1.misc) are produced by miscellaneous parts of the SESM server application. The “misc” file could contain critical errors such as startup errors in the SESM server application processes or OutOfMemory errors.

The logs are located in the /opt/nortel/NTsesm/admin/logs directory and should not be erased. They rotate when necessary, such that the file size or number of log files remain manageable. Display the log files using the UNIX command "ls -alt" in this directory. The newest logs will have a "1" in the title (assuming a default rotation) such as ptmdebuglog1.mi2. Older files that have been rotated may be named ptmdebuglog2.mi2 or ptmdebuglog3.mi2. The oldest file, for example ptmdebulog7.mi2, is deleted during the next rotation.

The /opt/nortel/NTsesm/admin/logs directory contains the createDB_<date>.log file created during the installation of the SESM server application. This file contains debug information from the initial creation of the SESM server application data base schema. This log file does not persist across upgrades of the SESM software.

CS 2000 Management Tools logs

All applications on the CS 2000 Management Tools server and network elements managed by the CS 2000 Management Tools use the SSPFS logging Application Program Interface (API) to record their logs. This API also provides the customer log feed to the OSS Fault Collector. The API supports five levels of custlogs:

- critical
- major
- minor
- warning
- none

The SSPFS logging API also provides four types of logs:

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

Note: Syslog has built-in capabilities to forward logs to another IP address. This functionality is used to send the logs in the SSPFS custlog feed to the OSS Fault Collector.

Syslog forwarding is configured using the Syslog Configuration option at the CS 2000 Management Tools server command line interface (CLI). This option modifies the syslog.conf text file (a standard syslog file) which dictates how syslog operates. It can define whether to record the logs on the local machine and/or whether to send them to another machine (such as the OSS Fault Collector). Syslogs are controlled on a log-level basis, such that critical logs can be handled one way and warning logs another way.

In general, the only logs that will be forwarded are customer logs which contain alarm logs. Although, this can be customized using Syslog Configuration.

Note: Third party tools can also be used to set up the CS 2000 Management Tools server to forward syslog alarms to the OSS in standard formats (Switch Control Center (SCC2) or Nortel Networks STD).

Accessing the Alarm Manager

Application

This procedure provides access to service-related alarms on the hardware application. The Alarm Manager provides information on the fields described in the following table:

Alarm Manager field details

Field Name	Description
Network Element name	Provides the name of the Network Element for which the selected alarm is being raised.
Category	Represents the alarm problem category values (ITU-T X.733): “Communications” “Quality of Service” “Processing Error” “Equipment Error” “Environment”
Alarm Time	Represents the time that the alarm was raised in the following format: HH:MM:SS day-Month-year
Severity	Provides the associated severity of the alarm being raised. The range of values is as follows: “Critical” “Major” “Minor” “Warning”

Alarm Manager field details

Field Name	Description
Probable Cause	Provides the probable cause of the particular alarm (X.733 Probable Cause): “Adapter Error” “Non-Repudiation Failure” “Bandwidth Reduced” “Call Establishment Error” “Communications Protocol Error” “Communications Subsystem Error” “Configuration or Customization Error” “Congestion” “Corrupt Data” “CPU Cycles Limit Exceeded” “Data Set or Modem Error” “Degraded Signal” “DTE DCE Interface Error” “Enclosure Door Open” “Equipment Malfunction” “Excessive Vibration” “File Error” “Fire Detected” “Flood Detected”

Alarm Manager field details

Field Name	Description
	“Framing Error” “Heating, Ventilation, or Cooling System Problem” “Humidity Unacceptable” “Input Output Device Error” “Input Device Error” “LAN Error” “Leak Detected” “Local Node Transmission Error” “Loss of Frame” “Loss of Signal” “Material Supply Exhausted” “Multiplexer Problem” “Out of Memory” “Output Device Error” “Performance Degraded” “Pressure Unacceptable” “Pump Failure” “Queue Size Exceeded” “Receive Failure” “Remote Node Transmission Error” “Resource At or Nearing Capacity” “Response Time Excessive”

Alarm Manager field details

Field Name	Description
	“Retransmission Rate Excessive” “Software Error” “Software Program Abnormally Terminated” “Software Program Error” “Storage Capacity Problem” “Temperature Unacceptable” “Threshold Crossed” “Timing Problem” “Toxic Leak Detected” “Transmit Failure” “Transmitter Failure” “Underlying Resources Unavailable” “Version Mismatch” “Authentication Failure” “Breach of Confidentiality” “Cable Tamper” “Delayed Information” “Denial of Service” “Duplicate Information” “Information Modification Detected” “Information Out of Sequence” “Intrusion Detection” “Key Expired” “Non-Repudiation Failure” “Out of Hours Activity” “Out of Service” “Procedural Error” “Unauthorized Access Attempt” “Unexpected Information” “Unspecified Reason” other = “Unknown Error”

To avoid using too much memory to display the alarms, only 1000 alarms are displayed at any given time. Alarms that are no longer displayed on the Alarm Manager can be viewed using the Alarm History window, which uses paging to minimize the size to the GUI.

Prerequisites

None

Action

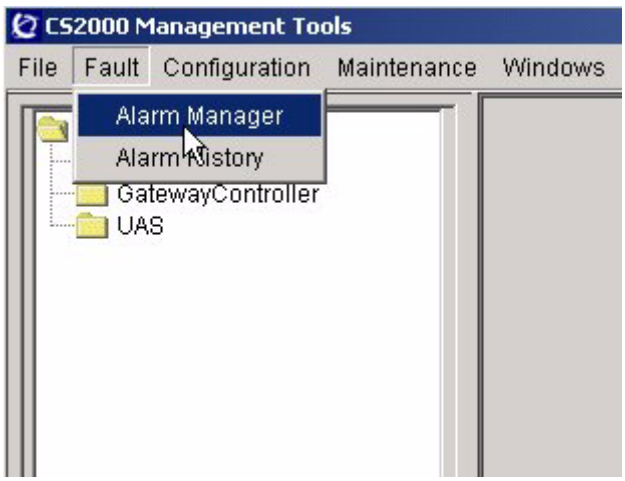
Perform the following steps to complete this procedure.

At your workstation

1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools client applications, if required.

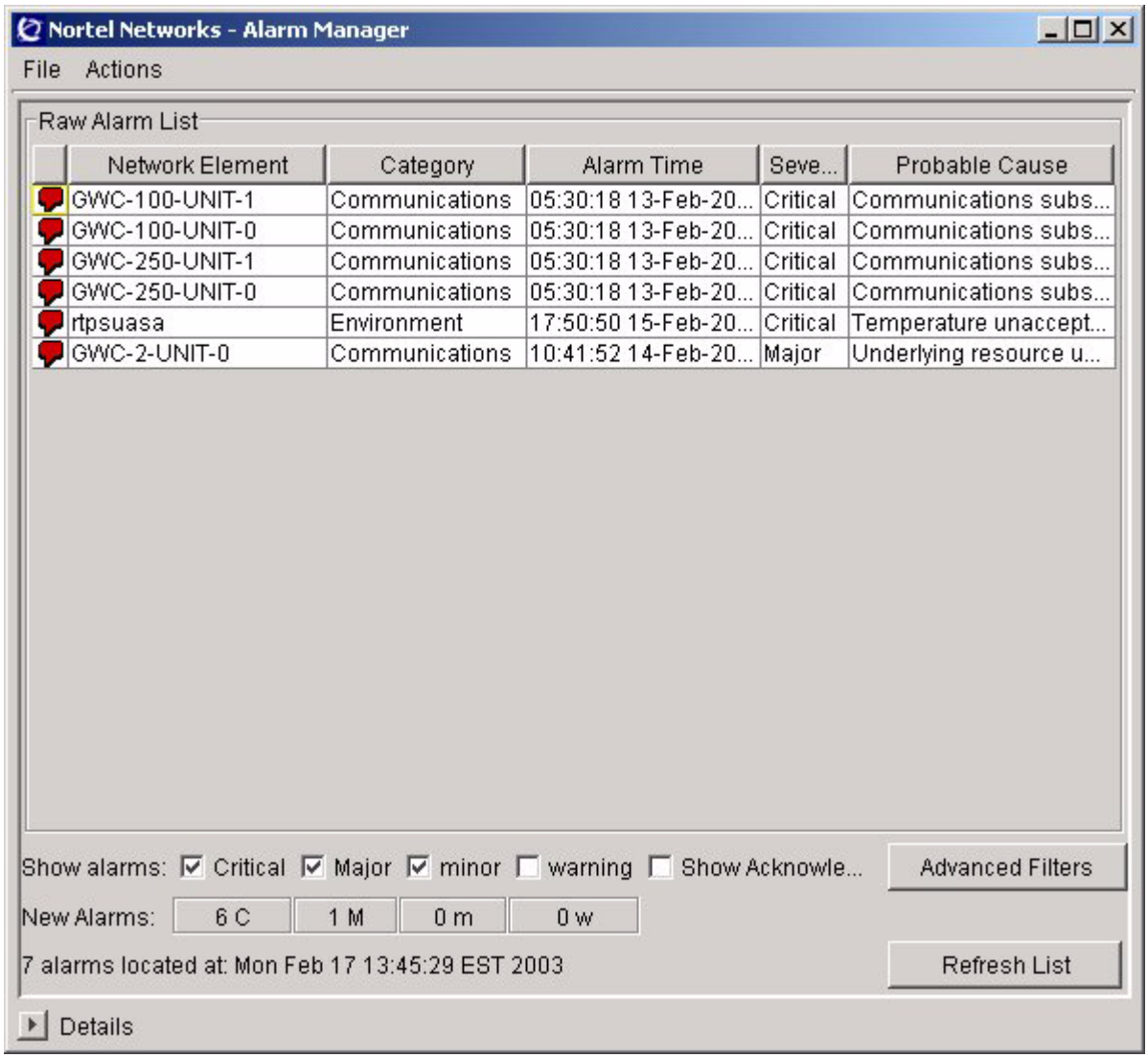
At the CS2000 Management Tools GUI

2 On the **Fault** menu, click **Alarm Manager**.



The Alarm Manager window, similar to following, appears.

Alarm Manager window



3 You have completed this procedure.

Retrieving details about an alarm

Application

Use this procedure to display detailed information about service-related alarms on the managed network elements. The detailed view provides information on the items in the following table:

Alarm details fields

Field Name	Description
NE Name	Provides the name of the Network Element for which the selected alarm is being raised.
Alarm Level	Provides the associated severity of the alarm being raised. The range of values is as follows: “Critical” “Major” “Minor” “Warning”
Category	Represents the alarm problem category values (ITU-T X.733): “Communications” “Quality of Service” “Processing Error” “Equipment Error” “Environment”
Alarm Time	Represents the time that the alarm was raised in the following format: HH:MM:SS day-Month-year
Probable Cause	Provides the probable cause of the particular alarm (X.733 Probable Cause). See the procedure Accessing the Alarm Manager on page 11 for a list of possible entries in the Probably Cause field.

Alarm details fields

Field Name	Description
Acknowledged at	Represents the time the alarm was acknowledged in the following format: HH:MM:SS day-Month-year The text “Not Yet” indicates that the alarm has not been acknowledged.
System uptime	Represents the time since the network element was last re-initialized. Here is an example of how system uptime is displayed: 2 hours, 10 minutes, 30 seconds
Component ID	Represents the distinguished name (DN) (refer X.720) of the component object against which the particular alarm is raised. Example: GWC=GWC-3-UNIT-1;Version=PGC91AFZ; Unit=unit_1;Software=NODEMTC
Alarm Description	Provides the description text for the particular alarm. (X.733 Additional text) Example: Element Manager communication failure.
Specific Problem	Provides the specific problem data (ITU-T X.733) to further qualify the probable cause of the particular alarm. (X.733 Specific Problem) Example: EM not responding, provisioned data loaded from local Flash.

Prerequisites

This procedure has no prerequisites.

Action

Perform the following steps to complete this procedure.

At your workstation

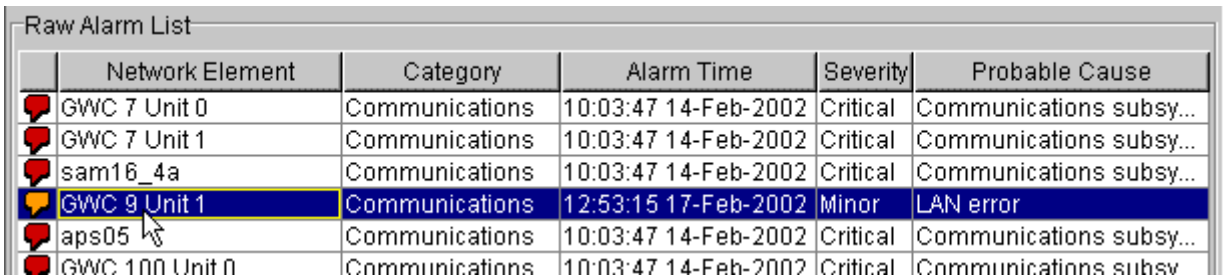
1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the CS2000 Management Tools application GUI

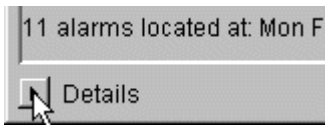
2 On the **Fault** menu, click **Alarm Manager**.

The Alarm Manager window opens.

3 Select an alarm in the Alarm Manager window.

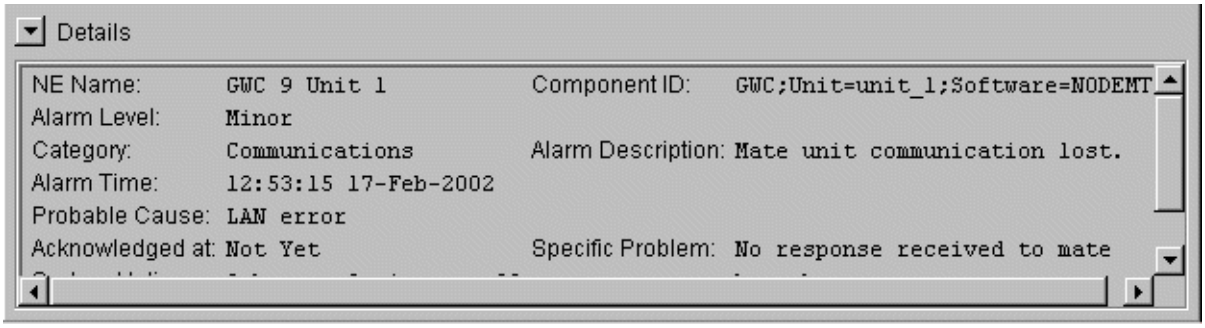


4 Click **Details**.



Detailed information about the alarm is displayed.

Alarm details



5 You have completed this procedure.

Accessing the Alarm History

Application

Use this procedure to access the Alarm History window, which provides a list of active and inactive alarms.

Prerequisites

None

Action

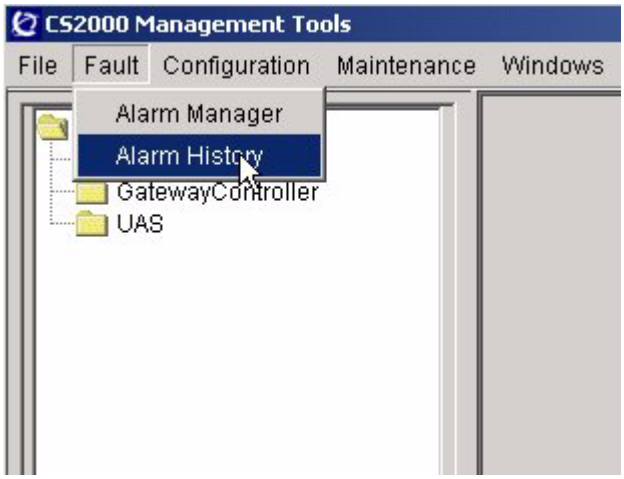
Perform the following steps to complete this procedure.

At your workstation

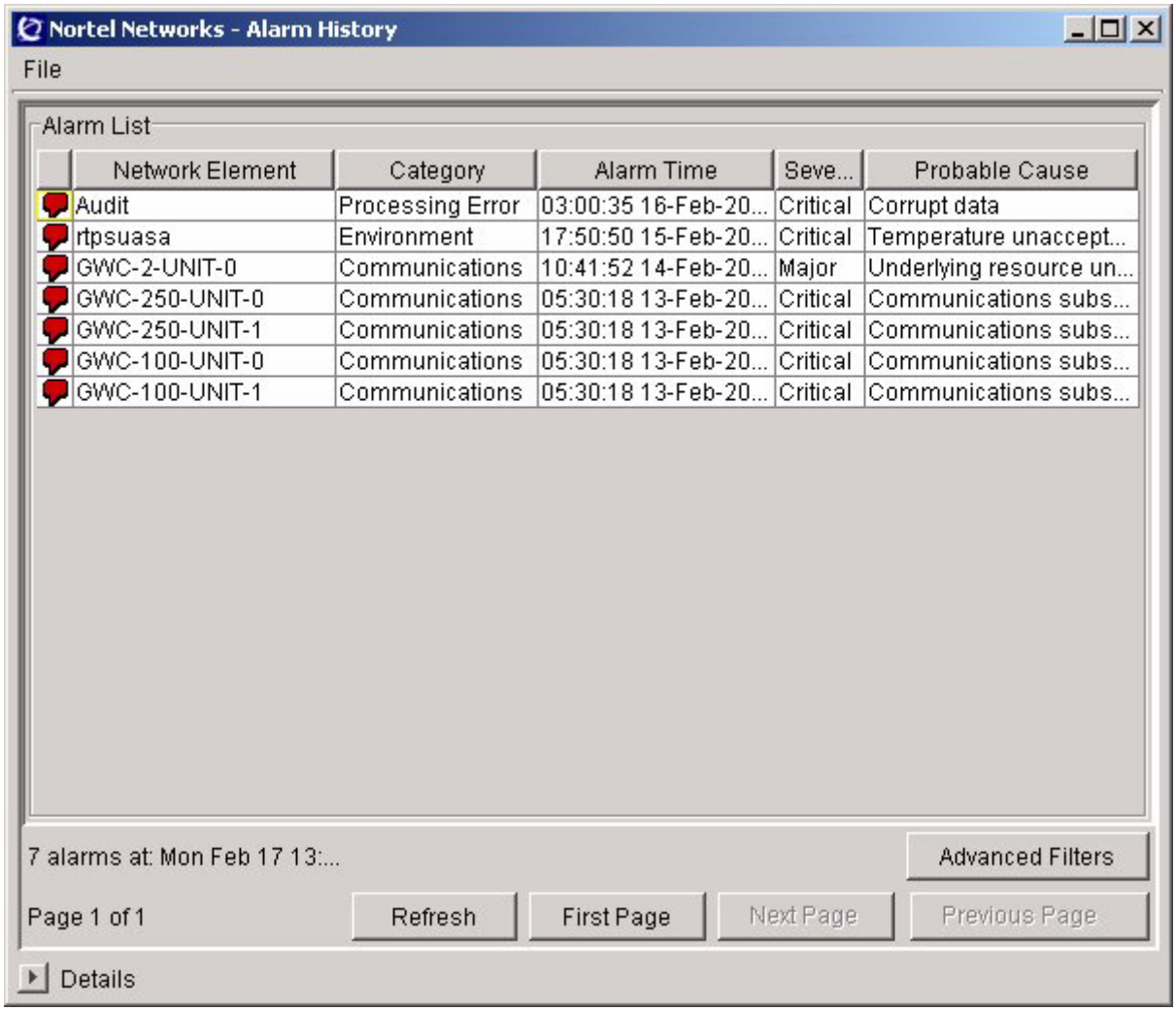
1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the CS2000 Management Tools GUI

2 On the **Fault** menu, click **Alarm History**.



The Alarm History window, similar to following, appears.



3 You have completed this procedure.

Acknowledging alarms

Application

Use this procedure to silence service-related alarms at the Alarm Manager.

Prerequisites

None

Action

At your workstation

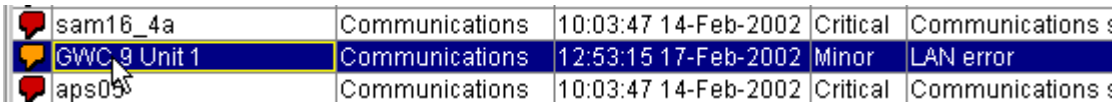
1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the CS2000 Management Tools GUI

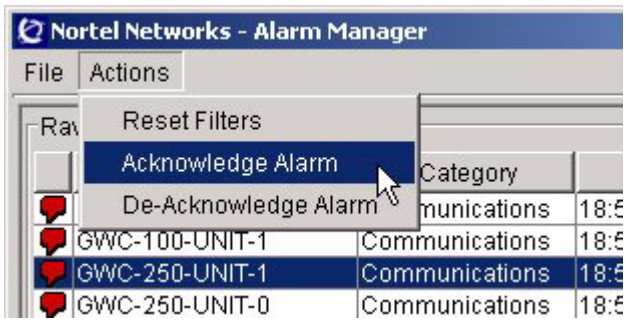
2 On the **Fault** menu, click **Alarm Manager**.

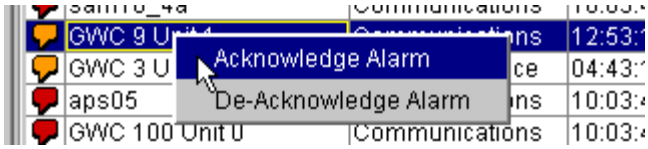
The Alarm Manager window opens.

3 Select the alarm you want to acknowledge.

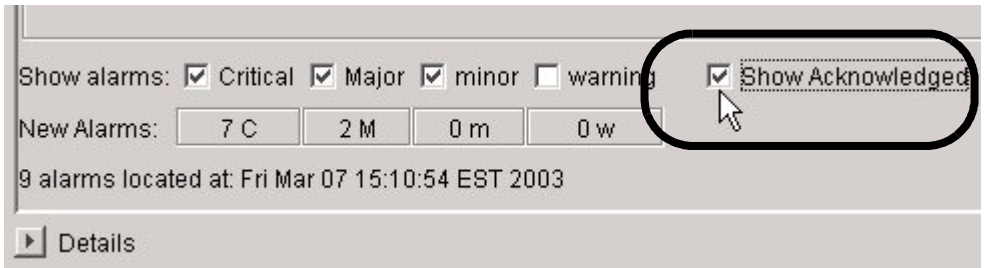


4 On the **Actions** menu, click **Acknowledge Alarm**, or right-click on the selected alarm and click **Acknowledge Alarm**.





If the Show Acknowledged checkbox is checked, as shown below, the acknowledged alarm appears in the Alarm Manager window with a White status. Otherwise, it is removed from the list of alarms.



5 You have completed this procedure.

De-acknowledging alarms

Application

This procedure unsilences service-related alarms at the Alarm Manager.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

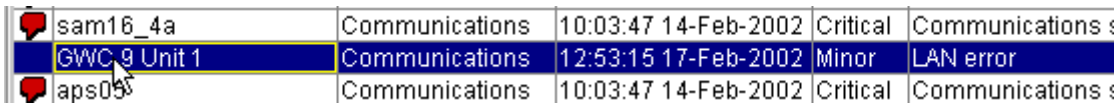
1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the CS2000 Management Tools GUI

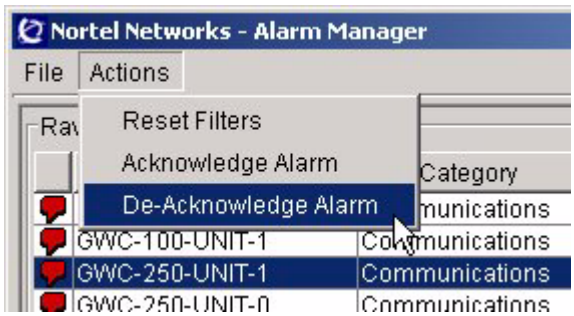
1 On the **Fault** menu, click **Alarm Manager**.

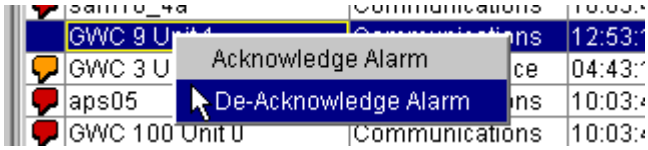
The **Alarm Manager** window opens.

2 In the **Alarm Manager** window, select the alarm you want to de-acknowledge.



3 On the **Actions** menu, click **De-Acknowledge Alarm**, or right-click on the alarm, then click **De-Acknowledge Alarm**





The alarm appears in the Alarm Manager window with a colored status indicator dependant on the status of the alarm.

4 You have completed this procedure.

Viewing acknowledged alarms

Application

Use this procedure to view silenced service-related alarms at the Alarm Manager.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

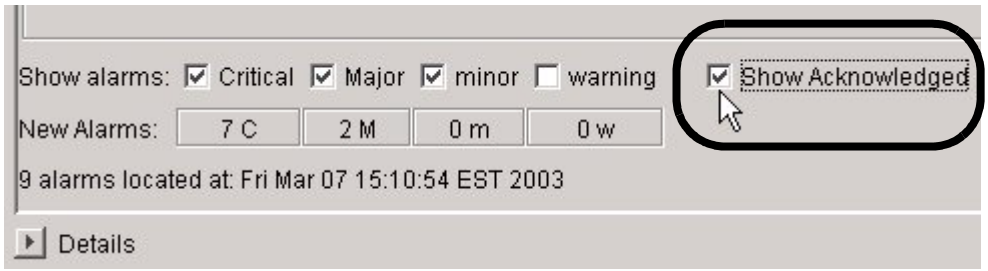
1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the CS2000 Management Tools GUI

2 On the **Fault** menu, click **Alarm Manager**.

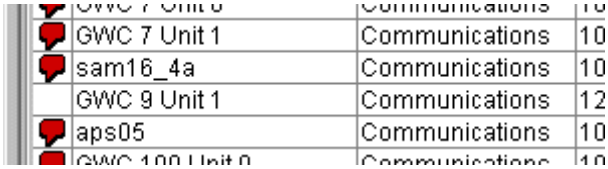
The **Alarm Manager** window opens.

3 Click the **Show Acknowledged** checkbox.



4 Click **Refresh List** to refresh the list of alarms.

The acknowledged alarm appear in the list of alarms with a severity color code of white.



5 You have completed this procedure.

Filtering alarms

Application

Use this procedure to filter the alarms you want to view. You can filter by alarm severity, network element and type of alarm (alarm category).

Note: This procedure provides the steps to filter alarms in the Alarm Manager, but similar filtering capabilities are also available in the Alarm History.

Prerequisites

None

Action

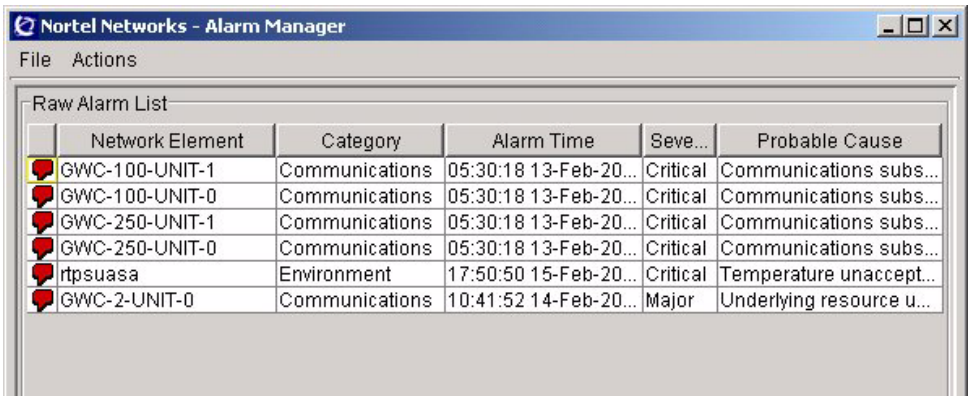
At your workstation

1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the CS2000 Management Tools GUI

2 On the **Fault** menu, click **Alarm Manager**.

The Alarm Manager window opens.



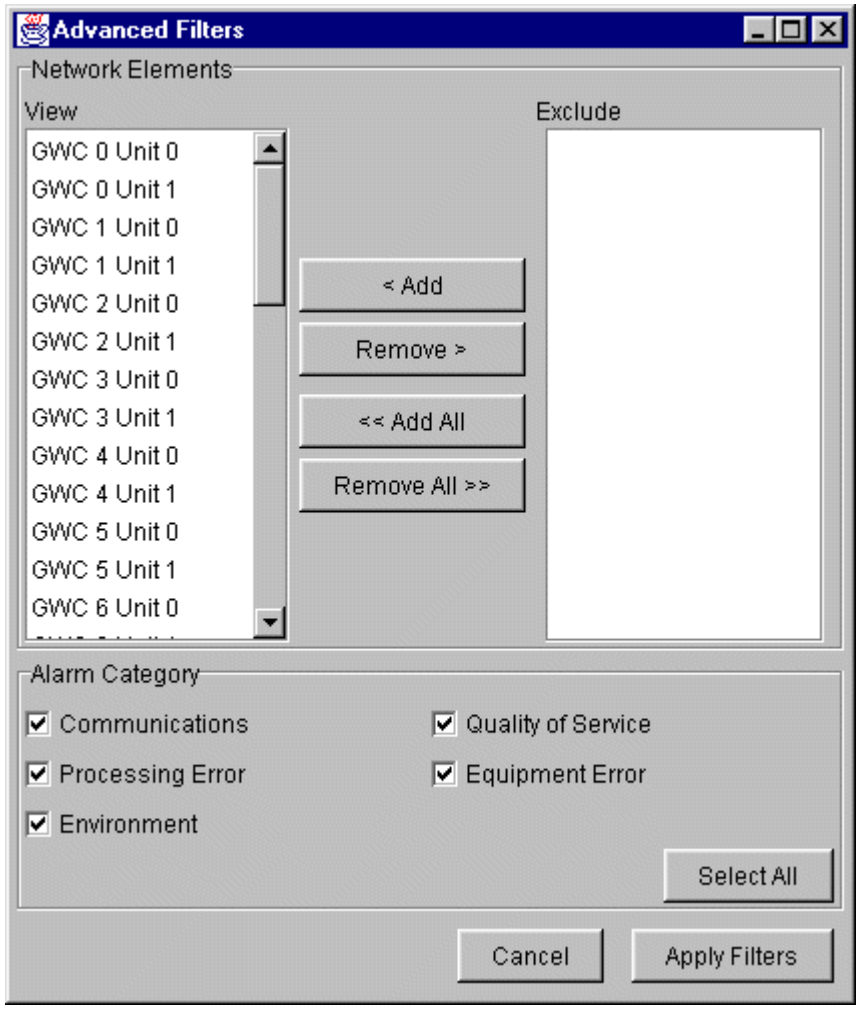
3 Use the following table to determine your next step.

If you want to filter by	Do
network element or alarm category	step 4
severity	step 5

4 Filter by network element or alarm category as follows:

a In the **Alarm Manager** window, click **Advanced Filters**.

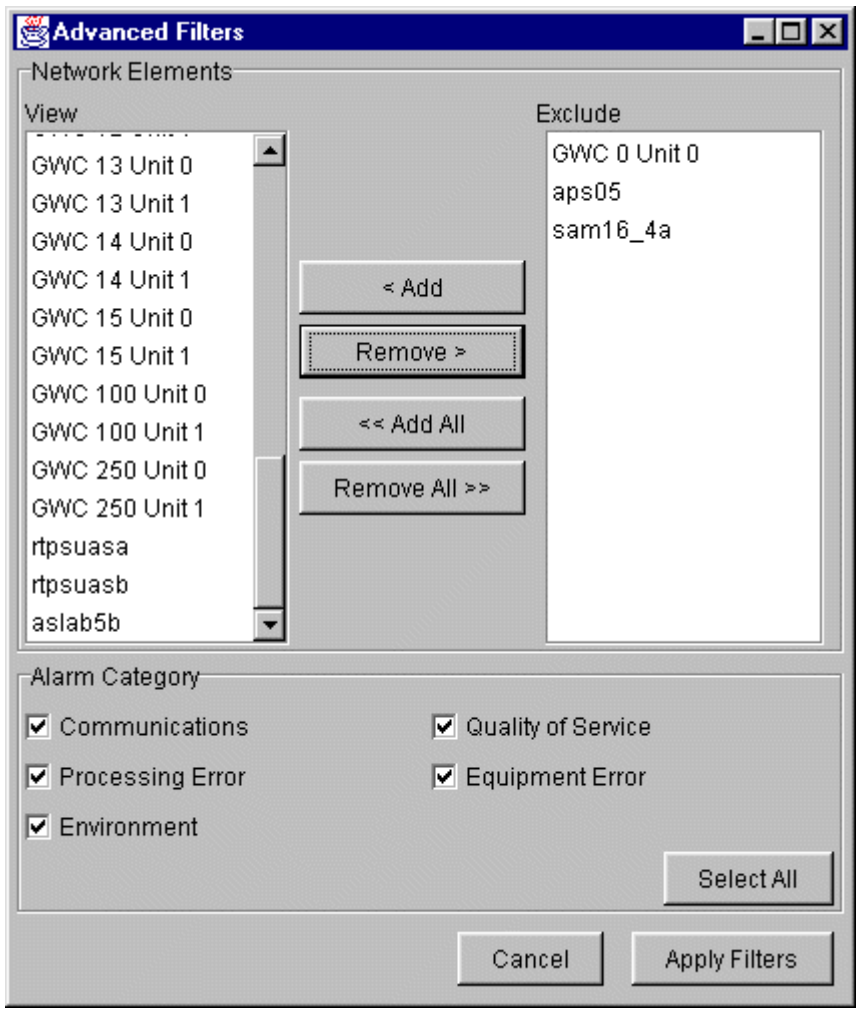
The Advanced Filters window opens.



b Select the network elements you want to exclude from the viewable alarms in the View column, then click **Remove**.

The network elements you have selected move to the **Exclude** column.

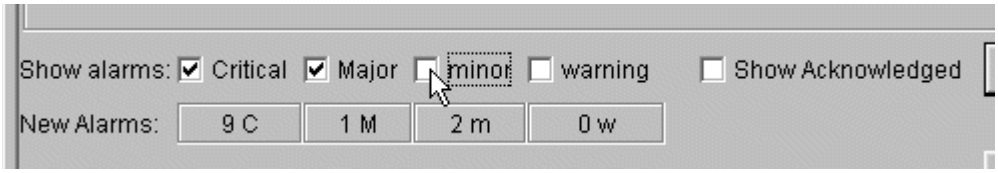
Note: If you move all Network Elements to the **Exclude** column, the filters based on Network Element node names will be deactivated. As a result, the alarm manager will display alarms from all managed devices and alarms from internal Call server applications (for example, Call Server Data Audit).



c Under **Alarm Category**, check the box next to the type of alarms you want to view for the network elements, then click **Apply filters**.

5 Filter by severity as follows:

a If checked, uncheck the severity type(s) you want to filter.



b Click **Refresh** to refresh the alarm list.

The alarms of the unchecked severity type(s) no longer appear in the **Alarm Manager** window.

6 You have completed this procedure.

Resetting the filters for alarms

Application

Use this procedure to reset the filters for service-related alarms at the Alarm Manager. This applies only for alarm severity.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

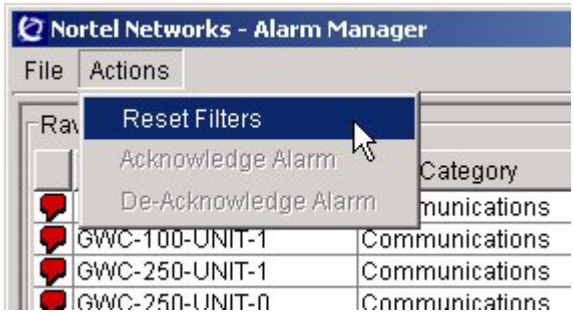
1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the CS2000 Management Tools GUI

1 On the **Fault** menu, click **Alarm Manager**.

The Alarm Manager window opens.

2 On the **Actions** menu, click **Reset Filters**.



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

The alarms of the previous default severity types appear in the Alarm Manager window.

4 You have completed this procedure.

Defining alarms using the NPM

Application

Use this procedure to define user-specific alarms using the Network Patch Manager (NPM). You can define alarms using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

In addition to the system-defined alarms for the Network Patch Manager (NPM), you can create your own alarms to match your specific criteria.

Prerequisites

None

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

1 Define an alarm by typing

```
npm> addalarm <alarm_name> <alarm_enable>
<alarm_severity> "<alarm_pd> <alarm_criteria>"
'<alarm_desc>'
```

and pressing the Enter key.

where

alarm_name
is the name of the alarm being defined

alarm_enable
identifies whether the alarm will be enabled initially (Y, N)

alarm_severity
identifies the alarm severity (NONE, MINOR, MAJOR, or CRITICAL)

alarm_pd
identifies whether the alarm is from a patch or device (PATCH, DEVICE)

alarm_criteria
is the SQL statement that defines the alarm condition

alarm_desc
is a brief description of the alarm

Example

```
addalarm PATCHUNAVAIL Y CRITICAL "PATCH where
PATCH.FILEAVAILABLE='FALSE'" 'No patch file
available'
```

2 You have completed this procedure.

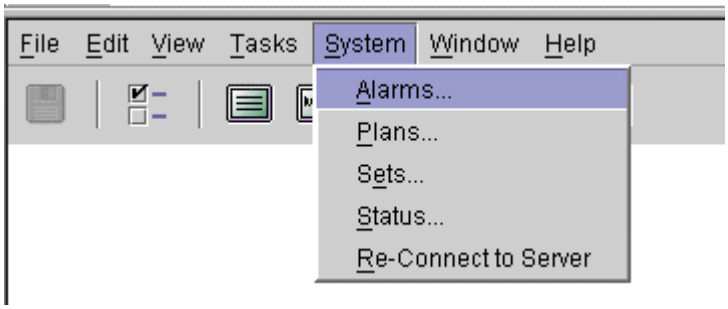
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the NPM GUI

2 On the **System** menu, click **Alarms...**.

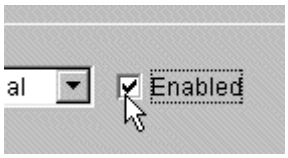


The Alarms window opens.

3 Select an alarm type from the **Alarm Type** list.

4 Select a severity level from the **Severity** list.

5 Click the **Enabled** checkbox to enable the alarm.

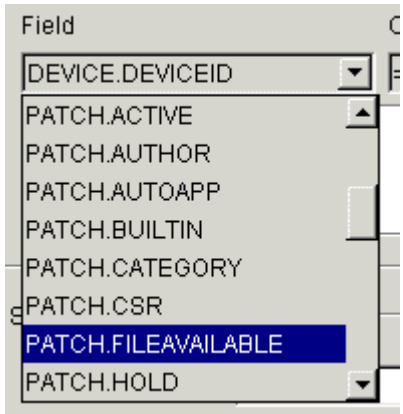


6 In the **Alarm Criteria** panel, enter the criteria for the alarm.

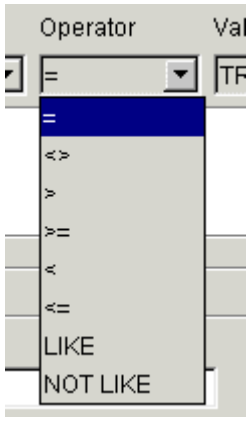
If you want to enter the alarm criteria	Do
using the boxes	step 7
using a command string	step 8

7 Using the boxes, specify the alarm criteria as follows:

a Select the field from the **Field** list.



b Select the operator from the **Operator** list.



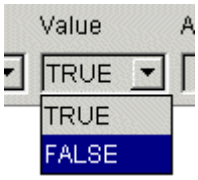
The table below lists the supported operators and their meaning.

Supported operators

Operator	Meaning
=	Equal
<>	Not equal
>	Greater than
>=	Greater than or equal
<	Less than
<=	Less than or equal
LIKE	Matches string with wildcard (%)
NOT LIKE	Does not match string with wildcard (%)

c Select the value from the **Value** list, or enter the value.

Note: The data type for **Value** will change depending on the data type of the field. For alphanumeric data, enter the value. For boolean data, select the value.

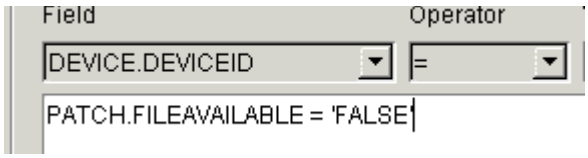


d To combine multiple criteria statements, select the AND or the OR options from the **And/Or** box.

e Go to step 9.

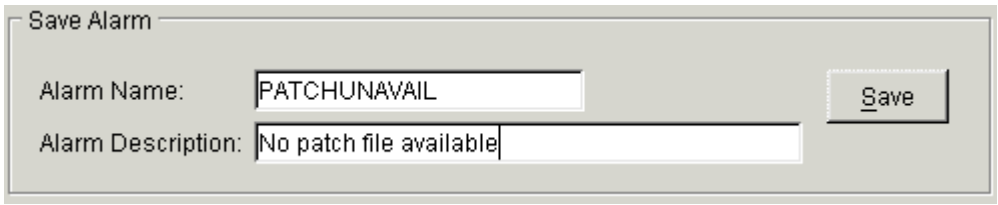
8 Using a command string, specify the alarm criteria in the text area.

Note: Parenthesis "()" may be inserted to define precedence for multiple criteria statements.



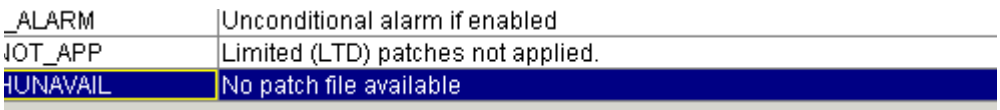
9 Enter a unique name for the alarm in the **Alarm Name** box.

10 Optionally enter a description for the alarm in the **Alarm description** box.



11 Click **Save** to save the alarm.

The new alarm will be displayed in the Alarm List once the NPM Server has saved the alarm.



12 You have completed this procedure.

Enabling and disabling alarms using the NPM

Application

Use this procedure to enable or disable an alarm using the Network Patch Manager (NPM). You can enable or disable alarms using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

Prerequisites

None

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Accessing the Network Patch Manager CLUI in this document, if required.

At the NPM CLUI

2 Enable or disable an alarm by typing

```
npm> alarm <alarm_name> <alarm_option>
```

and pressing the Enter key.

where

alarm_name
is the name of the alarm

alarm_option
indicates what is to be done to the alarm (enable, disable, delete, matches)

Example for enabling an alarm:

```
npm> alarm DEVICE_ONHOLD enable
```

Example for disabling an alarm:

```
npm> alarm DEVICE_ONHOLD disable
```

3 You have completed this procedure.

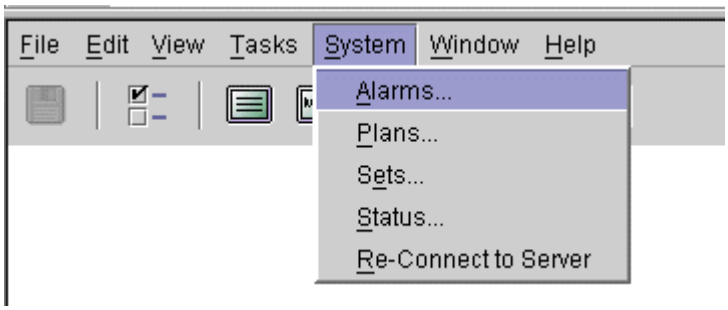
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the NPM GUI

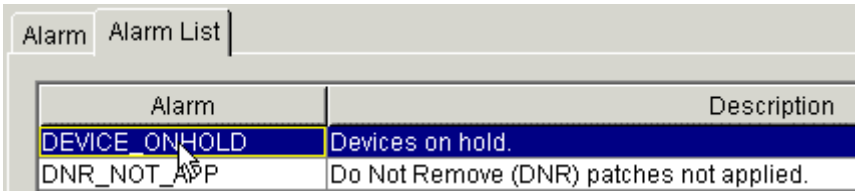
2 On the **System** menu, click **Alarms...**.



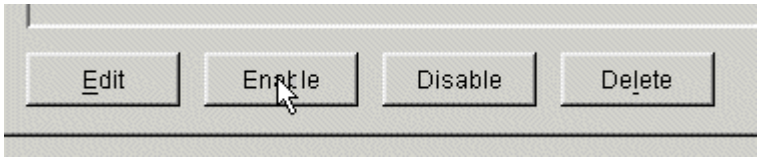
The Alarms window opens.

3 Click the **Alarm List** tab to display a list of all defined alarms.

4 Select the alarm you want to enable or disable from the alarm list.



5 Click **Enable** or **Disable**.



6 You have completed this procedure.

Performing an audit

Application

Use this procedure to manually perform a line, trunk, V5.2 interface, or CS 2000 (CS2K) data audit.

Note: The V5.2 audit is only available in the international version of the software and not in the North American.

You can set the audit to run automatically at a specific time on a daily or a weekly basis. Refer to procedure “Configuring an audit schedule” in the CS 2000 Management Tools Configuration Management document, NN10106-511.

CS 2000 data audit

For a CS2K data audit, the system compares the GWC element manager database (part of the CS 2000 GWC Manager database) with the CS 2000 XA-Core database and flags any mismatches between the two databases. The XA-Core is considered to hold the ‘master’ database.

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

Line audit

For a line audit, the system compares the ENDPOINTENTRY area in the CS 2000 GWC Manager database with the following tables in the CS 2000 XA-Core database:

- DNINV
- LGRPINV
- LNINV
- HUNTMEM (if hunt groups have been provisioned)
- MDNMEM (if MADN groups have been provisioned)

The system writes the results of the audit into two files, one containing a list of valid data and the other containing a list of problem data. The files are stored on the CS 2000 Management Tools server.

Trunk audit

For a trunk audit, the system compares the ENDPOINTENTRY area in the CS 2000 GWC Manager database with the following tables in the CS 2000 XA-Core database:

- SERVRINV
- TRKMEM
- LTMAP
- TRKSGRP

The system writes the results of the audit into two files, one containing a list of valid data and the other containing a list of problem data. The files are stored on the CS 2000 Management Tools server.

V5.2 audit

For a V5.2 data integrity audit, the system compares data in the following databases and flags any mismatches:

- V5.2 interface data stored in the Network View database
- V5.2 endpoint data stored in the CS 2000 GWC Manger database
- V5.2 interface data stored in the table GPPTRNSL in the CS 2000 XA-Core database

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

Prerequisites

It is recommended to run only one audit at a time, therefore, ensure your manual audit does not conflict with another scheduled audit. Running multiple audits at the same time may cause some unexpected errors.

You must be assigned to user group “mgcadm” to run an audit. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the following steps to complete this procedure.

At your workstation

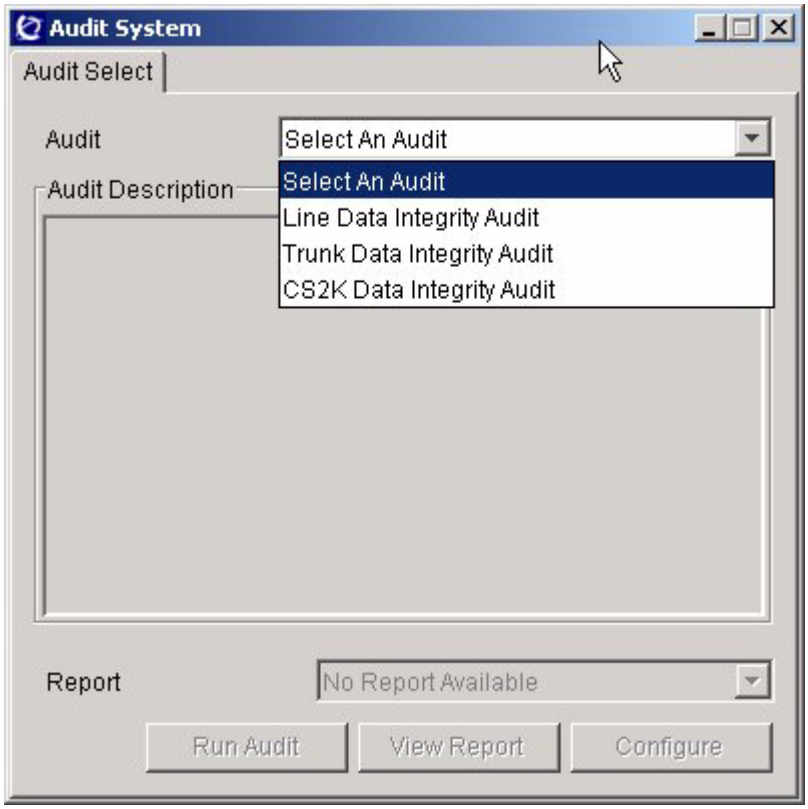
1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the CS2000 Management Tools GUI

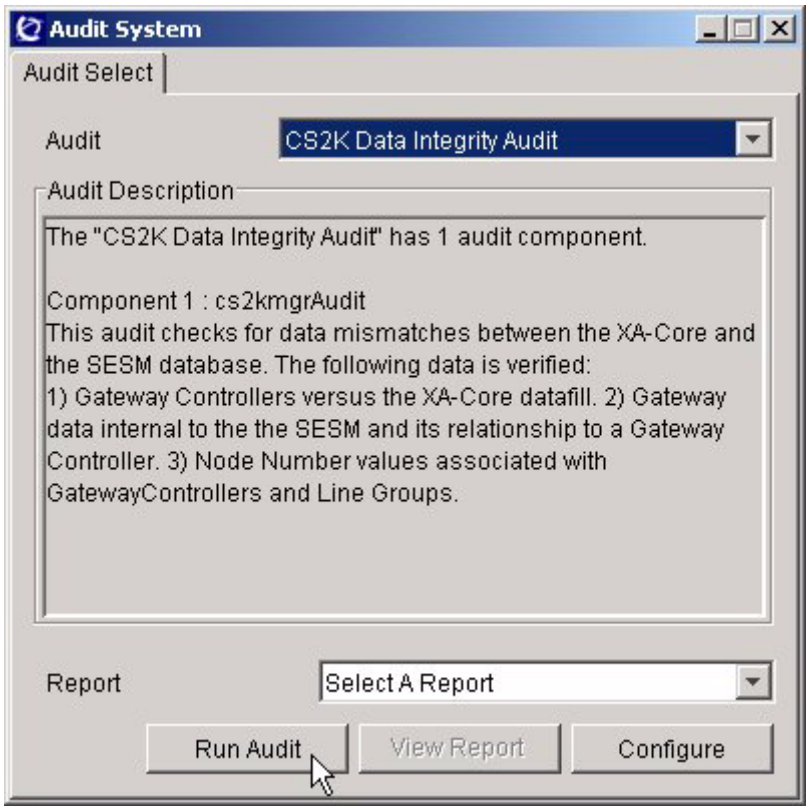
2 On the **Maintenance** menu, click **Audit System**.

The Audit System window opens.

3 In the **Audit** list, click the type of audit you want to perform.



4 Click **Run Audit**.



During the audit, an Audit Status window is displayed to indicate the audit is in progress. The Audit Status window indicates when the audit is complete.

Note: If the audit does not execute successfully, the Audit Status window indicates that the audit failed and provides the reason. Contact your next level of support to resolve the problem if required.

5 Click **Close** to close the Audit Status window.

6 Use the following table to determine your next step.

If you performed a	Do
CS2K Data Integrity Audit	step 7
Line Data Integrity Audit	step 11
Trunk Data Integrity Audit	step 14
V5.2 Data Integrity Audit	step 17

7 Proceed as follows for a CS2K Data Integrity Audit:

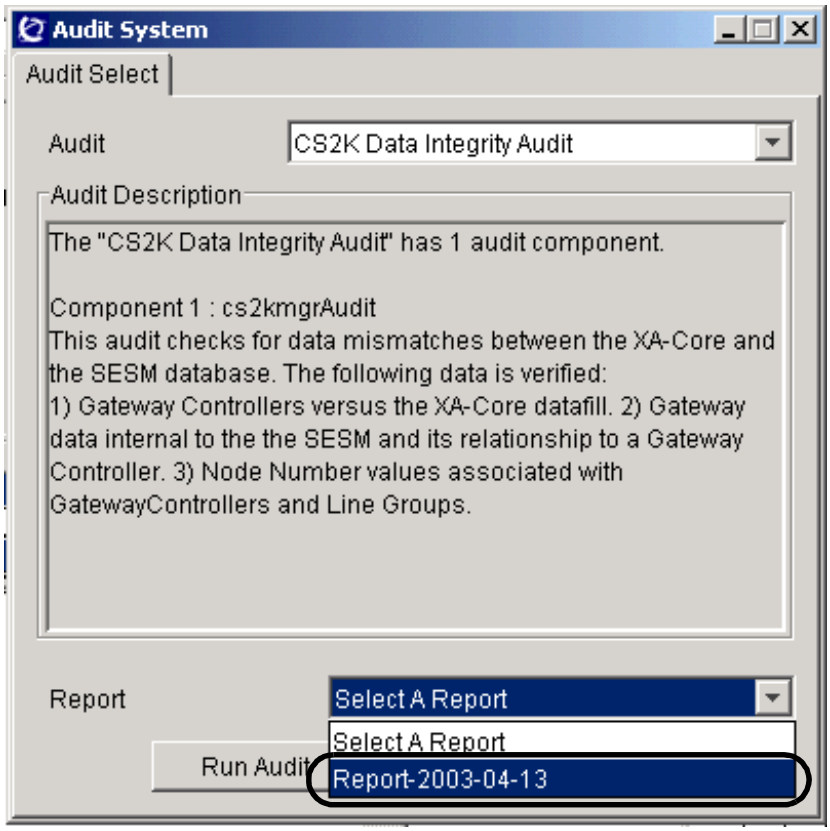
a Ensure that you have selected **CS2K Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.

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

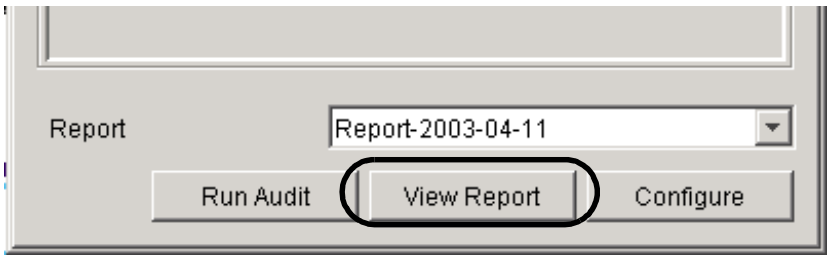
The file name has the following format:

Report-<date>

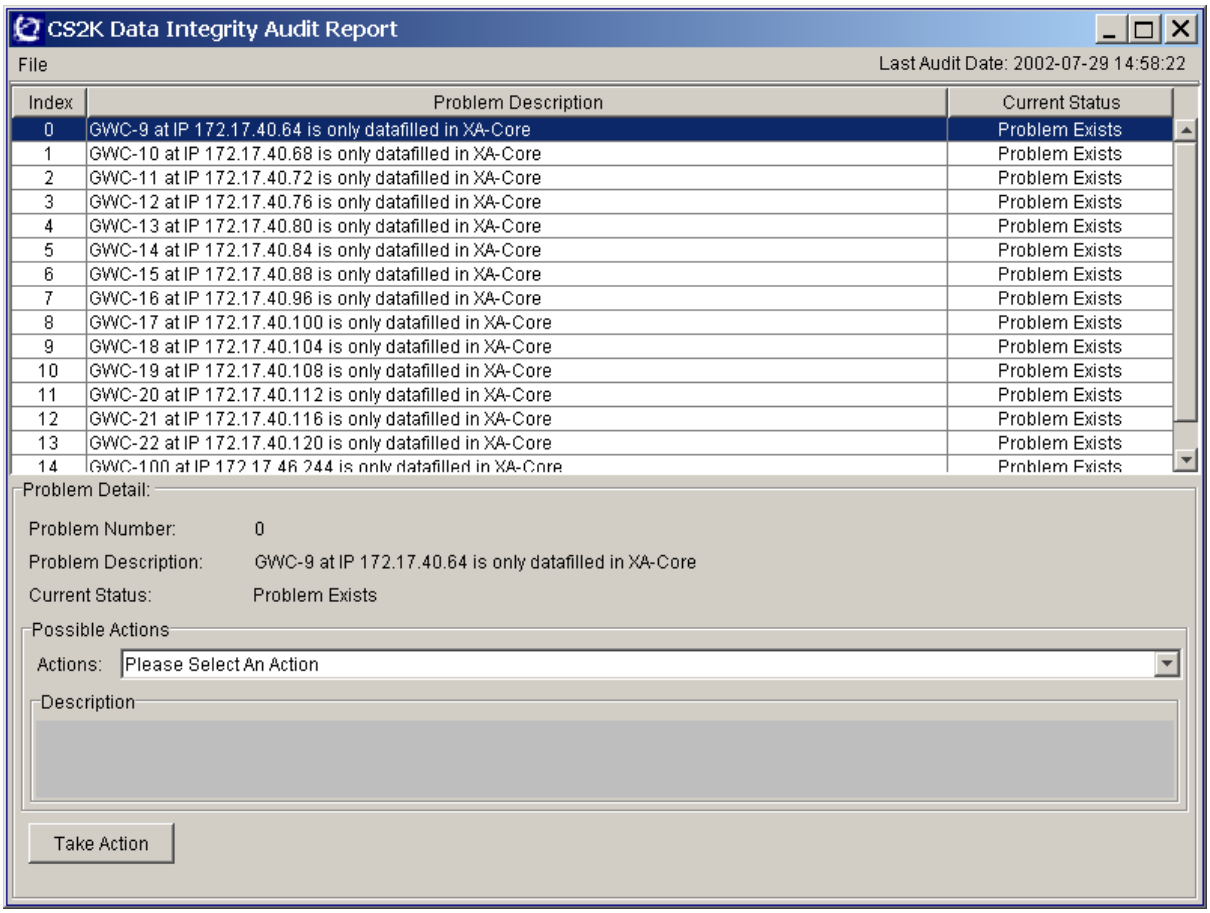
where
<date> is the date in yyyy-mm-dd format, for example, 2003-02-15.



c Click the **View Report** button.



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



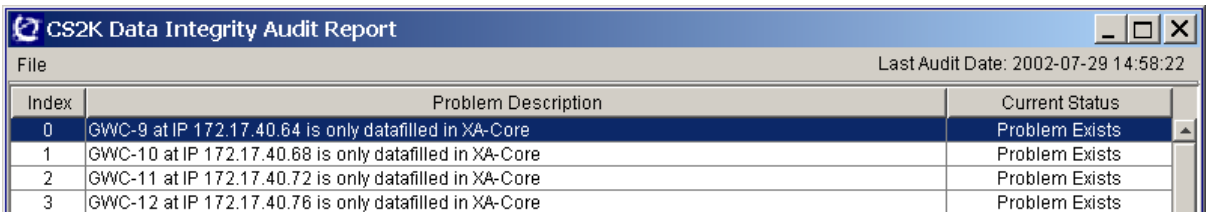
Note 1: The CS 2000 Management Tools server retains the most recent CS 2000 audit report. When a new audit occurs, the server deletes the previous report.

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

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

8 Review the results of the audit and click on a problem to resolve.

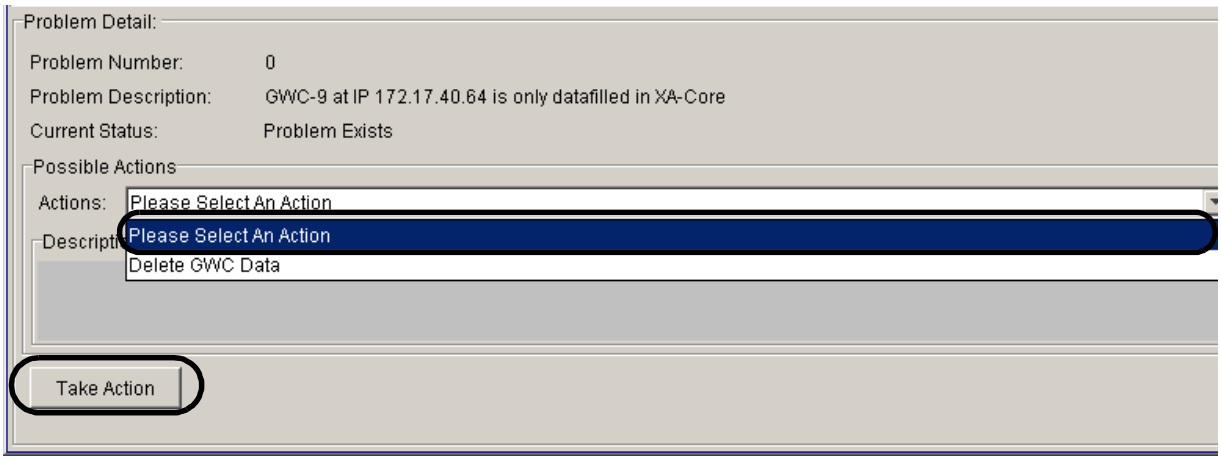
Note: If necessary, resize the entire window to completely view the Problem Description field.



9 Evaluate actions to resolve a problem and take action.

a Click and hold on the Action pull-down menu near the bottom of the screen to assess any possible actions.

b If appropriate, select an action. Read the description of the action and ensure that you observe any recommended steps or cautions.



c Click the **Take Action** button.

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

10 Return to step 8 to review another problem.

11 Proceed as follows for a Line Data Integrity Audit:

If you want to view	Do
the line valid-data report	step 12
the line problem-data report	step 13

12 View the line valid-data report as follows:

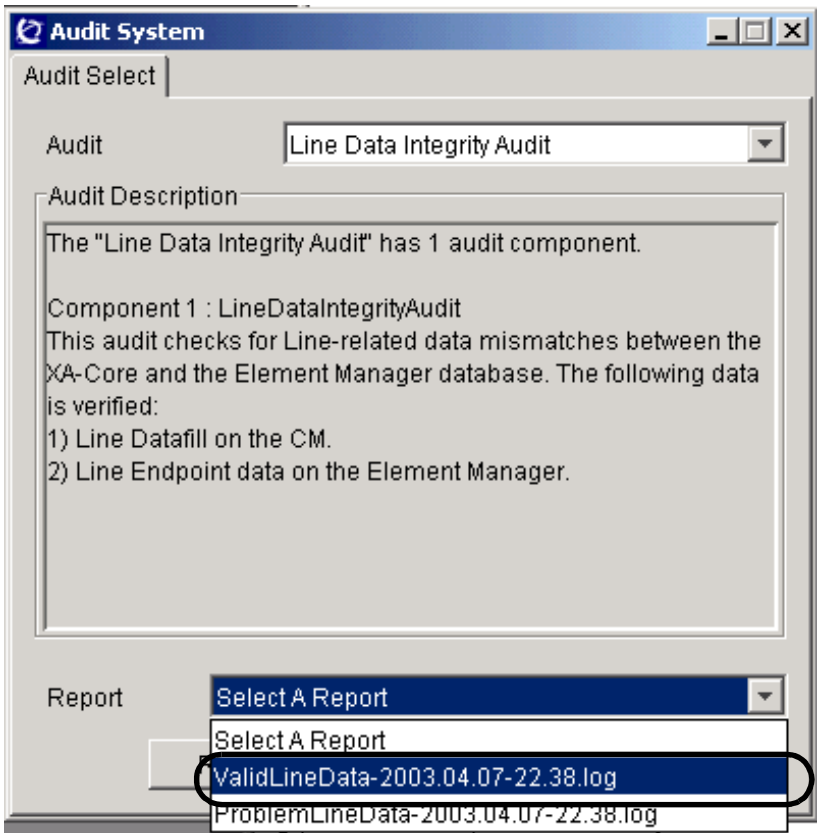
a Ensure that you have selected **Line Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.

b Select **ValidLineData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ValidLineData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

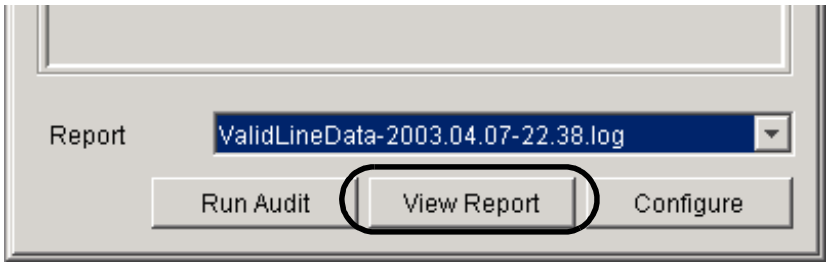
The file name has the following format:

ValidLineData-<date>-<time>.log

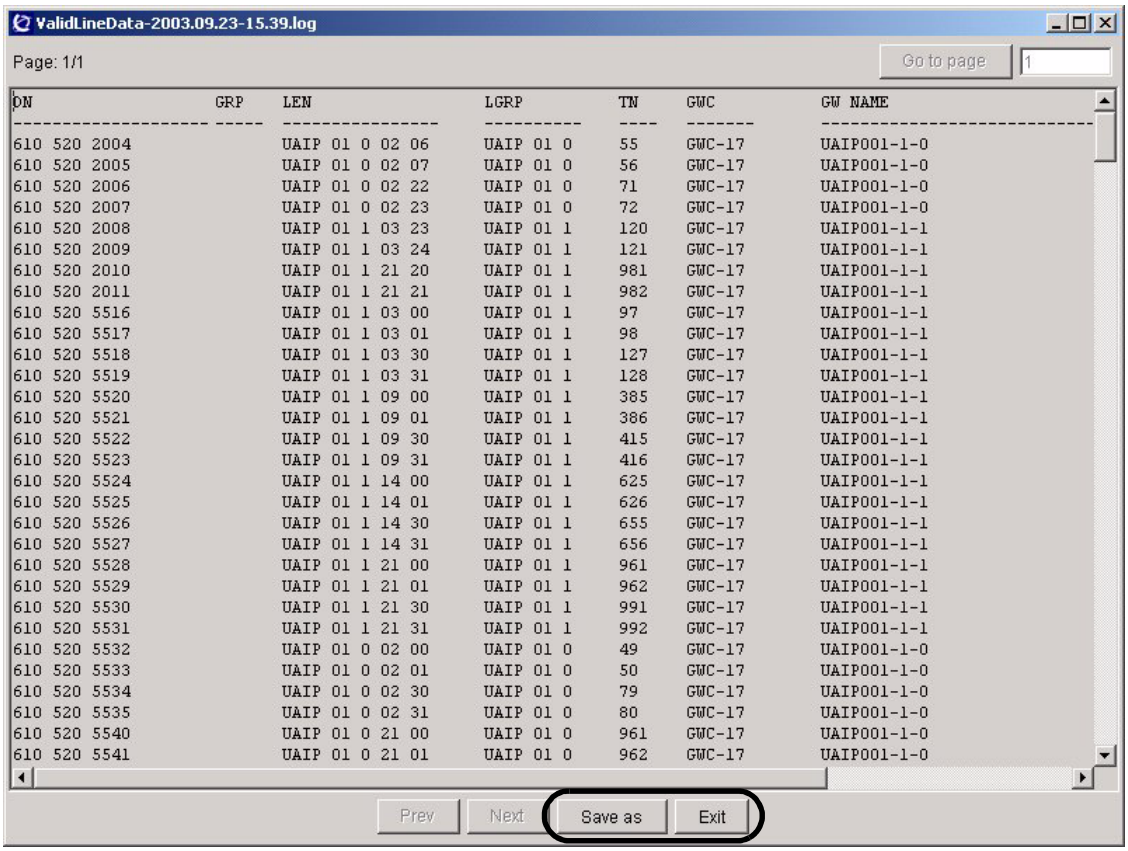
where
<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.
<time> is the time in hh.mm format, for example 17.30.



c Click **View Report**.



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



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

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

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

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

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

13 View the line problem-data report as follows:

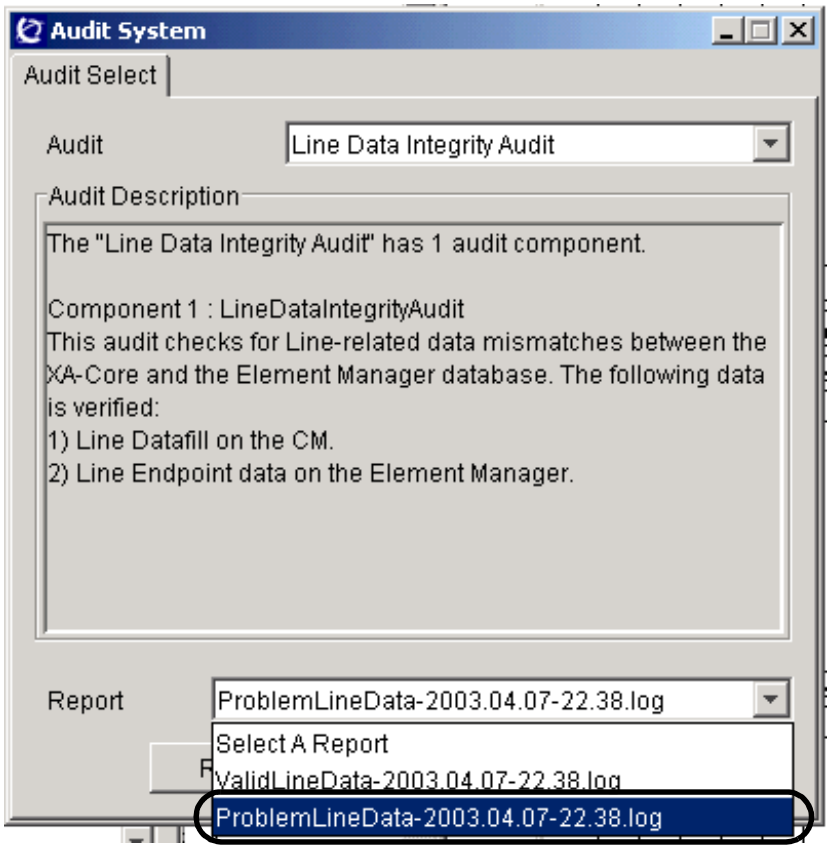
a Ensure that you have selected **Line Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.

b Select **ProblemLineData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ProblemLineData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

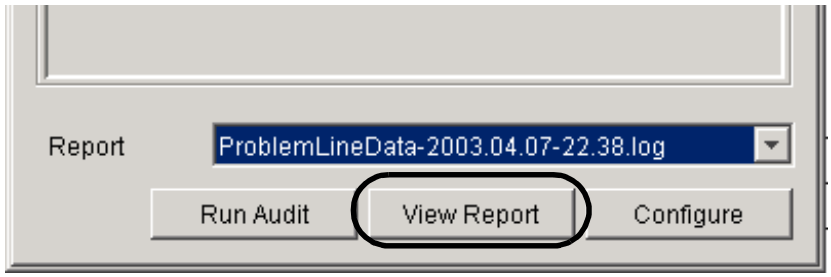
The file name has the following format:

ProblemLineData-<date>-<time>.log

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



c Click the **View Report** button.



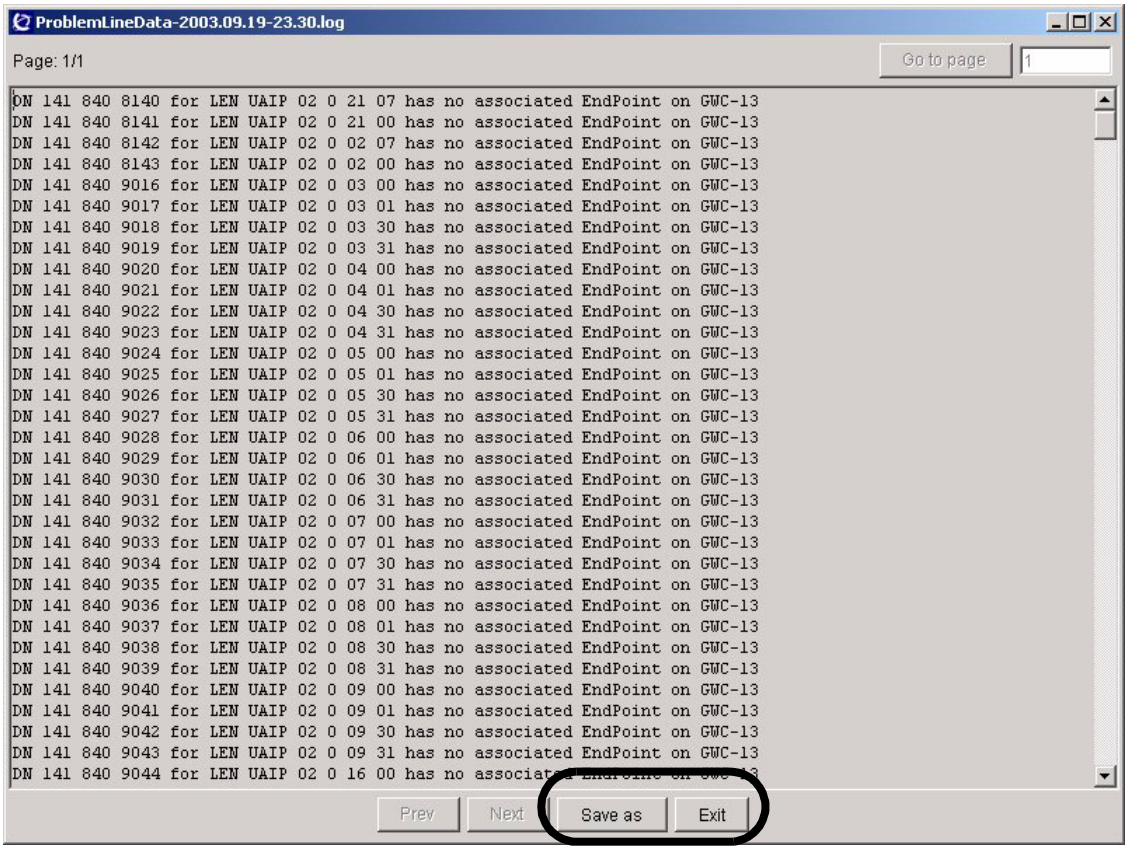
The system displays the selected report.

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

The “Problem” report produced by a line audit can contain messages in the following formats:

- DN <DN> for LEN <len> has no associated endpoint on <GWC ID>.
- Endpoint <endpointname> on gateway <gatewayname> on GWC <GWCname> has no associated DN/LEN on CM.

Here is an example of a “ProblemLineData” report:



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

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

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

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

f To correct the problems, refer to the printed copy of the report. You will need to delete and then reprovision the listed lines.

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

14 Proceed as follows for a Trunk Data Integrity Audit:

If you want to view	Do
the trunk valid-data report	step 15
the trunk problem-data report	step 16

15 View the trunk valid-data report as follows:

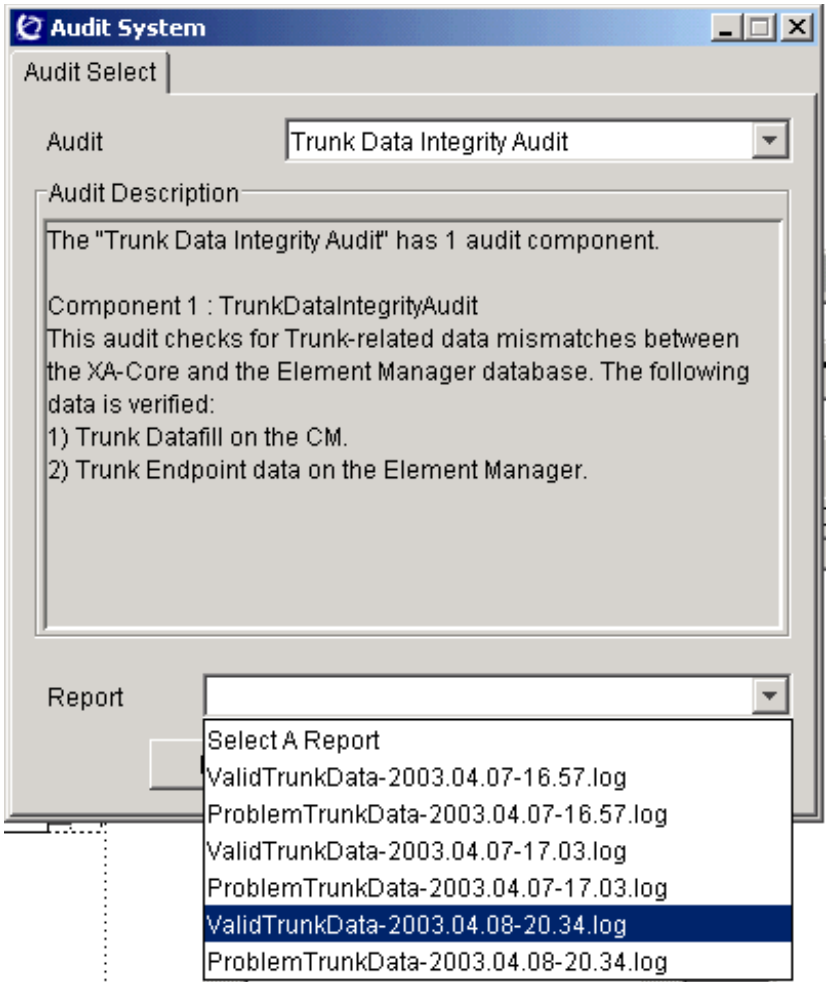
a Ensure that you have selected **Trunk Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.

b Select **ValidTrunkData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ValidTrunkData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

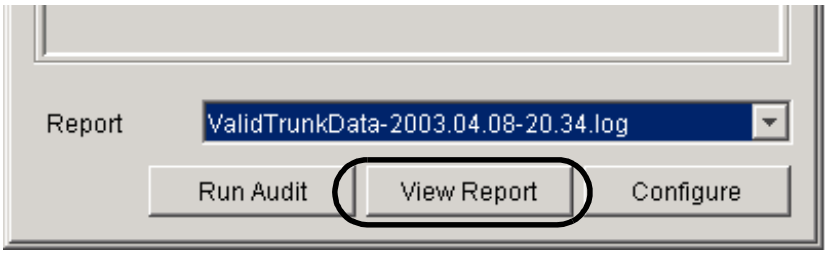
The file name has the following format:

ValidTrunkData-<date>-<time>.log

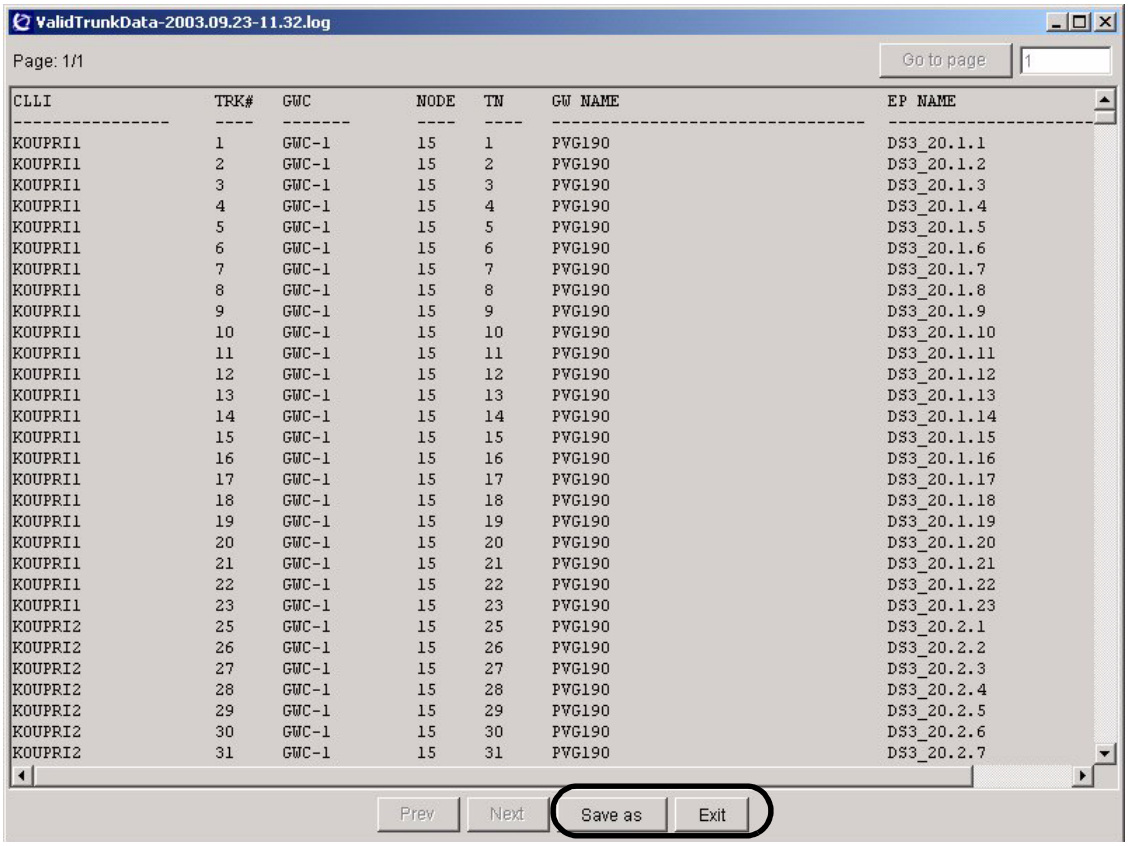
where
<date> is the date in yyyy.mm.dd format, for example, 2003.02.15.
<time> is the time in hh.mm format, for example 17.30.



c Click **View Report**.



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



CLLI	TRK#	GWC	NODE	TN	GW NAME	EP NAME
KOUPRI1	1	GWC-1	15	1	PVG190	DS3_20.1.1
KOUPRI1	2	GWC-1	15	2	PVG190	DS3_20.1.2
KOUPRI1	3	GWC-1	15	3	PVG190	DS3_20.1.3
KOUPRI1	4	GWC-1	15	4	PVG190	DS3_20.1.4
KOUPRI1	5	GWC-1	15	5	PVG190	DS3_20.1.5
KOUPRI1	6	GWC-1	15	6	PVG190	DS3_20.1.6
KOUPRI1	7	GWC-1	15	7	PVG190	DS3_20.1.7
KOUPRI1	8	GWC-1	15	8	PVG190	DS3_20.1.8
KOUPRI1	9	GWC-1	15	9	PVG190	DS3_20.1.9
KOUPRI1	10	GWC-1	15	10	PVG190	DS3_20.1.10
KOUPRI1	11	GWC-1	15	11	PVG190	DS3_20.1.11
KOUPRI1	12	GWC-1	15	12	PVG190	DS3_20.1.12
KOUPRI1	13	GWC-1	15	13	PVG190	DS3_20.1.13
KOUPRI1	14	GWC-1	15	14	PVG190	DS3_20.1.14
KOUPRI1	15	GWC-1	15	15	PVG190	DS3_20.1.15
KOUPRI1	16	GWC-1	15	16	PVG190	DS3_20.1.16
KOUPRI1	17	GWC-1	15	17	PVG190	DS3_20.1.17
KOUPRI1	18	GWC-1	15	18	PVG190	DS3_20.1.18
KOUPRI1	19	GWC-1	15	19	PVG190	DS3_20.1.19
KOUPRI1	20	GWC-1	15	20	PVG190	DS3_20.1.20
KOUPRI1	21	GWC-1	15	21	PVG190	DS3_20.1.21
KOUPRI1	22	GWC-1	15	22	PVG190	DS3_20.1.22
KOUPRI1	23	GWC-1	15	23	PVG190	DS3_20.1.23
KOUPRI2	25	GWC-1	15	25	PVG190	DS3_20.2.1
KOUPRI2	26	GWC-1	15	26	PVG190	DS3_20.2.2
KOUPRI2	27	GWC-1	15	27	PVG190	DS3_20.2.3
KOUPRI2	28	GWC-1	15	28	PVG190	DS3_20.2.4
KOUPRI2	29	GWC-1	15	29	PVG190	DS3_20.2.5
KOUPRI2	30	GWC-1	15	30	PVG190	DS3_20.2.6
KOUPRI2	31	GWC-1	15	31	PVG190	DS3_20.2.7

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

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

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

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

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

16 View the trunk problem-data report as follows:

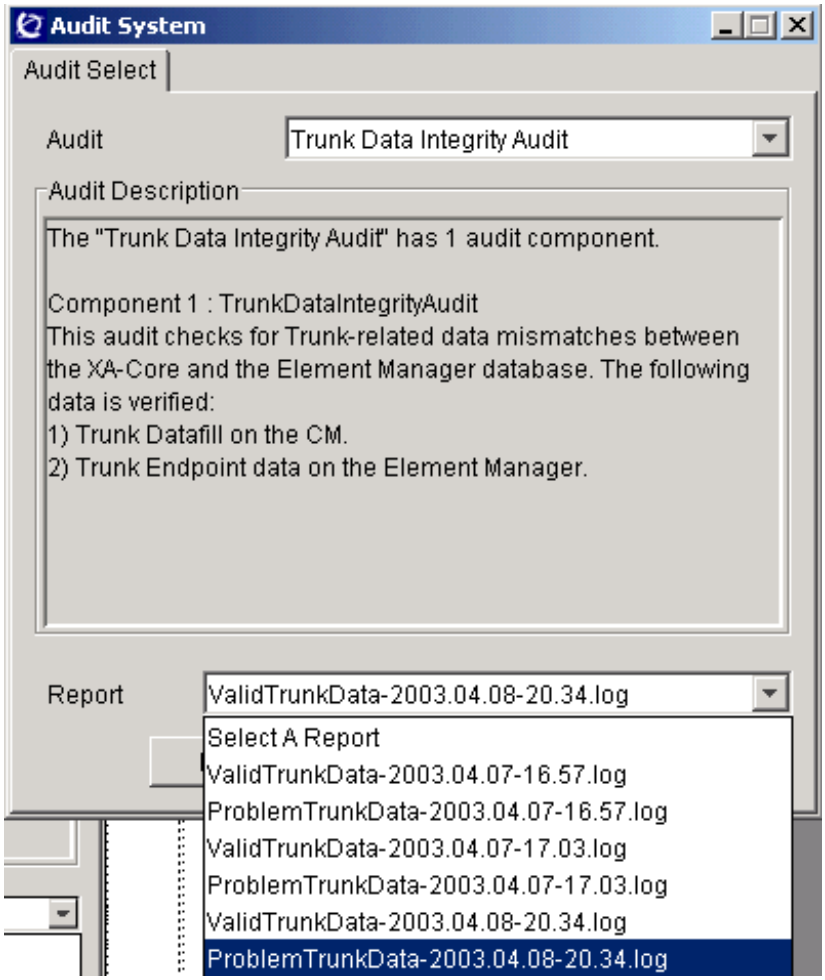
a Ensure that you have selected **Trunk Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit system dialog box.

b Select **ProblemTrunkData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ProblemTrunkData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

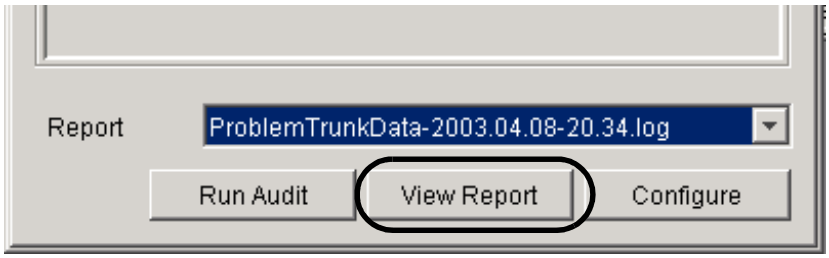
The file name has the following format:

ProblemTrunkData-<date>-<time>.log

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



c Click the **View Report** button.



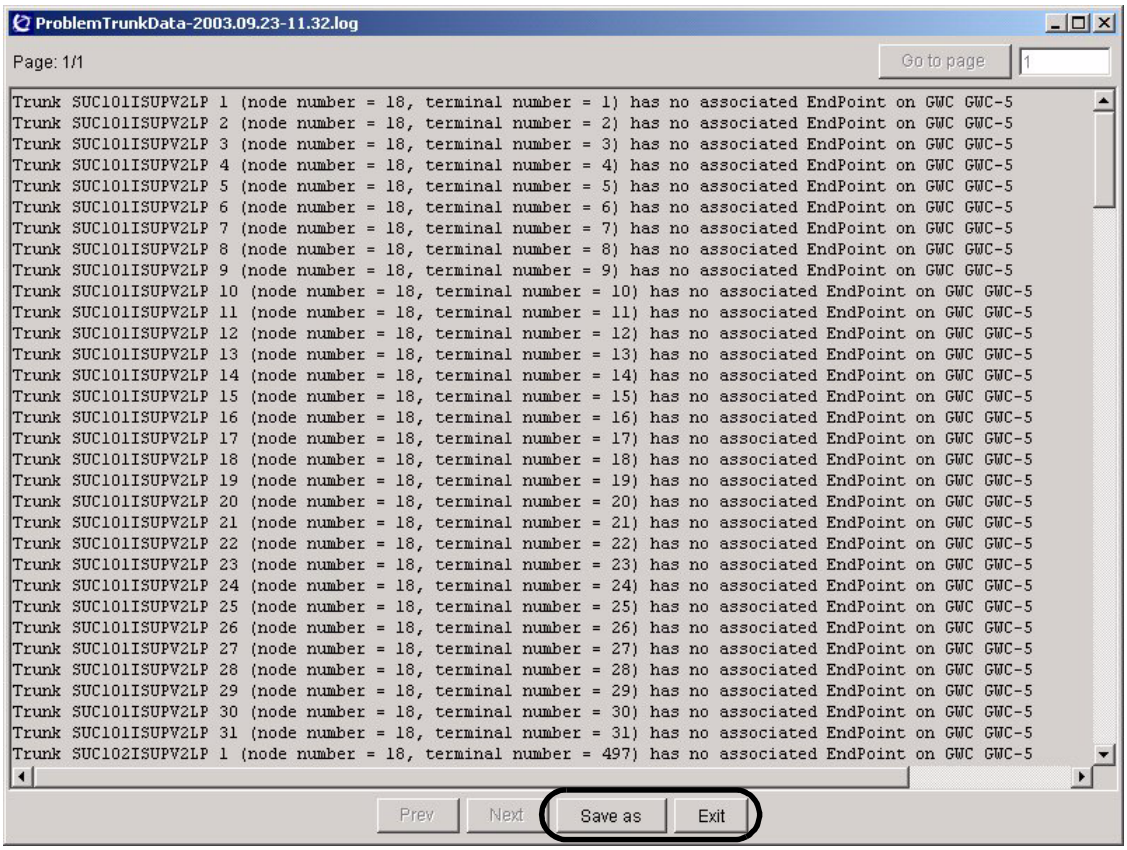
The system displays the selected report.

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

The “Problem” report produced by a trunk audit can contain messages in the following formats:

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

Here is an example of a “ProblemTrunkData” report:



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

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

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

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

f To correct the problems, refer to the printed copy of the report. You will need to delete and then reprovision the listed trunks.

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

17 View a V5.2 audit report as follows:

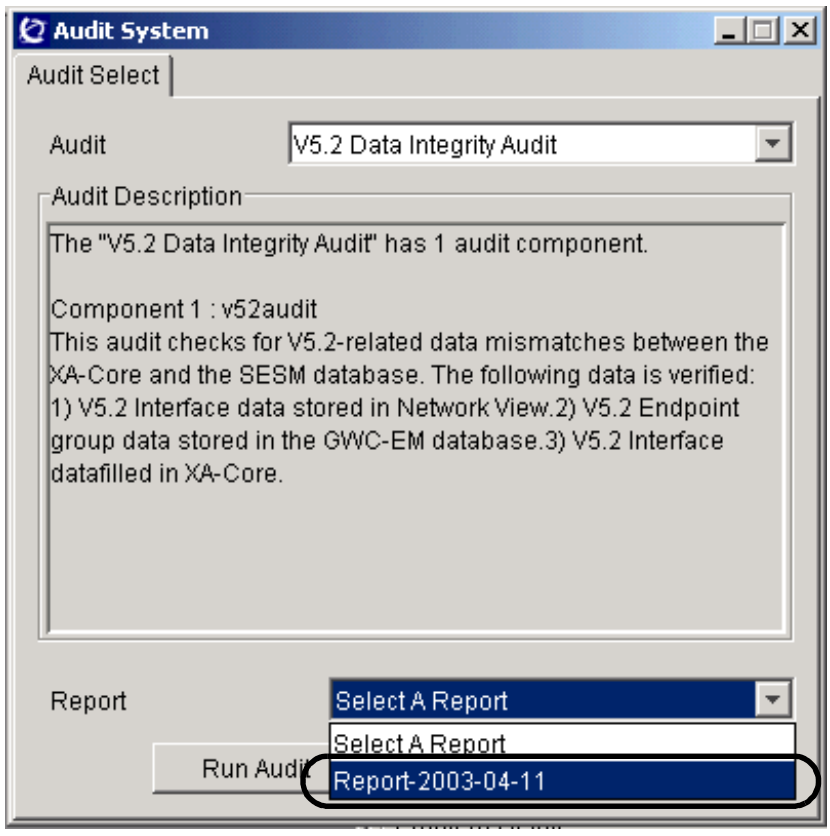
a Ensure that you have selected **V5.2 Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.

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

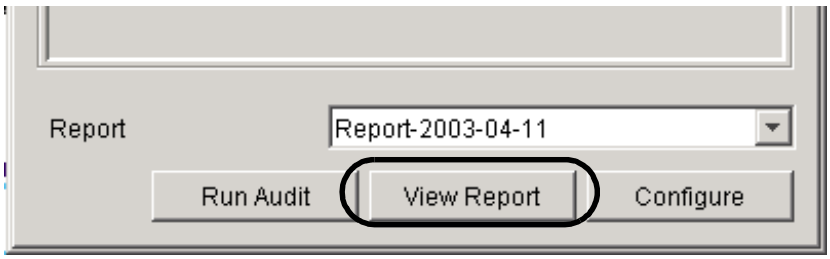
The file name has the following format:

Report-<date>

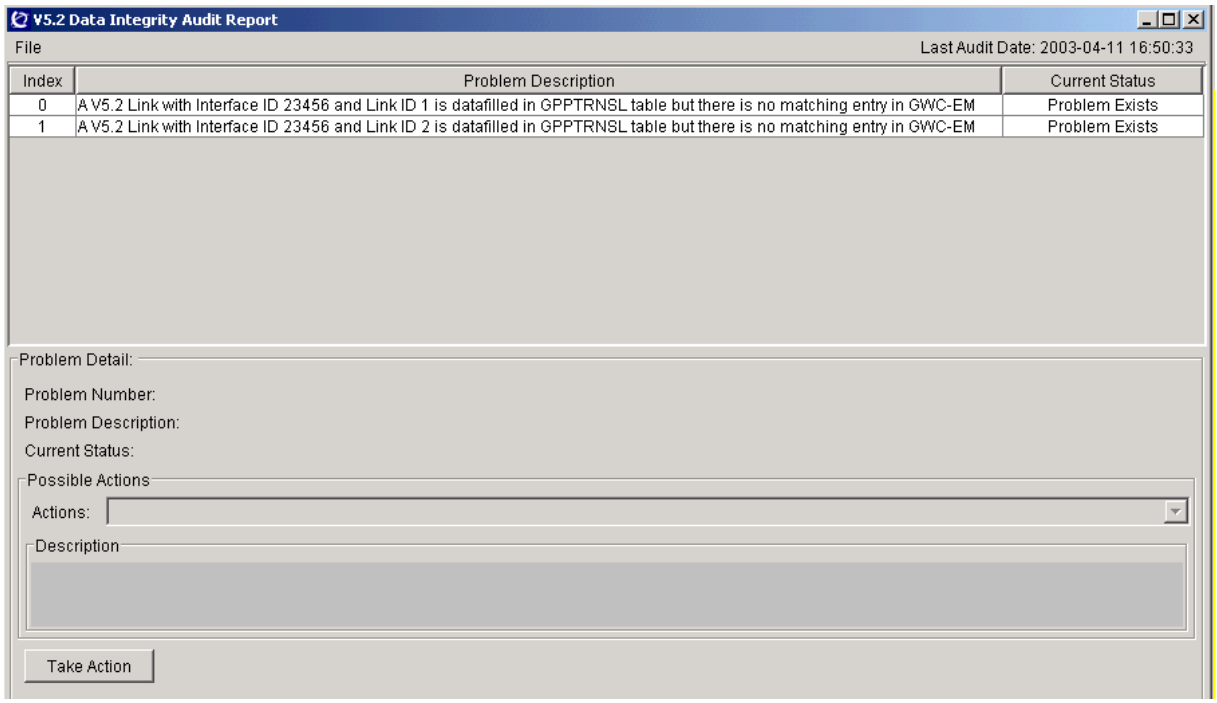
where
<date> is the date in yyyy-mm-dd format, for example, 2003-02-15.



c Click **View Report**.



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



Note 1: The CS 2000 Management Tools server retains the most recent V5.2 audit report. When a new audit occurs, the server deletes the previous report.

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

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

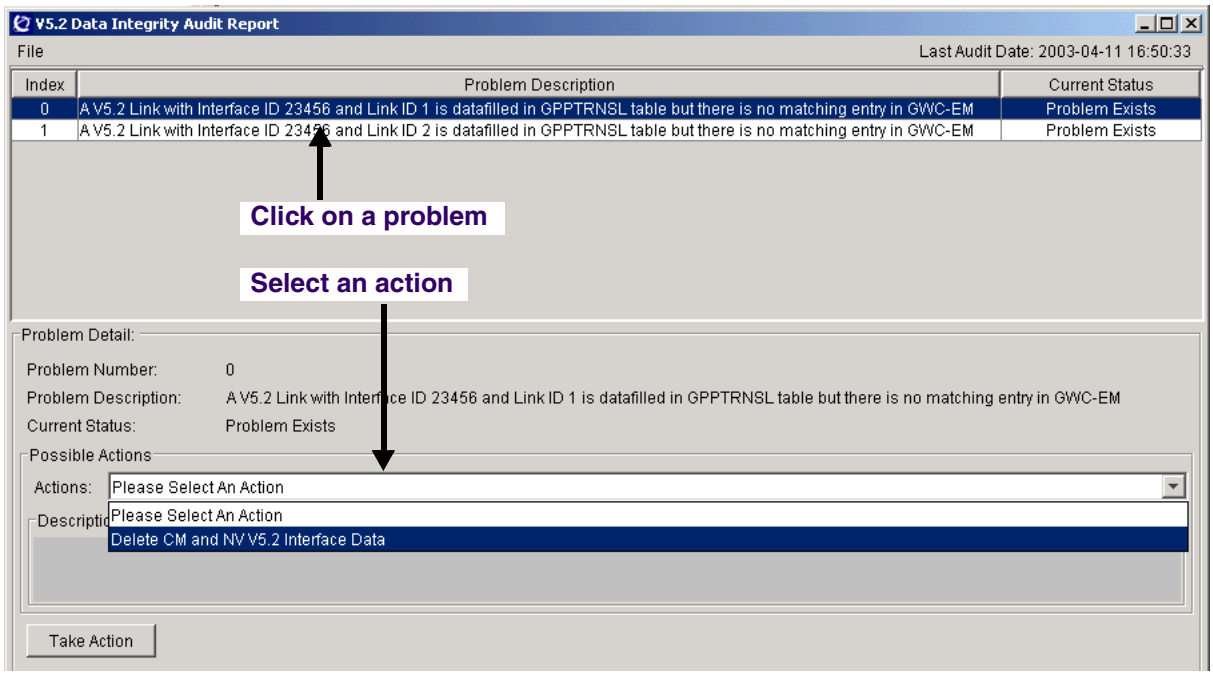
18 Review the results of the audit and click on a problem to resolve.

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

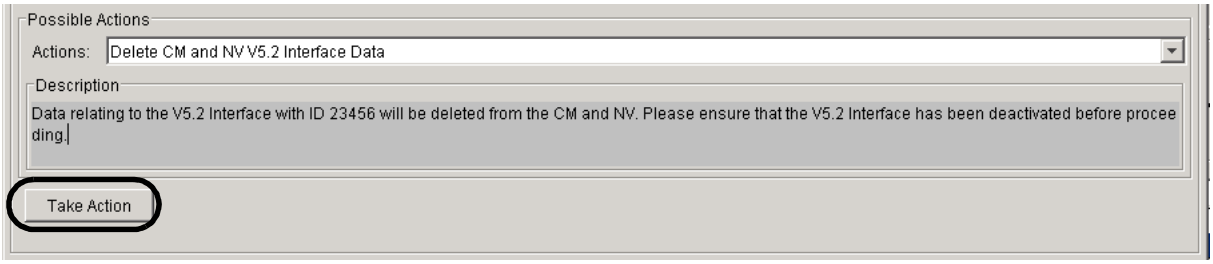
19 Evaluate actions to resolve a problem and take action.

a Click and hold on the Action pull-down menu near the bottom of the screen to assess any possible actions.

b If appropriate, select an action. Read the description of the action and ensure that you observe any recommended steps or cautions.



c Click **Take Action**.



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

20 Return to step 18 to review another problem.

21 You have completed this procedure.

Posting a line by directory number

Application

Use this procedure to post a line by its directory number (DN) so you can perform maintenance on the line.

Restrictions

V5.2 line maintenance is not supported using the Line Maintenance Manager (LMM). V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface.

Since the CS 2000 supports both legacy DMS TDM lines as well as Succession lines, TDM lines can be posted on LMM and maintenance operations like BSY/RTS/FRLS/INB can be performed; however, the CS Line State column will not be displayed accurately. The Endpoint State column will show "Legacy Line" and the GW Profile column and all properties not applicable to TDM lines will display as "Not Available".

When using hunt groups, you can only post the primary DN using the Line Maintenance Manager. You cannot perform line maintenance operations on all members of a hunt group using the LMM. If you need to perform line maintenance on all members of a hunt group, use the CS 2000 XA-Core MAPCI interface. For details, refer to the DMS-100 Family National ISDN BRI Service Implementation Guide, 297-2401-201.

Prerequisites

All Line Maintenance Manager (LMM) status fields must be Green (OK) in order to post lines.

Action

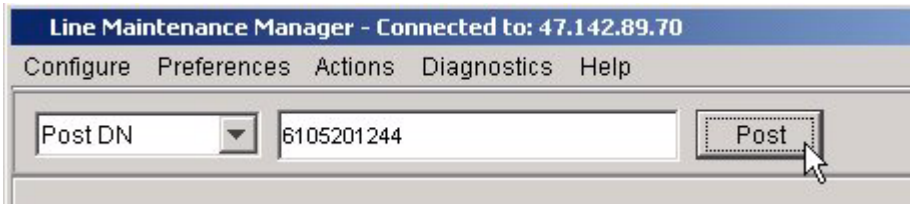
Perform the following steps to complete this procedure.

At your workstation

1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the LMM GUI

2 Select **Post DN**, enter the directory number, and click **Post**.



3 You have completed this procedure.

Posting a line by gateway

Application

Use this procedure to post one or more lines by their associated gateway so you can perform maintenance on the lines.

Use this procedure after adding a gateway and before performing maintenance on that gateway.

Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager (LMM). V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

Only line gateways can be posted.

Prerequisites

The following prerequisites apply to posting one or more lines by gateway:

- The associated gateway must be provisioned with endpoints in the CS 2000 GWC Manager database
- All LMM status fields must be Green (OK) in order to post lines.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the LMM GUI

2 Select **Post by Gateway**, enter the name of the gateway and its path, then click **Post**.

3 You have completed this procedure.

Additional information

When post-by-gateway is selected on the LMM GUI, the line state at the CM is displayed. A on-demand audit to identify the state of the endpoint on the gateway is also done through the CS 2000 GWC Manager and the endpoint state is displayed at the LMM GUI Endpoint State field. This audit is done in a protocol independent manner by the LMM. Any errors produced during the posting activity will be displayed on the status panel shown below.

A list of currently supported LMM GUI error codes with descriptions is shown in the following table.

Error Code	LMM client text displayed in status panel	Description
1000	OK	Audit response received from endpoint
1010	Wait_GW_response	GWC waiting for gateway audit response
1020	GW_Protocol_Unsupported	Unsupported gateway protocol
1100	GWC_Unavailable	GWC not available for endpoint query
1200	IP_Unavailable	Unable to retrieve IP address for gateway
2000	SNMP_exception	SNMP error between LMM and GWC

Error Code	LMM client text displayed in status panel	Description
2010	EP_Not_Found	Endpoint status expired in GWC before retrieval
2020	Invalid_EP	Endpoint does not exist in GWC
3000	GWC_LoadName_error	Incompatible GWC load version detected
3010	Unsupported_GWC_Load	GWC is running an unknown or unsupported load
4000	Decode_Failure	Error decoding Gateway IP address
4010	Unknown_Endpoint	LMM could not get endpoint state

Busying a line

Application

Use this procedure to busy (BSY) a line and put it into a maintenance busy (MB) state. Once busied, the line cannot perform call processing.

Use this procedure during maintenance or alarm clearing activities.

Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

Prerequisites

The line must be posted. Refer to procedures Posting a line by gateway or Posting a line by directory number in this document, if required.

Action

Perform the following steps to complete this procedure.

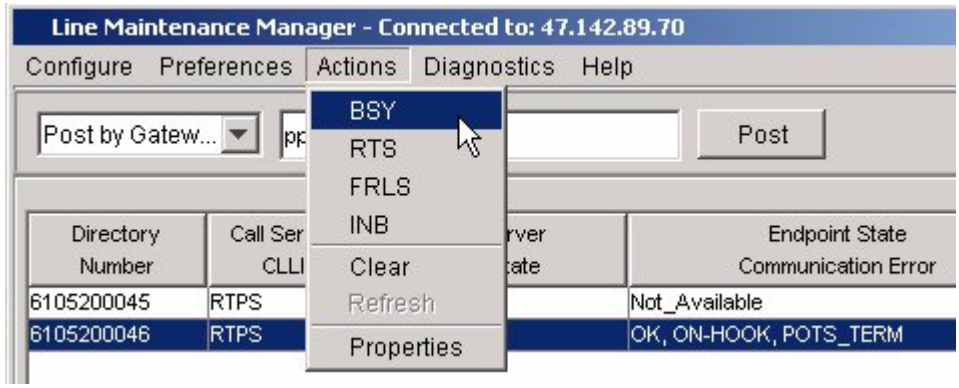
At your workstation

1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the LMM GUI

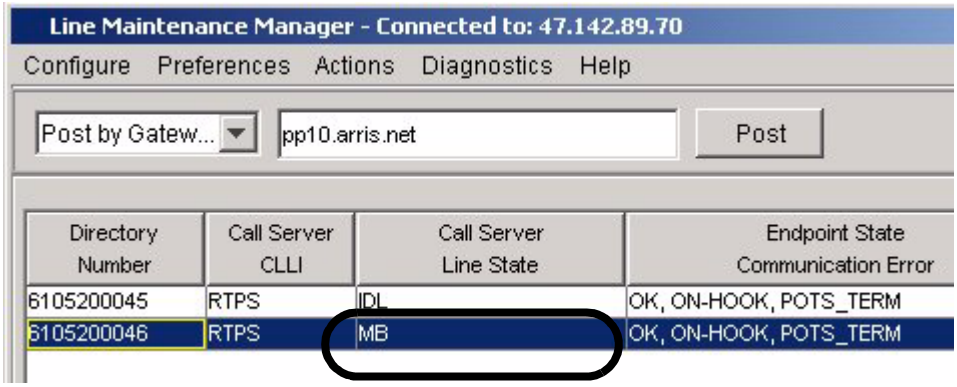
2 Select the DN you want to busy, then on the **Actions** menu, click **BSY**, or right-click on the selected DN then click **BSY**.

Note: You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.



3 Observe that the selected DN(s) are put into a maintenance busy (MB) state as shown below.

Note: The line state will be CPD if the original line state was CPB prior to Busy.



4 You have completed this procedure.

Installation busying a line

Application

Use this procedure to set a line to the installation busy (INB) state.

Use this procedure during maintenance and fault clearing activities.

Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

Prerequisites

The line must be posted. Refer to procedures Posting a line by gateway or Posting a line by directory number in this document, if required.

Action

Perform the following steps to complete this procedure.

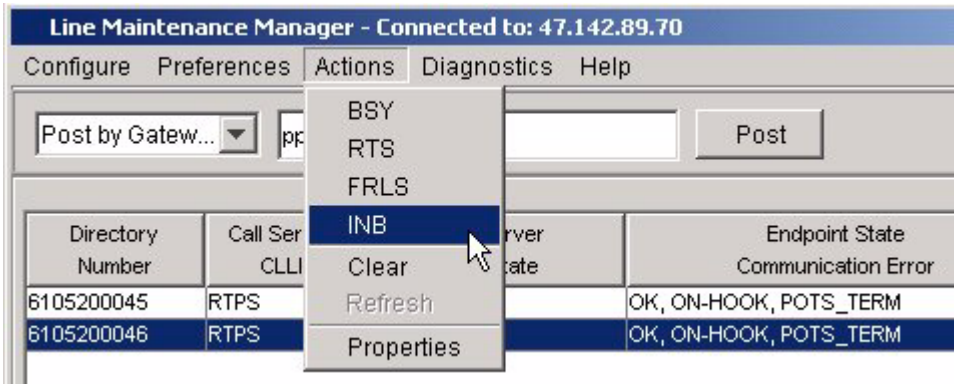
At your workstation

1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

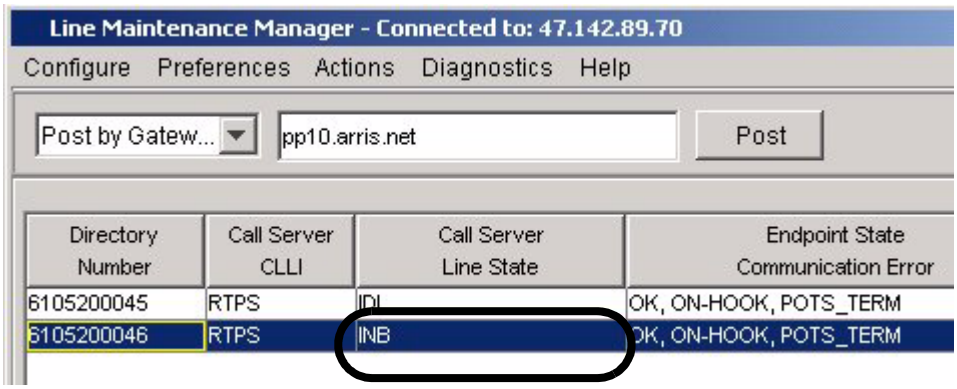
At the LMM GUI

2 Select the DN you want to installation busy, then on the **Actions** menu, click **INB**, or right-click on the selected DN then click **INB**.

Note: ou can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.



3 Observe that the selected DN(s) are put into an installation busy (INB) state as shown below.



4 You have completed this procedure.

Force releasing a line

Application

Use this procedure to force release (FRLS) a line, putting it into a maintenance busy (MB) state.

Use this procedure if Nortel Networks support personnel indicate its use.

Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

Prerequisites

The line must be posted. Refer to procedures Posting a line by gateway or Posting a line by directory number in this document, if required.

Action

Perform the following steps to complete this procedure.

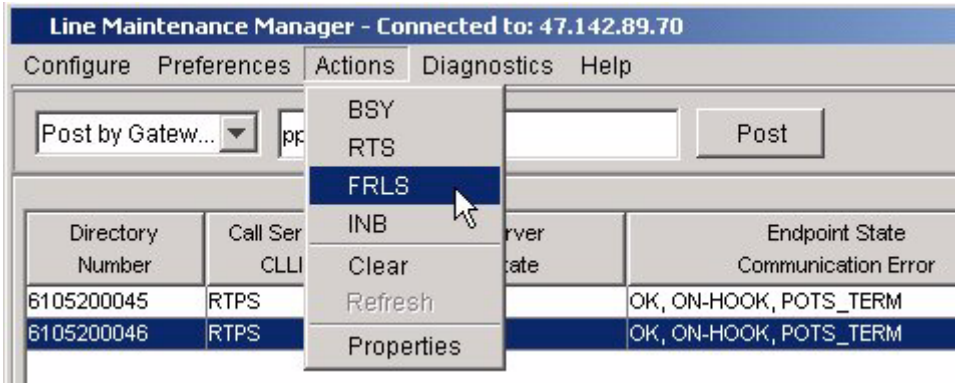
At your workstation

1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the LMM GUI

2 Select the DN you want to force a release on, then on the **Actions** menu, click **FRLS**, or right-click on the selected DN then click **FRLS**.

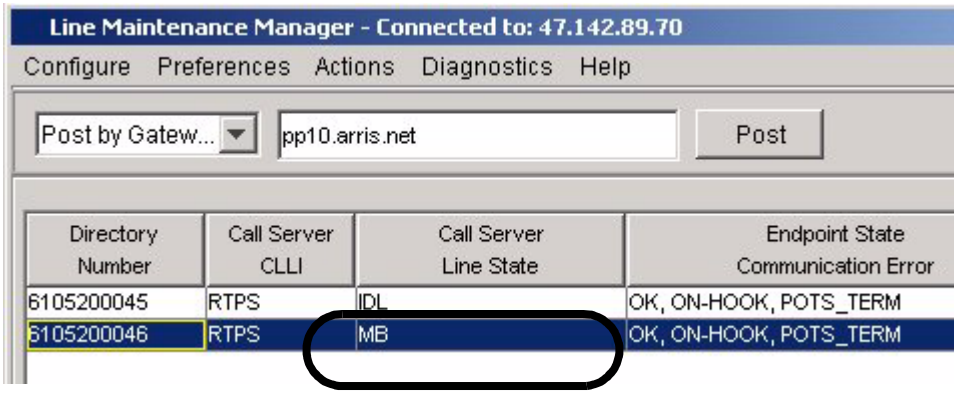
Note: You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.



3 Click **OK** to confirm the force release of the line(s).

Note: The call will be dropped if there was a call on the selected DN.

4 Observe that the selected DN(s) are put into an maintenance busy (MB) state as indicated in the following figure.



5 You have completed this procedure.

Returning a line to service

Application

Use this procedure to return a busied line to service (RTS). Once returned to service, the line can then perform call processing.

Use this procedure after maintenance has been performed on a busied line.

Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

Prerequisites

The line must be in a maintenance busy (MB) state. Refer to procedure Busying a line in this document, if required.

Action

Perform the following steps to complete this procedure.

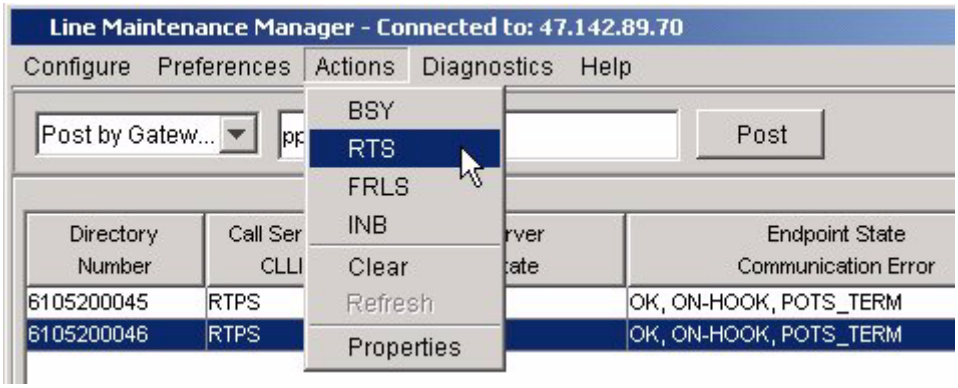
At your workstation

1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

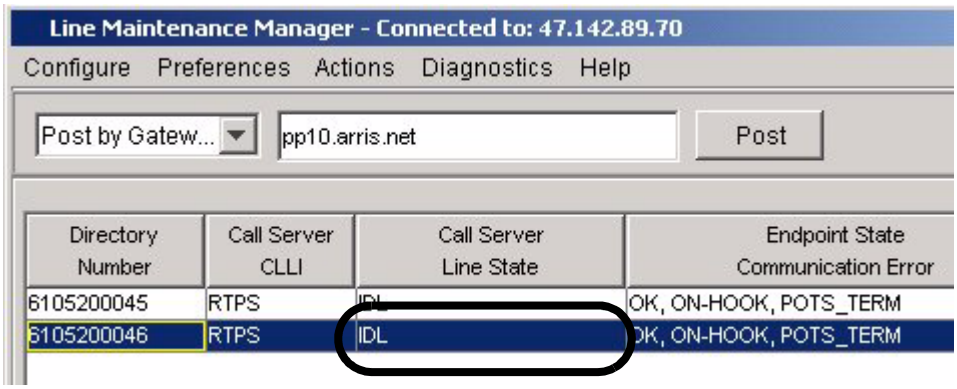
At the LMM GUI

2 Select the DN you want to return to service, then on the **Actions** menu, click **RTS**, or right-click on the selected DN then click **RTS**.

Note: You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.



3 Observe that the state of the selected DN(s) is changed from maintenance busy (MB) to idle (IDL) as shown below.



4 You have completed this procedure.

Clearing one or more posted lines from the display

Application

Use this procedure to remove a directory number (DN) from the list of posted DNs.

Use this procedure before performing maintenance on a posted set of lines or when the posted lines no longer need to be monitored.

Restrictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

Prerequisites

The line must be posted. Refer to procedures Posting a line by gateway or Posting a line by directory number in this document, if required.

Action

Perform the following steps to complete this procedure.

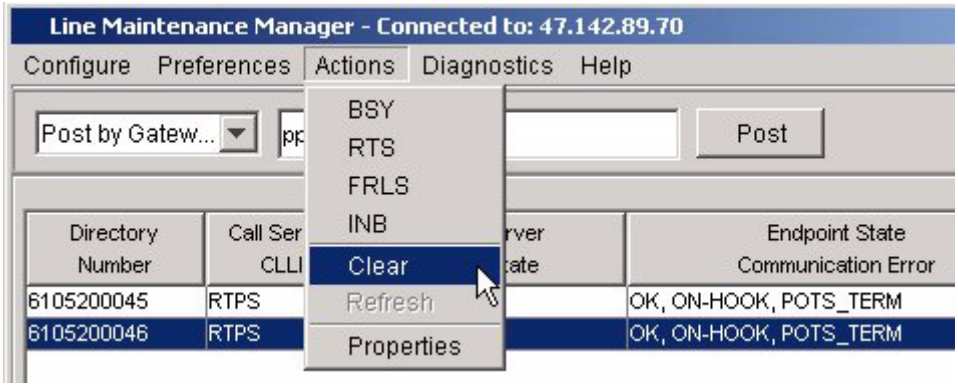
At your workstation

1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the LMM GUI

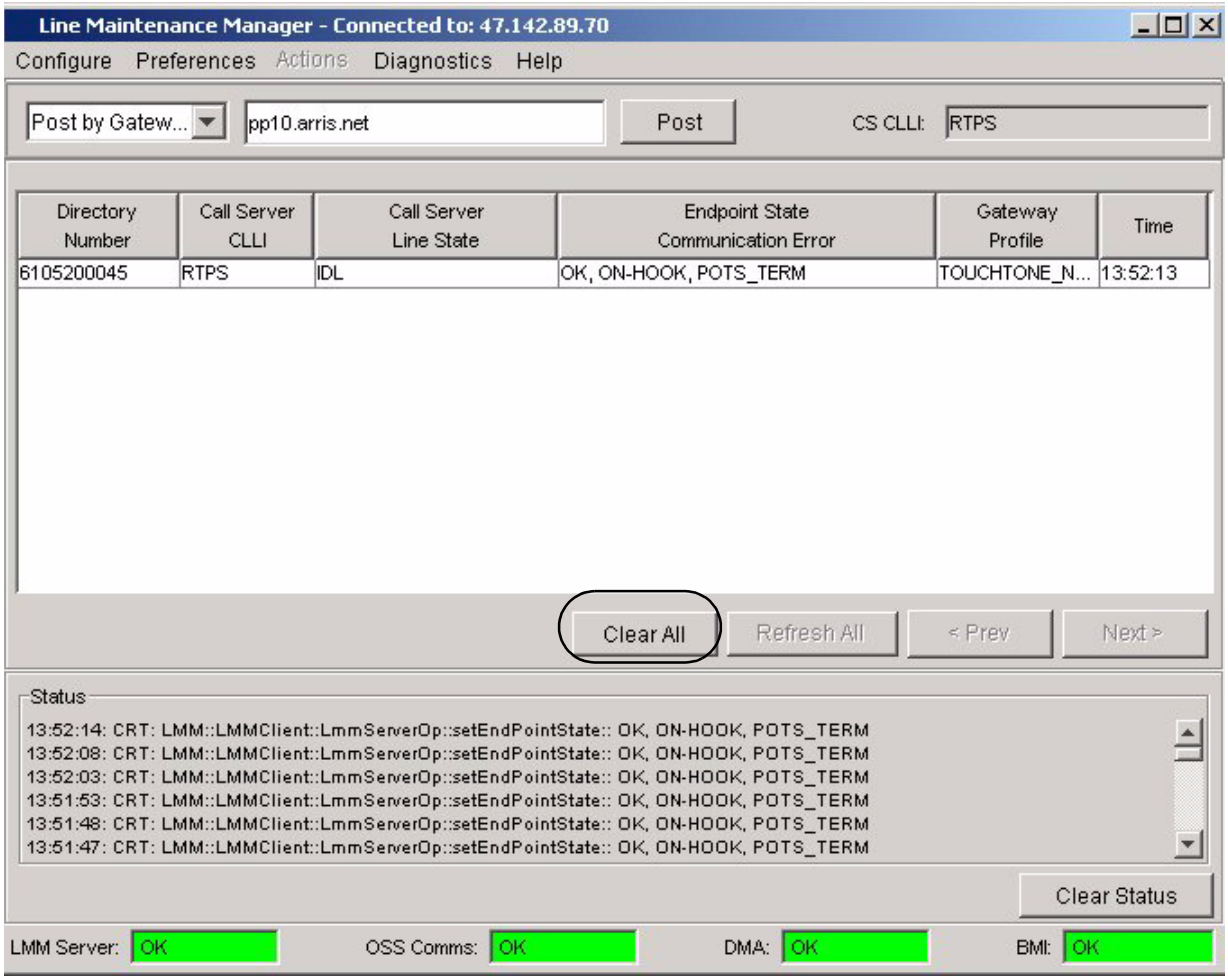
2 Select the DN you want to remove from the display of posted lines, then on the **Actions** menu, click **Clear**, or right-click on the selected DN then click **Clear**.

Note: You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.



3 Observe that the selected DN(s) are cleared from the list as shown below.

Note: To clear all posted DN, click **Clear All**.



4 You have completed this procedure.

Retrieving line properties

Application

Use this procedure to retrieve and display the line properties for a selected directory number (DN) or group of DNs.

Use this procedure as a part of fault clearing activities.

Restictions

V5.2 line maintenance is not supported using Line Maintenance Manager. V5.2 line maintenance is performed using the CS 2000 XA-Core MAPCI interface

Prerequisites

The line must be posted. Refer to procedures Posting a line by gateway or Posting a line by directory number in this document, if required.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

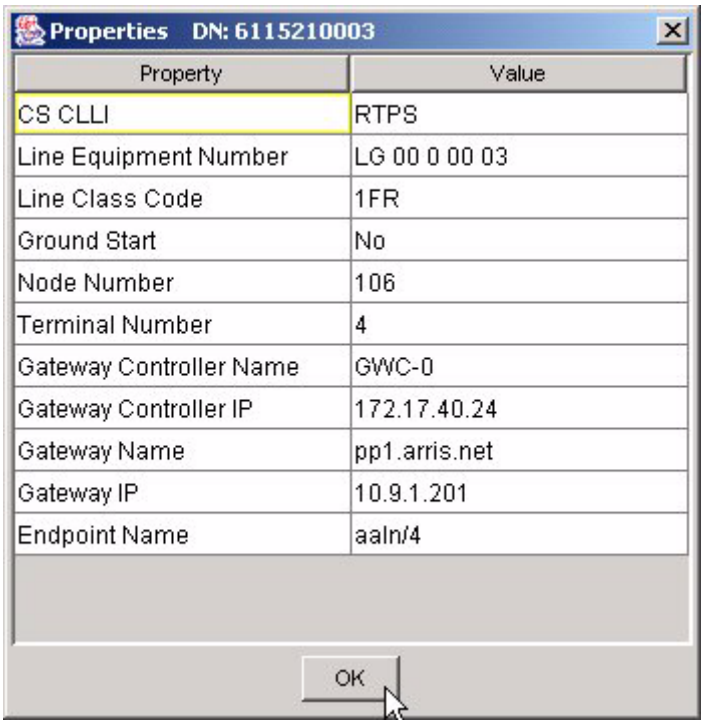
At the LMM GUI

2 Select the DN you want to view the properties for, then on the **Actions** menu, click **Properties**, or right-click on the selected DN then click **Properties**.

Note: You can perform this operation on one or more posted lines at the same time. You can use the **Shift** key to select multiple lines consecutively, or the **Ctrl** key to select multiple lines non-consecutively.

The Properties window opens.

3 Click **OK** to close the Properties window.



4 You have completed this procedure.

Querying line gateways in a trouble state

Application

This procedure describes how to perform a query on line gateways in a trouble state, and view reports.

> ***Note:*** You can configure a query to run on a daily or weekly basis at a specific time. Refer to procedure "Configuring a query for line gateways in a trouble state" in the CS 2000 Management Tools Configuration Management document, NN10106-511.

Use this procedure to troubleshoot line gateways.

Prerequisites

All Line Maintenance Manager (LMM) status fields must be Green (OK) in order to perform a query.

Action

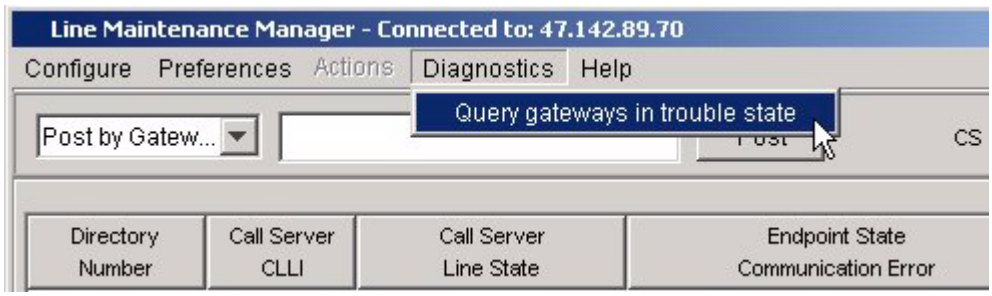
Perform the following steps to complete this procedure.

At your workstation

1 Launch the Line Maintenance Manager (LMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document, if required.

At the LMM GUI

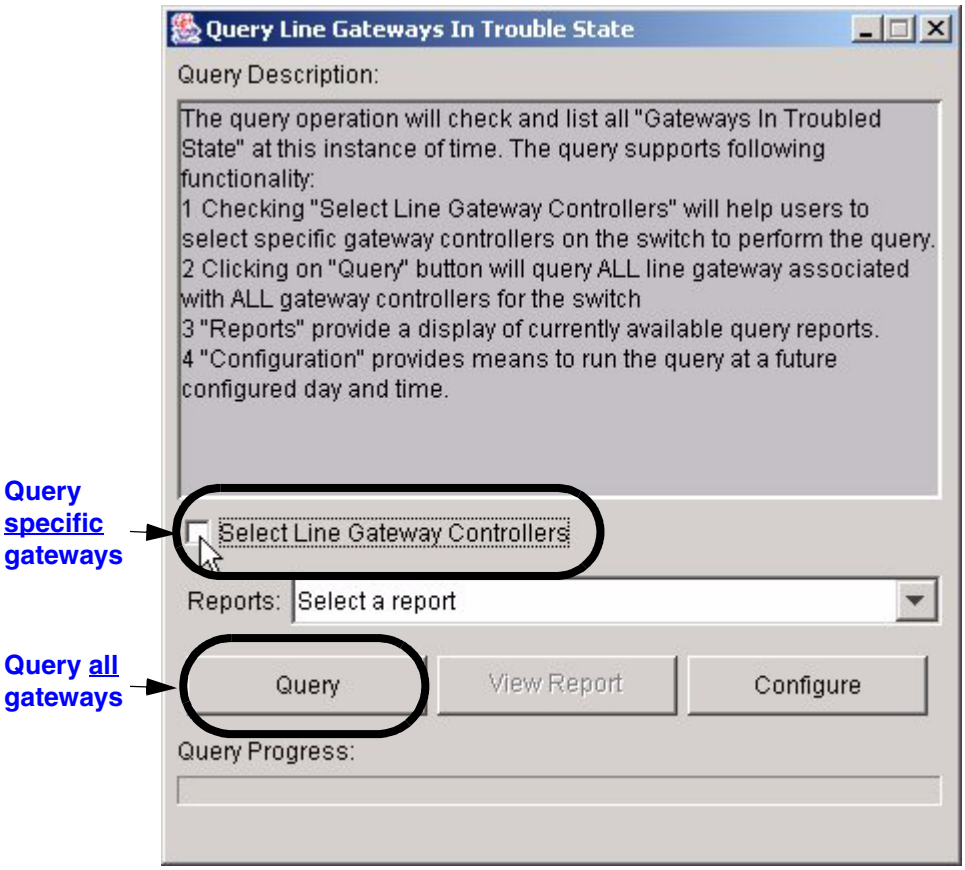
2 On the **Diagnostics** menu, click **Query gateways in trouble state**.



3 Use the following table to determine your next step.

If you want to	Do
perform a query	step 4
view reports	step 8

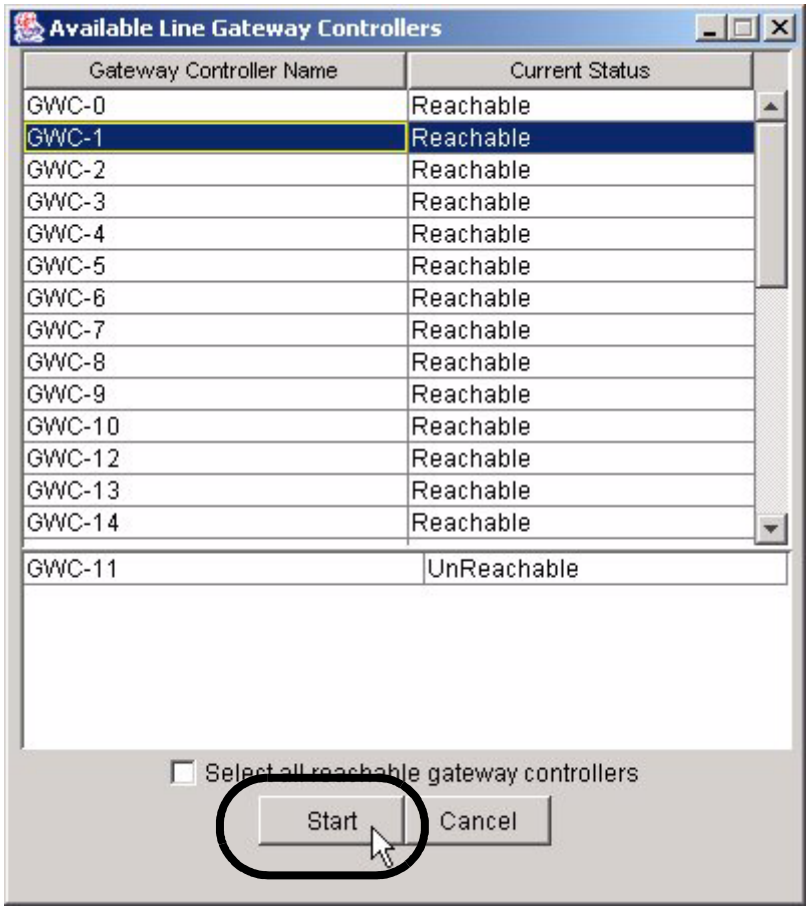
4 Click **Query** to query all line gateways associated with all gateway controllers for the switch, or click the **Select line gateway controllers** check box to query all line gateways associated with specific gateway controllers .



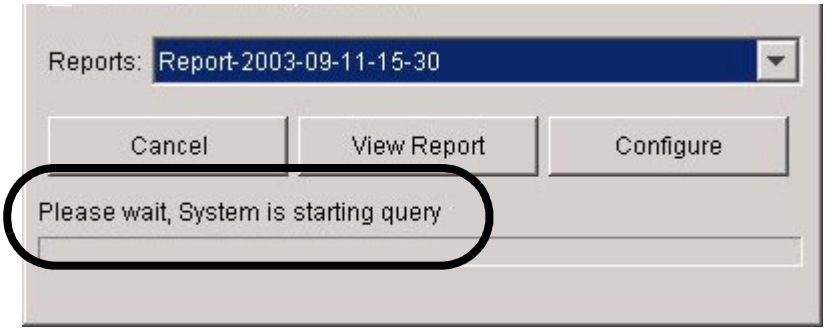
5 Use the following table to determine your next step.

If you are querying	Do
specific gateways	step 6
all gateways	step 7

6 Select the reachable gateway controller(s) of your choice, press **Ctrl+a**, or click the **Select all reachable gateway controllers** check box, then click **Start**.



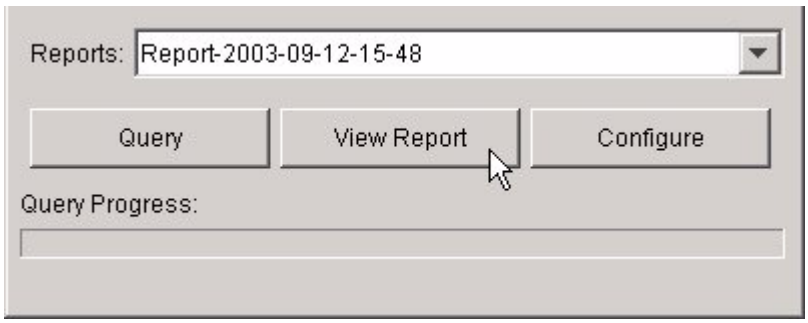
The system starts the query.



Note: Click **Cancel** at any time to cancel the query.

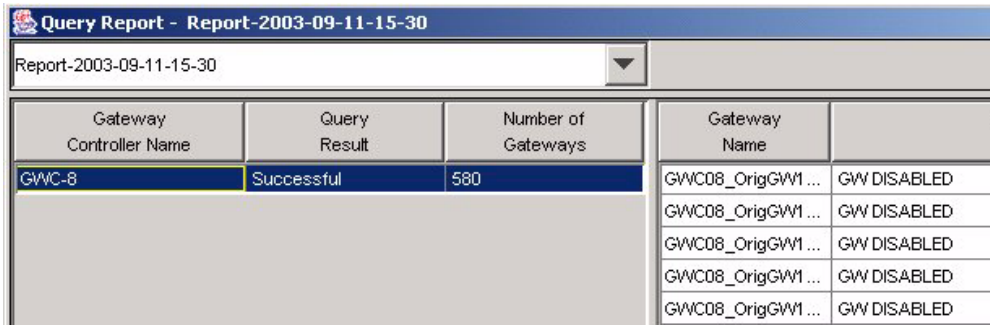
7 Click **OK** once it completes.

8 Select a report from the list and click **View Report**. If you just performed a query, the report is the one dispayed in the **Reports:** box.



Note: The system maintains a maximum number of seven reports for each gateway controller.

9 Click on the gateway controller of your choice to display the associated gateways and their trouble state information.



Note: From the **Query Report** window, you can select other reports as required. You can scroll through the list of gateways using the **Prev** (previous) and **Next** buttons.

10 You have completed this procedure.

Posting a trunk member

Application

Use this procedure to post trunk members by CLLI code.

Note: The Trunk Maintenance Manager (TMM) only supports ISUP and PRI trunks in Succession. Other trunk types can work, but they are not explicitly supported. Maintenance on those trunks, such as UAS and SIP-T trunks, needs to be performed using the CS 2000 XA-Core MAPCI interface.

Prerequisites

You need the CLLI code for the trunk you want to post. Refer to procedure Displaying trunk CLLI codes by gateway in this document, if required.

Action

Perform the following steps to complete this procedure.

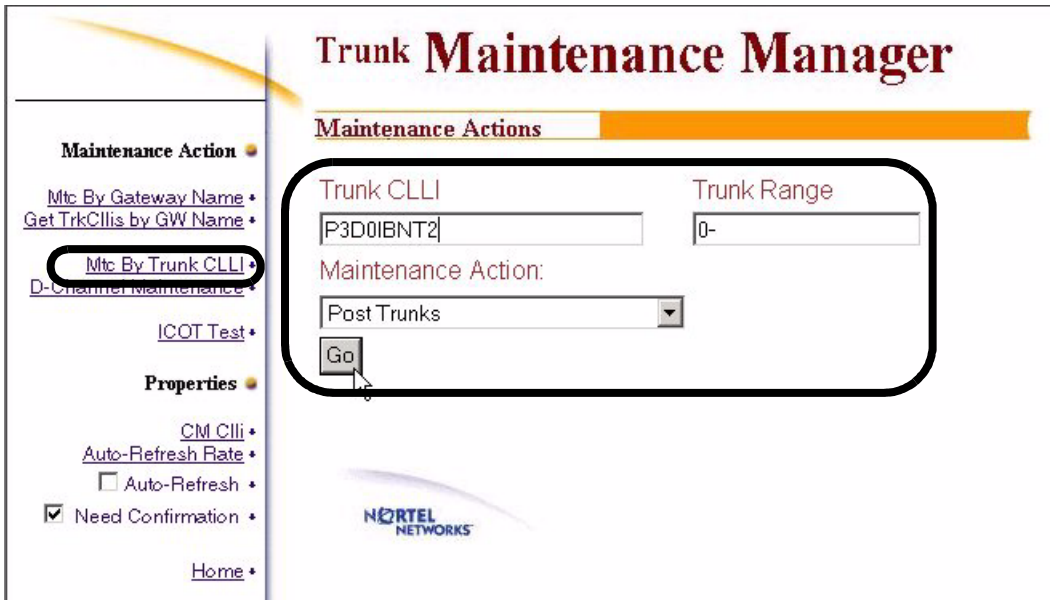
At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the TMM GUI

2 Click **Mtc By Trunk CLLI**.

3 Enter the trunk CLLI name and optionally a Trunk Range value (or use the default [0-] value for all trunk members), then select **Post Trunks** from the **Maintenance Action** drop down menu, and click **Go**.



The trunk members are displayed as shown in the following example.

CM CLLI:	Trunk CLLI:	First Member:	Group Size:
RTPS	P3D0IBNT2	1	24

Number	State	Connected To	Direction	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Name
1	IDL		2W	S7 S7	GWC_NODE	1	13	1057	PVG193	STS/6/0/3/VT15/2/1/3/1
2	IDL		2W	S7 S7	GWC_NODE	1	13	1058	PVG193	STS/6/0/3/VT15/2/1/3/2
3	IDL		2W	S7 S7	GWC_NODE	1	13	1059	PVG193	STS/6/0/3/VT15/2/1/3/3
4	IDL		2W	S7 S7	GWC_NODE	1	13	1060	PVG193	STS/6/0/3/VT15/2/1/3/4
5	IDL		2W	S7 S7	GWC_NODE	1	13	1061	PVG193	STS/6/0/3/VT15/2/1/3/5
6	IDL		2W	S7 S7	GWC_NODE	1	13	1062	PVG193	STS/6/0/3/VT15/2/1/3/6
7	IDL		2W	S7 S7	GWC_NODE	1	13	1063	PVG193	STS/6/0/3/VT15/2/1/3/7
8	IDL		2W	S7 S7	GWC_NODE	1	13	1064	PVG193	STS/6/0/3/VT15/2/1/3/8
9	IDL		2W	S7 S7	GWC_NODE	1	13	1065	PVG193	STS/6/0/3/VT15/2/1/3/9

4 You have completed this procedure.

Busying a trunk member

Application

Use this procedure to busy one or more trunk members by CLLI code.

Note: The Trunk Maintenance Manager (TMM) only supports ISUP and PRI trunks in Succession. Other trunk types can work, but they are not explicitly supported. Maintenance on those trunks, such as UAS and SIP-T trunks, needs to be performed using the CS 2000 XA-Core MAPCI interface.

Prerequisites

You must first post the trunk you want to busy. Refer to procedure Posting a trunk member in this document, if required.

Action

Perform the following steps to complete this procedure.

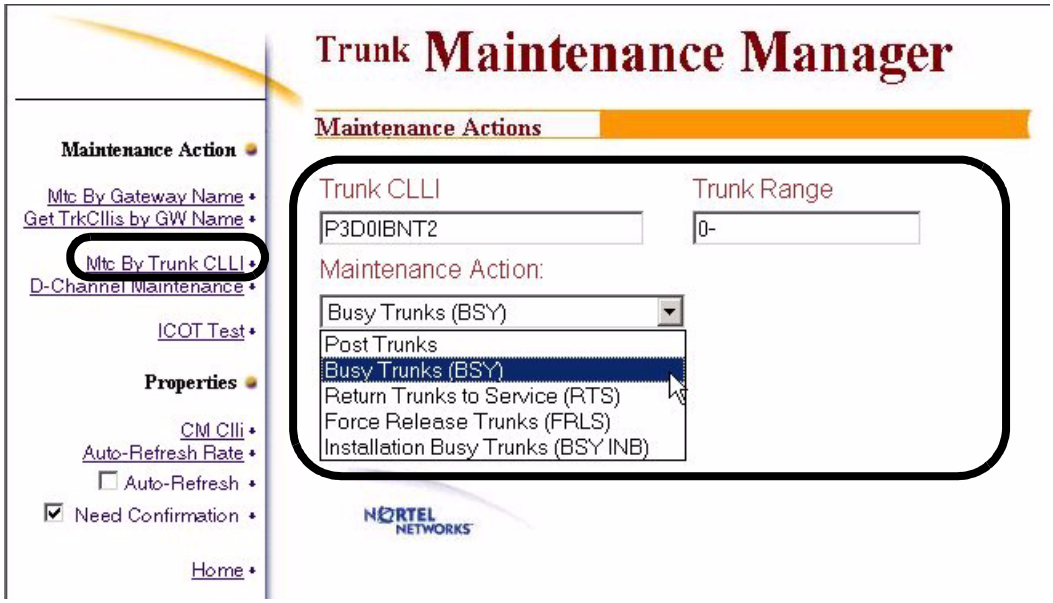
At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

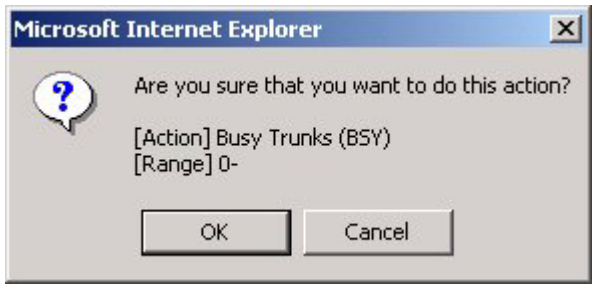
At the TMM GUI

2 Click **Mtc By Trunk CLLI**.

3 Enter the trunk CLLI name and optionally a Trunk Range value (or use the default [0-] value for all trunk members), then select **Busy Trunks (BSY)** from the **Maintenance Action** drop down menu, and click **Go**.



If you attempted to busy more than one trunk member and the "Need Confirmation" check box is checked, you need to confirm the busy action as shown in the following figure.



4 If it is acceptable to busy more than one trunk member, click **OK**.

5 Observe that the selected range of trunk members are in the maintenance busy (MB) as shown in the following example.

CM CLLI:	Trunk CLLI:	First Member:	Group Size:
RTPS	RTP5IBNT2OG	1	4

Number	State	Connected To	Direction	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Name
1	MB		2W	S7 S7	GWC_NODE	1	13	365	PVG190	DS3/02/0/16/5
2	MB		2W	S7 S7	GWC_NODE	1	13	366	PVG190	DS3/02/0/16/6
3	MB		2W	S7 S7	GWC_NODE	1	13	367	PVG190	DS3/02/0/16/7
4	MB		2W	S7 S7	GWC_NODE	1	13	368	PVG190	DS3/02/0/16/8

Last Refreshed: Wed Sep 24 13:46:10 EDT 2003

6 You have completed this procedure.

Installation busying a trunk member

Application

Use this procedure to installation busy (INB) one or more trunk members by CLLI code.

Note: TheTrunk Maintenance Manager (TMM) only supports ISUP and PRI trunks in Succession. Other trunk types can work, but they are not explicitly supported. Maintenance on those trunks, such as UAS and SIP-T trunks, needs to be performed using the CS 2000 XA-Core MAPCI interface.

Prerequisites

You must first post the trunk you want to intallation busy. Refer to procedure Posting a trunk member in this document, if required.

Action

Perform the following steps to complete this procedure.

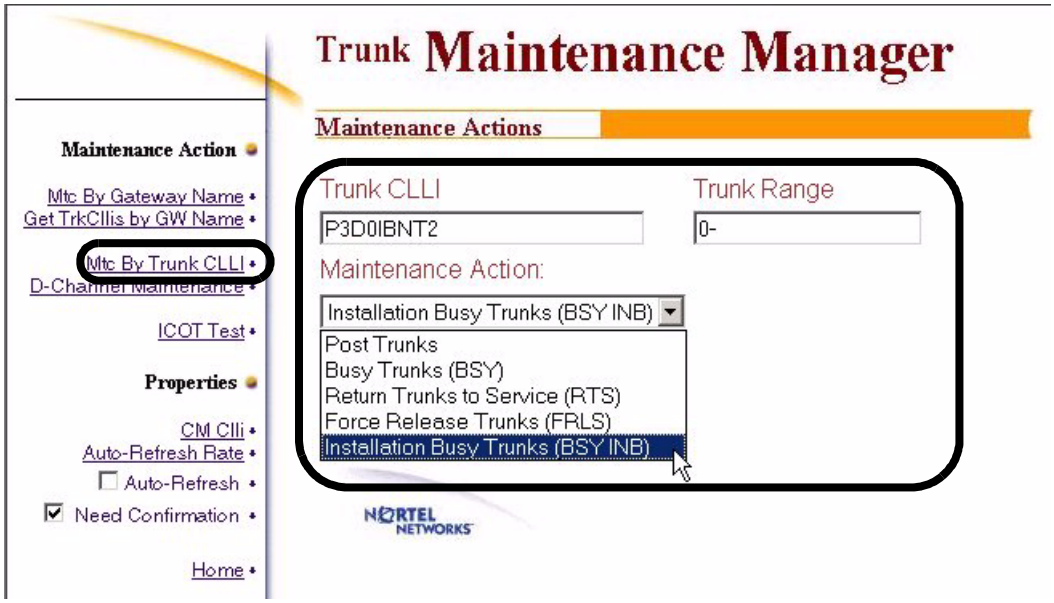
At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the TMM GUI

2 Click **Mtc By Trunk CLLI**.

3 Enter the trunk CLLI name and optionally a Trunk Range value (or use the default [0-] value for all trunk members), then select **Installation Busy Trunks (BSY INB)** from the **Maintenance Action** drop down menu, and click **Go**.



4 Observe that the selected range of trunk members are in the installation busy (INB) state as shown in the following example.

CM CLLI:	Trunk CLLI:	First Member:	Group Size:
COMPACT2	KOUISUP26	121	24

Number	State	Connected To	Direction	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Name
121	INB		2W	S7 S7	GWC_NODE	1	15	1081	PVG190	DS3_22.6.1
122	INB		2W	S7 S7	GWC_NODE	1	15	1082	PVG190	DS3_22.6.2
123	INB		2W	S7 S7	GWC_NODE	1	15	1083	PVG190	DS3_22.6.3
124	INB		2W	S7 S7	GWC_NODE	1	15	1084	PVG190	DS3_22.6.4
125	INB		2W	S7 S7	GWC_NODE	1	15	1085	PVG190	DS3_22.6.5
126	INB		2W	S7 S7	GWC_NODE	1	15	1086	PVG190	DS3_22.6.6
127	INB		2W	S7 S7	GWC_NODE	1	15	1087	PVG190	DS3_22.6.7
128	INB		2W	S7 S7	GWC_NODE	1	15	1088	PVG190	DS3_22.6.8

5 You have completed this procedure.

Force releasing a trunk member

Application

Use this procedure to force release one or more trunk members by CLLI code.

Note: The Trunk Maintenance Manager (TMM) only supports ISUP and PRI trunks in Succession. Other trunk types can work, but they are not explicitly supported. Maintenance on those trunks, such as UAS and SIP-T trunks, needs to be performed using the CS 2000 XA-Core MAPCI interface.

Prerequisites

You must first post the trunk you want to force release. Refer to procedure Posting a trunk member in this document, if required.

Action

Perform the following steps to complete this procedure.

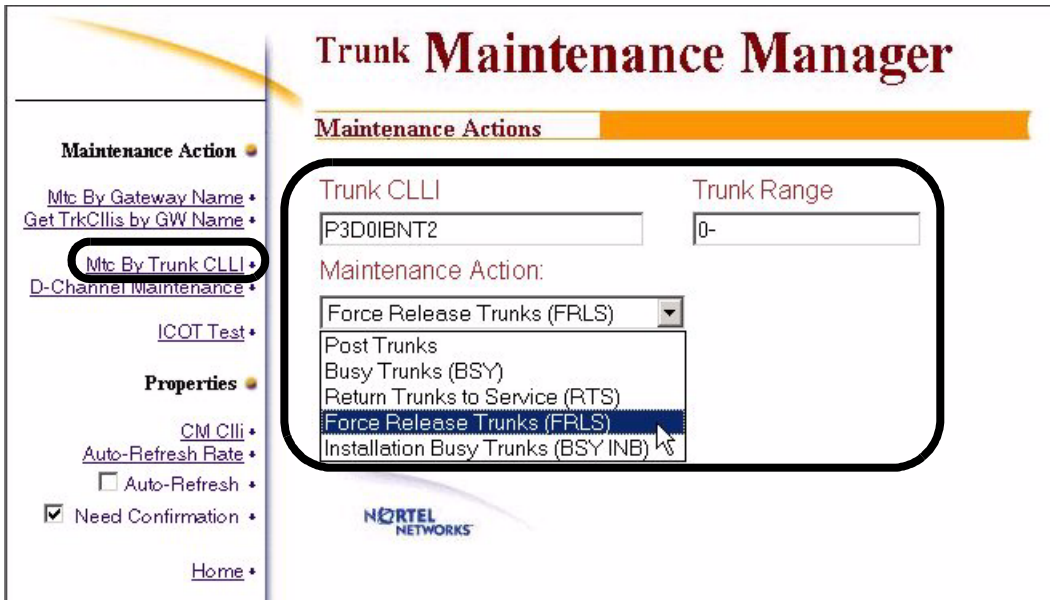
At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the TMM GUI

2 Click **Mtc By Trunk CLLI**.

3 Enter the trunk CLLI name and optionally a Trunk Range value (or use the default [0-] value for all trunk members), then select **Force Release Trunks (FRLS)** from the **Maintenance Action** drop down menu, and click **Go**.



4 Observe that the selected range of trunk members are force released to a maintenance busy (MB) state as shown in the following example.

CM CLLI:	Trunk CLLI:	First Member:	Group Size:
RTPS	RTP5IBNT2OG	1	4

Number	State	Connected To	Direction	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Name
1	MB		2W	S7 S7	GWC_NODE	1	13	365	PVG190	DS3/02/0/16
2	MB		2W	S7 S7	GWC_NODE	1	13	366	PVG190	DS3/02/0/16
3	MB		2W	S7 S7	GWC_NODE	1	13	367	PVG190	DS3/02/0/16
4	MB		2W	S7 S7	GWC_NODE	1	13	368	PVG190	DS3/02/0/16

Last Refreshed: Wed Sep 24 13:46:10 EDT 2003

5 You have completed this procedure.

Returning a trunk member to service

Application

Use this procedure to return one or more trunk members to service (RTS) by CLLI code.

Note: The Trunk Maintenance Manager (TMM) only supports ISUP and PRI trunks in Succession. Other trunk types can work, but they are not explicitly supported. Maintenance on those trunks, such as UAS and SIP-T trunks, needs to be performed using the CS 2000 XA-Core MAPCI interface.

Prerequisites

You must first post the trunk you want to return to service. Refer to procedure Posting a trunk member in this document, if required.

The trunk members must be in a maintenance busied (MB) state or in other proper states such as CPD.

Action

Perform the following steps to complete this procedure.

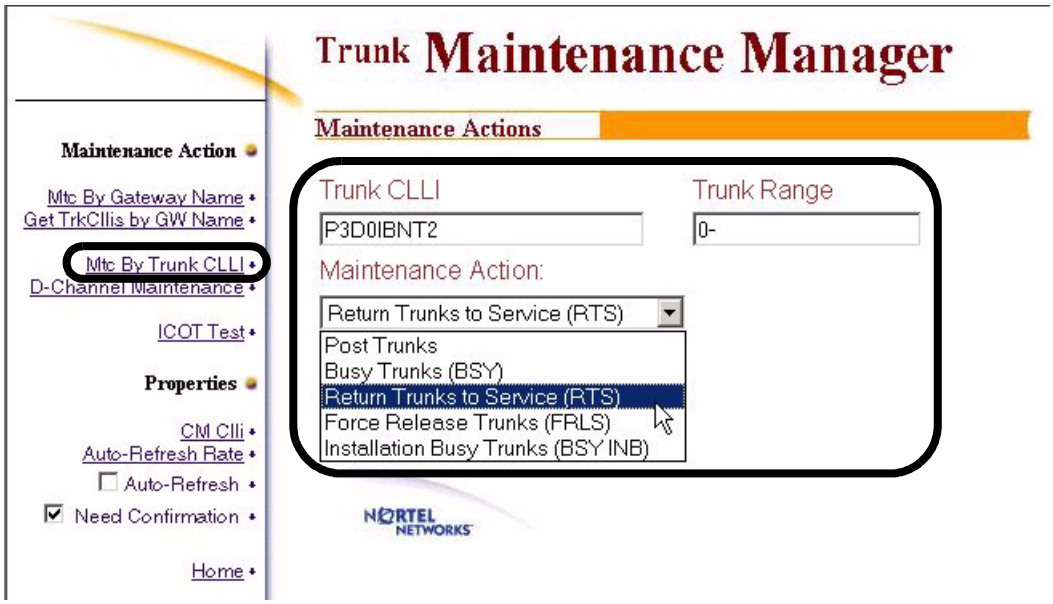
At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the TMM GUI

2 Click **Mtc By Trunk CLLI**.

3 Enter the trunk CLLI name and optionally a Trunk Range value (or use the default [0-] value for all trunk members), then select **Return Trunks to Service (RTS)** from the **Maintenance Action** drop down menu, and click **Go**.



4 Observe that the selected trunk members are in the idle (IDL) state as shown in the following example.

CM CLLI:	Trunk CLLI:	First Member:	Group Size:
RTPS	AL7ITICS7	0	4

Number	State	Connected To	Direction	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Name
0	IDL		IC	S7	GWC_NODE	1	13	627	PVG190	DS3/02/0/27/3
1	IDL		IC	S7	GWC_NODE	1	13	628	PVG190	DS3/02/0/27/4
2	IDL		IC	S7	GWC_NODE	1	13	629	PVG190	DS3/02/0/27/5
3	IDL		IC	S7	GWC_NODE	1	13	630	PVG190	DS3/02/0/27/6

Last Refreshed: Wed Sep 24 13:42:27 EDT 2003

5 You have completed this procedure.

Posting trunk endpoints

Application

Use this procedure to post trunk endpoints by gateway.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

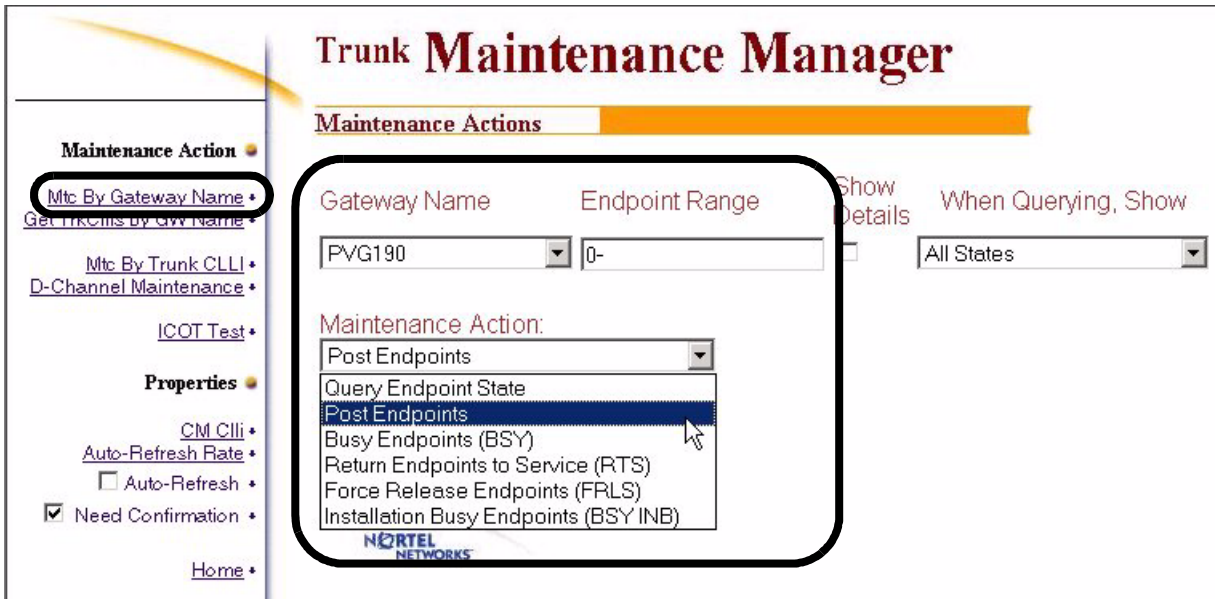
1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the TMM GUI

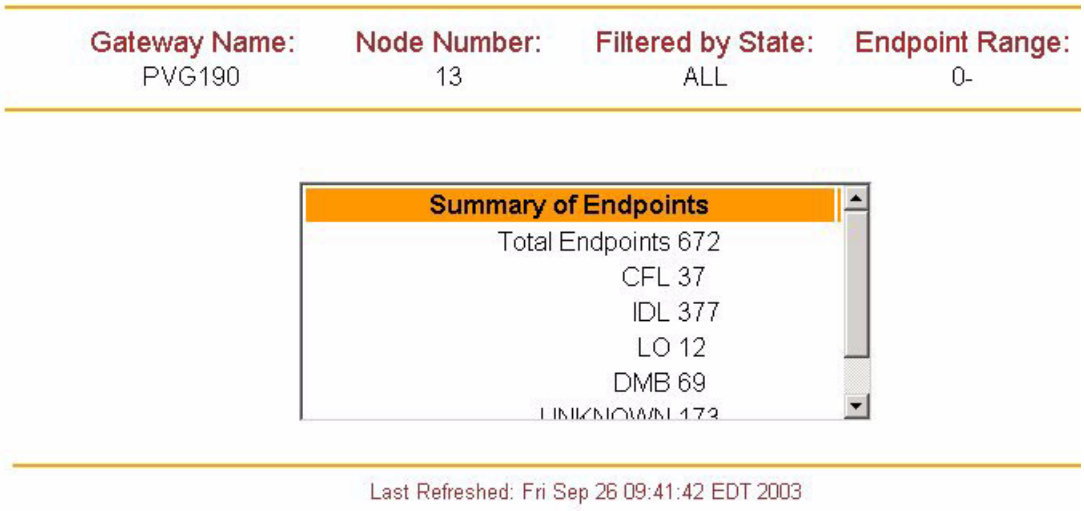
2 Click **Mtc By Gateway Name**.

3 Enter the gateway name and optionally an Endpoint Range value (or use the default [0-] value for all endpoints), then select **Post Endpoints** from the **Maintenance Action** drop down menu, and click **Go**.

Note: Click the Show Details checkbox if you want to display additional details about the endpoints.



4 Observe that the selected range of endpoints are displayed, along with other applicable properties as shown in the following example.



5 You have completed this procedure.

Querying the state of trunk endpoints

Application

Use this procedure to query the state of one or more trunk endpoints.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

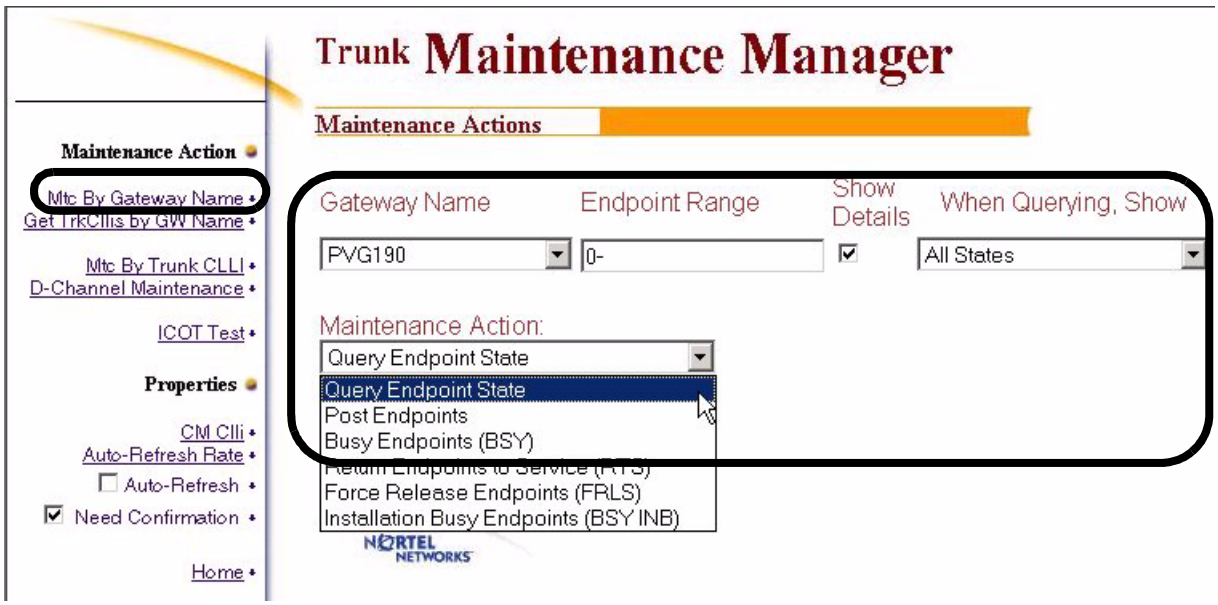
At the TMM GUI

2 Click **Mtc By Gateway Name**.

3 Enter the query criteria as follows:

- **a** From the **Gateway Name** list, select the trunk's gateway name.
- **b** In the **Endpoint Range** box, enter an endpoint range value to query the state of specific endpoints, or use the default value of "0-" to query the state of all endpoints.
- **c** Click the **Show Details** checkbox to display the state of the selected endpoints, otherwise only a summary of endpoint states will be displayed.
- **d** From the **When Querying, Show** list, select a state, or use the default value of "All States" to query all endpoints in the selected gateway.

4 From the **Maintenance Action** list, select **Query Endpoint State**, and click **Go**.



5 Observe that a summary of selected endpoints and details, if checked, are displayed as shown in the following example.

Gateway Name:	Node Number:	Filtered by State:	Endpoint Range:
PVG190	13	ALL	0-

Summary of Endpoints
Total Endpoints 672
STB 1
INB 8
CPB 6
DMB 69

Endpoint Number	State
1	IDL
2	IDL
3	IDL

6 You have completed this procedure.

Busying trunk endpoints

Application

Use this procedure to busy trunk endpoints so maintenance on the trunk member can be performed.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

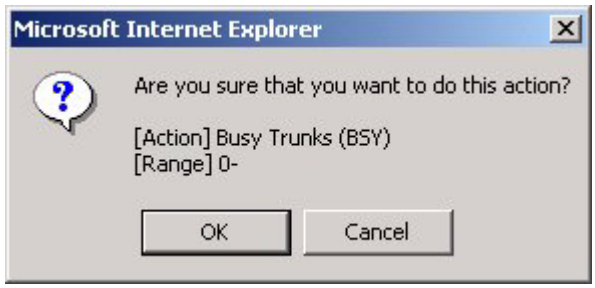
1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the TMM GUI

2 Click **Mtc By Gateway Name**.

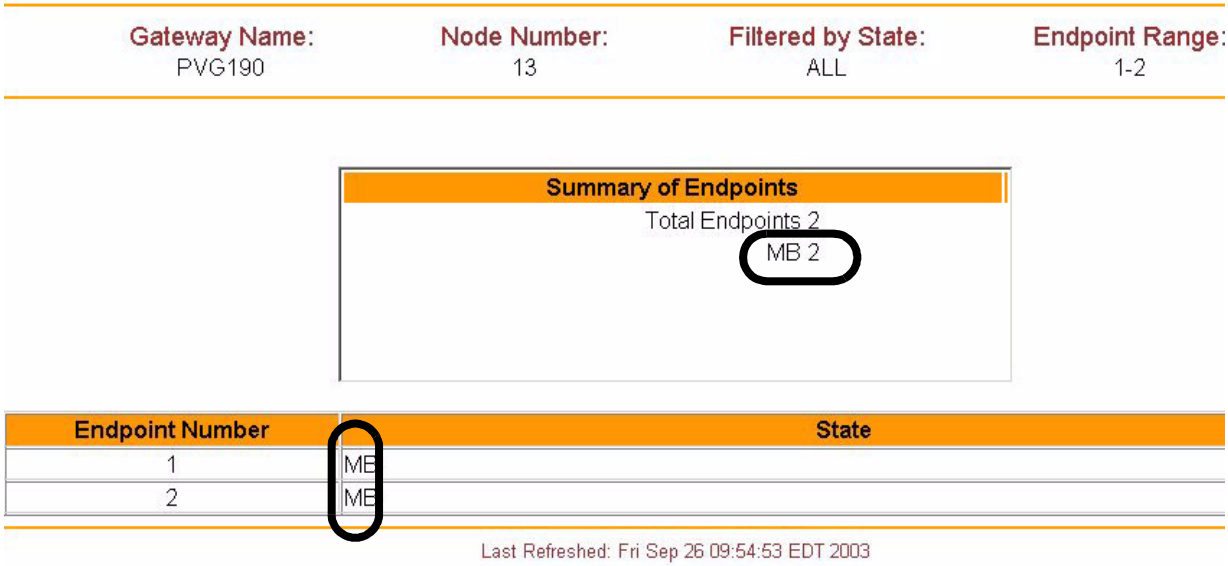
3 Enter the gateway name and optionally an Endpoint Range value (or use the default [0-] value for all endpoints), then select **Busy Endpoints (BSY)** from the **Maintenance Action** drop down menu, and click **Go**.

If you attempted to busy more than one trunk endpoint and the "Need Confirmation" check box is checked, you need to confirm the busy action as shown in the following figure.



4 If it is acceptable to busy more than one trunk endpoint, click **OK**.

5 Observe that the selected trunk endpoints are maintenance busied (MB) as indicated in the following figure.



6 You have completed this procedure.

Returning trunk endpoints to service

Application

Use this procedure to return trunk endpoints to service (RTS).

Prerequisites

The trunk member must be in a maintenance busied (MB) state.

Action

Perform the following steps to complete this procedure.

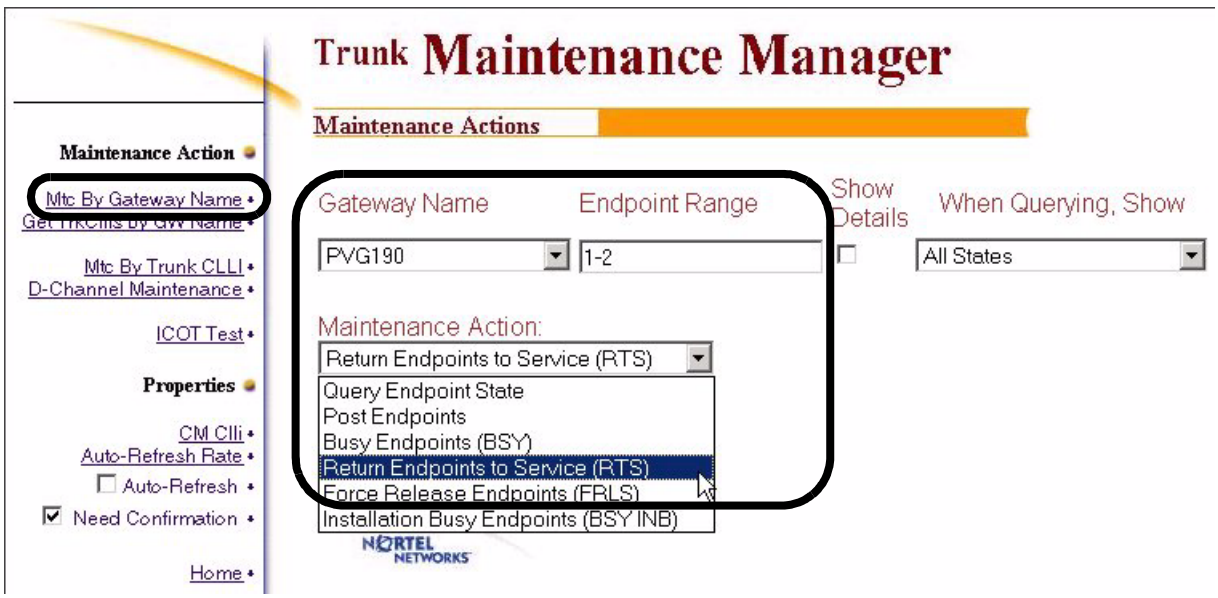
At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

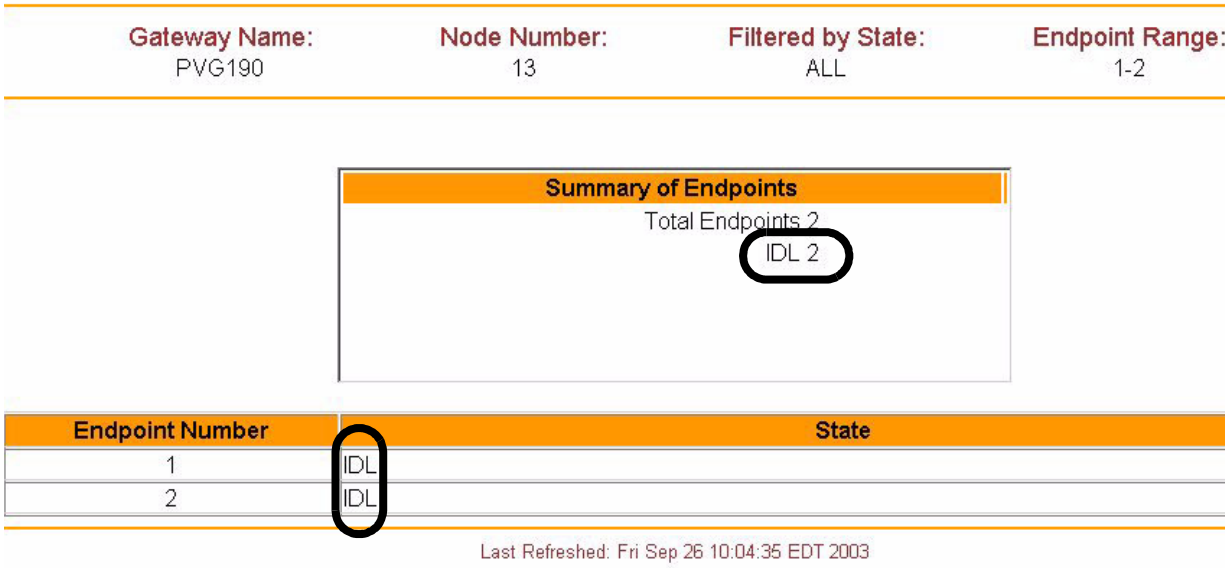
At the TMM GUI

2 Click **Mtc By Gateway Name**.

3 Enter the gateway name and optionally an Endpoint Range value (or use the default [0-] value for all endpoints), then select **Return Endpoints to Service (RTS)** from the **Maintenance Action** drop down menu, and click **Go**.



4 Observe that the selected trunk endpoints are returned to service and in an idle (IDL) state, or other proper state such as CPD, as shown in the following example.



Gateway Name:	Node Number:	Filtered by State:	Endpoint Range:
PVG190	13	ALL	1-2

Summary of Endpoints

Total Endpoints 2

IDL 2

Endpoint Number	State
1	IDL
2	IDL

Last Refreshed: Fri Sep 26 10:04:35 EDT 2003

5 You have completed this procedure.

Installation busying trunk endpoints

Application

Use this procedure to installation busy (BSY INB) trunk endpoints.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

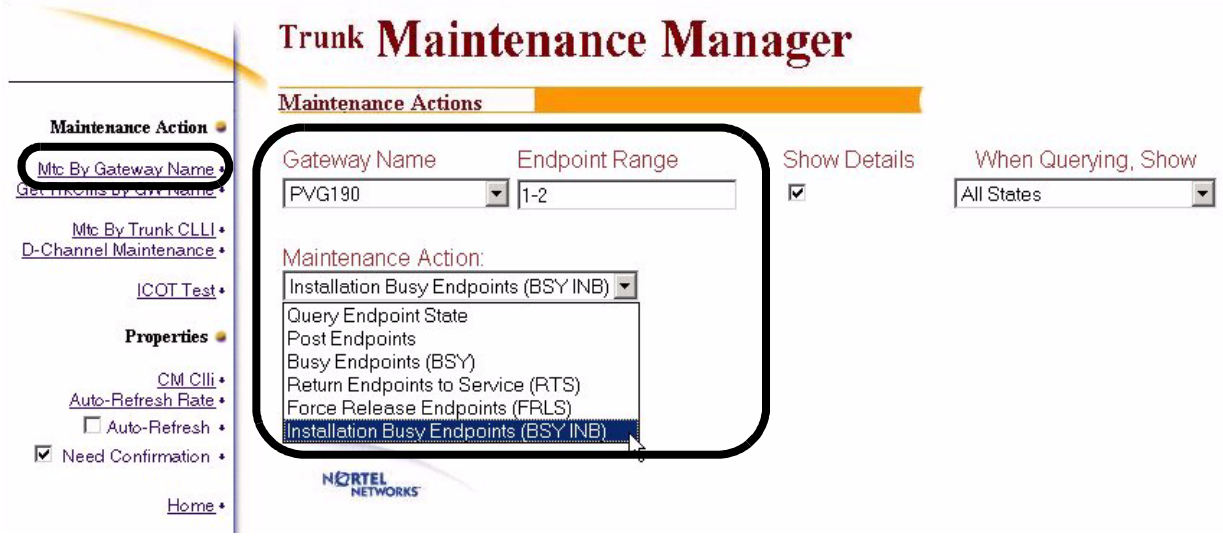
At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

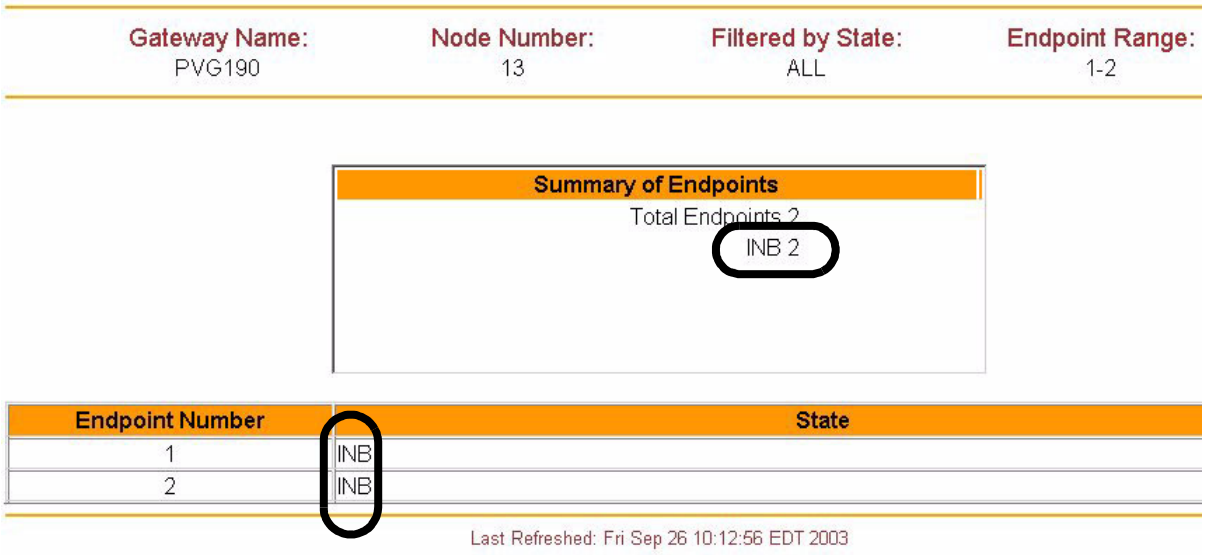
At the TMM GUI

2 Click **Mtc By Gateway Name**.

3 Enter the gateway name and optionally an Endpoint Range value (or use the default [0-] value for all endpoints), then select **Installation Busy Endpoints (BSY INB)** from the **Maintenance Action** drop down menu, and click **Go**.



4 Observe that the selected trunk endpoints are in an installation busy (INB) state as shown in the following example.



Gateway Name:	Node Number:	Filtered by State:	Endpoint Range:
PVG190	13	ALL	1-2

Summary of Endpoints

Total Endpoints 2

INB 2

Endpoint Number	State
1	INB
2	INB

Last Refreshed: Fri Sep 26 10:12:56 EDT 2003

5 You have completed this procedure.

Force releasing trunk endpoints

Application

Use this procedure to force release trunk endpoints and place them in a maintenance busy (MB) state.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the TMM GUI

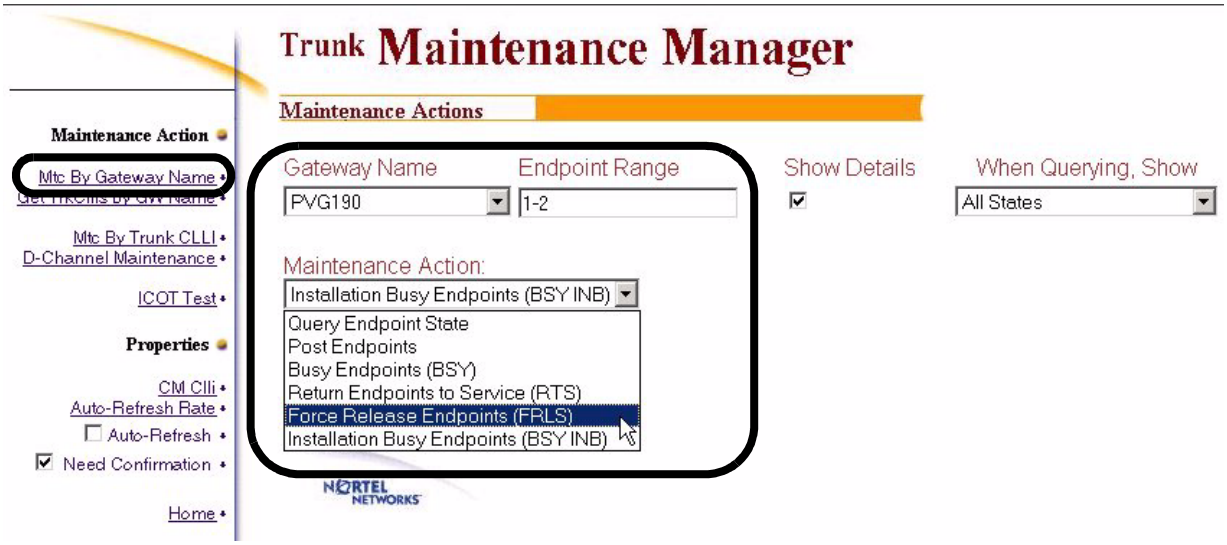
2 Click **Mtc By Gateway Name**.

3

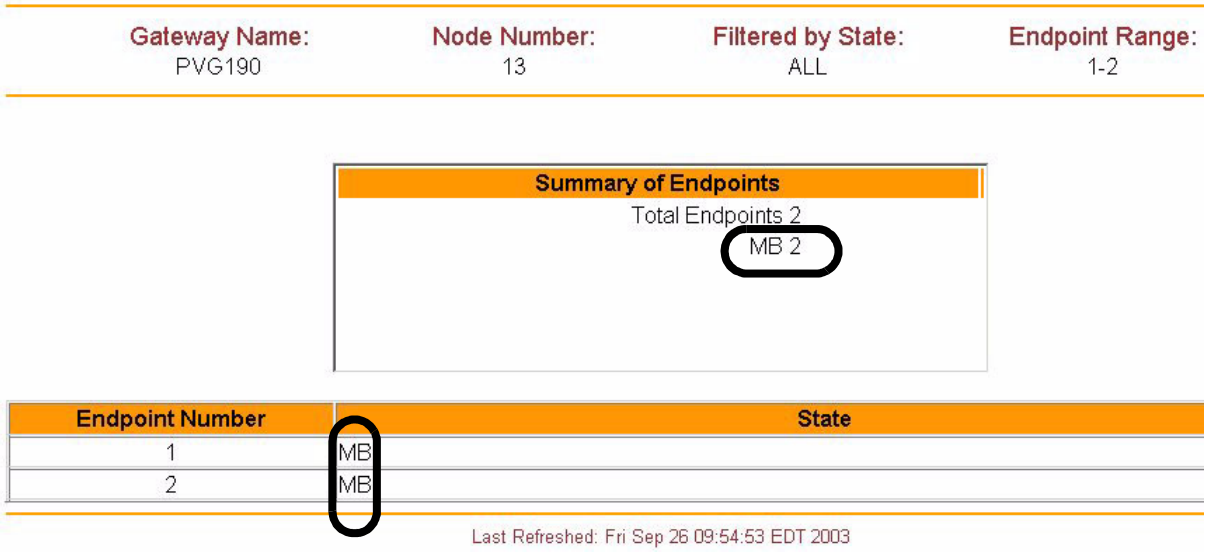
CAUTION
Call loss
If you force release trunk endpoints connected in a call process, the endpoints will transition to manual busy (MB) and the calls in progress will be dropped.

Enter the gateway name and an endpoint range value (endpoints must be separated by commas; for instance, 1,3,5,10), then select **Force Release Endpoints (FRLS)** from the **Maintenance Action** drop down menu, and click **Go**.

Note: Click the Show Details checkbox if you want to display additional details about the endpoints.



4 Observe that the selected trunk endpoints are in a maintenance busy (MB) state as shown in the example below.



5 You have completed this procedure.

Posting PRI Group D-channels

Application

Use this procedure to display statistics about the D-channels for a selected PRI trunk and perform maintenance operations.

This procedure can only be performed on Succession PRI trunks.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

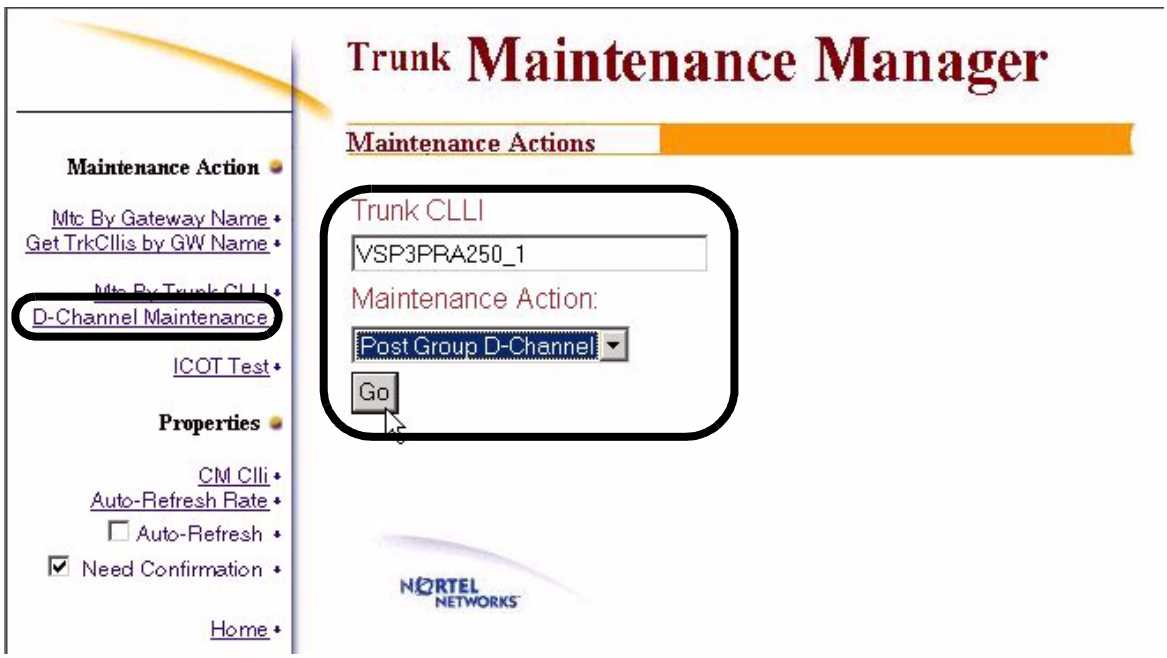
At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

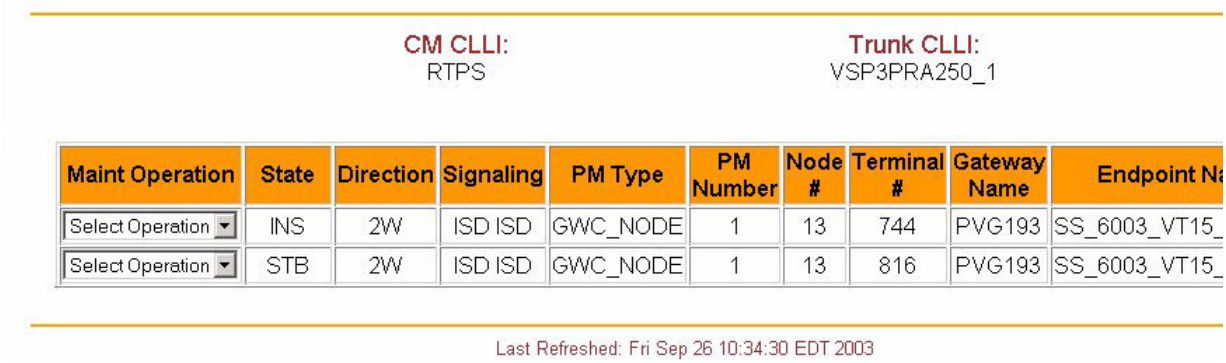
At the TMM GUI

2 Click **D-Channel Maintenance**.

3 Enter the trunk CLLI name, then select **Post Group D-Channel** from the **Maintenance Action** drop down menu, and click **Go**.



4 Observe that the selected range of PRI trunk D-channel is displayed as shown in the following example.



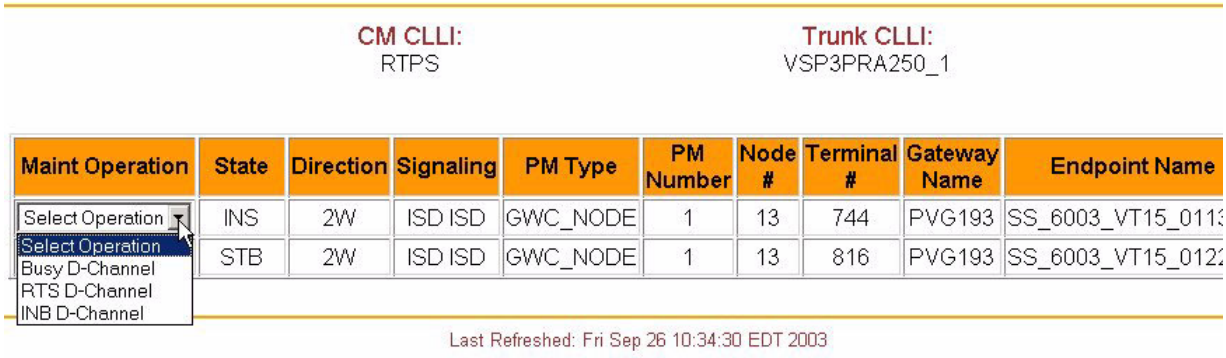
CM CLLI: RTPS

Trunk CLLI: VSP3PRA250_1

Maint Operation	State	Direction	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Na
Select Operation	INS	2W	ISD ISD	GWC_NODE	1	13	744	PVG193	SS_6003_VT15_
Select Operation	STB	2W	ISD ISD	GWC_NODE	1	13	816	PVG193	SS_6003_VT15_

Last Refreshed: Fri Sep 26 10:34:30 EDT 2003

5 Select the desired maintenance operation as shown in the following example.



CM CLLI: RTPS

Trunk CLLI: VSP3PRA250_1

Maint Operation	State	Direction	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Name
Select Operation	INS	2W	ISD ISD	GWC_NODE	1	13	744	PVG193	SS_6003_VT15_011
Select Operation	STB	2W	ISD ISD	GWC_NODE	1	13	816	PVG193	SS_6003_VT15_012

Select Operation
Busy D-Channel
RTS D-Channel
INB D-Channel

Last Refreshed: Fri Sep 26 10:34:30 EDT 2003

6 You have completed this procedure.

Displaying trunk CLLI codes by gateway

Action

Use this procedure to retrieve a list of trunk CLLI codes associated with a specific trunk gateway.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

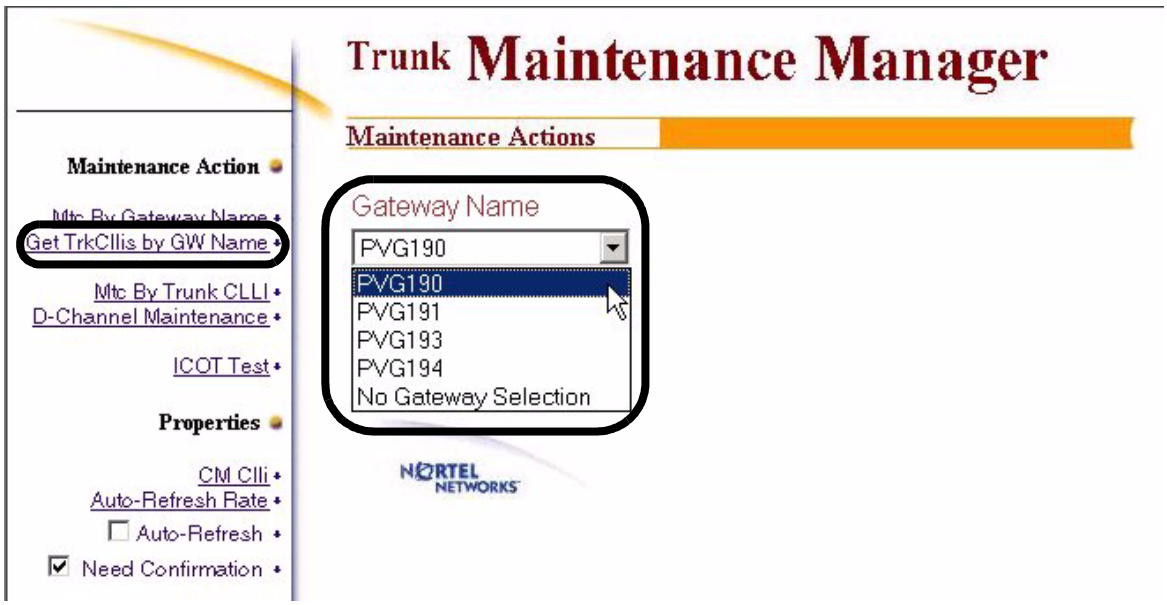
At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

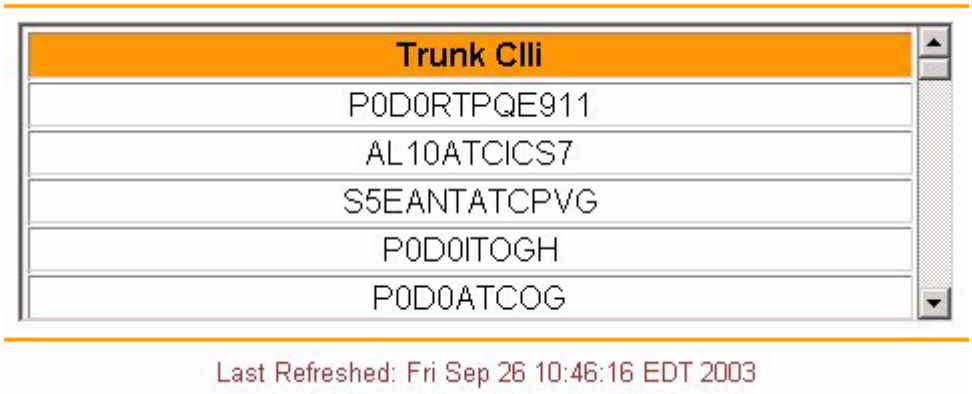
At the TMM GUI

2 Click **Get TrkCllis by GW Name**.

3 From the **Gateway Name** list, select a gateway, then click **Go**.



The trunk CLLI codes associated with the trunk gateway are displayed as shown in the following example.



Trunk Clli
P0D0RTPQE911
AL10ATCICS7
S5EANTATCPVG
P0D0ITOGH
P0D0ATCOG

Last Refreshed: Fri Sep 26 10:46:16 EDT 2003

4 You have completed this procedure.

Performing an ISUP Continuity Test

Application

Use this procedure to perform an ISUP (Integrated Services Digital Network User Part) continuity test (ICOT) on a trunk or group of trunks for a specific CLLI.

This test can only be performed on outgoing or 2-way ISUP trunks.

Prerequisites

The trunks must be in a maintenance busy (MB) state. Refer to procedure Busying a trunk member in this document, if required.

Action

Perform the following steps to complete this procedure.

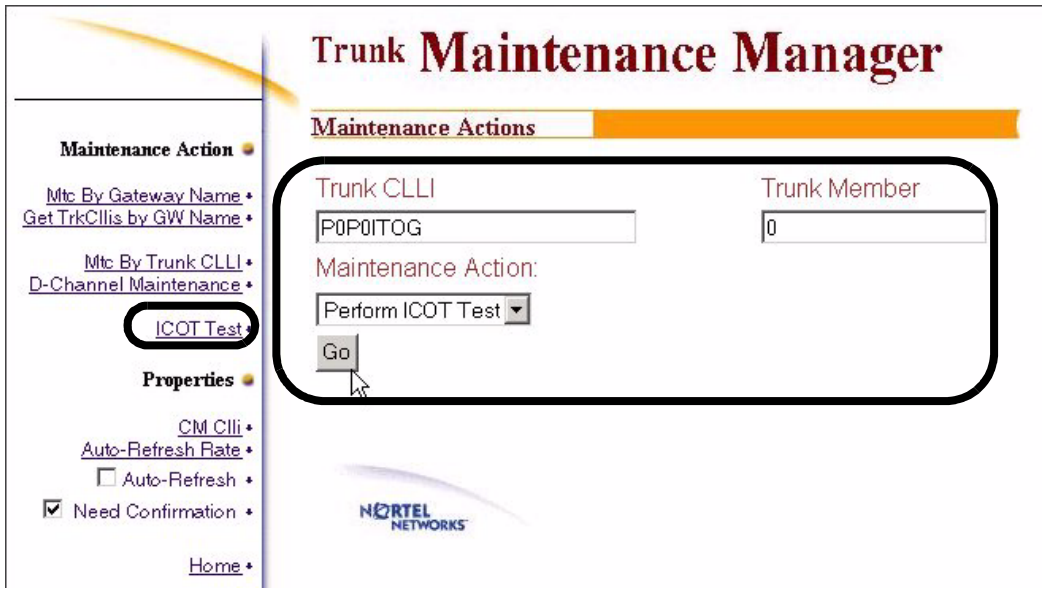
At your workstation

1 Launch the Trunk Maintenance Manager (TMM) GUI. Refer to procedure Launching CS 2000 Management Tools client applications in this document if required.

At the TMM GUI

2 Click **ICOT Test**.

3 Enter the trunk CLLI name and optionally a Trunk Member value (or use the default [0] value), then select **Perform ICOT Test** from the **Maintenance Action** drop down menu, and click **Go**.



4 Observe that the test results and continuity conditions for the trunk number are displayed as shown in the example below.

If you encounter any unexpected errors such as “test failed”, review any details and determine a solution, or contact your next level of support.

CM CLLI: RTPS

Trunk CLLI: P0P0ITOG

Number	Test Result	Continuity Condition	Additional Info
1	TEST_PASSED		

5 You have completed this procedure.

Routing customer logs to a remote host

Application

Use this procedure to route customer logs to a remote host such as the CS 2000 Core Manager (SDM).

Prerequisites

You must have the IP address of the remote host.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address
is the IP address of the Sun server where the CS 2000 Management Tools reside

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

7 Select the “Syslog Configuration” option by typing

```
select - 8
```

and pressing the Enter key.

Response

```
Syslog Configuration
 1 - list_syslog (List a system’s syslog
     configuration)
 2 - add_syslog (Add a syslog configuration
     entry)
 3 - del_syslog (Remove a syslog configuration
     entry)
 4 - route_syslog_on (Route syslog to the SDM)
 5 - route_syslog_off (Turn off syslog
     re-direction to SDM)


 X - exit

select -
```

8 Select the route_syslog_on option by typing

```
select - 4
```

and pressing the Enter key.

9 When prompted, enter ”local1.notice” as the facility to be routed.

10 When prompted, enter the IP address of the remote host.

11 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

12 You have completed this procedure.

Configuring log reporting

Application

Use this procedure to configure log reporting, which includes enabling or disabling syslog alarm logging.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address
is the IP address of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Execute the configuration script by typing

```
# configure
```

and pressing the Enter key.

Response

```
SESM configuration
 1 - SESM common configuration (IP addresses,
     Market, CM CLLI)
 2 - SESM database tools
 3 - SESM related applications configuration
     (MG9K, LMM)
 4 - SESM provisioning configuration
 5 - SESM logging configuration (syslog, sesm
     debug log)

 6 - view sesm configuration settings

 X - exit

select -
```

6 Select the “SESM logging configuration (syslog, sesm debug log)” option by typing

```
select - 5
```

and pressing the Enter key.

Response

```
SESM Logging Configuration
 1 - SESM Syslog configuration
 2 - SESM Debug Log configuration
 3 - SESM Alarm Logging configuration
 4 - SESM Alarm GUI configuration


 X - exit

select -
```

7 Configure syslog as follows:

a Select the “SESM Syslog configuration” option by typing

```
select - 1
```

and pressing the Enter key.

b When prompted, enter the maximum file size (in megabytes) of SESM Syslog, or press the Enter key to accept the default value of “3 meg”.

c When prompted, enter the SESM Syslog Backup Hour (for daily file rotation, or press the Enter key to accept the default value of “3” hours.

d When prompted, enter the SESM Syslog Backup Minute, or press the Enter key to accept the default value of “0” minutes.

The system sets the values you selected and returns you to the SESM Logging Configuration menu.

8 Configure debug log as follows:

a Select the “SESM Debug Log configuration” option by typing

```
select - 2
```

and pressing the Enter key.

b When prompted, enter the maximum file size of SESM Debug Log, or press the Enter key to accept the default value of
“20560 KB”.

c When prompted, enter the maximum number of SESM Debug Log files, or press the Enter key to accept the default value of “7”.

d When prompted, enter the MI2 default log level, or press the Enter key to accept the default value of “MNR”.

e When prompted, enter the Proxy Agent default log level, or press the Enter key to accept the default value of “CRT”.

f When prompted, enter the SESM log file name, or press the Enter key to accept the default value of “ptmdebuglog”.

g When prompted, enter the log file rotation method, or press the Enter key to accept the default value of “Size based”.

The system sets the values you selected and returns you to the SESM Logging Configuration menu.

9 Enable or disable syslog alarm logging as follows:

a Select the “SESM Alarm Logging configuration” option by typing

```
select - 3
```

and pressing the Enter key.

b When prompted, enter Y if you want enable syslog alarm logging, or N if you want to disable syslog alarm logging.

The system returns you to the SESM Logging Configuration menu.

10 Exit SESM Logging Configuration by typing

`select - x`

and pressing the Enter key.

11 Exit SESM configuration by typing

`select - x`

and pressing the Enter key.

12 You have completed this procedure.

Viewing debug logs

Application

Use this procedure to view debug logs.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address
is the IP address of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Display the debug logs by typing

```
# ptmctl display <log_type>
```

and pressing the Enter key.

where

log_type
is MI2, PA, or MISC

6 You have completed this procedure.

Viewing OMPUSH logs

Application

Use this procedure to view OMPUSH logs.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address
is the IP address of the Sun server where OMPUSH resides

2 When prompted, enter your user ID and password.

3 Use the following table to determine your next step.

If you want to	Do
monitor the OMPUSH syslog stream	step a
view the OMPUSH history log file	step b
save the OMPUSH history log file to a file	step c

a Monitor the OMPUSH syslog stream by typing

```
# tail -f /var/adm/messages |grep -i ompush
```

and pressing the Enter key.

b Display the OMPUSH history log file by typing

```
# cat /var/adm/messages |grep -i ompush
```

and pressing the Enter key.

c Save the OMPUSH history log file to a file by typing

```
# cat /var/adm/messages |grep -i ompush >
<filename>
```

and pressing the Enter key.

Where

filename
is the name you want to give to the OMPUSH history log file you are saving

4 You have completed this procedure.

SPFS310

Log report SPFS310 indicates one of the following events:

- loss of network connectivity
- fan failure on a t1400 or Netra 240 server
- disk failure
- high temperature
- power supply unit failure
- cluster node failover
- cluster node out of sync

Note: Log report SPFS310 also indicates when any of the above events is cleared.

Format

The format for log report SPFS310 when a loss of network connectivity has occured is as follows:

```
**SPFS310 JUL17 22:20:05 0805 TBL SPFS Fault
 Location: SSPFS - <host>
 Time: Thu Jul 17 22:20:05 EDT 2003
 State: Raised
 Category: Equipment
 Cause: Network Interface down
 ProbableCause: communicationSubsystemFailure
 Component ID: NIC=hme0
 Description: SUNW, hme0 : No response from Ethernet network: Link down --
 cable problem?
 Recovery Action: Check Ethernet cable
```

The format for log report SPFS310 when network connectivity has been restored is as follows

```
SPFS310 JUL17 22:20:05 0807 INFO SPFS Fault Cleared
Location: SSPFS - <host>
Time: Thu Jul 17 22:20:05 EDT 2003
State: Cleared
Category: Equipment
Component ID: NIC=hme0
Description: SUNW, hme0 : 100 Mbps Full-Duplex Link Up
```

The format for log report SPFS310 when a fan failure on a t1400 server has occurred is as follows:

```
**SPFS310 JUL17 22:20:05 0805 TBL SPFS Fault
 Location: SSPFS - <host>
 Time: Thu Jul 17 22:20:05 EDT 2003
 State: Raised
 Category: Equipment
 Cause: Fan failure
 ProbableCause: outOfService
 Component ID: FAN=Fan 1
 Description: Fan 1 Failed
 Recovery Action: Contact Support.
```

The format for log report SPFS310 when a fan failure has cleared is as follows:

```
SPFS310 JUL17 22:20:05 0807 INFO SPFS Fault Cleared
Location: SSPFS - <host>
Time: Thu Jul 17 22:20:05 EDT 2003
State: Cleared
Category: Equipment
Component ID: FAN=Fan 1
Description: Fan 1 Restored
```

The format for log report SPFS310 when a fan failure on a Netra 240 server has occurred is as follows:

```
**SPFS310 JUL17 22:20:05 0805 TBL SPFS Fault
 Location: SSPFS - <host>
 Time: Thu Jul 17 22:20:05 EDT 2003
 State: Raised
 Category: Equipment
 Cause: Fan failure
 ProbableCause: outOfService
 Component ID: FAN=Fan 1
 Description: CPU_FAN @ MB.P0.F0.RS has FAILED
 Recovery Action: Contact Support. Clear alarm light manually.
```

The format for log report SPFS310 when a disk failure has occurred is as follows:

```
**SPFS310 JUL17 22:20:05 0805 TBL SPFS Fault
 Location: SSPFS - <host>
 Time: Thu Jul 17 22:20:05 EDT 2003
 State: Raised
 Category: Hardware
 Cause: Disk Failed
 Component ID: Disk
 Description: A disk is under maintenance on the machine
 Recovery Action: Check Disk
```

The format for log report SPFS310 when a disk failure has been cleared is as follows:

```
SPFS310 JUL17 22:20:05 0807 INFO SPFS Fault Cleared
Location: SSPFS - <host>
Time: Thu Jul 17 22:20:05 EDT 2003
State: Cleared
Category: Hardware
Component ID: Disk
Description: No disk problems reported at this time
```

The format for log report SPFS310 when the temperature of the system has exceeded its threshold is as follows:

```
**SPFS310 JUL17 22:20:05 0805 TBL SPFS Fault
 Location: SSPFS - <host>
 Time: Thu Jul 17 22:20:05 EDT 2003
 State: Raised
 Category: Hardware
 Cause: Temperature threshold exceeded
 ProbableCause: thresholdCrossed
 Component ID: Temperature
 Description: A temperature threshold was exceeded
 Recovery Action: Reduce temperature of environment
```

The format for log report SPFS310 when the high temperature has been cleared is as follows:

```
SPFS310 JUL17 22:20:05 0807 INFO SPFS Fault Cleared
Location: SSPFS - <host>
Time: Thu Jul 17 22:20:05 EDT 2003
State: Cleared
Category: Hardware
Component ID: Temperature
Description: No temperature problems reported at this time
```

The format for log report SPFS310 when a power supply unit failure has occured is as follows:

```
**SPFS310 JUL17 22:20:05 0093 TBL SPFS Fault
 Location: SSPFS - <host>
 Time: Thu Jul 17 22:20:05 EDT 2003
 State: Raised
 Category: Hardware
 Cause: PSU Input unavailable
 ProbableCause: powerProblem
 Component ID: PSU0
 Description: LOMlite PSU 0 Input failed
 Recovery Action: Contact support
```

The format for log report SPFS310 when a power supply unit failure has been cleared is as follows:

```
SPFS310 JUL17 22:20:05 0812 INFO SPFS Fault Cleared
Location: SSPFS - <host>
Time: Thu Jul 17 22:20:05 EDT 2003
State: Cleared
Category: Hardware
Component ID: PSU0
Description: LOMlite PSU 0 Input A restored
```

The format for log report SPFS310 when a cluster node failover has occurred is as follows:

```
**SPFS310 JUL17 22:20:05 0093 TBL SPFS Fault
 Location: SSPFS - <host>
 Time: Thu Jul 17 22:20:05 EDT 2003
 State: Raised
 Category: Equipment
 Cause: Cluster Node failed over
 ProbableCause: outOfService
 Component ID: NodeFailOver
 Description: SSPFSHA Cluster failover took place
 Recovery Action:
```

The format for log report SPFS310 when a cluster node is out of sync is as follows:

```
**SPFS310 JUL17 22:20:05 0093 TBL SPFS Fault
 Location: SSPFS - <host>
 Time: Thu Jul 17 22:20:05 EDT 2003
 State: Raised
 Category: Equipment
 Cause: Cluster nodes out of Sync
 ProbableCause: outOfService
 Component ID: Cluster=Cluster_Component
 Description: MSH: Cluster nodes out of Sync
 Recovery Action: Contact support
```

The format for log report SPFS310 when a cluster node out of sync has been cleared is as follows:

```
SPFS310 JUL17 22:20:05 0812 INFO SPFS Fault Cleared
Location: SSPFS - <host>
Time: Thu Jul 17 22:20:05 EDT 2003
State: Cleared
Category: Equipment
Component ID: Cluster=Cluster_Component
Description: /usr/bin/startb:Cluster nodes in sync
```

Selected field descriptions

This log report has no selected fields.

Action

The following table lists probable causes and suggested actions:

Probable cause	Required action
Loss of network connectivity.	Check the Ethernet cable. Contact support if necessary.
Fan failure.	Check the fan. If required, replace the fan using the document that came with your server. Contact support if necessary.
Disk failure.	Check the disk. If required, replace the disk using procedure “Replacing a failed disk drive in-service” in the Fault Management document.

Probable cause	Required action
Temperature threshold exceeded.	Reduce the temperature of the environment.
Power supply unit failure	Check the power supply unit. If required, replace it using the document that came with your server. Contact support if necessary.
Cluster node failover	None.
Cluster node out of sync	Contact support.
No active cluster node	Contact support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SPFS320

Log report SPFS320 indicates when an automated data backup has failed, and when an automated data backup failure has cleared.

Format

The format for log report SPFS320 shows when an automated data backup has failed:

```
SPFS320 JUL17 22:20:05 0000 MINOR TBL SPFS Fault
Location: SSPFS - <host>
Time: Thu Jul 17 22:20:05 EDT 2003
State: Raised
Category: Data Backup
Cause: Drive/Media error
ProbableCause: Drive not ready or invalid media
Component ID: SSPFS_BKUP
Description: Data Backup Failure
```

The format for log report SPFS 320 shows when an automated data backup failure has cleared:

```
SPFS320 JUL17 22:20:05 0000 NONE INF SPFS Fault
Location: SSPFS - <host>
Time: Thu Jul 17 22:20:05 EDT 2003
State: Cleared
Category: Data Backup
Component ID: SSPFS_BKUP
Description: Backup Completes Successfully
```

Selected field descriptions

This log report has no selected fields.

Action

When the log indicates that the data backup failed, ensure the correct media is in the drive.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SPFS330

Log report SPFS330 indicates when there is no active cluster node.

Format

The format for log report SPFS330 when there is no active cluster node is as follows:

```
**SPFS320 JUL17 22:20:05 0093 TBL SPFSHA Warning: No active cluster node.
User intervention required!
```

Selected field descriptions

This log report has no selected fields.

Action

Contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SPFS350

Log report SPFS350 is generated when the threshold of a file system has been exceeded.

Format

The format for log report SPFS350 is as follows:

```
SPFS310 JUL17 22:20:05 0805 TBL SPFS Fault
Location: SSPFS - <host>
Time: Thu Jul 17 22:20:05 EDT 2003
State: Raised
Category: Equipment
Cause: Filesystem is filling up
ProbableCause: thresholdCrossed
Component ID: FILESYSTEM=/data
Description: Current filesystem usage = 100%
Recovery Action: Remove files from filesystem
```

Selected field descriptions

This log report has no selected fields.

Action

Remove any unneeded files or files generated in error that could be taking up disk space. If required, increase the size of the file system using procedure “Increasing the size of a file system” in the Configuration Management document.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM360

Log report NPM360 indicates an alarm has been raised.

Format

The format for log report NPM360 is as follows:

```
*** NPM360 JAN25 17:37:2 0100 INFO Alarm Raise

Alarm <alarm name> has been raised.

Alarm Description: <alarm description>
```

Selected field descriptions

This log report has no selected fields.

Action

Consult the alarm definition to see a list of conditions that satisfy the alarmable condition.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM370

Log report NPM370 indicates when an alarm has been cleared.

Format

The format for log report NPM370 is as follows:

```
NPM370 JAN25 18:34:44 0300 INFO Alarm Cleared

Alarm <alarm name> has been cleared.

Alarm Description: <alarm description>
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM400

Log report NPM400 indicates the results of an attempted apply, remove, and audit command.

Format

The format for log report NPM400 is as follows:

```
NPM400 APR29 16:57:24 0400 SUMM Action Summary

Patch ID, Device ID, Command, Pass/Fail, Time Complete

-------------------------------------------------

NONE, gwc9-Unit-0-47.142.108.62, AUDIT, Pass, 4:57:24 PM

NONE, gwc9-Unit-1-47.142.108.63, AUDIT, Fail, 4:57:24 PM
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM600

Log report NPM600 indicates when the NPM server has been started, either through a reboot or manual restart.

Format

The format for log report NPM600 is as follows:

```
NPM600 Jan 4, 2001 10:34:28 AM INFO General Information

The NPM Server has been started.
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM601

Log report NPM601 relates to patch files.

Format

The format for log report NPM601 is as follows:

```
NPM601 OCT23 13:51:16 78900 TBL File Failure

There was an i/o exception using patchfile

File: ftp://47.142.84.207/data/npm/Au/heu00u62.ptchmg9p
```

Selected field descriptions

This log report has no selected fields.

Action

The following table lists probable causes and suggested actions..

Probable cause	Required action
The contents of the patchfile were incorrect.	Contact the source of the patch for further investigation.
The specified patchfile was not readable.	Verify that the patchfile is in the specified location. Make sure the directories leading to the file are readable and executable by the NPM server. Also verify that the patch file is readable by the NPM server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM603

Log report NPM603 indicates problems between the database and the device during a device audit.

Format

The format for log report NPM603 is as follows:

```
NPM603 Jan 4, 2001 10:34:28 AM TBL Device Audit Failure

The audit of the following device was not successful

device: <device ID>
```

Selected field descriptions

This log report has no selected fields.

Action

Verify the device and OAM system are running normally

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM605

Log report NPM605 indicates a patch application or removal failed.

Format

The format for log report NPM605 is as follows:

```
NPM605 OCT23 3:13:39 5700 TBL General Trouble

Apply failed

Patch: <PATCH>

Device: <DEVICE>

DeviceMessage: <error message from device>
```

Selected field descriptions

This log report has no selected fields.

Action

Contact the source of the patch for further investigation.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM610

Log report NPM610 provides information related to the execution of a task.

Format

The format for log report NPM610 is as follows:

```
NPM610 NOV11 11:43:16 4900 INFO Task Information

Command: APPLY Task Name: MYTASK1 TaskId: 26

Requestor's Name: npm Execution: Non-Interactive

Execution of the Apply Task has been terminated because no operations have
passed the pre-apply step.
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM620

Log report NPM620 provides information about restarts initiated and completed through the NPM GUI or CLUI.

Format

The format for log report NPM620 is as follows:

```
NPM620 SEP6 21:3:34 5100 INFO NPM Initiated Restart

A restart has been initiated by the NPM on device: PSE_snc0s0jy


* NPM620 SEP6 21:3:34 5100 INFO NPM Initiated Restart

A restart initiated by the NPM on device PSE_snc0s0jy has completed
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM660

Log report NPM660 indicates problems when a plan fails to execute.

Format

The format for log report is as follows:

```
NPM660 OCT23 0:43:43 97100 TBL Automated Process Failure

Plan SYSTEMPLAN executed but had failures.
```

Selected field descriptions

This log report has no selected fields.

Action

Look for related logs on the target devices.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NPM680

Log report NPM680 is generated when a plan is automatically executed.

Format

The format for log report NPM680 is as follows:

```
NPM680 OCT23 15:22:39 44700 INFO Automated Process Information

Plan AUDPSEPLAN was executed successfully.
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CMT300

Log report CMT300 indicates a data mismatch between the server where the Succession Element and Sub-network Manager (SESM) software is installed and the Communication Server 2000.

Format

The format for log report CMT300 when a data mismatch has occured is as follows:

```
CMT300 JUL17 22:20:05 0805 TBL CMT Fault
        Location: audit
        Notification ID: 1000
        State: Raise
        Category: Processing Error
        Cause: Corrupt data
        Time: Jul 17 22:20:05 2003
        Component ID: SESM-AuditSystem;Audit=CS2K DAta Inegrity Audit
        Specific Problem: Data mismatches detected
        Description: The SESM audit; CS2K Data Integrity Audit, has 10
        unresolved problems. To view and correct the problems, open the
        audit problem report from the Audit System found under the SESM
        Maintenance menu item.
```

Selected field descriptions

This log report has no selected fields.

Action

View the report generated from the CS2K Data Integrity Audit. Refer to procedure "Performing an audit" in the CS 2000 Management Tools Fault Management document, NN10084-911, if required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CMT301

Log report CMT301 indicates that the CS 2000 GWC Manager cannot download data to a Gateway Controller (GWC) on recovery.

Format

The format for log report CMT301 when the CS 2000 GWC Manager cannot download data to a GWC on recovery is as follows:

```
CMT301 JUL17 22:20:05 0805 TBL CMT Fault
        Location: gwcem
        Notification ID: 681
        State: Raise
        Category: Processing Error
        Cause: Corrupt data
        Time: Jul 17 22:20:05 2003
        Component ID: SESM-=GWCEMalarm; GWCEM=Recovery: GWC=GWC-1 UNIT-1
        Specific Problem: GWC Recovery failed. Check PTM MI2 logs
        Description: Problem detected in GWC Recovery Subsystem
```

Selected field descriptions

This log report has no selected fields.

Action

Check the MI2 logs on the server where the CS 2000 Management Tools reside. Refer to procedure "Viewing debug logs" in the CS 2000 Management Tools Fault Management document, NN10084-911, if required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

OSSGate logs

The OSSGate application generates several logs to provide users with useful information during startup, shutdown, and information processing.

The logs for OSSGate are by default routed to the ptmdebuglog1.mi2 unless the user has specified a different log file name at startup.

Performing a manual failover on a Sun Netra 240 in a two-server configuration

Application

Use this procedure when you want to perform maintenance or software upgrades on the active node of a Cabinetized Operations, Administration, and Maintenance (COAM) server pair.

The failover causes the standby (inactive) node to take over and start providing OAM&P services as the new active node.

ATTENTION
During an automatic or manual failover, the high-availability (HA) cluster takes approximately 5 minutes to failover and bring up the standby node to Active state.

Prerequisites

You must perform this procedure on the active node.

Action

Perform the following steps to complete this procedure.

At the active node console

1 Log in to the active node through the console (port A) using the root user ID and password.

2 Initiate the manual failover by typing

```
# init 6
```

and pressing the Enter key.

3 You have completed this procedure.

Replacing a failed disk drive in-service

Application

Use this procedure to replace a disk drive in-service on the Netra t1400 or the Netra 240 server.

ATTENTION
This procedure replaces a disk drive in-service. Do not take the server down when performing this procedure.

Disk failures will appear as IO errors or SCSI errors from the Solaris kernel. These messages will appear in the system log and on the console terminal. To indicate a disk failure, an alarm light will be illuminated on the front panel, and a major alarm will be received if the office alarm cable is connected. Any failing disk should be replaced. After the disk is replaced, the alarm light will go off within a few minutes.

Systems installed with SSPFS use disk mirroring. With mirrored hot-swap disks, a single failed disk can be replaced without interrupting the applications running on the Netra server. Thus, a disk can be replaced while the system is in-service.

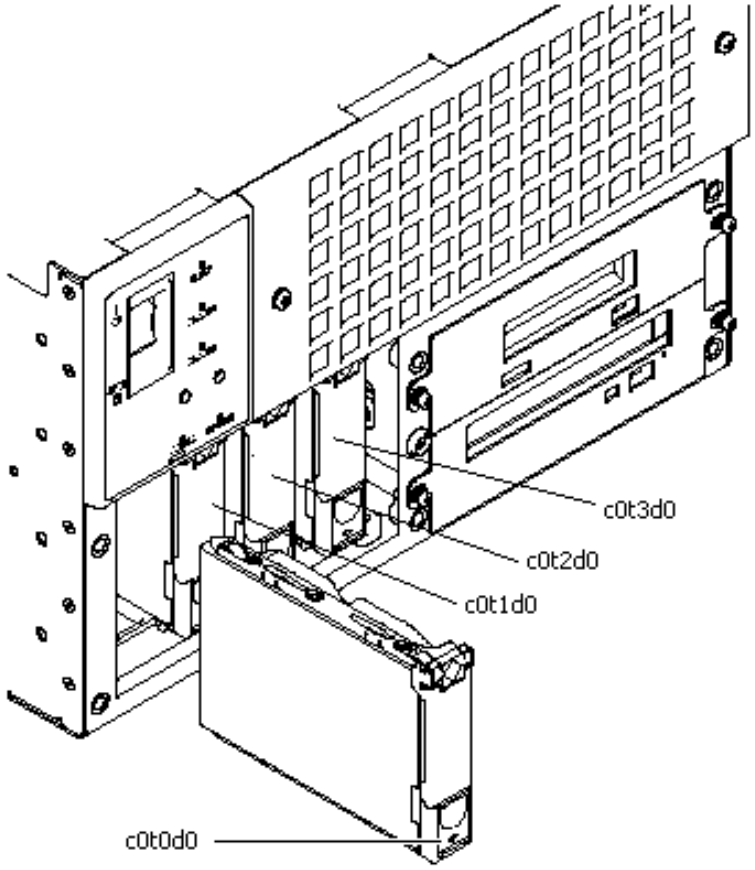
The steps to replace a failed drive are to identify the failed drive, replace it physically, remove it logically, and add the replacement drive into the disk mirror.

Netra t1400

Each Netra t1400 is equipped with four hot-swap drives: “c0t0d0”, “c0t1d0”, “c0t2d0”, and “c0t3d0”. Each physical drive is divided into slices, which are named based on the physical disk and a slice number. For example, “c0t0d0s0” is the first slice of the physical disk “c0t0d0”.

The following figure identifies the hard drives of the Netra t1400.

Netra t1400 hard drives

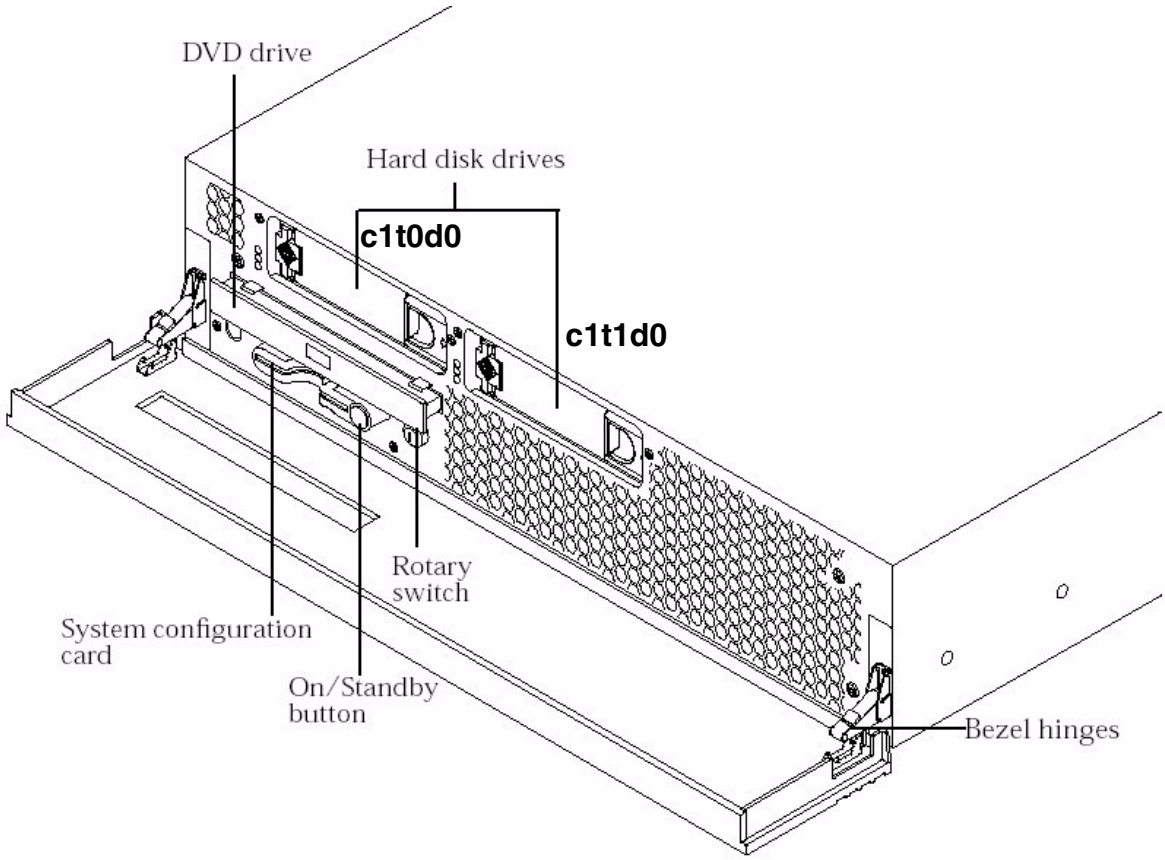


Netra 240

Each Netra 240 is equipped with two hot-swap drives: “c1t0d0”, and “c1t1d0”.

The following figure identifies the hard drives of the Netra 240.

Netra 240 hard drives



Prerequisites

At least one of the hard drives must be functioning.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Netra t1400 or Netra 240 server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Check the health of the system's disks by typing

```
# metastat
```

and pressing the Enter key.

Note: Information about each system disk will be displayed. The normal state is "Okay". The state "Resyncing" means the mirror was broken and is being re-created. The state "Needs Maintenance" or "Maintenance" means that the disk needs to be replaced.

6 Use the following table to determine your next step.

If you are replacing a disk drive on the	Do
Netra t1400	step 7
Netra 240	step 16

7 Determine the disk that needs to be replaced on the Netra t1400 by viewing the results from step 5.

If you are replacing	Do
c0t0d0	step 8
c0t1d0	step 10
c0t2d0	step 12
c0t3d0	step 14

8 Locate disk "c0t0d0" using the Netra t1400 hard drives figure. Use the documentation for the Netra t1400 to physically replace the disk. When complete, return to this procedure, and do step 9.

9 Logically replace disk “c0t0d0” by entering the following sequence of commands:

```
# metadb -d c0t0d0s7
# prtvtoc -h /dev/rdsk/c0t1d0s2 | fmthard -s -
/dev/rdsk/c0t0d0s2
# metadb -a -c 2 c0t0d0s7
# metareplace -e d2 c0t0d0s1
# metareplace -e d5 c0t0d0s0
# metareplace -e d8 c0t0d0s3
# metareplace -e d11 c0t0d0s4
# metareplace -e d100 c0t0d0s5
```

10 Locate disk “c0t1d0” using the Netra t1400 hard drives figure. Use the documentation for the Netra t1400 to physically replace the disk. When complete, return to this procedure, and do step 11.

11 Logically replace disk “c0t1d0” by entering the following sequence of commands.

```
# metadb -d c0t1d0s7
# prtvtoc -h /dev/rdsk/c0t0d0s2 | fmthard -s -
/dev/rdsk/c0t1d0s2
# metadb -a -c 2 c0t1d0s7
# metareplace -e d2 c0t1d0s1
# metareplace -e d5 c0t1d0s0
# metareplace -e d8 c0t1d0s3
# metareplace -e d11 c0t1d0s4
# metareplace -e d100 c0t1d0s5
```

12 Locate disk “c0t2d0” using the Netra t1400 hard drives figure. Use the documentation for the Netra t1400 to physically replace the disk. When complete, return to this procedure, and do step 13.

13 Logically replace disk “c0t2d0” by entering the following sequence of commands.

```
# metadb -d c0t2d0s7
# prtvtoc -h /dev/rdsk/c0t3d0s2 | fmthard -s -
/dev/rdsk/c0t2d0s2
# metadb -a -c 2 cot2d0s7
# metareplace -e d100 c0t2d0s0
```

14 Locate disk “c0t3d0” using the Netra t1400 hard drives figure. Use the documentation for the Netra t1400 to physically replace the disk. When complete, return to this procedure, and do step 15.

15 Logically replace disk “c0t3d0” by entering the following sequence of commands.

```
# metadb -d c0t3d0s7
# prtvtoc -h /dev/rdsk/c0t2d0s2 | fmthard -s -
/dev/rdsk/c0t3d0s2
# metadb -a -c 2 c0t3d0s7
# metareplace -e d100 c0t3d0s0
```

16 Determine the disk that needs to be replaced on the Netra 240 by viewing the results from step 5.

If you are replacing	Do
c1t0d0	step 17
c1t1d0	step 19

17 Locate disk “c1t0d0” using the Netra 240 hard drives figure. Use the documentation for the Netra 240 to physically replace the disk. When complete, return to this procedure, and do step 18.

18 Logically replace disk “c1t0d0” by entering the following sequence of commands:

```
# metadb -d c1t0d0s7
# prtvtoc -h /dev/rdsk/c1t1d0s2 | fmthard -s -
/dev/rdsk/c1t0d0s2
# metadb -a -c 2 c1t0d0s7
# metareplace -e d2 c1t0d0s1
# metareplace -e d5 c1t0d0s0
# metareplace -e d8 c1t0d0s3
# metareplace -e d11 c1t0d0s4
# metareplace -e d100 c1t0d0s5
```

19 Locate disk “c1t1d0” using the Netra 240 hard drives figure. Use the documentation for the Netra 240 to physically replace the disk. When complete, return to this procedure, and do step 20.

20 Logically replace disk “c1t1d0” by entering the following sequence of commands:

```
# metadb -d c1t1d0s7
# prtvtoc -h /dev/rdsk/c1t1d0s2 | fmthard -s -
/dev/rdsk/c1t1d0s2
# metadb -a -c 2 c1t1d0s7
# metareplace -e d2 c1t1d0s1
# metareplace -e d5 c1t1d0s0
# metareplace -e d8 c1t1d0s3
# metareplace -e d11 c1t1d0s4
# metareplace -e d100 c1t1d0s5
```

21 You have completed this procedure.

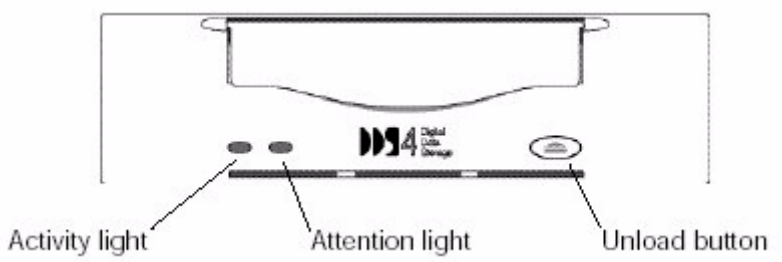
Cleaning the DAT drive on the Netra T1400

Application

Use this procedure to clean the digital audio tape (DAT) drive on the Netra T1400.

The DAT drive has an Activity light and an Attention light on the front panel as shown below.

DAT drive



The Activity light flashes green to show activity (loading, unloading, reading, and writing). It is a steady green when a tape is loaded and the DAT drive is ready to begin operations.

The Attention light flashes amber to indicate that a tape is near the end of its life, or that the DAT drive needs cleaning. It is a steady amber when there is a hardware fault.

When the Attention light flashes amber, clean the DAT drive as described in this procedure.

Schedule

The table below provides the recommended cleaning interval.

Number of tapes used each day	Cleaning interval
1 or less	8 weeks
2	4 weeks
3	3 weeks
4 or more	weekly

To clean the DAT drive, use an appropriate DAT drive cleaning tape. Nortel recommends the Maxell cleaning tape (HS-4/CL or equivalent). Refer to the documentation that accompanies the cleaning tape for additional information about its use, and the life expectancy of the cleaning tape.

Prerequisites

None

Action

Perform the following steps to complete this procedure

At the front of the Netra T1400

1 Obtain a cleaning tape (Maxell HS-4/CL or equivalent).

2 If a tape is already in the DAT drive, press the Unload button on the DAT drive to eject the tape.

3 Insert the cleaning tape into the DAT drive. Cleaning begins automatically. When cleaning is complete, the tape is automatically ejected.

Note: The Attention light should go off. If the Attention light is still flashing amber after cleaning the DAT drive. Repeat the operation with a different cleaning tape.

4 Remove the cleaning tape from the DAT drive.

5 If you removed a tape in step 2, reinsert the tape. If the Attention light flashes amber, the tape is nearing the end of its life. Copy the data onto a new tape and discard the old one.

6 You have completed this procedure.

Restoring SSH communication between the CS 2000 Management Tools server and the CS 2000 Core Manager

Application

Use this procedure to re-establish SSH communication between the CS 2000 Management Tools server and the CS 2000 Core Manager if either one undergoes a fresh install after the CS 2000 SAM21 Manager has been migrated from the CS 2000 Core Manager to the CS 2000 Managemen Tools server.

Prerequisites

None

Action

Perform the steps in one of the following procedures depending on which platform underwent a fresh install:

- Re-establishing SSH communication after a CS 2000 Core Manager fresh install
- Re-establishing SSH communication after an SSPFS fresh install

Re-establishing SSH communication after a CS 2000 Core Manager fresh install

At the SDM

1 Log in to the CS 2000 Core Manager.

2 Access the SWIM level of the maintenance interface by typing

```
# sdmmtc swim
```

and pressing the Enter key.

3 Access the Details level by typing

```
> details
```

and pressing the Enter key.

4 Ensure the following filesets are applied.

- OpenSSH
- Bootp Loading Service

Note: Use the up/down commands to scroll through the list of applications if required.

At the CS 2000 Management Tools server (SSPFS)

5 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

6 When prompted, enter your user ID and password.

7 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

8 When prompted, enter the root password.

9 Change to the CS 2000 SAM21 Manager user by typing

```
# su - sam21em
```

and pressing the Enter key.

10 Remove the existing entry for the SDM in file "/export/home/sam21em/.ssh/known_hosts".

11 Secure-append the public key to the authorized key's list that resides on the SDM (CS 2000 Core Manager) by typing

```
$ cat .ssh/id_rsa.pub | ssh root@$SDM_IP 'cat >>
/home/swld/.ssh/authorized_keys2'
```

and pressing the Enter key.

Example response:

```
The authenticity of host '47.142.128.16
(47.142.128.16)' can't be established. RSA key
fingerprint is
21:cb:c6:7f:df:05:f8:4a:2f:23:e9:09:c8:37
bc:1e sam21em@znc0s0j6
Are you sure you want to continue connecting
(yes/no)?
```

12 When prompted, confirm you want to continue connecting by typing

```
# yes
```

and pressing the Enter key.

Example response:

```
Warning: Permanently added '47.142.128.16'
(RSA) to the list of known hosts.
root@47.142.128.16's password:
```

13 When prompted, enter the password for the SDM root user.

14 Ensure the "authorized_keys2" file has the proper ownership on the SDM by typing

```
$ ssh root@$SDM_IP chown swld:swld
/home/swld/.ssh/authorized_keys2
```

and pressing the Enter key.

Example response:

```
root@47.142.128.16's password:
```

15 When prompted, enter the password for the SDM root user.

16 Propagate the SDM's bootptab file with the entries from SSPFS by typing

```
$ /usr/bin/scp -q /etc/bootp/bootptab
${SDM_USER}@{SDM_IP}:/etc/bootptab
```

and pressing the Enter key.

```
$ /usr/bin/ssh -q -l ${SDM_USER}
${SDM_USER}@{SDM_IP} /sdm/swld/loadtab
```

and pressing the Enter key.

17 You have completed this procedure.

Re-establishing SSH communication after an SSPFS fresh install

At the SDM

1 Log in to the SDM.

2 Access the SWIM level of the maintenance interface by typing

```
# sdmmtc swim
```

and pressing the Enter key.

3 Access the Details level by typing

```
> details
```

and pressing the Enter key.

4 Ensure the OpenSSH fileset is applied.

Note: Use the up/down commands to scroll through the list of applications if required.

5 Perform procedure “Setting up the BootP file on SSPFS” in the Upgrade document.

6 You have completed this procedure.

Correcting a CORBA configuration issue between the CS 2000 Management Tools server and the MG 9000 Manager server

Application

Use this procedure when you are unable to provision MG 9000 lines or asynchronous digital subscriber lines (ADSLs) through OSSGate, or provision virtual media gateways (VMGs) from the MG 9000 Manager graphical user interface (GUI).

This procedure provides the steps to configure the naming service between the CS 2000 Management Tools server and the server where the MG 9000 Manager resides.

You must configure the naming service on both servers using the steps under

- Configuring the naming service on the CS 2000 Management Tools server
- Configuring the naming service on the server where the MG 9000 Manager resides

Once you have configured the naming service on both servers, you can verify the naming service is set up correctly using the steps under Verifying the naming service is configured correctly.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Configuring the naming service on the CS 2000 Management Tools server

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

7 Select the “CORBA Configuration” option by typing

```
select - 5
```

and pressing the Enter key.

Example response

```
CORBA Configuration
 1 - nsmirror (CORBA Naming Context Mirroring)


 X - exit

select -
```

8 Select the “nsmirror” option by typing

```
select - 1
```

and pressing the Enter key.

Example response

```
===Executing “nsmirror”

 1 - Add CORBA Naming Context Mirror
 2 - Remove CORBA Naming Context Mirror
 3 - Display Current Configuration
 4 - Exit

Configuraton
file:/opt/corba/rcscripts/NamingServiceMirrors.cfg

Please enter selection (1, 2, 3 or 4):
```

9 Select option “Add CORBA Naming Context Mirror by typing

1

and pressing the Enter key.

10 When prompted, enter the Application Name for the Succession Element and Sub-Network Manager by typing

sesm

and pressing the Enter key.

11 When prompted, enter the Host Name or IP address of the server where the MG 9000 resides.

12 When prompted, enter the Context Path by typing

NameService/Subnet_<release>

and pressing the Enter key.

Where

release
is the current release of the software, for example 062 for SN06.2

Note: The command is case sensitive.

13 When prompted, enter the Context Name by typing

`Subnet_<release>`

and pressing the Enter key.

Where

release
is the current release of the software, for example 062 for SN06.2

Note: The command is case sensitive.

14 When prompted, press the Enter key to accept the default value (2001) for the Local Port.

15 When prompted, press the Enter key to accept the default value (2001) for the Remote Port.

Example response:

```
You have selected to bind the remote naming
context as follow:

 Application Name    :SESM
 Host Name           :47.142.89.70
 Context Path        :NameService/Subnet_062
 Context Name        :Subnet_062
 Local Port          :2001
 Remote Port         :2001

Continue with configuration? (default:Y[Y/N/Q])
```

16 When prompted, confirm the configuration by typing.

`y`

and pressing the Enter key.

17 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

18 You have completed this procedure. Proceed to Configuring the naming service on the server where the MG 9000 Manager resides.

Configuring the naming service on the server where the MG 9000 Manager resides

At your workstation

1 Telnet to the server where the MG 9000 Manager resides by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the server where the MG 9000 Manager resides

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

6 Select the “Configuration” option by typing

```
select - 2
```

and pressing the Enter key.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Succession Element Configuration
 14 - chg_tz (Change Timezone)
 15 - login_session_timeout (Login Session
      Timeout Configuration)
 16 - snmp_poller (SNMP Poller Configuration)

 X - exit

select -
```

7 Select the “CORBA Configuration” option by typing

```
select - 5
```

and pressing the Enter key.

Example response

```
CORBA Configuration
 1 - nsmirror (CORBA Naming Context Mirroring)


 X - exit

select -
```

8 Select the “nsmirror” option by typing

```
select - 1
```

and pressing the Enter key.

Example response

```
===Executing “nsmirror”

 1 - Add CORBA Naming Context Mirror
 2 - Remove CORBA Naming Context Mirror
 3 - Display Current Configuration
 4 - Exit

Configuraton
file:/opt/corba/rcscripts/NamingServiceMirrors.cfg

Please enter selection (1, 2, 3 or 4):
```

9 Select option “Add CORBA Naming Context Mirror by typing

1

and pressing the Enter key.

10 When prompted, enter the Application Name for the MG 9000 Manager by typing

mgems

and pressing the Enter key.

11 When prompted, enter the Host Name or IP address of the CS 2000 Management Tools server where the SESM resides.

12 When prompted, enter the Context Path by typing

NameService/Nortel

and pressing the Enter key.

Note: The command is case sensitive.

13 When prompted, enter the Context Name by typing

Nortel

and pressing the Enter key.

Note: The command is case sensitive.

14 When prompted, press the Enter key to accept the default value (2001) for the Local Port.

15 When prompted, press the Enter key to accept the default value (2001) for the Remote Port.

Example response:

```
You have selected to bind the remote naming
context as follow:

 Application Name    :MGEMS
 Host Name           :47.142.85.56
 Context Path        :NameService/Nortel
 Context Name        :Nortel
 Local Port          :2001
 Remote Port         :2001

Continue with configuration? (default:Y[Y/N/Q])
```

16 When prompted, confirm the configuration by typing.

Y

and pressing the Enter key.

17 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

select - **x**

and pressing the Enter key.

18 You have completed this procedure. Proceed to Verifying the naming service is configured correctly.

Verifying the naming service is configured correctly

At your workstation

1 Close all GUIs and OSSGate telnet sessions if any.

2 Restart the SESM server application. Refer to procedure “Starting the SESM server application” in the CS 2000 Management Tools Administration and Security document, NN10172-611, if required.

3 Restart the MG 9000 Manager server application. Refer to the corresponding procedure in the MG 9000 Administration and Security document, NN10162-611, if required.

4 Start OSSgate client and provision one or more lines or ADSLs. Refer to the OSSgate User Guide, if required.

5 Access the MG 9000 Manager and provision a VMG. Refer to the corresponding procedure in the MG 9000 Administration and Security document, NN10162-611, if required.

Launching CS 2000 Management Tools client applications

Application

Use this procedure to launch any one of the following CS 2000 Management Tools client application graphical user interfaces (GUIs):

- Trunk Maintenance Manager
- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

  Note: The Network Patch Manager also has a command line user interface (CLUI). Refer to procedure Accessing the Network Patch Manager CLUI in this document.

- Batch Configuration Monitor

This procedure offers the following four methods to launch a CS 2000 Management Tools client application:

- Launching applications from a web browser. You must use this method when launching an application for the first time.
- Launching applications from the JWS Application Manager.

  Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- Launching applications from a desktop icon or Start menu (Windows only).

  Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- Launching specific applications using a URL.

Prerequisites

Ensure the client workstation meets the minimum requirements. Refer to section “Client workstation requirements” in the CS 2000 Management Tools Basics document, NN10020-111.

ATTENTION

If you have an ATI Raedon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you may experience the “blue screen of death” in your Windows environment. You can obtain information on this issue at the following URL: http://developer.java.sun.com/developer/bugParade/bugs/4713003.html. A workaround for this issue is to download the latest ATI graphics driver from the following web site http://mirror.ati.com/support/driver.html. Contact your IT support team if you need assistance.

You need the IP address or host name of the CS 2000 Management Tools server, and a valid user name and password to launch an application.

Note: Users of the CS 2000 Management Tools client applications must belong to the primary user group “succssn” for login access, and to one or more secondary user groups, which specify the operations a user is authorized to perform. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN102172-611.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.1_02 and Java™ Web Start (JWS) version 1.2.0_02 installed to launch the following applications:

- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

Note: JWS 1.2.0_02 is included as part of JRE 1.4.1_02.

Action

Launching applications from a web browser

At your workstation

1 Launch your web browser.

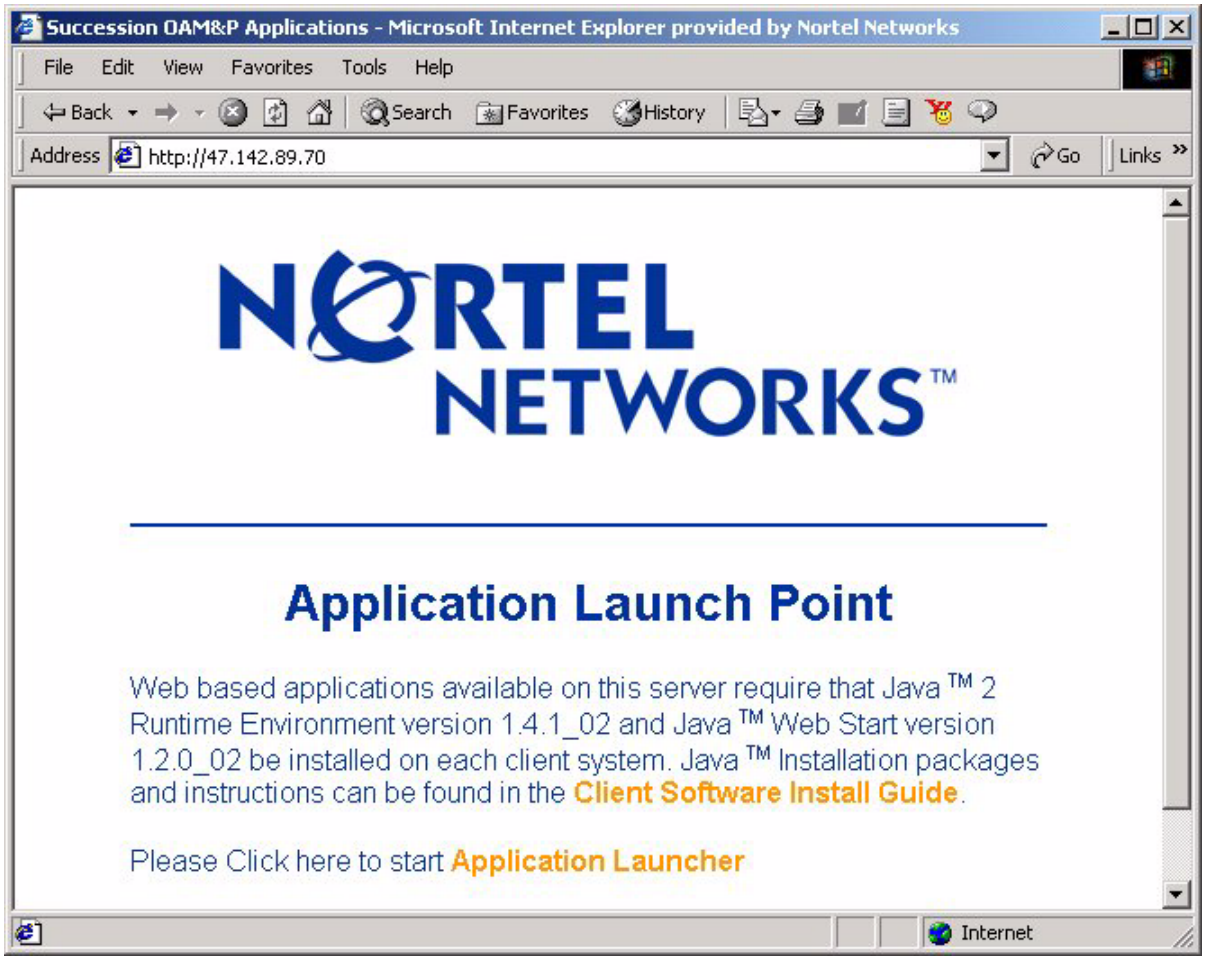
2 Access the CS 2000 Management Tools server by typing

>http://<host>

where

<host>
is the name or IP address of the CS 2000 Management Tools server where the CS2M software package is installed

The “Application Launch Point” page appears.



3 Refer to the following table to determine your next step.

If	Do
you have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 9
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 4
you do not know which version of JRE and JWS you have	step 4

4 Click **Client Software Install Guide** and follow the instructions under “How to check version” to verify your client setup.

If	Do
you have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 8
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 5

5 Click **Java 2 Runtime Environment Install Guide** under “Microsoft Windows” or “Sun Solaris” for system requirements and installation instructions.

6 Once you have read through the “Java 2 Runtime Environment Install Guide”, click the **Back** button to return to the “Client Software Installation” page.

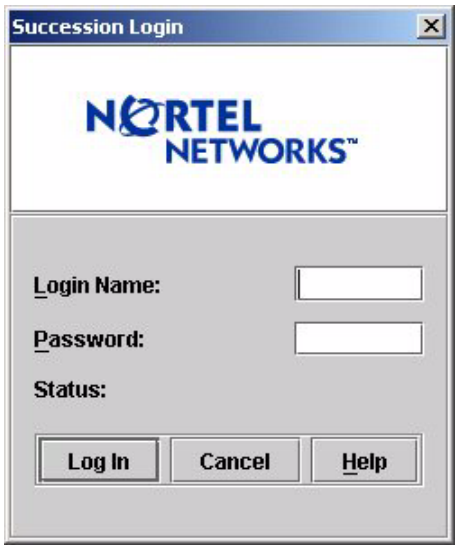
7 Click **Java 2 Runtime Environment Software Download** under “Microsoft Windows” or “Sun Solaris” to download and install the software.

Note: You must have administrative privileges to install the software on the workstation.

8 Click the **Back** button to return to the “Application Launch Point”.

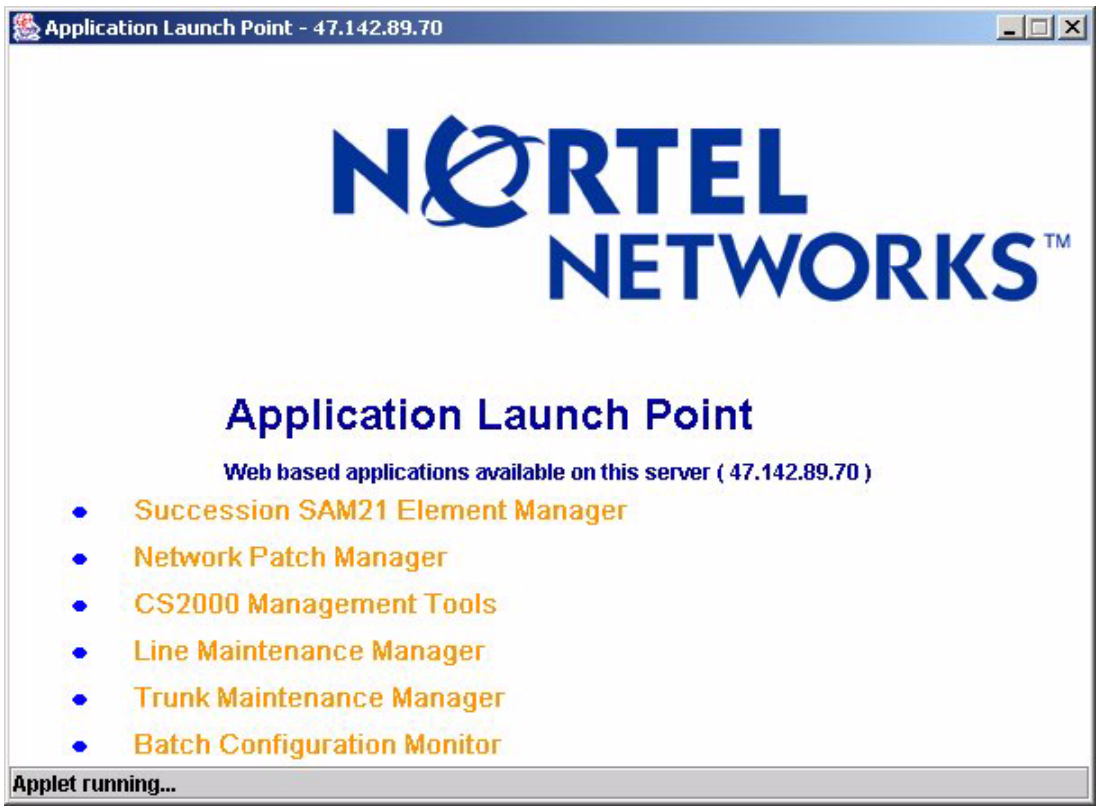
9 Click **Application Launcher**.

The Login window appears.



10 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.



11 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

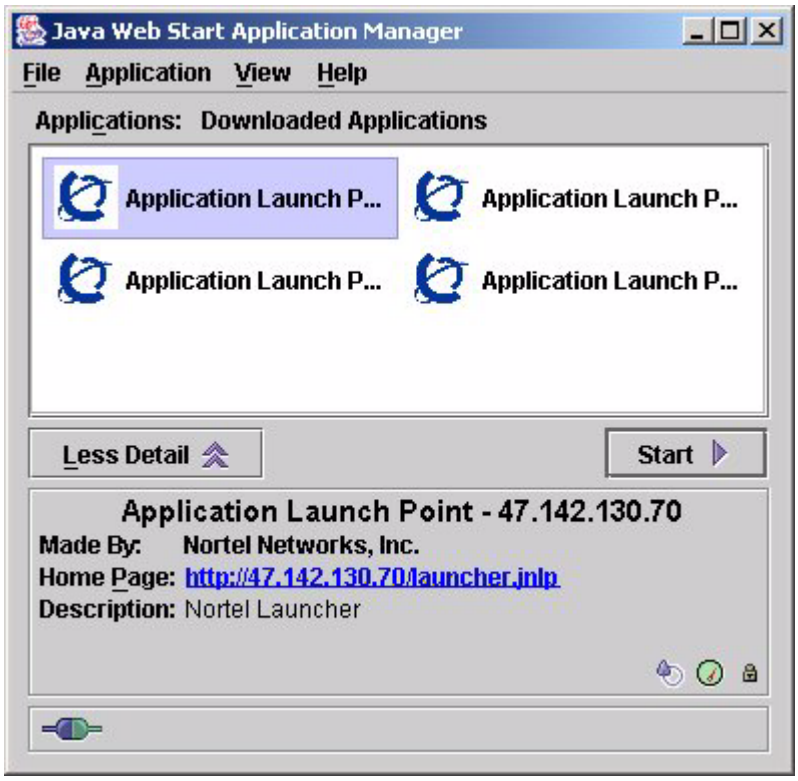
12 You have completed this procedure.

Launching applications from the JWS Application Manager

ATTENTION
You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

1 Launch the Java Web Start Application Manager.

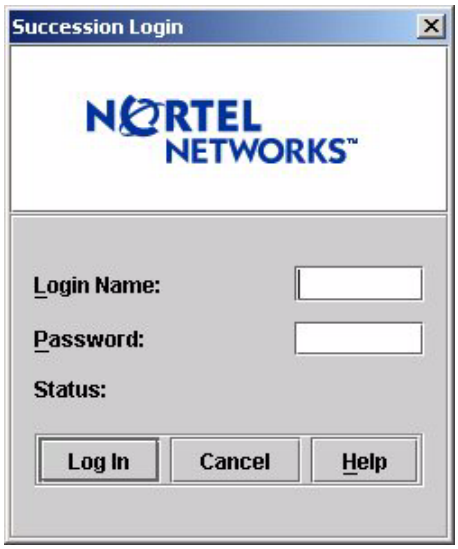


Note: If you do not see the downloaded applications as shown in the example above, on the **View** menu, click **Downloaded Applications**.

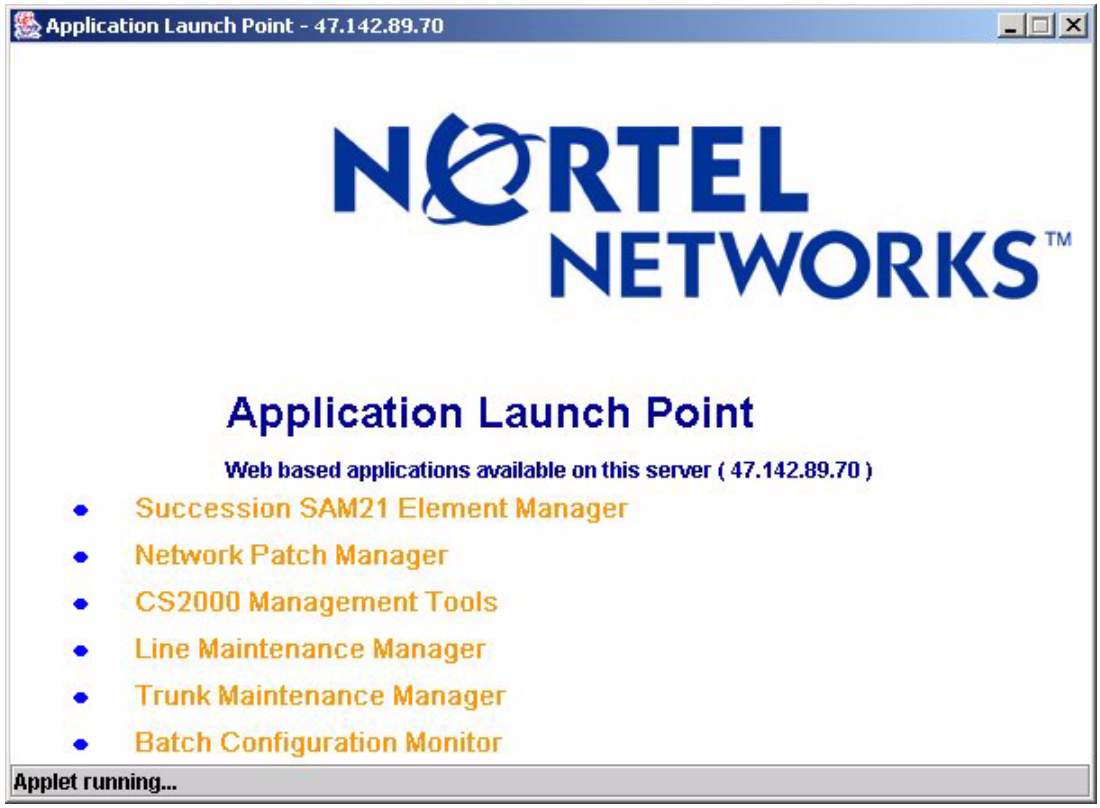
2 Double click on the Application Launch Point you want to access, or select the Application Launch Point and click **Start**.

The Login window appears.

3 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



4 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

5 You have completed this procedure.

Launching applications from a desktop icon or Start menu (Windows only)

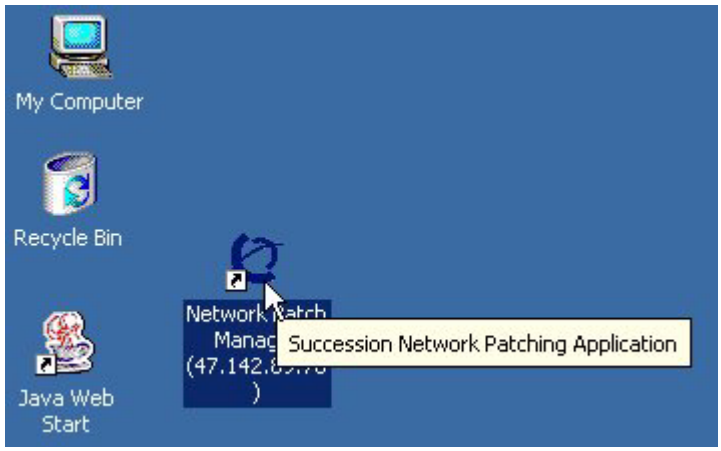
ATTENTION
You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

1 Perform step a to launch an application from a desktop icon, or b to launch an application from the Start menu.

a Locate the short-cut icon on your desktop, and double click on it to start the application.

Note: For short-cut icons to be present on your desktop, you must have the right settings under the Shortcut Options tab, which is accessed through **File->Preferences** in the JWS Application Manager.

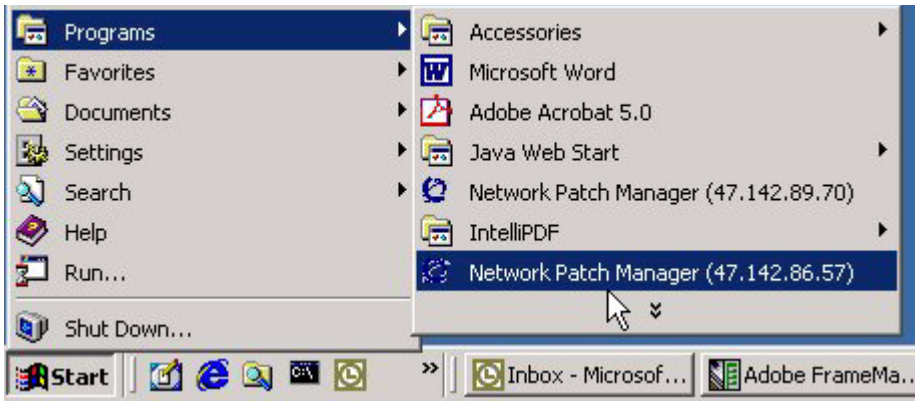


The Login window appears.

Proceed to step 2.

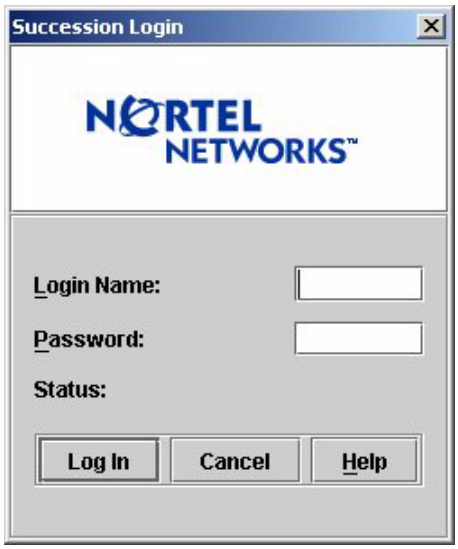
OR

b To launch a CS 2000 Management Tools client application from the Start menu, click **Start->Programs**, then click on the CS 2000 Management Tools client application you want to launch.

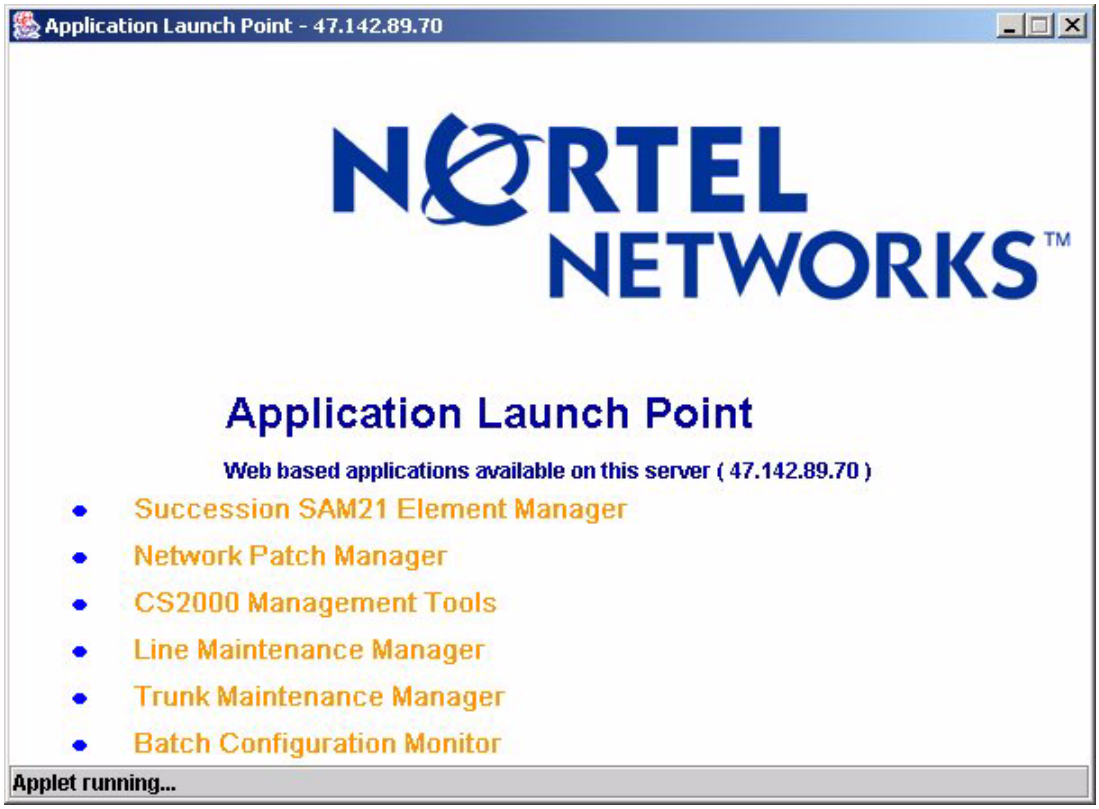


The Login window appears.

2 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



3 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

4 You have completed this procedure.

Launching specific applications using a URL

ATTENTION

You must have Java™ 2 Runtime Environment (JRE) version 1.4.1_02 and Java™ Web Start (JWS) version 1.2.0_02 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in this procedure Launching applications from a web browser.

At your workstation

1 Launch your web browser.

2 In the Address field, enter one of the following URLs for the application you want to launch:

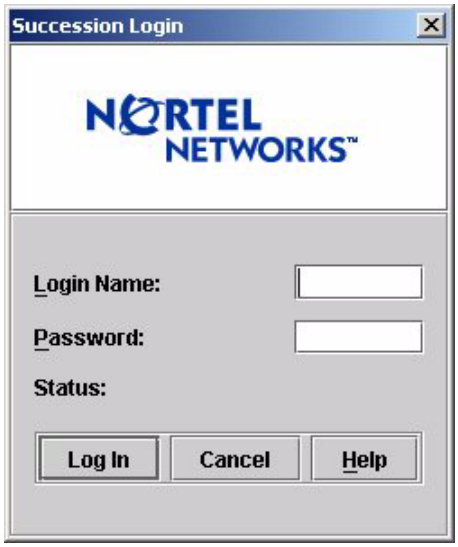
- CS2000 Management Tools - http://<host>/sesm/sesm.jnlp
- Line Maintenance Manager - http://<host>/sesm/lmm.jnlp
- Trunk Maintenance Manager - http://<host>/sesm/tmm.html
- Batch Configuration Monitor - http://<host>/sesm/bpt.html
- CS2000 SAM21 Manager - http://<host>/sam21em/sam21em.jnlp
- Network Patch Manager - http://<host>/npm/npm.jnlp

Where

host
is the host name or IP address of the CS 2000 Management Tools server

The Login window appears.

3 Enter your user name and password, then click **Log In**.



The interface for the application you launched, is displayed.

4 You have completed this procedure.

Accessing the Network Patch Manager CLUI

Application

Use this procedure to access the Network Patch Manager (NPM) command line user interface (CLUI).

Note: The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure Launching CS 2000 Management Tools client applications in this document.

Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

4 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode: Enter 'npm' commands, help
or quit to exit.

npm>
```

5 You have completed this procedure.