



Nortel Carrier Voice over IP Network Upgrades and Patches

ATTENTION

For all components that do not use the Network Patch Manager (NPM), if a patch file contains a “.patch” extension, remove that extension before applying the patch.

Contact your next level of support if assistance is required.

ATTENTION

Prepare all external systems before beginning a Nortel equipment network upgrade.

Check with the appropriate vendor or provider of all provisioning, billing, and other external network management systems to ensure that they are compatible with the new software release planned for the Nortel devices they manage.

All external systems, tools, and customer procedures must be ready prior to upgrading the Nortel network and devices. Failure to consider these external factors could cause disruption of operational or management procedures after a successful Nortel equipment upgrade.

Prior to the upgrade, ensure there are no active alarms on the IEMS. Refer to the IEMS documentation for details on displaying alarm status. Contact your next level of support on clearing active alarms.

ATTENTION

Prior to the upgrade, ensure there are no active alarms on the IEMS. Refer to the IEMS documentation for details on displaying alarm status. Contact your next level of support on clearing active alarms.

**CAUTION****Possible service outage**

Performing an end-to-end Carrier Voice over IP network upgrade requires upgrading individual component software in a specific order. Failing to follow the required order can result in a service outage.

This document describes the upgrade order and corresponding procedures for the following configurations:

- ATM networks
- IP networks
- Tri-Modal networks

Tri-Modal configurations allow Universal Access AAL1 (UA-AAL1) and UA-IP configuration interworking in a multi-bearer network configuration.

This document describes the upgrade process from an existing Nortel Networks software release to a later software release. New installations and conversions are not considered as upgrades and do not pertain to the information available in this document.

Any conversions or installations of new components introduced in the solution cannot be performed until after the solution has been upgraded to the new software release.

New in this release

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

The following changes were introduced to this document in SN09U:

- The document title was changed from *Upgrading a Carrier Voice over IP Network* to *Nortel Carrier Voice over IP Network Upgrades and Patches*
- Rollback and downgrade procedures were added to the document
- Each component upgrade procedure begins with the following four sections:
 - Component upgrade introduction
 - Component upgrade preparation
 - Component upgrade process
 - Component post upgrade process
- MCS Management Server and Border Control Point 7100 upgrades were removed from the book. Nortel requires that all customers contact their Nortel Customer Service representative to engage the appropriate Nortel Software Delivery team to perform this upgrade.

How to use this document

This document includes details about supported solutions and the required component upgrade order. The upgrade order for each solution is provided in the table [Component Upgrade Order on page 6](#). This document also includes copies of the basic component upgrade procedures.

For the list of included upgrade procedures and to navigate between sections, refer to the Adobe Acrobat Bookmarks in the document viewer.

For details about Carrier Voice over IP networks and new and changed hardware and software refer to the document *IP Solutions Basics*, NN10300-100 and *ATM Solutions Basics*, NN10320-100.

Note: This document applies to both North American and International solutions and the prefix “i” in release numbers, for example, “(i)SN09U”, indicates that both market segments apply.

Statements in this document about upgrades from prior releases assume that all regular maintenance release (RMR) upgrades have been applied unless explicitly stated otherwise.

Electronically viewing this document

When viewing this document electronically, hyperlinks are provided to automatically view referenced sections. Navigating between hyperlinks is an Acrobat Reader function managed by Adobe.

Clicking on a hyperlink reference, which appears underlined and in blue, automatically navigates to the associated reference point in the document.

Returning back to the hyperlink reference is accomplished by either of the following methods:

- on a keyboard, the hot-key combination of “Alt/arrow” navigates back and forth between hyperlinks. “Alt/left” and “Alt/right” toggle back and forth between the reference hyperlink page and the page where the hyperlink originated.
- on the screen bottom, the right and left arrow keys toggle back and forth between hyperlinks. A green arrow indicates that hyperlink activation has occurred and arrow navigation is available.

Limitations and restrictions

This document excludes the following components:

- network management layer components such as third-party fault aggregation or service activation systems
- transport layer components such as edge and core routers with the exception of the routers used as part of the central office Local Area Network (LAN) and data service components such as Shasta
- Signaling System No. 7 (SS7) network components such as broadband Signaling Transfer Points (STP) and Signaling Control Points (SCP)
- third-party offboard systems such as voice mail systems, protocol converters, or test trunk termination systems

In addition, this document excludes the following content:

- strategy for upgrading the transport components, for example, ATM switches and IP routers that form the data backbone, and Multiplexers (MUX) for Common Channel Signaling No. 7 (CCS7) backhauling
- strategy for upgrading the Network Management Layer Components such as Third Party Fault Aggregation or Service Activation Systems
- details on Digital Multiplex System (DMS) to the Carrier Voice over IP conversions

SN09U Upgrade Paths

Each new software release supports an upgrade, based on dependencies, from up to two previous releases. The SN09U software release supports the following upgrade paths:

ATM Upgrade paths

Upgrading from SN08 or SN09 to software release SN09U is supported for the following solutions:

- Packet Trunking - AAL1 (PT-AAL1 North American)
- Universal Access - AAL1 (UA-AAL1)
- Packet Transit - AAL2 (PT-AAL2 International)

Note: Hybrid configurations of the PT-AAL1 and UA-AAL1 solutions are also supported.

IP Upgrade paths

Upgrading from SN08 or SN09 to software release SN09U is supported for the following solutions:

- Packet Transit - IP (PT-IP - International)
- Packet Trunking - IP (PT-IP - North American)
- Integrated Access - Wireline (IAW)
- Integrated Access - Cable (IAC)
- Carrier Hosted Services (CHS)

Note: Hybrid configurations of the PT-IP, IAW, and IAC solutions are also supported.

Supported Tri-Modal Upgrade paths

Tri-Modal configurations support SN09U upgrades from SN08 or SN09.

Component Upgrade order

This section summarizes the required component order to upgrade software to release SN09U for all components in an upgrade path. The order applies to all solutions and applications. If a component is not part of a solution or application, the upgrade must follow the listed order for the next component that applies to the configured application.

The component names provide hyperlinks to detailed upgrade procedures that include estimated times to assist in planning required upgrade maintenance windows. The actual upgrade times may vary

from the estimated times due to the variety of different office configurations.

Component Upgrade Order

Component Name	
<u>Preparatory Upgrade</u>	
1	Device Manager upgrade
2	Ethernet Routing Switch 8600 software for the CS-LAN upgrade
<u>Carrier Voice over IP Upgrade Order</u>	
3	IEMS upgrade ATTENTION: Perform this upgrade only if the IEMS resides on a standalone server. ATTENTION: If the IEMS is on the same server as the CS 2000 Management Tools (CMT) application, go directly to the CMT upgrade. ATTENTION: If this is a geographically-redundant configuration, the standby server must also be upgraded. • SPFS • IEMS
4	CS 2000 Management Tools upgrade ATTENTION: Perform the IEMS upgrade at this time only if the IEMS is on the same server as the CS 2000 Management Tools. ATTENTION: If this is a geographically-redundant configuration, the standby server must also be upgraded. • SPFS • IEMS • CS2M • APS • ABS

Component Upgrade Order (Continued)

Component Name	
5	CS 2000 Core Manager upgrade or Core and Billing Manager 850 Upgrades ATTENTION: If this is a geographically-redundant configuration, the standby server must also be upgraded.
	• SPFS • CBM
6	Multiservice Data Manager upgrade
	• SPFS or Solaris OS • MDM
7	Multiservice Switch (MSS) 15000 upgrade
8	Peripheral Module upgrade
9	MG 9000 Manager upgrade ATTENTION: If this is a geographically-redundant configuration, the standby server must also be upgraded.
	• SPFS • MG 9000 Manager
10	Session Server-Lines upgrade ¹
	• Linux OS • MCS
11	Session Server Trunks upgrade
12	Policy Controller upgrade
13	Nortel SAM21 Shelf Controller Upgrades
14	GWC upgrade

Component Upgrade Order (Continued)

Component Name	
15	MS 2000 Series upgrade Universal Audio Server (UAS) does not require an upgrade. The UAS must be at the UAS08MM (or higher) software release before beginning the network upgrade.
16	MG 9000 upgrade
17	Nortel USP Upgrades or USP-Compact upgrade
18	Enhanced Network and Message Switch
19	XA-Core upgrade or Compact Call Agent upgrade
20	Media Gateway 15000 upgrade
21	CICM upgrade
22	Original Equipment Manufacturer (OEM) gateways and gateway managers²
23	MCS upgrade (see footnote 1)
24	BCP upgrade (see footnote 1)

1. Due to the complexity of the upgrade for the MCS 5200, Border Control Point 7100/7200, and Session Server-Lines product, Nortel requires that all customers contact their Nortel Customer Service representative to engage the appropriate Nortel Software Delivery team to perform this upgrade.

2. Upgrade the element manager (EM) for one type of gateway and immediately upgrade all corresponding gateways of the same type before upgrading the next EM type.

Preparing to upgrade the Carrier Voice over IP Network

ATTENTION

Beginning in the SN09 software release, the "Start of Log string" in the IEMS NT STD log feed to an OSS has changed from being a carriage return character (0D in Hexidecimal, 13 in Decimal) in previous software releases to a line feed followed by a carriage return (0A0D in Hexidecimal, 1013 in Decimal).

Any fault OSS receiving logs from the IEMS in NT STD must be prepared for this change prior to upgrading to SN09 or higher to ensure that the log stream continues to be parsed properly.

Failure of the fault OSS to parse the changed NT STD log stream will result in an inability to report failures in the office. The SN09 IEMS NT STD log delimiter summary (in hexidecimal) is as follows:

Start of Log string: 0A0D; End of Line string: 0A0D; End of Log string: 0A0D000A



CAUTION

Security certificates are required for all SPFS-based servers. All security certificates must be available prior to starting the upgrade.



CAUTION

Do not activate any patches until instructed to do so in the upgrade documentation.

The following procedure provides the high-level steps you need to execute prior to upgrading this solution. Where applicable, a reference to the step-by-step procedure is provided.

Required pre-upgrade procedures

A series of procedures are required before beginning a component network upgrade. The following table contains a summary of required pre-upgrade procedures.

Required pre-upgrade procedures

Requirement	Applicable Solutions	Documentation
Make sure you have the latest version of this document.	All	Nortel frequently updates this document. Go to www.nortel.com and check the current version for your solution and release. If necessary, refer to Checking the latest version of the upgrade documentation on page 28 .
Download and review the (I)SN09U Upgrade Bulletin.	All	Go to www.nortel.com and download the latest version of Bulletin 2006007082.
Check for any critical Software Upgrade bulletins.	All	Go to www.nortel.com and check for any additional Software Upgrade bulletins. Use the Filter/Sort option to view Software Upgrade bulletins for the components you will upgrade.
Make sure console access is available for all element managers.	All	A software upgrade requires console access. If necessary, refer to Configuring SPFS console access on page 51 .
Make sure all components use the latest software.	All	Make sure all components use the latest software before you upgrade to (I)SN09U. Refer to (I)SN09U software load lineup and baseline on page 30 .
Make sure all components are patch current	All	Go to www.nortel.com and use the Regional Patch Selector (RPS) tool to determine which patches you require. Refer to Ensuring patch currency on page 12 .
Verify your lab or network against the hardware baseline for a release	All	Contact your Nortel customer support representative.

Required pre-upgrade procedures

Requirement	Applicable Solutions	Documentation
Make sure all patches for the new loads being upgraded to are available	All	Go to www.nortel.com and use the Pre-Upgrade Patch Calculator and Patch Audit tool to determine which patches you require. Refer to Ensuring patch currency on page 12 .
If Nortel Software Delivery will perform your upgrade, complete the pre-upgrade checklist.	All	If Nortel Software Delivery performs your software upgrade, go to Preparing for Nortel to perform a software upgrade on page 23 .
Complete the network and component backups	All	<i>Nortel ATM/IP Solution-level Administration and Security</i> , NN10402-600
Disable the Network Patch Manager patch autoapply function	All	Disable the patch autoapply function for the duration of the office upgrade. This activity entails disabling the execution of the SYSTEMPLAN, which includes the AUTOAPPLY task. Refer to Modifying NPM patching plans on page 2409 .
Complete the Device Manager for Ethernet Routing Switch 8600 upgrade	All	Refer to Device Manager upgrade .
Complete the Ethernet Routing Switch 8600 (CS-LAN) upgrade	All	Refer to Ethernet Routing Switch 8600 software for the CS-LAN upgrade on page 73 .

OAM guidelines

Nortel recommends that redundant Multiservice Data Managers (MDM) be installed to ensure the maintenance view of the Multiservice Switch element is maintained even when the element manager is being upgraded.

Parallel GWC upgrades are not recommended or supported. While it is possible to save time by loading all GWCs of a given GWC type and

performing all the switch of activities (SWACT) at the same time, doing so is not recommended or supported for live office upgrades.

If your MG configuration does not support Hitless Software Migration (HSM), use the Post By Gateway feature within the Trunk Maintenance Manager (TMM) to post all the trunks on the MGs on that shelf and busy (BSY) them out. This must be done prior to the MG upgrade to prevent active calls from being dropped during the upgrade.

This feature allows active calls to complete before the trunk goes busy, but will not allow new calls to originate on those MGs on the selected shelf.

For UAS and MS 2010 redundancy, there must be N+1 sparing for UAS units for the following reasons:

- UAS units are simplex, and therefore a spare must be provided for redundancy. Even though two UAS units can fit on a SAM16 shelf, spreading them across shelves will provide complete redundancy in case of a shelf problem.
- A UAS unit goes out of service during its upgrade, and active calls are dropped. Having another UAS unit during this upgrade avoids loss of service.

Ensuring patch currency

Ensure that the baseline software is patch current, and that you have any required patches prior to starting the upgrade.

How to check for the latest patches

At a web browser

- 1 Go to <http://www.nortel.com>.
- 2 Select "Support & Training".
- 3 Select "Technical Support".
- 4 Select "Software Downloads".
- 5 Select "Find Products - Categories".
- 6 Select "Voice & IP Communications" as Product Category.
- 7 Scroll to "Communication Servers -Communication Server 2000".

- 8 Select "Tools" as Content.

If you want to

Do

query for patches for the loads you are upgrading to

steps [9](#) and [10](#)

query for patches for your baseline software

steps [11](#) through [39](#)

- 9 To query for patches for the loads you are upgrading to, select "Pre Upgrade Patch Calculator".

- 10 Select "Pre Upgrade Patch Calculator Readme[readme]" for instructions.

Also refer to [Carrier Voice over IP Network patching on page 2265](#)

- 11 To query for patches for your baseline software, select "Patch Audit for Inform Lists".

- 12 Select "Patch Audit User Guide [readme]" for instructions.

- 13 Verify the NPM server application is running by typing

servquery -status -group NPM

and pressing the enter key.

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

If the NPM is

Do

running

[step 16](#)

Not running

[step 15](#)

- 15 Start the NPM server application by typing

servstart NPM

and pressing the enter key.

- 16 Use one of the following methods to generate and send the inform file to the patch dropbox:

- [Generating the inform file using the NPM CLUI on page 15](#)
- [Generating the inform file using the NPM GUI on page 16](#)

- 17 Transfer the inform file to a machine running the web browser and add the file extension .txt to the end of the filename.

- 18 Return to your web browser.

- 19 Select "Patch Audit Application".

- 20 Enter path and filename of the inform list from site (or use Browse to find the file).
- 21 Press the process inform button.
- 22 Follow the directions in the Patch Audit User Guide to download patch files from nortel.com and then transfer these files to the patch dropbox.
- 23 Look for an email from PatchAudit user.
- 24 Download the recommended patches to your PC.
- 25 If required, unzip the file on the PC and transfer the individual patch files to the patch dropbox. Use the FTP userid and password as configured in PFRS.
- 26 Retrieve the patches that were delivered and place them in the NPM database using the procedure [Manually placing patches in the NPM database on page 2301](#).
- 27 Access the NPM CLUI.
For detailed steps, refer to [Accessing the Network Patch Manager CLUI on page 2284](#).
- 28 Apply the patches:

apply set EMG_NOT_APP set GEN_NOT_APP set ACT_NOT_ACT in set ALLDEVICES

Respond to the prompts to apply the patches. Take note of any patches with special application instructions. Some patches for SPFS devices require server reboots.

Note that this step can take a long time if there are many patches to apply.
- 29 Restart any devices that require a restart

restart set OAMDEVICES

Respond appropriately to any prompts about the restarts. If no devices require a restart, NPM will display that there is no work to do.
- 30 Following the restart, follow any special instructions which were displayed for the patches applied to devices, in particular devices with a deviceid that begins with SSPFS or SPFS.
- 31 You have completed this procedure. If applicable, return to the higher level procedure or task flow that directed you to this procedure.

Generating the inform file using the NPM CLUI

At your workstation

- 1 Access the NPM command line interface (CLUI) by typing

```
# npm
```

and pressing the enter key.

If required, refer to the procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

At the NPM CLUI

- 2 Verify Patch File Retrieval Settings (PFRS) are configured by typing

```
npm> viewpfrs
```

If response is	Do
Retrieving PFRS settings... No PFRS Preferences have currently been set	Configuring NPM for automatic patch file delivery on page 493 Note: The steps to enable the plans in Configuring NPM for automatic patch file delivery are not required for this case.
otherwise	step 3

- 3 Create and transfer the inform file to the patch dropbox by typing

```
npm> runtask PFRSGENREPORT
```

and pressing the enter key.

Example response of successful transfer

```
NPM>
```

```
Reason : Passed
```

```
Detail : PFRS Gen Report was successful.
```

If the results indicate the patch transfer was not successful, then use the following to determine corrective action.

- The following message indicates the configured patch drop box does not have its FTP server running.

```
java.lang.Exception: An Exception occurred
while verifying the remote server information
during a PFRS operation. Connection is
refused.
```

Either start the FTP server on the patch drop box or reconfigure PFRS to another patch drop box server by performing the procedure [Configuring NPM for automatic patch file delivery on page 493](#) and redo this step.

- The following message indicates the configured password has expired.

```
java.lang.Exception: An Exception occurred
while verifying the remote server information
during a PFRS Operation. Not logged in -
password incorrect
```

Reconfigure PFRS by performing the procedure [Configuring NPM for automatic patch file delivery on page 493](#) and redo this step.

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

Generating the inform file using the NPM GUI

At your workstation

- 1 Access the NPM GUI. If required, refer to the procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

At the NPM GUI

- 2 Select **Edit > Preferences...**
The preferences window opens.
- 3 Click on the **System Preferences** tab.
- 4 Verify the Patch File Retrieval Settings (PFRS) are configured. If the settings are configured, then close the Preferences window and proceed to [step 5](#). If the PFRS fields are blank, then perform the procedure [Configuring NPM for automatic patch file delivery on page 493](#).

- 5 Select **Tasks > Maintenance...**
The Maintenance window opens.
- 6 Click the **Task List** tab.
- 7 Select the PFRSGENREPORT task and click **Execute**.
The PFRSFGENREPORT Task popup menu window opens displaying the PRFS configuration.
- 8 Click **Continue**.
The PFRSGENREPORT task executes and the results are displayed in the PFRSFNEREPORT Results window that opens.
- 9 Review the results to verify that the patch retrieval was successful.

If the results indicate the patch transfer was not successful, then use the following to determine corrective action.
 - The following response in the Detail column indicates the configured patch drop box does not have its FTP server running.

`java.lang.Exception: An Exception occurred while verifying the remote server information during a PFRS operation. Connection is refused.`

Either start the FTP server on the patch drop box or reconfigure PFRS to another patch drop box server by performing the procedure [Configuring NPM for automatic patch file delivery on page 493](#) and redo this step.
 - The following response in the Detail column indicates the configured password has expired.

`java.lang.Exception: An Exception occurred while verifying the remote server information during a PFRS Operation. Not logged in - password incorrect`

Reconfigure PFRS by performing the procedure [Configuring NPM for automatic patch file delivery on page 493](#) and redo this step.
- 10 You have completed this procedure. If applicable, return to the higher level procedure or task flow that directed you to this procedure.

Patch order and procedures

For patch order and procedures, refer to [Carrier Voice over IP Network patching on page 2265](#).

Upgrading the Carrier Voice over IP Network Components

ATTENTION

This book contains upgrade procedures only. Conversions and installations are documented in Installation Methods. Software roll backs (downgrades) are documented in the component upgrade documents.

This document includes software procedures for possible components in a Carrier Voice over IP Network. Please disregard information about components that do not apply to your network.

Refer to the individual network component sections for upgrade procedures.

Prerequisites

Complete the following tasks described in [Preparing to upgrade the Carrier Voice over IP Network on page 9](#):

Component upgrade order

Follow the upgrade order described in the table [Component Upgrade order on page 5](#).

Completing the Carrier Voice over IP Network upgrade

After completing a network upgrade a series of additional procedures can be required. This section contains a summary of post-upgrade procedures, depending on the network configuration, that are required after a network upgrade.

Prerequisites

Complete [Upgrading the Carrier Voice over IP Network Components on page 18](#):

Action

Perform the following procedures to complete the solution upgrade.

Post-upgrade procedures

Requirement	Applicable Solutions	Documentation
Re-enable the Network Patch Manager patch autoapply function	All solutions	Re-enable the patch autoapply function after the completion of the office upgrade. This activity entails enabling the execution of the SYSTEMPLAN, which includes the AUTOAPPLY task. Refer to Modifying NPM patching plans on page 2409
Remove or update DCE	IP solutions only: PT-IP PT-AAL2 IAW	CS 2000 Core Manager Security and Administration, NN10170-611
Add OMI input for Session Server-Lines	IP solutions only	If your solution contains a Session Server lines component, you need to add an OMI input on the CS 2000 Management Tools. Refer to Adding a maintenance interface for Session Server-Lines on page 2431
Cutover USP messaging from core bounce to direct messaging	IP solutions only	USP core bounce to direct messaging cutover on page 1815

Post-upgrade procedures

Requirement	Applicable Solutions	Documentation
Complete any required post-upgrade tasks for each component	All solutions	Refer to the individual component upgrade procedures for post upgrade tasks.

Post-upgrade procedures

Requirement	Applicable Solutions	Documentation
Clean up old data in the NPM database	All solutions	Refer to Cleaning up old data in the NPM database on page 2437

Post-upgrade procedures

Requirement	Applicable Solutions	Documentation
Manually activate patches (if required)	All solutions except PT-AAL1	Refer to Manually activating patches on page 2424 .
Update new loads to the IEMS topology for required components	All solutions except PT-AAL1	Refer to Editing and viewing object properties using Java Web Start Client on page 2255 and Editing and viewing object properties using Web Client on page 2261
If you have upgraded your MDM device from release SN07: 1) Delete the SN07 MDM platform under the EMS Platforms in the IEMS Topology tree for the MDM node that was upgraded. 2) Update the device version field for the MDM-EM under the Element Managers to reflect the software release the MDM box was upgraded to. When the MDM-EM version is updated to a version of 08 or above the corresponding MDM platforms will be automatically discovered and added under the MDM topology (present under the Platforms topology in the IEMS Topologies tree).	All solutions	Refer to Editing and viewing object properties using Java Web Start Client on page 2255 and Editing and viewing object properties using Web Client on page 2261

Preparing for Nortel to perform a software upgrade

This section identifies the tasks you must complete to prepare for the software upgrade of a Carrier VoIP network when the upgrade is performed by Nortel Global Software Delivery personnel. This section includes the following information:

- task checklist
- description of each task

Task checklist

Use the following checklist to make sure each task is completed before Nortel begins the software upgrade.

Pre-upgrade task checklist

Task	Prime	Status	Date
Complete all pre-upgrade procedures			
Provide Nortel a list of all software received			
Provide Nortel the license key for MDM software			
Provide Nortel the license key for BCP software			
Provide Nortel an updated spec book			
Provide Nortel information on Contivity access			
Backup the CS 2000 Core Manager			
Backup the SPFS server			
Install an HTTPS certificate on the SPFS server			
Check the disk space on the SPFS server			

Description of tasks

This section provides a brief description of each task that must be completed before Nortel Global Software Delivery begins a software upgrade of a Carrier VoIP network.

Complete all pre-upgrade procedures

In this document, review the section [Preparing to upgrade the Carrier Voice over IP Network on page 9](#) and complete all pre-upgrade procedures listed in the section.

Provide Nortel a list of all software received

Provide Nortel a list of all new software for this release received by this office.

- If you receive software on CD, include all information on the label of the CD.
- If you receive software through ESD, include the names of the software loads in your dropbox.

Nortel uses this information to verify your office has the correct software before beginning the upgrade.

Provide Nortel the license key for MDM software

If your office uses an MDM, provide Nortel the license key for the MDM software. Nortel needs the license key to upgrade the MDM software.

Provide Nortel the license key for BCP software

If your office uses any model of the Border Control Point (BCP), provide Nortel the license key for the BCP software. Nortel needs the license key to upgrade the BCP software.

Provide Nortel an updated spec book

Provide Nortel an updated spec with valid usernames and passwords for all network elements to be upgraded. Nortel personnel will use the information to log into the elements to perform the upgrade.

Provide Nortel information on Contivity access

Provide Nortel information on how to use Contivity to access your network. This information may be included in your spec book or a separate document.

Make sure onsite support is available for a CS 2000 Core Manager upgrade

If your office uses a CS 2000 and CS 2000 Core Manager, make sure a technician is onsite during the software upgrade. The technician must RTS the CS 2000 Core Manager after the upgrade through the MAP terminal or a modem.

Backup the CS 2000 Core Manager

If you have a CS 2000 Core Manager, perform a full system backup before Nortel begins the upgrade. Refer to the procedure to perform an S-tape backup in your current CS 2000 Core Manager documentation.

The backup requires a 3-gigabyte blank DAT tape that meets the following requirements:

- One of the following approved brands:
 - Hewlett Packard
 - Maxell
 - Verbatim
 - Imation
- One of the following approved lengths:
- 90-meter (90m)
- 120-meter (120m)
- 125-meter (125m)

Approved use of a 125m tape is limited to UMFIOs on systems with DDS3-capable devices.

Performing this step before the upgrade allows Nortel to skip the step during the pre-check and reduce the time to perform the upgrade.

Check the backup space on the Core

If your office uses a CBM or CS 2000 Core Manager, make sure your CS 2000 or CS 2000 - Compact has enough backup space. The billing application on the CBM and CS 2000 Core Manager goes into backup mode during the upgrade.

For more information, refer to one of the procedures in one following documents:

- CBM 850 Accounting, NN10363-811
- CS 2000 Core Manager Accounting, NN10126-811

Task	Procedure
Determine the amount of required disk space	Disk Space Requirements in the section "Preparing for SBA installation and configuration"
Reconfigure backup volumes	"Configuring SBA backup volumes on the Core"

Backup the SPFS server

Backup all applications and data on all SPFS-based servers before Nortel begins the upgrade.

- If the SPFS-based server is a Netra t1400, use blank 4mm DDS3 tape of 125m and 12 GB.
- If the SPFS-based server is a Netra 240, use blank DVD-R or DVD-RW disks.

The following table lists the backup tasks for each SPFS application. Refer to your current documentation for the procedure to perform the task for your SPFS platform.

SPFS applications and backup tasks

Application	Task
SPFS	Back up the Oracle data Back up all file systems
APS	Backup the APS audio files Backup the APS oracle data
IEMS	Perform full system backup
MG 9000 Mgr	Perform full system backup.
CBM	Perform full system backup

Performing this step before the upgrade allows Nortel to reduce the time to upgrade SPFS-based servers and applications

Install an HTTPS certificate on the SPFS server

If HTTPS is not installed on the SPFS-based server, install an HTTPS certificate before Nortel begins the upgrade. Refer to your current documentation for the procedure. Installing the certificate before Nortel begins the upgrade reduces the time to complete the upgrade.

Check the disk space on the SPFS server

Make sure the SPFS-based server has enough space for the new software. The following table lists filesystems on the SPFS-based server, the minimum available disk space for the filesystem to support

the upgrade, and the command to display minimum available disk space.

SPFS disk space requirements

Filesystem	Minimum available disk space	Command
/opt	1,800,000 kilobytes	df -k /opt
/var	1,200,000 kilobytes	df -k /var
/tmp	200,000 kilobytes	df -k /tmp
root (/)	1,550,000 kilobytes	df -k /

Checking the latest version of the upgrade documentation

Use this procedure to make sure you are using the latest version of upgrade documentation.

Prerequisites

This procedure has the following prerequisites:

- Your workstation must have Internet access and a web browser.
- You must have a valid User ID and Password to access the Technical Support pages at www.nortel.com
- Your User ID must have permission to access technical documentation thru the Technical Support pages.

Action

Perform the following steps to complete this procedure.

Checking the latest version of upgrade documentation

At your workstation

- 1 Use your web browser to go to www.nortel.com/support.

Response

The browser shows the Technical Support page.

- 2 Log in to the Technical Support page. On the left side, click the Log In link.

Response

A Log In window appears

- 3 Enter your User ID and Password and click the Log In button.

The Technical Support page appears and shows your name under the Welcome banner.

- 4 Select the Browse Product Support tab.

Response

The Browse Product Support tab appears.

- 5** In the first field Product Categories, scroll through the list of categories and find Voice and IP Communications. Under Voice and IP Communications, select Packet Networks.

Response

The Technical Support page displays a list of products in the second field.

- 6** In the second field, scroll through the list of products and select the name of your solution.

Response

The Technical Support page displays a list of available content in the third field.

- 7** Select Documentation and click the Go button.

Response

The Technical Support page displays a list of available documentation for the solution.

- 8** Scroll through the list of documentation and select the Upgrade guide for this release.

Response

The Technical Support page displays Detail Information on the document.

- 9** Compare the version of the document available through the Technical Support page with the version of the document you are using.

If	Do
a newer version of the document is available	step 10
you are using the latest version of the document	step 11

- 10** Click the link next to File Download to download the latest version of the document.

Response

A pdf file of the document downloads to your workstation

- 11** You have completed this procedure. Return to the upgrade preparation section of this document and complete the next preparation task.

(I)SN09U software load lineup and baseline

The upgrade to (I)SN09U consists of the following types of upgrades:

- required upgrades to a new SN09U software load
- required upgrades to a specific Maintenance Release (MR)

The following table lists the Load ID and order code for each Nortel Carrier VoIP product. Use this information to complete the following tasks:

- Identify the products and software loads that require a software upgrade to (I)SN09U.
- Make sure each product you will upgrade uses the latest version of (I)SN08 or (I)SN09 software.
- Make sure your office has the correct (I)SN09U software.

(I)SN09U software loads and software baseline (Sheet 1 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
BCP				
BCP 7100	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	MCP04.0.3.0	MCS09 - 9.0.2.0	MCS09.1.5
	<i>Order code</i>	RMPC0080 RMPD0080 RMPP0080 RMPF0080 RMPT0080	RMPC0090 RMPD0090 RMPP0090 RMPF0090 RMPK0090 RMPT0090	MCPA0091 MCPB0091 MCPC0091 MCPD0091 MCPF0091 MCPH0091 MCPI0091 MCPK0091 MCPM0091 MCPN0091 MCPP0091 MCPQ0091 MCPT0091 MCPU0091 MCPV0091 MCPW0091 MCPX0091 USP00081

(I)SN09U software loads and software baseline (Sheet 2 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
BCP 7200	<i>Upgrade to (I)SN09U</i>	Not available in this release	Not available in this release	
	<i>Load ID</i>			MCS09.1.5
	<i>Order code</i>			MCPA0091 MCPB0091 MCPC0091 MCPD0091 MCPF0091 MCPH0091 MCPI0091 MCPK0091 MCPM0091 MCPN0091 MCPP0091 MCPQ0091 MCPT0091 MCPU0091 MCPV0091 MCPW0091 MCPX0091 USP00081
CBM				
CBM	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	CBM00080	CBM00090	UCBM0010
	<i>Order code</i>	CBM00080	CBM00090	UCBM0010

(I)SN09U software loads and software baseline (Sheet 3 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
CICM				
Gateway	<i>Upgrade to (I)SN09U</i>	Required 1. Upgrade from SN08 to SN09 MR1. 2. Upgrade from SN09 MR1 to SN09 MR3. 3. Upgrade from SN09 MR3 to SN09 MR4.	Not required	
	<i>Load ID</i>	MR5 Build 8.10.304	MR4 Build 9.20.235	MR4 Build 9.20.235
	<i>Order code</i>	CICM0080	CICM0090	CICM0090
Element Mgr.	<i>Upgrade to (I)SN09U</i>	Required 1. Upgrade from SN08 to SN09 MR1. 2. Upgrade from SN09 MR1 to SN09 MR3. 3. Upgrade from SN09 MR3 to SN09 MR4.	Not required	
	<i>Load ID</i>	MR5 Build 8.10.284	MR4 Build 9.20.235	MR4 Build 9.20.235
	<i>Order code</i>	CICE0080	CICE0090	CICE0090

(I)SN09U software loads and software baseline (Sheet 4 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
CS 2000				
Core - North America	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	PSNNC08	PSNNC09BS	PSNNC09BS
	<i>Order code</i>	SN000008	SN000009	SN000009
Core - International (MMP/ GMP/ ISN)	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	PSNGSC08	PSNGCSC09	PSNGCSC09
	<i>Order code</i>	SG000008	SG000009	SG000009
Core - International (MMP/ ISN)	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	PSNWC08	PSNWC09	PSNWC09
	<i>Order code</i>	SW000008	SW000009	SW000009

(I)SN09U software loads and software baseline (Sheet 5 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
CS 2000 Compact Call Agent				
Call Agent platform (NTRX51GZ)	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	ncgl_cca_image_7.09.1.0	ncgl_cca_765_image_9.11.1.0	ncgl_cca_765_image_9.11.2.1
	<i>Order code</i>	CCA00080	CCA00090	CCA00090
Call Agent platform (NTRX51HZ)	<i>Upgrade to (I)SN09U</i>	Not available in this release	Not required	
	<i>Load ID</i>		ncgl_cca_905_image_9.11.1.0	ncgl_cca_905_image_9.11.2.1
	<i>Order code</i>		CCA00090	CCA00090
SOS - North America	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	CSNNC08	CSNNC09	CSNNC09
	<i>Order code</i>	SNC0008	SNC00009	SNC00009
SOS - International	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	CSNWC08	CSNWC09	CSNWC09
	<i>Order code</i>	SWC0008	SWC00009	SWC00009
MC	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	ncgl_mc_image_7.0.9.10	ncgl_mc_image_9.11.1.0	ncgl_mc_image_9.11.2.1
	<i>Order code</i>	CCA00080	CCA00090	CCA00090

(I)SN09U software loads and software baseline (Sheet 6 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
CS 2000 Compact STORM				
Dothill platform	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	STM02	STM02	STM02
	<i>Order code</i>	STRM0004	STRM0004	STRM0004
HP platform	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	STM04	STM04	STM04
	<i>Order code</i>	STRM0006	STRM0006	STRM0006
CS 2000 Core Manager				
CS2E	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	CS2E0080	CS2E0090	CS2E0090
	<i>Order code</i>	CS2E0080	CS2E0090	CS2E0090

(I)SN09U software loads and software baseline (Sheet 7 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
CS 2000 Management Tools				
CS2M	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	CS2M08MA	CS2M0090_040_0	CS2M0090_135_1
	<i>Order code</i>	CSM0080	CS2M0090	CS2M0091
SPFS	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	SPFS_08.0_200511323	SPPFS_09.0_200534323 + SSPFS09MB	SPFS_09.1_200615214
	<i>Order code</i>	SPFS0080	SPFS0090 SPFR0090	SPFS0091 SPFR0091
	Note: Use the SPFSn order code when ordering SPFS software. The SPFSn order code includes the SPFRn order code. - ESD customers receive the following software: - Disk 1, 2, and 3 through ESD - Disk 1 on CD with the SPFRn order code to support system restore - CD customers receive the following software: - Disk 1 on CD with the SPFRn order code - Disks 2 and 3 on CD with the SPFSn order code			
IEMS	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	IEMS08MA	IEMS_09_33FC	IEMS_0910AB34
	<i>Order code</i>	IEMS0080	IEMS0090	IEMS0091
APS	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	APS10-27 (APS10MR-MC)	APS11-21 (APS11MR_MA)	APS11-21 (APS11 MR_MA)
	<i>Order code</i>	APS00100	APS00110	APS00110

(I)SN09U software loads and software baseline (Sheet 8 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
DPT SPM				
MG4K IW CEM	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	IWS21BO	IWS21BO	IWS21BO
	<i>Order code</i>	DPTS0080	DPTS0080	DPTS0080
MG4K DA ATM	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	ATC21BO	ATC21BO	ATC21BO
	<i>Order code</i>	DPTS0080	DPTS0080	DPTS0080
Coherent ECAN	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	COH21BO	COH21BO	COH21BO
	<i>Order code</i>	DPTS0080	DPTS0080	DPTS0080
SPM DSP VSP: Nortel ECAN	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	DSP21BN	DSP21BN	DSP21BN
	<i>Order code</i>	DPTS0080	DPTS0080	DPTS0080
ERS 8600				
ERS 8600	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	3.7.13	3.7.13	3.7.13
	<i>Order code</i>	P86S0070	P86S0090	P86S0090

(I)SN09U software loads and software baseline (Sheet 9 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
Gateway Controller				
GWC - North America	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	GN080BV	GN090CE	GN091BV
	<i>Order code</i>	GWCC0080	GWCN0090	GWCN0091
GWC - International	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	GI080BV	GI090CE	GI091BV
	<i>Order code</i>	GWCW0080	GWCW0090	GWCW0091
IW SPM ATM				
MG4K IW CEM	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	IWS21BO	IWS21BO	IWS21BO
	<i>Order code</i>	SPMI0080	SPMI0080	SPMI0080
MG4K DA ATM	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	ATC21BO	ATC21BO	ATC21BO
	<i>Order code</i>	SPMI0080	SPMI0080	SPMI0080
SPM Sync RN	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	SYN21BN	SYN21BN	SYN21BN
	<i>Order code</i>	SPMI0080	SPMI0080	SPMI0080

(I)SN09U software loads and software baseline (Sheet 10 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
IW SPM IP				
MG4K IW CEM	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	IWS21BO	IWS22CC	IWS22CC
	<i>Order code</i>	SIWI0080	SIWI0090	SIWI0090
Gigabit Ethernet	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	GEM21BQ	GEM22CC	GEM22CC
	<i>Order code</i>	SIWI0080	SIWI0090	SIWI0090
SPM Sync RN	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	SYN21BN	SYN22CC	SYN22CC
	<i>Order code</i>	SIWI0080	SIWI0090	SIWI0090
JDM				
JDM	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	5.8.8.0	5.8.8.0	5.8.8.0
	<i>Order code</i>	P86S0070	P86S0090	P86S0090
Keymile UMUX 1500				
Keymile UMUX 1500	<i>Upgrade to (I)SN09U</i>	Not available in this release	Not required	
	<i>Load ID</i>		Rls 7A	Rls 7B
	<i>Order code</i>		KEYM0070	KEYM0071

(I)SN09U software loads and software baseline (Sheet 11 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
MCS 5200				
MCS 5200	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	MCS4.0.3.0. 2005-06-23-2335	MCS09 - 9.0.6	MCS09.1.5
	<i>Order code</i>	Not applicable (Limited deployment)	MCPAM090 MCPBM090 MCPCM090 MCPDM090 MCPFM090 MCPHM090 MCPIM090 MCPKM090 MCPNM090 MCPPM090 MCPQM090 MCPTM090 MCPUM090 MCPVM090 MCPWM090 MCPXM090	MCPA0091 MCPB0091 MCPC0091 MCPD0091 MCPF0091 MCPH0091 MCPI0091 MCPK0091 MCPM0091 MCPN0091 MCPP0091 MCPQ0091 MCPT0091 MCPU0091 MCPV0091 MCPW0091 MCPX0091 USP00081

(I)SN09U software loads and software baseline (Sheet 12 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
MDM				
MDM	Upgrade to (I)SN09U	Required	Required	
	Load ID	15.2	15.3	15.4
	Order code			
SPFS	Upgrade to (I)SN09U	Required	Required	
	Load ID	SSPFS_09.0_200534323 + SSPFS09MB	SSPFS_09.0_200534323 + SSPFS09MB	SPFS091AB82
	Order code	SPFS0090 SPFR0090	SPFS0090 SPFR0090	SPFS0091 SPFR0091
	Note 1: Order SPFS0090 for (I)SN08 only if MDM resides on CMT server. Note 2: Use the SPFSn order code when ordering SPFS software. The SPFSn order code includes the SPFRn order code. - ESD customers receive the following software: - Disk 1, 2, and 3 through ESD - Disk 1 on CD with the SPFRn order code to support system restore - CD customers receive the following software: - Disk 1 on CD with the SPFRn order code - Disks 2 and 3 on CD with the SPFSn order code			
MG 3200				
MG 3200	Upgrade to (I)SN09U	Required	Not required	
	Load ID	4.60B.003	4.60D.014.003	4.60D.014.003
	Order code	AMG20080	MG320090	MG320090
EMS	Upgrade to (I)SN09U	Required	Not required	
	Load ID	2.2.114	3.0.111	3.0.111
	Order code		MG3E0090	MG3E0090

(I)SN09U software loads and software baseline (Sheet 13 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
MG 3500				
MG 3500	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	2.1.25	3.0.27_1.29	3.0.27_1.29
	<i>Order code</i>		MG350090	MG350090
EMS	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	2.2.114	3.0.111	3.0.111
	<i>Order code</i>		MG3E0090	MG3E0090
MG 4000				
MG4K DA CEM	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	MG421BO	MG421BO	MG421BO
	<i>Order code</i>	MG4D0080	MG4D0080	MG4D0080
MG4K DA ATM	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	ATC21BO	ATC21BO	ATC21BO
	<i>Order code</i>	MG4D0080	MG4D0080	MG4D0080
Coherent ECAN	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	COH21BO	COH21BO	COH21BO
	<i>Order code</i>	MG4D0080	MG4D0080	MG4D0080
SPM HDLC (PRI)	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	DL221BN	DL221BN	DL221BN
	<i>Order code</i>	MG4D0080	MG4D0080	MG4D0080

(I)SN09U software loads and software baseline (Sheet 14 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
SPM HDLC (PRI)	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	DL221BN DLC21BN	DL221BN DLC21BN	DL221BN DLC21BN
	<i>Order code</i>	MG4D0080	MG4D0080	MG4D0080
SPM DSP VSP: Nortel ECAN	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	DSP21BN	DSP21BN	DSP21BN
	<i>Order code</i>	MG4D0080	MG4D0080	MG4D0080
MG4K LSA-DS1	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	IED21BP	IED21BP	IED21BP
	<i>Order code</i>	MG4D0080	MG4D0080	MG4D0080
MG4K OC3	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	OC421BO	OC421BO	OC421BO
	<i>Order code</i>	MG4D0080	MG4D0080	MG4D0080
STS1 RM	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	STS21BO	STS21BO	STS21BO
	<i>Order code</i>	MG4D0080	MG4D0080	MG4D0080
SPM Sync RN	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	SYN21BN	SYN21BN	SYN21BN
	<i>Order code</i>	MG4D0080	MG4D0080	MG4D0080
MG 7000				
MG 7000	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	SPCR 6.1	PCR 7.1	PCR 7.2
	<i>Order code</i>			

(I)SN09U software loads and software baseline (Sheet 15 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
MG 9000				
MTA card	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	MTAG08BR	MTAG09BO	MTAG09FZ
	<i>Order code</i>	MG9K0080	MG9K0090	MG9K0091
DSL card	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	DSLA08AE	DSLA09BO	DSLA09FZ
	<i>Order code</i>	MG9K0080	MG9K0090	MG9K0091
DS1 card	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	DS1G08BJ	DS1G09BO	DS1G09FZ
	<i>Order code</i>	MG9K0080	MG9K0090	MG9K0091
ABI card	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	ABIG08BJ	ABIG09BO	ABIG09FZ
	<i>Order code</i>	MG9K0080	MG9K0090	MG9K0091
ITP card	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	ITPA08BP	ITPA09BO	ITA09FZ
	<i>Order code</i>	MG9K0080	MG9K0090	MG9K0091
ITX card	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	ITXA08BJ	ITXA09BO	ITXA09FZ
	<i>Order code</i>	MG9K0080	MG9K0090	MG9K0091

(I)SN09U software loads and software baseline (Sheet 16 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
SCO card	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	SCOA08BJ	SCOA09BO	SCOA09FZ
	<i>Order code</i>	MG9K0080	MG9K0090	MG9K0091
SCI card	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	SCIA08BJ	SCIA09BO	SCIA09FZ
	<i>Order code</i>	MG9K0080	MG9K0090	MG9K0091
MG 9000 Manager				
MG 9000 Mgr	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	UEEMS08	UEEMS09	UEEMS091_15a
	<i>Order code</i>	9KEM0080	9KEM0090	9KEM0091
SPFS	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	SSPFS_09.0_200534323 + SSPFS09MB	SSPFS_09.0_200534323 + SSPFS09MB	SPFS091AB82
	<i>Order code</i>	SPFS0090 SPFR0090	SPFS0090 SPFR0090	SPFS0091 SPFR0091
Note: Use the SPFSn order code when ordering SPFS software. The SPFSn order code includes the SPFRn order code. - ESD customers receive the following software: - Disk 1, 2, and 3 through ESD - Disk 1 on CD with the SPFRn order code to support system restore - CD customers receive the following software: - Disk 1 on CD with the SPFRn order code - Disks 2 and 3 on CD with the SPFSn order code				

(I)SN09U software loads and software baseline (Sheet 17 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
MG 15000				
MG 15000	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	SPCR 6.1	PCR 7.1	PCR 7.2
	<i>Order code</i>			
MS				
MS load	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	MUC21	MUC22	MUC22
	<i>Order code</i>	MUC00021	MUC00022	MUC00022
MS 2010				
MS 2010	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	4.60.038.000	4.60D.018	4.60D.018
	<i>Order code</i>	MS200080	MS200090	MS200090
MS 2020				
MS 2020	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	4.60.009.004	4.60D.017.002	4.60D.017.002
	<i>Order code</i>	MS2A0080	MS2A0090	MS2A0090
MSS 15000				
MSS 15000	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	SPCR 6.1	PCR 7.1	PCR 7.2
	<i>Order code</i>			

(I)SN09U software loads and software baseline (Sheet 18 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
Policy Controller				
Policy Controller	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	NGSS08MF2	NGSS09MB	NGSS09MB
	<i>Order code</i>	NGSS0090	NGSS0090	NGSS0090
SAM21 Shelf Controller				
SAM21 SC	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	SCU11.0.3	SCU13.0.1	SCU13.0.1
	<i>Order code</i>	SAM20080	SAM20090	SAM20090

(I)SN09U software loads and software baseline (Sheet 19 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
SPM				
SPM NA CEM	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	CEM21BN	CEM21BN	CEM21BN
	<i>Order code</i>	SPM00210	SPM00210	SPM00210
Coherent ECAN	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	COH21BO	COH21BO	COH21BO
	<i>Order code</i>	SPM00210	SPM00210	SPM00210
SPM HDLC (PRI)	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	DLC21BN	DLC21BN	DLC21BN
	<i>Order code</i>	SPM00210	SPM00210	SPM00210
SPM HDLC (PRI)	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	DL221BN	DL221BN	DL221BN
	<i>Order code</i>	SPM00210	SPM00210	SPM00210
SPM DSP VSP: Nortel ECAN	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	DSP21BN	DSP21BN	DSP21BN
	<i>Order code</i>	SPM00210	SPM00210	SPM00210
SPM OC3	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	OC321BN	OC321BN	OC321BN
	<i>Order code</i>	SPM00210	SPM00210	SPM00210
SPM Sync RN	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	SYN21BN	SYN21BN	SYN21BN
	<i>Order code</i>	SPM00210	SPM00210	SPM00210

(I)SN09U software loads and software baseline (Sheet 20 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
SSL				
SSL Platform	<i>Upgrade to (I)SN09U</i>	Not available in this release	Required	
	<i>Load ID</i>		SSL09 - 9.0.5	SSL9.1.5
	<i>Order code</i>		SSPAM090 SSPBM090 SSPCM090 SSPIM090 SSPKM090 SSPQM090 SSPRM090 RMPKM090	SSPA0091 SSPB0091 SSPC0091 SSPI0091 SSPK0091 SSPQ0091 SSPR0091 SSPX0091
SST				
NGSS	<i>Upgrade to (I)SN09U</i>	Required	Not required	
	<i>Load ID</i>	NGSS08MF2	NGSS09MB	NGSS09MB
	<i>Order code</i>	NGSS0090	NGSS0090	NGSS0090
TDM Peripherals				
North America	<i>Upgrade to (I)SN09U</i>	Refer to the <i>Peripheral Module Release Document</i> for SN09U for information on TDM peripheral loads.		
	<i>Load ID</i>	PLLT21	PLLT22	PLLT22
	<i>Order code</i>	PLLT0021	PLLT0022	PLLT0022
International	<i>Upgrade to (I)SN09U</i>	Refer to the <i>Peripheral Module Release Document</i> for ISN09U for information on TDM peripheral loads.		
	<i>Load ID</i>	PSNW21	PSNW22	PSNW22
	<i>Order code</i>	PSNW0008	PSNW0009	PSNW0009

(I)SN09U software loads and software baseline (Sheet 21 of 21)

Software load		From		To
		(I)SN08	(I)SN09	(I)SN09U
UAS				
UAS	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	UAS08MN	UAS08MN	UAS08MN
	<i>Order code</i>	UAS0080	UASA0090	UASA0090
SAM16 Platform	<i>Upgrade to (I)SN09U</i>	Not required	Not required	
	<i>Load ID</i>	NGS033 Rel3.3	NGS033 Rel3.3	NGS033 Rel3.3
	<i>Order code</i>	GSS00033	GSS00033	GSS00033
USP				
USP	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	USP10.0.8.40D	USP11.0.1.49E	USP11.1.3.37C
	<i>Order code</i>	USP00100	USP00110	USP00111
USP-Compact				
USP-Compact	<i>Upgrade to (I)SN09U</i>	Required	Required	
	<i>Load ID</i>	USPL10.0.5.01E	USPC11.0.1.47E	USPC11.1.3.38C
	<i>Order code</i>	USPL0100	USPC0110	USPC0111

Configuring SPFS console access

Purpose

Use this procedure when you are performing a procedure that requires a direct connection to the Sun Server console port, as opposed to telnet/ssh access.

Application

The following procedures require console access:

- Fresh SPFS installations
- Upgrades and fallbacks
- Performing a full system restore on an SPFS-based server
- Network IP changes
- Cloning the image of one server in a cluster to the other server
- Shutting down an SPFS-based server
- Initiating a manual failover on a Sun Netra 240 server pair
- Replacing one or more failed disk drives on an SPFS-based server
- Changing an expired root password on an SPFS-based server

Console access can be achieved in two distinct methods:

- locally
- remotely

Prerequisites

This procedure describes how to configure both methods of console access. Additional information about setting up console access can be found in the *Sun Netra Server 240 Installation Guide*:

<http://docs.sun.com/app/docs>

You will not be able to make use of the serial console if the Sun server was booted with the keyboard/mouse plugged in. In order to make use of the serial console, you will need to disconnect the keyboard/mouse and reboot the Sun server.

Procedures

RS-232 device connection and configuration

There are two steps as follows:

- Physically connecting the desired RS-232 device to the serial management (Serial MGT) port.
- Configuring the RS-232 device with adequate RS-232 protocol settings.

Configuring and connecting the RS-232 device

At your workstation

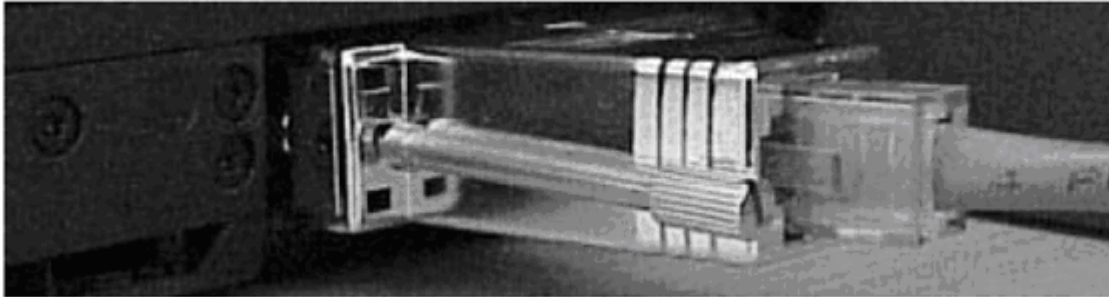
- 1 Physical connection is established by using the correct cable to interconnect the RS-232 device to the serial management RJ-45 console port. This port is located on the back of the Sun T1400/N240 and is labeled "Serial MGT".
- 2 Connection to the Sun T1400/N240 can be established using a RJ-45 cable and a RJ-45-DB9 adaptor. Connect one end of the RJ-45 cable to the N240 Serial MGT port (located on the rear of the Netra). Connect the other end to the RJ-45-DB9 adaptor and then to the client PC/laptop as shown in the figure below. The Sun part number for the RJ-45-DB9 adaptor is Sun Part #530-2103.

Note: A crossover or rollover cable connecting the RS-232 device and the console port might be required, so that each pin of the Netra 240 matches that of the terminal server's serial port.

More information about pinout configurations can be found in the Sun Netra 240 Server Service Manual:

<http://www.sun.com/products-n-solutions/hardware/docs/html/817-2699-13/>

Sun 240 DB9 connector on COM1 port of a laptop



- 3 By default, the console port requires the connecting RS-232 device to be configured as follows:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow Control: Xon/Xoff
- 4 You have completed this procedure. If applicable, return to the higher-level procedure or task flow that directed you to this procedure.

Configuring local console access

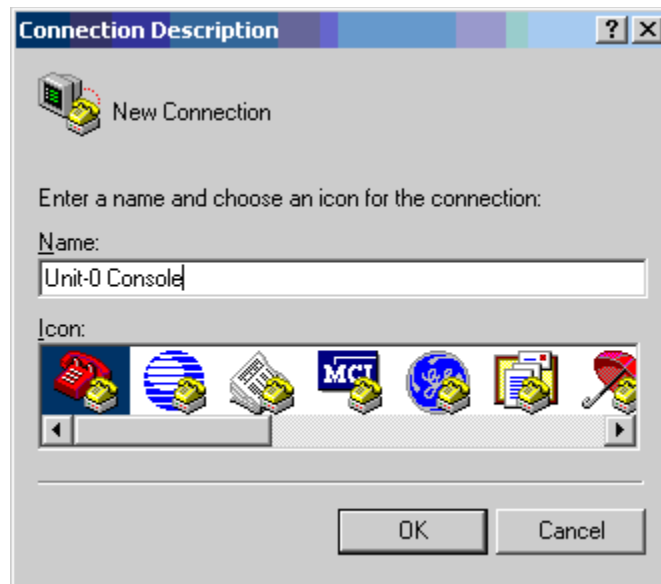
To gain local console access to the T1400/N240, use a co-resident vt-100 terminal or laptop with vt-100 terminal emulation software (such as the Microsoft Windows Hyperterm application) as the RS-232 device. Use the device configuration parameters in [RS-232 device connection and configuration on page 52](#).

Configuring local console access

At your workstation

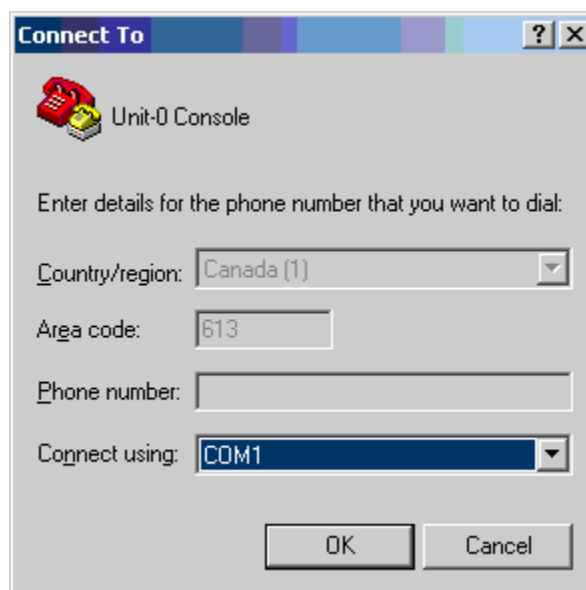
- 1 You can use HyperTerminal.
Click Start ->
Programs/Accessories/Communications/HyperTerminal
- 2 Give the session a name, such as "unit0 Console".

New connection dialog



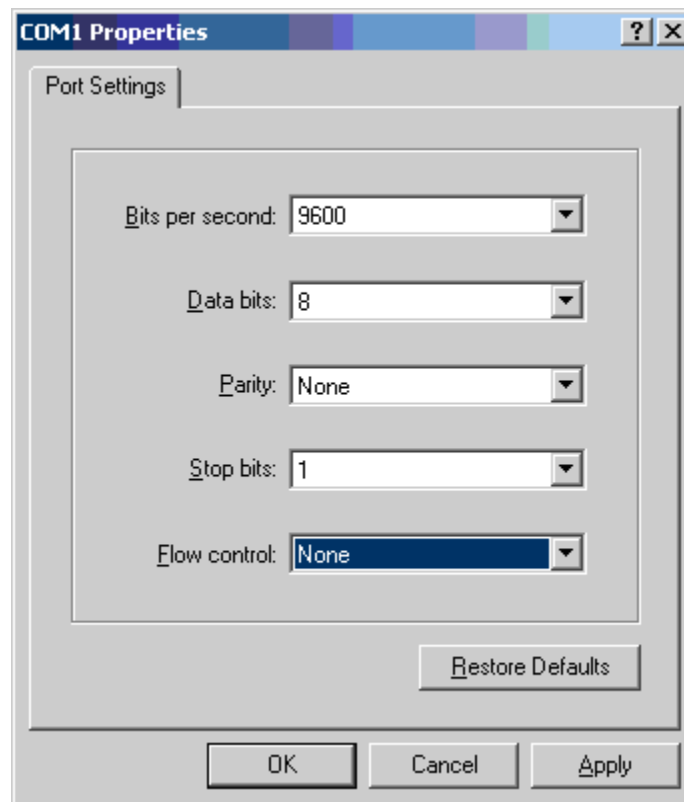
- 3 Configure the correct COM port setting, depending on the port to which you connected the serial adaptor. The default should usually be COM1.

Connection details



- 4 Configure the port settings as described above in [RS-232 device connection and configuration on page 52](#).

Port settings



- 5 Once connected, press Enter and you should see a response from the machine, such as a session login prompt or the Open Firmware OK prompt. You now have console access.
- 6 You have completed this procedure. If applicable, return to the higher level procedure or task flow that directed you to this procedure.

Configuring remote console access

While terminal server and modems are supported for remote access, Nortel recommends using a terminal server as it is more secure, and console access for both units is readily available and remotely accessible. Nortel does not recommend modems as they are inherently insecure when connected to the PSTN. The customer's security policy must be followed regardless of Nortel recommendations.

To gain remote console access to the T1400/N240, use a terminal server as the RS-232 device. The terminal server allows seamless connections from its LAN connection (TCP/IP protocol), to multiple serial ports (RS-232 protocol) of the console port. Typically, each physical RJ-45 port on the terminal server is assigned to a virtual telnet

port. Once configured, establish a telnet session to the terminal server with a specific telnet port.

Note: Supplying and configuring a terminal server or modems is the customer's responsibility.

Configuring remote console access

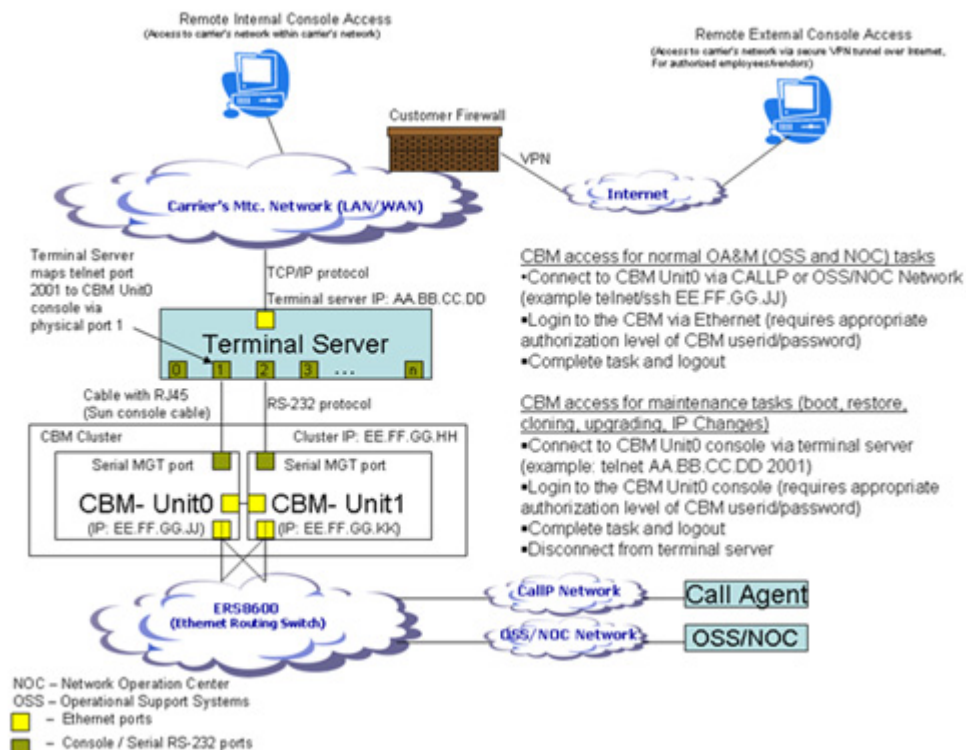
From your workstation

- 1 Connect the unit0 Serial MGT port to the physical RS-232 port 1 of the terminal server, and the unit1 Serial MGT port to the physical RS-232 port 2 of the terminal server.
- 2 If the IP address of the terminal server is AA.BB.CC.DD, and terminal server physical ports 1 and 2 have been configured to telnet ports 2001 and 2002 respectively, then the unit console ports can be accessed directly using telnet.

unit0: telnet AA.BB.CC.DD 2001

unit1: telnet AA.BB.CC.DD 2002

Remote terminal server console access - example network configuration



- 3** Once connected, press Enter and you should see a response from the machine, such as a session login prompt or the Open Firmware OK prompt. You now have console access.
- 4** You have completed this procedure. If applicable, return to the higher level procedure or task flow that directed you to this procedure.



Device Manager upgrade

This procedure enables you to upgrade the Device Manager software. The Device Manager is also called the Java Device Manager. The Device Manager is an SNMP-based graphical user interface (GUI) designed to manage the Ethernet Routing Switch 8600.

If upgrading to a current Device Manager software version, remove the existing version before installing the current Device Manager software. Use the software removal utility that your operating system (for example, Windows, Solaris, HP UNIX, or Linux) supports to remove the existing version of the Device Manager software.

What's new in Device Manager upgrades in SN09U

Feature changes

There are no feature changes in the Device Manager upgrade.

Upgrade paths

Nortel supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U
- SN09U to SN09U

Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade

Time to complete an upgrade

The following table lists the tasks to upgrade Device Manager software and the estimated time to complete each task.

Estimated time to complete a software upgrade

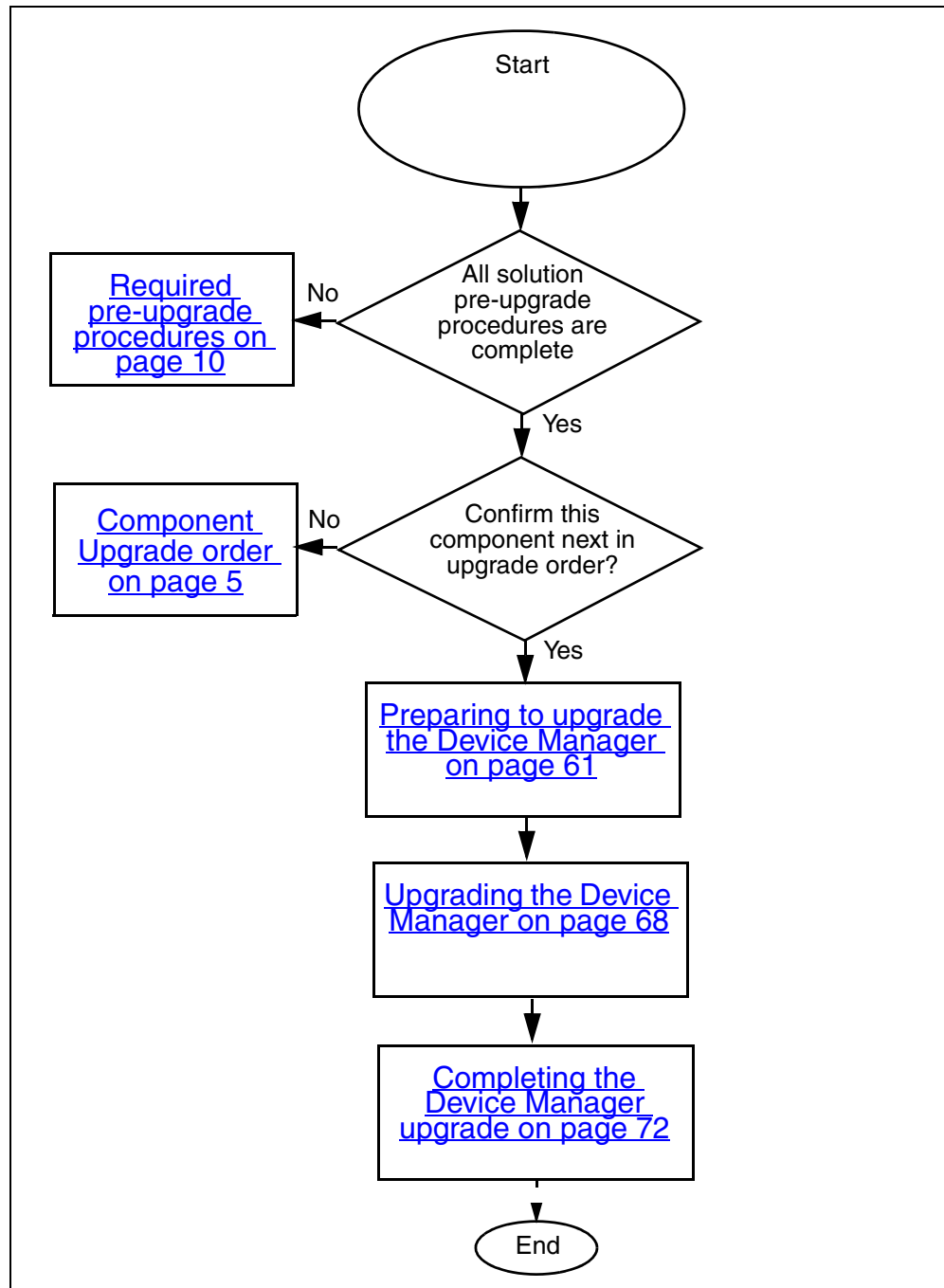
Task	Time
Preparing for the software	10 minutes
Upgrading the software	5 minutes
Completing the upgrade	5 minutes
Total estimated upgrade time	20 minutes
Performing a rollback	20 minutes

Service impacts

The upgrade of Device Manager software does not impact service.

Device Manager upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

Device Manager upgrade tasks

Preparing to upgrade the Device Manager

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

Complete the following tasks:

- [Required pre-upgrade procedures on page 10](#)
- the upgrade of all components that precede the Device Manager in the [Component Upgrade order on page 5](#)

Acquiring Device Manager software

Software for the Device Manager is stored in the Nortel Software Vault. The Software Vault is a repository for maintaining and distributing controlled copies of software loads to Nortel customers.

The Software Vault provides the following benefits:

- version control
- access control
- query and persistency capabilities using a distributed multi-client, multi-server architecture
- transaction control

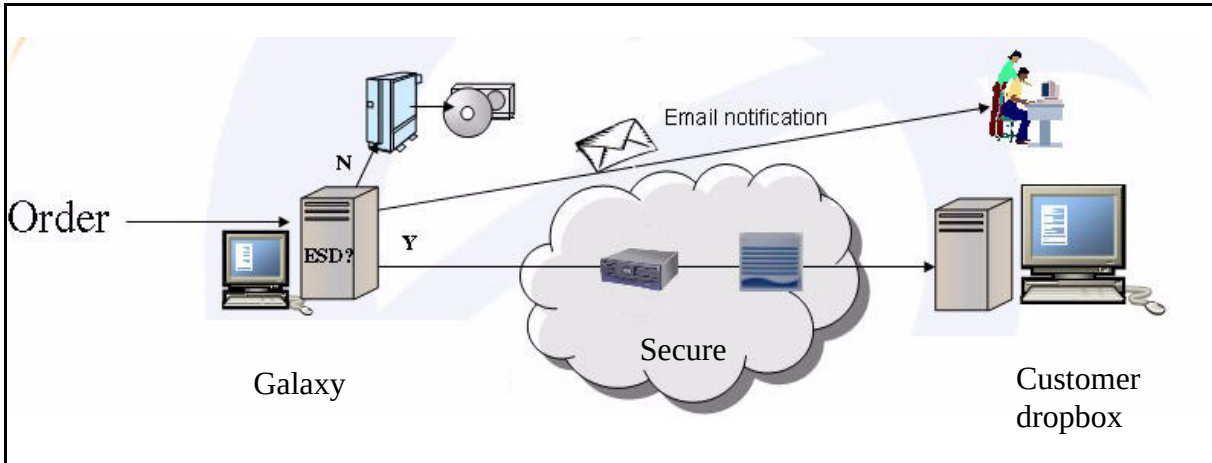
Software delivery methods

Customers receive the Device Manager software either through electronic software delivery (ESD) or manufactured on physical media, such as a compact disk (CD), and couriered to the customer site.

The Galaxy ESD tool accommodates global software delivery using business-to-business processes and automated electronic distribution of Nortel products to customer locations.

The following figure shows a high-level example of how the software is released to the customer site through ESD.

Software order and ESD delivery overview



Galaxy compresses the software file into a tar.gz file for delivery. The file adheres to ESD filenames conventions. The following is an example of the vaulted software load file for the Ethernet Routing Switch 8600:

Example

P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz

where

P86S00X0.X

refers to the ordering code for the Ethernet Routing Switch 8600 software for the SN0X release (this value changes for each release)

V

refers to the product release (V for VO; R for Released)

NCL

refers to the software load type (NCL for non-CM load; MNCL for maintenance non-CM load)

NAP

refers to the processor type

VAULT

refers to the Nortel software repository source

X

refers to the Nortel product repository version (if applicable)

D

refers to the software file format reason (Distribution)

tar

refers to a tarred file

gz

refers to a zipped file

Preparing the software file for an upgrade

Before starting an upgrade on the Ethernet Routing Switch 8600, perform the following software preparative measures:

- Move the software [load] file(s) to the appropriate directory on the CS 2000 Core Manager or the Core and Billing Manager (CBM). If retrieving the software from ESD, the software load file is located in the ESD drop box.

where

P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz

is the software load file

- Unzip and untar the software load file.
- Rename, unzip, and untar the Device Manager file.

where

device_mgr_XXXX_tar.gz.tape

is the Device Manager file

The final destination for the software file is on a personal computer (PC) where the Device Manager application operates, such as a PC in a network operations center.

Action

Perform the following procedures to prepare the component for upgrade.

- [Preparing the ESD version of the Device Manager software for an upgrade on page 64](#)
- [Preparing the CD version of the Device Manager software for an upgrade on page 66](#)

Preparing the ESD version of the Device Manager software for an upgrade

At the workstation

- 1 Select the first step as follows:

If your core manager is a	Do
CS 2000 Core Manager	step 2
CBM	step 5

- 2 Verify that the correct directory path, as shown in the following command, exists on the CS 2000 Core Manager:

```
> cd /swd/sdm/esd
```

If the path	Do
does not exist and the response "not found" displays	step 3
exists	step 5

- 3 Create the directory path.

- a Access the storage level from the CS 2000 Core Manager .

```
# sdmmtc storage
```

- b Add a logical volume in which to store the ESD file.

```
> esdadd
```

The system prompts you to enter a logical volume to be converted to the /swd/sdm/esd standard.

- 4 Ensure that the correct directory path has been accessed.

```
> cd /swd/sdm/esd
```

- 5 Use trivial file transfer protocol (TFTP) or file transfer protocol (FTP) to transfer the software load file as a binary file to the directory appropriate to the core manager platform.

- /swd/sdm/esd (CS 2000 Core Manager)
- /swd (CBM)

Note: Accessing the /swd link using the CBM is equivalent to accessing the /data/swd path.

- 6 Access the directory on the core manager that contains the software load file.

```
> cd /<directory>
```

where

<directory>

is /swd/sdm/esd for the CS 2000 Core Manager, or
/data/swd for the CBM

- 7 Uncompress the software load file.

```
gzip -d P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz
```

- 8 Untar the software load file.

```
tar -xvf P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar
```

The following individual files result from uncompressing and untarring the vaulted software load file and are placed in a new directory:

- device_mgr_XXXX_tar.gz.tape – compressed software file of the Device Manager
- pp8600_XXXX_tar.gz.tape – compressed software file of the Ethernet Routing Switch 8600

where

XXXX

is the release of the software being upgraded

- 9 Access the new directory that contains the individual files.

```
cd /P86S00X0.X.V.NCL.NAP.VAULT.D
```

- 10 Rename and move the Device Manager file for it to be recognizable for uncompression into the directory.

```
mv device_mgr_XXXX_tar.gz.tape  
/swd/device_mgr_XXXX.tar.gz
```

- 11 Reaccess the directory on the core manager that contains the Device Manager software file.

```
> cd /<directory>
```

where

<directory>

is /swd/sdm/esd for the CS 2000 Core Manager, or
/data/swd for the CBM

- 12 Uncompress the Device Manager file.

```
gzip -d device_mgr_XXXX.tar.gz
```

- 13 Untar the Device Manager file to create the files in the appropriate directory structure.

```
tar -xvf device_mgr_XXXX.tar
```

The directory structure for the files is created under the directory path .../dm/XXXX.

where

XXXX

is the new directory to hold the files for this release

The files are prepared for the software upgrade process.

- 14 You have completed this procedure. Proceed to [Upgrading the Device Manager software on page 68](#) to continue with upgrading the Device Manager Software.

Preparing the CD version of the Device Manager software for an upgrade

At the workstation

- 1 Enter the following commands as the root user to set up the directory structures on the core manager into which the Device Manager files are to reside.

```
cd /swd
```

```
mkdir dm
```

```
chmod 755 dm
```

```
cd dm
```

```
mkdir XXXX
```

where

XXXX

matches the new release of the Device Manager software (for example, 5821)

```
chmod 755 XXXX
```

- 2 Select the core manager used in the network configuration.

If the core manager is a	Do
CBM	step 3
CS 2000 Core Manager	step 7

- 3 Insert the CD into the CD drive on the CBM, and access the appropriate CD ROM directories.

```
cd /cdrom/cdrom0
```

- 4 Copy each of the Device Manager software files from the CD into the /swd/dm/XXXX directory of the CBM.
cp * /swd/dm/XXXX/
- 5 Change directory by typing
cd /
- 6 Eject the CD.
eject cdrom
Continue to [step 11](#).
- 7 Insert the CD into the drive of the SPFS-based server that hosts the CS 2000 Management Tools, and access the appropriate CD ROM directories.
cd /cdrom/cdrom0
- 8 Copy each of the Device Manager software files from the CD into a temporary location on the SPFS-based server that hosts the CS 2000 Management Tools.
cp * /tmp/
- 9 Eject the CD.
eject cdrom
- 10 Use TFTP or FTP to transfer each of Device Manager files as binary files from the /tmp directory to the /swd/dm/XXXX directory of the CS 2000 Core Manager.
- 11 Access the directory on the appropriate core manager that contains the Device Manager software files.
cd /swd/dm/XXXX
- 12 Change the access permissions on all the files in the directory.
chmod 755 *
- 13 You have completed this procedure. Proceed to [Upgrading the Device Manager software on page 68](#) to continue with upgrading the Device Manager Software.

Upgrading the Device Manager

The following procedure provides the steps to upgrade this component. Refer to *Installing and Using Device Manager*, Part No. 316341-B, within this Solution documentation collection for information on system requirements for installing Device Manager software in a Windows PC or Solaris/Unix environment.

Prerequisites

Complete the following tasks:

- [Preparing to upgrade the Device Manager on page 61](#)

Action

Upgrading the Device Manager software

At the Windows PC or Unix workstation where the Device Manager is run

- 1 Use procedure [Transferring a file to your workstation on page 2590](#), to FTP the Device Manager software load from the appropriate core manager to the Solaris or Unix workstation or Windows PC on which the Device Manager is to be upgraded.
- 2 Use the following table to determine the next step.

If installing Device Manager software on	Do
a Windows PC	step 3
a Solaris/Unix machine	step 20
- 3 Select Start->Settings->Control Panel->Add/Remove Programs
- 4 From the list of currently installed programs, select Java Device Manager and click on Change/Remove.
The Uninstall Java Device Manager dialog appears. Click Uninstall.
- 5 Click Done. Close the Add/Remove Programs window when complete.
- 6 Navigate to the directory on your system where you moved the Device Manager software.
- 7 Double-click the jdm_XXXX.exe file.
An install screen opens, followed by a Nortel dialog box. Then, the Introduction dialog box appears.

- 8 Click Next to continue the installation process.
The License Agreement dialog box opens.
- 9 Click I accept the terms of the license agreement.
- 10 Click Next to continue the installation process.
- 11 Do one of the following:
 - Select Typical installation to install the common set features, as well as online help.
 - Select Minimal installation to select minimal features to install (recommended for those with limited disk space)
 - Select Help to install only the online help.
 - Select Custom installation to customize the features prior to installation. Click Next. The Choose Install Set dialog box opens.
- 12 Click Next. The Choose Install Folder dialog box opens.
- 13 Click Restore Default Folder or click Choose to select the storage path.
- 14 Click Next. The Choose Shortcut Folder dialog box opens.
- 15 Select a shortcut path, if desired.
- 16 Click Next. The Pre-Installation Summary dialog box opens.
- 17 Verify the folder, shortcut, and disk space required to install the software. Use the Previous button to return to the appropriate dialog box to make changes.
- 18 Click Install. When the installation is complete, the Install Complete dialog box opens.
- 19 Click Done to exit the installation. Go to step [35](#).
- 20 Close all programs. Observe the following for the operating system on which the JDM software is to be installed.

Note 1: Java Device Manager installation procedures are now standardized across all platforms. In addition, the required Java Runtime Environment (JRE) (version 1.4.1) is now part of the JDM installation package and does not require a separate installation. The bundled JRE is used with this JDM only and should not affect other JAVA applications on the same system.

Note 2: For Solaris and HP-UX, certain OS patches are required for JDM/JRE to function properly. Consult SUN or HP to install the appropriate OS patches before launching JDM.

- 21 Navigate to the directory on your system where you loaded the Device Manager software.
- 22 Make the file executable by typing
 - for Solaris environment

```
chmod a+x dm_XXXX_solaris_sparc.sh
```
 - for HP-UX environment

```
chmod a+x jdm_XXXX_hpux_pa-risc.sh
```
- 23 Run the executable
 - for Solaris environment

```
dm_XXXX_solaris_sparc.sh
```
 - for HP-UX environment

```
jdm_XXXX_hpux_pa-risc.sh
```

An install screen, followed by a Nortel dialog box opens. Then, the Introduction dialog box appears.
- 24 Click Next to continue the installation process. The License Agreement dialog box opens.
- 25 Click I accept the terms of the license agreement.
- 26 Click Next. The Choose Install Set dialog box opens.
- 27 Do one of the following:
 - Select Typical installation to install the common set features, as well as online help.
 - Select Minimal installation to select minimal features to install (recommended for those with limited disk space).
 - Select Help to install only the online help.
 - Select Custom installation to customize the features prior to installation
- 28 Click Next. The Choose Install Folder dialog box opens.
- 29 Click Restore Default Folder or click Choose to select the storage path.
- 30 Click Next. The Pre-Installation Summary dialog box opens
- 31 Verify the folder and disk space required to install the software. Use the Previous button to return to the appropriate dialog box to make changes.
- 32 Click Install. The installation process begins

- 33** When the installation is complete, the Install Complete dialog box opens.
- 34** Click Done to exit the installation. The Device Manager is now completely installed on your machine.
- 35** Refer to document *Installing and Using Device Manager*, Part No. 316341-B, within this Solution documentation collection for more information on configuring and managing the Java Device Manager software.
- 36** You have completed this procedure. Proceed to [Completing the Device Manager upgrade on page 72](#).

Completing the Device Manager upgrade

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

Complete the following tasks:

- [Upgrading the Device Manager on page 68](#)

Action

Completing the Device Manager upgrade

At the workstation

1

If you installed from	Do
ESD	step 3
CD	step 2

2 Delete the following files after the upgrade has been completed successfully:

- all files in the original directory on the corresponding core manager
- software load file in the /tmp directory on the SPFS-based server that is hosting the CS 2000 Management Tools (applies just to the CS 2000 Core Manager)

3 You have completed this procedure. Return to [Component Upgrade order on page 5](#) that directed you to this procedure.



Ethernet Routing Switch 8600 software for the CS-LAN upgrade

This procedure upgrades the Nortel Ethernet Routing Switch 8600 (formerly known as "Passport 8600") software on routers that support the Communication Server LAN (CS-LAN).

ATTENTION

Nortel urges users of this component upgrade to read thoroughly this Introduction, especially [Important upgrade considerations](#), before attempting the upgrade procedure.

ATTENTION

The GUI/HMI graphics that support this procedure are current as of (I)SN09U. Although these illustrations differ from the GUI/HMI you are using, perform all stepwise actions by accessing your element managers and making the equivalent choices.

ATTENTION

This upgrade procedure causes alarms to occur on CS-LAN components. These alarms report the loss of certain redundant paths during the upgrade process. These losses are not service affecting and the paths are restored on completion of the upgrade.

What's new in Ethernet Routing Switch 8600 software for the CS LAN Upgrades in (I)SN09U

Feature changes

Added steps addressing the Border Control Point 7100, whereby the portal must be shut down gracefully to prevent it from accepting service requests during an Ethernet Routing Switch 8600 upgrade.

Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U
- SN09U to SN09U

Supported solutions

The Ethernet Routing Switch 8600 Software Upgrade and Rollback (CS-LAN) procedures apply to all IP and ATM solutions, unless specified otherwise. One exception is the PT-AAL1 solution, in which the Ethernet Routing Switch 8600 does not carry call processing traffic. The PT-AAL1 solution includes the use of just the following Carrier VoIP components:

- Dynamic Packet Trunking (DPT) Spectrum Peripheral Modules (SPM)
- Interworking Spectrum Peripheral Modules (IW SPM)
- Multi-service Gateway 4000 (MG 4000)

Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade

Time to complete an upgrade

The following table lists the tasks to upgrade Ethernet Routing Switch 8600 software and the estimated time to complete each task.

Estimated time to complete a software upgrade

Task	Application	Time
Preparing for the upgrade	Verifying parameters settings Verifying sufficient space exists in directories /flash and /pcmcia Preparing software for upgrade Checking connectivity between XA-Core and HIOP Perform upgrade pre-checks Perform backups	45-60 minutes
Upgrading the software (depends on the number of GWC and SCs)	Splitting the CS-LAN into active and standby sides Disabling GWCs that subtend the slave Ethernet Routing Switch 8600 Locking the inactive Shelf Controller (SC) blade connected to Chassis N Upgrading the Ethernet Routing Switch 8600	30 minutes 5 minutes per Ethernet Routing Switch 8600 2 minutes per GWC 2 minutes per SC 5 minutes
Completing the upgrade		5 minutes
Total estimated upgrade time		1 hour 35 minutes
Performing a rollback		1 hour 35 minutes

Service impacts

The upgrade of Ethernet Routing Switch 8600 software does not impact service.

Prerequisites

Make sure a TFTP server is available. The CPU of each 8600 being upgraded must have console port access. In case there are two CPUs in each 8600, each CPU must have separate console port access.

If your network contains any Border Control Point 7100s directly connected to the Ethernet Routing Switch 8600s being upgraded, ensure that direct connectivity has been established according to the instructions in bulletin SEB-08-01-009.

Important upgrade considerations

Ensure that you read thoroughly and understand the following points prior to beginning this software upgrade procedure.

- Note any existing alarms before executing this software upgrade. Once the upgrade is completed, verify that no additional alarms have been raised.
- Review the network typology or Office Records to determine if the Ethernet Routing Switch 8600 is configured in high availability (HA) mode and if routing protocol OSPF or BGP is enabled. This information will be needed during the upgrade process.
- Refer to section [Text conventions on page 77](#) for brief descriptions and examples of filenames that appear in commands throughout this procedure. That section also includes descriptions for distinguishing between the master and standby CPUs in the command line interface (CLI).
- Execute all CPU-related commands on the master CPU in a dual-CPU configuration, except where otherwise noted.

Note: If your configuration involves a dual CPU, ensure you have access to both CPUs independently (that is, one established connection to each CPU).

- Note that the Universal Signaling Point-sdf (USP-Compact) is addressed in this upgrade and the corresponding “Rolling Back the Ethernet Routing Switch 8600 Software for the CS-LAN”

procedures. However, no specific steps addressing the Universal Signaling Point (USP) are required in these procedures.

- Refer to [Rolling back the Ethernet Routing Switch 8600 software for CS-LAN on page 2523](#) for the procedure on rolling back software for the Ethernet Routing Switch 8600

**CAUTION****Potential network services disruption**

To avoid network services disruption when upgrading the call processing unit (CPU) memory of an Ethernet Routing Switch 8600, perform the memory upgrade only when indicated in this procedure. At this point, all traffic has been migrated to the other Ethernet Routing Switch 8600 chassis before the CPU is powered down for the memory upgrade.

Text conventions

This briefly describes text conventions for displaying filenames that appear in commands throughout this procedure.

Note: Refer to this section, as needed throughout the course of the upgrade and rollback procedures, for clarifications on the different software files.

<a.b.c.d>

is the IP address of the TFTP server

<bootbkup>

is the name of the backup copy of the boot configuration file on the PCMCIA card

<cfgbkup>

is the name of the backup copy of the software configuration file on the PCMCIA card

<new3DES>

is the name of the new Triple data encryption standard (3DES) file on the PCMCIA card

for example:

p80cxxxx.img

where:

xxxx is the release number

<newATM>

is the name of the new ATM load file on the PCMCIA card

for example:
p80txxxx.dld

where:
xxxx is the release number of the load

<newboot>

is the name of the new boot monitor image file on the PCMCIA card

for example:
p80bxxxx.img

where:
xxxx is the release number of the load (for example,
p80b37130.img)

Note: Use the boot monitor image file when executing a boot command.

<newDES>

is the name of the new data encryption standard (DES) file on the PCMCIA card

for example:
p80cxxxx.des

where:
xxxx is the release number

<newPOS>

is the name of the new data encryption standard (POS) file on the PCMCIA card

for example:
p80cxxxx.pos

where:
xxxx is the release number

<newload>

is the name of the new software image file on the PCMCIA card

for example:
p80axxxx.img

where:
xxxx is the version of the software (for example, p80a3320)

Note: Use the primary or secondary (or both) software image files when configuring a bootconfig command.

<old3DES>

is the name of the original DES file

for example:
p80cxxxx.img

where:
xxxx is the release number

<oldATM>

is the name of the original ATM load file

for example:
p80txxxx.dld

where:
xxxx is the release number of the load

<oldboot>

is the name of the original boot monitor image file

for example:
p80bxxxx.img

where:
xxxx is the release number of the load (for example,
p80b37130.img)

<oldDES>

is the name of the original DES file

for example:
p80cxxxx.des

where:
xxxx is the release number

<oldload>

is the name of the original software image file

for example:
p80axxxx.img

where:
xxxx is the version of the software (for example, p80a37130)

<slot>

is the slot number for the Ethernet Routing Switch 8600

<sonetif >

is the Sonet interface on the ATM blade

<swloadbkup>

is the name of the backup version of the software image file

for example:
p80axxxx.img

where:

xxxx is the version of the software (for example, p80a37130)

<vid>

is the identifier of each virtual local area network (VLAN)

<vrid>

is the VRRP identifier

CPU syntax

The CLI prompt syntax for the CPUs is as follows:

<Ethernet_Routing_Switch_8600_chassis_name>:CPU-slot#

where:

the absence or inclusion of the “@” symbol at the beginning of the command syntax identifies the master or slave CPU, respectively.

8600_04:5#

refers to the master CPU, IP address is typically 127.0.0.5

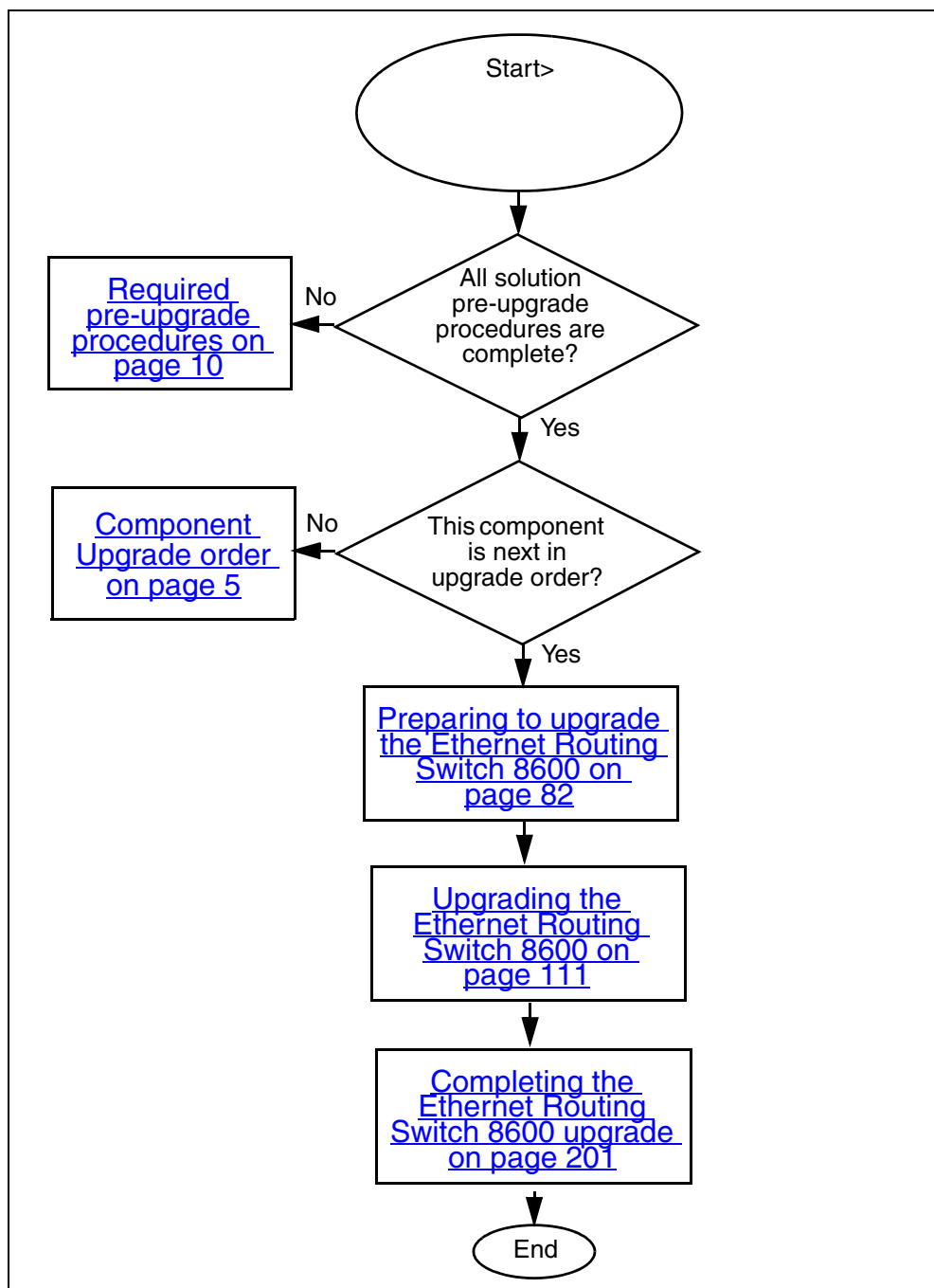
@8600_04:6#

refers to the standby CPU, IP address is typically 127.0.0.6

Note: This syntax applies only when dual CPUs are configured on a per Ethernet Routing Switch 8600 chassis basis

Ethernet Routing Switch 8600 upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

Ethernet Routing Switch 8600 upgrade tasks

Preparing to upgrade the Ethernet Routing Switch 8600

The following procedure provides the steps you need to execute prior to upgrading the Ethernet Routing Switch 8600. Where applicable, a reference to the procedure that contains the detailed steps is provided.

Prerequisites

You have completed the following tasks:

- all [Preparing to upgrade the Carrier Voice over IP Network on page 9](#)
- the upgrade of all components that precede the component in the [Component Upgrade order on page 5](#)

Determine if any Carrier Voice over IP-specific Release Notes are available on the software CD. Use the Release Notes to identify any changes or deviations from the upgrade procedure or any pre- or post-upgrade requirements.

Acquiring Ethernet Routing Switch 8600 software for the CS-LAN

Software for the Ethernet Routing Switch 8600 is stored in the Nortel Software Vault. The Software Vault is a repository for maintaining and distributing controlled copies of software loads to Nortel customers.

The Software Vault provides the following benefits:

- version control
- access control
- query and persistency capabilities using a distributed multi-client, multi-server architecture
- transaction control

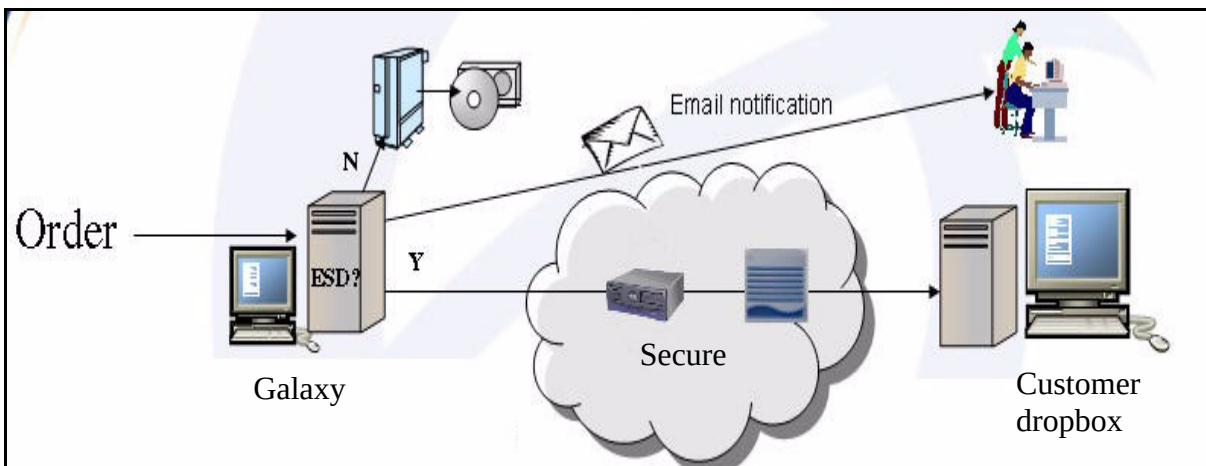
Software delivery methods

Customers receive the Ethernet Routing Switch 8600 software either through electronic software delivery (ESD) or manufactured on physical media, such as a compact disk (CD), and couriered to the customer site.

The Galaxy ESD tool accommodates global software delivery using business-to-business processes and automated electronic distribution of Nortel products to customer locations.

The following figure shows a high-level example of how the software is released to the customer site through ESD.

Software order and ESD delivery overview



Galaxy compresses the software file into a tar.gz file for delivery. The file adheres to ESD filenames conventions. The following is an example of the vaulted software load file for the Ethernet Routing Switch 8600:

Example

P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz

where

P86S00X0.X

refers to the ordering code for the Ethernet Routing Switch 8600 software for the SN0X release (this value changes for each release)

V

refers to the product release (V for VO; R for Released)

NCL

refers to the software load type (NCL for non-CM load; MNCL for maintenance non-CM load)

NAP

refers to the processor type

VAULT

refers to the Nortel software repository source

X

refers to the Nortel product repository version (if applicable)

D

refers to the software file format reason (Distribution)

tar

refers to a tarred file

gz

refers to a zipped file

Preparing the software file for an upgrade

Before starting an upgrade on the Ethernet Routing Switch 8600, perform the following software preparative measures:

- Move the Ethernet Routing Switch 8600 software [load] file(s) to the appropriate directory on the CS 2000 Core Manager or the Core and Billing Manager (CBM). If retrieving the software from ESD, the software load file is located in the ESD drop box.

where

P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz

is the software load file

- Unzip and untar the software load file.

The final destination for the Ethernet Routing Switch 8600 software file is the /flash/ directory on the Ethernet Routing Switch 8600.

ATTENTION

The file must be copied to the /flash/ directory in lower case.

Server types

This procedure provides the high-level steps to prepare to upgrade the following server types:

- Ethernet Routing Switch 8600 Router – Chassis 8010co

Action

Perform the following procedure to prepare the Ethernet Routing Switch 8600 for upgrade.

Preparing to upgrade the Ethernet Routing Switch 8600

- 1 Perform procedure [Verify parameters settings on page 86](#)
- 2 Perform procedure [Verifying sufficient space exists in directories /flash and /pcmcia on page 88](#)
- 3 Depending on whether you receive software from CD or ESD, perform one of the following procedures:
 - [Preparing the CD version of the Ethernet Routing Switch 8600 software for an upgrade on page 90](#)
 - [Preparing the ESD version of the Ethernet Routing Switch 8600 software for an upgrade on page 93](#)
- 4 Perform procedure [Checking connectivity between the XA-Core and HIOP and the Ethernet Routing Switch 8600 on page 96](#)
- 5 Perform procedure [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#)
- 6 Perform procedure [Performing Ethernet Routing Switch 8600 backups on page 107](#)
- 7 You have completed this high level activity.

Verify parameters settings

At the Ethernet Routing Switch 8600 CLI

- 1 Based on your configuration, telnet or directly connect and log into the console port of the CPU of the Ethernet Routing Switch 8600. If the Ethernet Routing Switch 8600 has dual CPUs, a separate logon is required for each CPU.
- 2 Use the following table to determine the next step.

If the Ethernet Routing Switch	Do
has dual CPUs and HA is not required	step 3
does not have dual CPUs	step 4

- 3 Determine the status of the savetostandby flag by typing
config bootconfig flags info
 or
sho boot config
 If the flag is disabled, on the master CPU, enable the flag by typing
config bootconfig flags savetostandby true

4



CAUTION

Potential loss of configuration

Before performing an upgrade and saving the bootconfig file, disable the bootconfig verify-config flag setting. Failure to observe this action can result in loss of configuration.

Note: Ensure the parameters settings are verified on each individual node and CPU.

Verify that the bootconfig is set to false by typing

config bootconfig flags verify-config false

- 5 Verify the timer for a single CPU is set for 2 seconds by typing
config sys set smlt-on-single-cp enable timer 2

- 6 This procedure is complete. Proceed to [Verifying sufficient space exists in directories /flash and /pcmcia on page 88](#) to continue with preparing for the Ethernet Routing Switch 8600 upgrade.

Verifying sufficient space exists in directories /flash and /pcmcia***At the Ethernet Routing Switch 8600 CLI***

- 1 Prior to starting the CS-LAN upgrade, sufficient space must be available in /flash and /pcmcia directories. To list the files in /flash or /pcmcia directories and identify the available space, type

dir

A sample output of the dir command follows:

```
ERS8600-C1:5# dir
size date time name
-----
59582 MAY-17-2006 12:24:50 /flash/config.cfg
5803006 MAR-24-2006 20:13:58 /flash/p80a37130.img
755719 MAR-24-2006 20:14:24 /flash/p80b37130.img
49996 MAR-24-2006 20:14:40 /flash/p80c37130.img
8581 FEB-27-2006 16:44:02 /flash/p80c3724.des
2048 FEB-08-2006 22:35:40 /flash/.ssh <DIR>
588 FEB-08-2006 22:35:40 /flash/.ssh/dsa_pub.key
8581 MAR-24-2006 20:14:54 /flash/p80c37130.des
total: 15297536 used: 6688101 free: 8609435 bytes
size date time name
-----
1071381 MAY-18-2006 19:01:44 /pcmcia/clilog.txt
59582 MAY-17-2006 12:24:50 /flash/config.cfg
5803006 MAR-24-2006 20:13:58 /flash/p80a37130.img
755719 MAR-24-2006 20:14:24 /flash/p80b37130.img
49996 MAR-24-2006 20:14:40 /flash/p80c37130.img
8581 FEB-27-2006 16:44:02 /flash/p80c3724.des
2048 FEB-08-2006 22:35:40 /flash/.ssh <DIR>
588 FEB-08-2006 22:35:40 /flash/.ssh/dsa_pub.key
8581 MAR-24-2006 20:14:54 /flash/p80c37130.des
total: 64405504 used: 15337472 free: 49068032 bytes
```

- 2 Observe the available space in response to the dir command. Ensure that at least 7 MBytes (7000000 bytes) is available in both the /flash and /pcmcia directories. If less than 7 MB is available, consult with your next level of support about deleting old image (.img), log (.txt), pcap (.cap), or bootconfig files.

3 Use the following table to determine the next step.

If	Do
sufficient space exists on /flash or PCMCIA	step 6
files must be removed to make space available on /flash or PCMCIA	step 4

4 To delete the previous files, excluding the current image files, from the /flash directory, type

remove /flash/<filename>

where

filename

is the name of the old image, log or bootconfig file, for example, p80axxxx.img and p80bxxxx.img, where xxxx is the version of the software

5 To delete the previous files, excluding the current image files, from the /pcmcia directory, type

remove /pcmcia/<filename>

where

filename

is the name of the old image, log, or bootconfig file, for example, p80axxxx.img and p80bxxxx.img, where xxxx is the version of the software

6 If this is a dual CPU configuration, verify the space available on /flash and /pcmcia on the slave CPU. If the files must be removed from the slave CPU, go to step [4](#).

7 This procedure is complete. Return to the procedure that sent you here or perform one of the following procedures, depending on whether you receive software from CD or ESD:

- [Preparing the CD version of the Ethernet Routing Switch 8600 software for an upgrade on page 90](#)
- [Preparing the ESD version of the Ethernet Routing Switch 8600 software for an upgrade on page 93](#)

Preparing the CD version of the Ethernet Routing Switch 8600 software for an upgrade

At the workstation

- 1 On the core manager (CBM or SDM), as the root user, type
cd /swd
- 2 List the contents of the swd directory to determine if the directory for the new software release already exists. If so, proceed to step [4](#); otherwise, continue.

ls

- 3 Set up the directory structures on the core manager where the new Ethernet Routing Switch 8600 files are to reside.

mkdir pp8600

chmod 755 pp8600

cd pp8600

mkdir XXXX

where

XXXX

matches the new release of the Ethernet Routing Switch 8600 software (for example, 37130)

- 4 Select the next step as follows:

If the core manager is a	Do
CBM	step 5
SDM/CS 2000 Core Manager	step 9

- 5 Insert the CD into the CD drive on the active CBM, and enter the following command to access the appropriate CD ROM directories.

cd /cdrom/cdrom0

- 6 Copy each of the Ethernet Routing Switch 8600 software files from the CD into the /swd/pp8600/XXXX directory of the active CBM. The software files to be copied are

- p80axxxx.img
- p80bxxxx.img
- p80cxxxx.des
- p80cxxxx.img

- p80pxxxxx.dld (only copied if POS IO modules are present)
- p80txxxxx.dld (only copied if ATM IO modules are present)

Enter the following command to copy the file onto the system in lower case.

```
cp <filename> /swd/pp8600/XXXX/<new_filename>
```

where

filename

is the name of the file to copy

new_filename

is the name of the copied file in lower case

XXXX

matches the new release of the Ethernet Routing Switch 8600 software (for example, 37130)

Note: Ensure the files were copied successfully by listing the directory on the remote device where the files came from, and on the local device to which the files were copied and compare the file sizes.

- 7 Change directory by typing

```
cd /
```

- 8 Enter the following command to eject the CD.

```
eject /cdrom
```

Proceed to [step 13](#).

- 9 Insert the CD into the drive of the SPFS-based server that is hosting the CS 2000 Management Tools, and enter the following command to access the appropriate CD ROM directories.

```
cd /cdrom/cdrom0
```

- 10 Enter the following command to copy each of the Ethernet Routing Switch 8600 software files from the CD into a temporary location on the SPFS-based server that is hosting the CS 2000 Management Tools. Copy the file onto the system in lower case.

```
cp <filename> /tmp/<new_filename>
```

where

filename

is the name of the file to copy

new_filename

is the name of the copied file in lower case

Use TFTP or FTP to transfer each of Ethernet Routing Switch 8600 files as binary files from the /tmp directory to the /swd/pp8600/XXXX directory of the CS 2000 Core Manager.

XXXX

matches the new release of the Ethernet Routing Switch 8600 software (for example, 37130)

Note: Ensure the files were copied successfully by listing the directory on the remote device where the files came from, and on the local device to which the files were copied and compare the file sizes.

- 11 Enter the following command to eject the CD.

eject cdrom

- 12 Refer to [Using FTP on page 2590](#) for information on using FTP.

- 13 Enter the following command to access the directory on the appropriate core manager that contains the Ethernet Routing Switch 8600 software files.

cd /swd/pp8600/XXXX

- 14 Enter the following command to change the access permissions on all the files in the directory.

chmod 755 *

- 15 This procedure is complete.

If configured with an XA-Core, proceed to procedure [Checking connectivity between the XA-Core and HIOP and the Ethernet Routing Switch 8600 on page 96](#).

Otherwise, continue to [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#) to upgrade the Ethernet Routing Switch 8600 software for the CS-LAN.

Preparing the ESD version of the Ethernet Routing Switch 8600 software for an upgrade

At the workstation

- 1 Select the first step as follows:

If your core manager is a	Do
SDM/CS 2000 Core Manager	step 2
CBM	step 5

- 2 Enter the following command to ensure the correct directory path exists on the SDM/CS 2000 Core Manager.

```
> cd /swd/sdm/esd
```

If the path	Do
does not exist and the response "not found" displays	step 3
exists	step 5

- 3 Create the directory path.

- a Enter the following command to access the storage level from the SDM/CS 2000 Core Manager.

```
# sdmmtc storage
```

- b Enter the following command to add a logical volume in which to store the ESD file.

```
> esdadd
```

The system prompts you to enter a logical volume to be converted to the /swd/sdm/esd standard.

- 4 Enter the following command to ensure the correct directory path has been accessed.

```
> cd /swd/sdm/esd
```

- 5 Use trivial file transfer protocol (TFTP) or file transfer protocol (FTP) to transfer the software load file as a binary file to the directory according to the core manager platform. Refer to [Using FTP on page 2590](#) for information on using FTP.

- /swd/sdm/esd (CS 2000 Core Manager)
- /swd (CBM)

Note: Accessing the /swd link on the CBM is equivalent to accessing the /data/swd path.

- 6 Enter the following command to access the directory on the core manager that contains the software load file.

```
cd /<directory>
```

where

```
<directory>
```

is /swd/sdm/esd for the SDM/CS 2000 Core Manager, or
/data/swd for the CBM

- 7 Enter the following command to uncompress the software load file.

```
gzip -d P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar.gz
```

- 8 Enter the following command to untar the software load file.

```
tar -xvf P86S00X0.X.V.NCL.NAP.VAULT.X.D.tar
```

- 9 Enter the following command to access the new directory that contains the individual files.

```
cd /P86S00X0.X.V.NCL.NAP.VAULT.D
```

- 10 Move the tar.gz file so it will recognize the command to uncompress the file.

```
mv pp8600_XXXXX.tar.gz.tape  
/swd/pp8600_XXXXX.tar.gz
```

- 11 Enter the following command to re-access the directory on the core manager that contains the Ethernet Routing Switch 8600 software file.

```
cd /swd
```

- 12 Enter the following command to uncompress the Ethernet Routing Switch 8600 file.

```
gzip -d pp8600_XXXX.tar.gz
```

- 13 Enter the following command to untar the Ethernet Routing Switch 8600 file to create the files in the appropriate directory structure.

```
tar -xvf pp8600_XXXX.tar
```

The directory structure for the files is created under the directory path .../pp8600/XXXX.

where

```
XXXX
```

is the new directory to hold the files for this release

The files are prepared for the software upgrade process, and this procedure is complete.

Note: Delete the following files after the upgrade has been completed successfully:

- all files in the original directory on the core manager
- software load file in the /tmp directory on the CS 2000 Management Tools server (applies just to the CS 2000 Core Manager)

14 This procedure is complete.

If configured with an XA-Core, proceed to procedure [Checking connectivity between the XA-Core and HIOP and the Ethernet Routing Switch 8600 on page 96](#).

Otherwise, continue to [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#) upgrade the Ethernet Routing Switch 8600 software for the CS-LAN.

Note: It is important to check that the IOP, HIOP, or HCMICs connections are wired properly to the Ethernet Routing Switch 8600s because disabling the wrong links could isolate the Communication Server.

Checking connectivity between the XA-Core and HIOP and the Ethernet Routing Switch 8600

At the workstation

- 1 Log on to the SDM/CBM server (using telnet) and access the Core by typing.

telnet CM

- 2 Open table CMIPADDR by typing

table CMIPADDR

- 3 Display all tuples in the table by typing

lis all

A sample output of the CMIPADDR table follows.

```

TOP
KEY DATA
-----
GATEWAY 0 GW (192 168 0 1) 0
CMHOST 0 HOST (192 168 2 28) 22 0
CMHOST 1 HOST (192 168 2 29) 22 0
ETHRLNK 1 ETHR 15 REAR NONE (192 168 2 25) 22 (192 168 2 31) 22
(192 168 0 2) 0
ETHRLNK 4 ETHR 4 REAR NONE (192 168 2 24) 22 (192 168 2 30) 22 (192 168 0 3)
0
BOTTOM

```

- 4 Record the Physical IP address of each Ethernet connection.
 - IOPs have four entries - ETHR 15 REAR, ETHR 6 REAR, ETHR 13 REAR, and ETHR 4 REAR
 - HIOPs/HCMICs have two entries - ETHR 4 REAR and ETHR 15 REAR.

Each entry has two Physical IP addresses and one Gateway address. The Gateway address is the last column in table CMIPADDR.

Use the following table to record the Physical IP addresses.

XA-Core Ethernet Connection				
Slot (such as ETHR 5)	First IP address	Second IP address	Connected to which 8600 (N=0 or N=1)	Third IP address

- 5 Log into Ethernet Routing Switch 8600, chassis 0 and execute the following commands for the first row entries from the table in step [4](#):

```
ping <First_IP_address>
```

```
ping <Second_IP_address>
```

```
show ip arp info <First_IP_address>
```

```
show ip arp info <Second_IP_address>
```

If these IP addresses cannot be found in the ARP table, contact your next level of support for help in identifying the connections.

A sample output from the ARP table follows.

```
CSLAN-00:6# show ip arp info 192.168.2.25
```

```
=====
                                Ip Arp
=====
IP_ADDRESS      MAC_ADDRESS      VLAN  PORT      TYPE      TTL(10 Sec)
-----
192.168.2.25    00:60:38:87:ff:b9    10    4/1    DYNAMIC    401
```

```
1 out of 265 ARP entries displayed
```

```
CSLAN-00:6# show ip arp info 192.168.2.31
```

```
=====
                                Ip Arp
=====
IP_ADDRESS      MAC_ADDRESS      VLAN  PORT      TYPE      TTL(10 Sec)
-----
192.168.2.31    00:60:38:87:ff:b9    10    4/1    DYNAMIC    2160
```

```
1 out of 265 ARP entries displayed
```

```
CSLAN-00:6# show ip arp info 192.168.2.24
```

```
=====
                                Ip Arp
=====
IP_ADDRESS      MAC_ADDRESS      VLAN  PORT      TYPE      TTL(10 Sec)
-----
192.168.2.24    00:11:f9:e7:10:fc    10    MLT 1    DYNAMIC    1065
```

```
1 out of 244 ARP entries displayed
```

```
CSLAN-00:6# show ip arp info 192.168.2.30
```

```
=====
                                Ip Arp
=====
IP_ADDRESS      MAC_ADDRESS      VLAN  PORT      TYPE      TTL(10 Sec)
-----
192.168.2.30    00:11:f9:e7:10:fc    10    MLT 1    DYNAMIC    2160
```

```
1 out of 245 ARP entries displayed
```

Check the PORT column of the command output above to see if it lists a specific port (for example, 2/1) or shows “MLT”. Entries with a specific port value are directly connected to this chassis (chassis 0). Entries with “MLT” in the PORT column are connected to Ethernet Routing Switch 8600, chassis 1. In the table in step 4, record which Ethernet Routing Switch 8600 chassis each IP address is connected to.

- 6 Repeat step [5](#) for each row in the table in step [4](#).
- 7 Execute the following command on each Ethernet Routing Switch 8600 chassis:

show vlan info ip

The third IP address in each row of the table in step [4](#) should be a VLAN IP address in the output of this command. Also, each third IP address should reside on the same chassis as the first and second IP addresses on the same table row. If either of these conditions is not met, contact your next level of support.

A sample output of the show vlan info ip command follows.

Vlan Ip						
VLAN ID	IP ADDRESS	NET MASK	BCASTADDR FORMAT	REASM MAXSIZE	ADVERTISE WHEN_DOWN	DIRECTED BROADCAST
4	47.142.116.66	255.255.255.0	ones	1500	disable	enable
10	192.168.0.2	255.255.252.0	ones	1500	disable	enable
11	192.168.7.2	255.255.255.0	ones	1500	disable	enable
12	192.168.8.2	255.255.255.0	ones	1500	disable	enable
13	192.168.9.2	255.255.255.0	ones	1500	disable	enable
14	192.168.10.2	255.255.255.224	ones	1500	disable	enable

- 8 Proceed to [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#) to upgrade the Ethernet Routing Switch 8600 software for the CS-LAN.

Performing Ethernet Routing Switch 8600 upgrade pre-checks

With reference to documentation supporting your CS-LAN (contact your system administrator if necessary), review your CS-LAN topology as follows:

- 1 Verify all unit 0 network elements subtend Ethernet Routing Switch 8600 Chassis 0, and all unit 1 network elements subtend Ethernet Routing Switch 8600 Chassis 1.

Note 1: If your CS-LAN does not conform with this topology, take local variations into account as you perform this procedure.

Note 2: The following table defines the Ethernet Routing Switch 8600 master/slave conventions throughout this procedure.

Iteration		Comment
First Pass	N = 1	Chassis 1 Master
Second Pass	N = 2	Chassis 0 Master

- 2 Check the Nortel website for any bulletins, release notes, and revisions that relate to this procedure.

Use the Ethernet Routing Switch 8600 CLI to verify Ethernet Routing Switch 8600 initial conditions:

- 3 To verify all subtending links and nodes, capture supplemental router port statistics by typing
sho port error extended
Review the output for the extended port error command (see the following figure).

C:\WINNT\system32\telnet.exe

SCS P8600-0:5# sho port error extended

```
=====
Port Ethernet Error Extended
=====
```

PORT NUM	MAC_RX ERRORS	MAC_TX ERRORS	DIFFER TX	PACKET ERRORS	LINK INACTIU	UNKNOWN PROTOS	IN FLWCTRL	OUT FLWCTRL
1/1	30	0	541	0	0	0	0	0
1/2	30	0	507778	0	0	0	0	0
1/3	2	0	111	0	0	0	0	0
1/4	0	0	0	0	0	0	0	0
1/5	2	0	10	0	0	0	0	0
1/6	0	0	2	0	0	0	0	0
1/7	0	0	0	0	0	0	0	0
1/8	0	0	0	0	0	0	0	0
1/9	0	0	2976	0	0	0	0	0
1/10	0	0	0	0	0	0	0	0
1/11	0	0	0	0	0	0	0	0
1/12	0	0	0	0	0	0	0	0
1/13	0	0	0	0	0	0	0	0
1/14	0	0	0	0	0	0	0	0
1/15	3	0	10113	0	0	0	0	0
1/16	0	0	0	0	0	0	0	0
1/17	0	0	0	0	0	0	0	0
1/18	4	0	3746	0	0	0	0	0
1/19	0	0	0	0	0	0	0	0
1/20	0	0	0	0	0	0	0	0

- 4 To capture router port error statistics, type
sho port error main
Review the output for the main port error command.
- 5 Repeat steps [3](#) and [4](#) to capture error count increases.
- 6 Complete the table that follows by performing the commands in steps [7](#) through [12](#).

Status					
VID (P/V)	VRID	Chassis 0		Chassis 1	
		OSPF Metric (see Note)	VRRP PRIO	OSPF Metric (see Note)	VRRP PRIO
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
Note: Only collect this metric if OSPF is configured on the Ethernet Routing Switch 8600.					

- 7 To display virtual router redundancy protocol information, type

sho ip vrrp info

Output for the virtual router redundancy protocol command appears.

VRID	P/U	IP	MAC	STATE	CONTROL	PRIO	ADU
1	116	10.64.16.1	00:00:5e:00:01:01	Back Up	Enabled	100	1
2	132	10.64.32.1	00:00:5e:00:01:02	Back Up	Enabled	100	1

VRID	P/U	MASTER	UP TIME	HLD DWN	CRITICAL	IP (ENABLED)
1	116	10.64.16.2	0 day(s), 01:50:46	0	10.64.16.3	(Yes)
2	132	10.64.32.2	0 day(s), 01:50:46	0	10.64.32.3	(Yes)

- 8 Review the State column and record the master (State = Master) and slave (State = Back Up) status for each Ethernet Routing Switch 8600 Chassis in the table.

Note: If you cannot determine the master/slave status, call the next level of support.

- 9 For each VLAN listed in the virtual router redundancy protocol file (see step 7), record the VID (P/V), VRID, and PRIO information for each CS LAN Ethernet Routing Switch 8600 Chassis 0 and 1 in the table.

Note: VID is the VLAN identifier of each VLAN. VRID is the VRRP identifier. PRIO determines the priority setting for the related chassis. Setting the PRIO setting on the master router to a value less than that for the slave causes a switch in master/slave status.

- 10 Display the status of OSPF by entering the following command

sho ip ospf info

- 11 Use the following table to determine the next step.

If	Do
AdminStat is enabled for OSPF	Step 12
otherwise	Step 13

- 12 Enter the following command to capture OSPF metrics for all VLANs that have OSPF ENABLE set to true, as shown in the figure that follows.

sho vlan info ospf

Output for the OSPF metrics appears.

Vlan Ospf									
VLAN ID	ENABLE	HELLO INTERVAL	RTRDEAD INTERVAL	DESIGRTB PRIORITY	METRIC	AUTHTYPE	AUTHKEY	INTF	AREAD
1	false	10	40	1	0	none		b	0.0.0.0
2	false	10	40	1	10	none		b	0.0.0.0
3	true	10	40	1	10	none		b	0.0.0.0
4	true	10	40	1	10	none		p	0.0.0.0
6	true	1	4	1	10	none		b	0.0.0.0
7	true	10	40	1	10	none		p	0.0.0.0
8	true	1	4	1	10	none		b	0.0.0.0
9	true	1	4	1	10	none		b	0.0.0.0
101	false	10	40	1	10	none		b	0.0.0.0
102	false	10	40	1	10	none		b	0.0.0.0
103	false	10	40	1	10	none		b	0.0.0.0
111	false	10	40	1	10	none		b	0.0.0.0
112	false	10	40	1	10	none		b	0.0.0.0
113	false	10	40	1	10	none		b	0.0.0.0
114	false	10	40	1	10	none		b	0.0.0.0
121	false	10	40	1	10	none		b	0.0.0.0

Note: Standard results can reflect just the VRRP or OSPF in some VIDs. In some instances, it is also typical for both values to be collected.

- 13** Display the status of BGP by entering the following command
sho ip bgp conf
- 14** Use the following table to determine the next step.

If	Do
BGP on/off = on	Step 15
otherwise	Step 19

- 15** If BGP is enabled on the Ethernet Routing Switch 8600, enter the following command:

sho ip bgp neighbor info

A sample output of the sho ip bgp neighbor info command follows:

```
BGP neighbor is 172.30.249.6 remote AS 65445, Internal Peer,  
BGP state [Established]  
remote router ID 192.168.223.103
```

```
admin-state - BGP ON  
connect-retry-interval - 120  
ebgp-multihop - disable  
hold-time - 6  
keepalive-time - 2  
hold-time-configured - 6  
keepalive-time-configured - 2  
max-prefix - 12000  
nexthop-self - enable  
originate-def-route - disable  
MD5-authentication - disable  
neighbor-debug - none  
remove-private-as - enable  
route-advertisement-interval - 5  
route-reflector-client - disable  
send-community - disable  
soft-reconfiguration-in - enable  
  
updt-source-interface - 0.0.0.0  
weight - 100  
Route Policy In -  
Route Policy Out -
```

```
BGP neighbor is 172.30.249.9 remote AS 65444, External Peer,  
BGP state [Established]  
remote router ID 192.168.223.101
```

```
admin-state - BGP ON  
connect-retry-interval - 120  
ebgp-multihop - disable  
hold-time - 6  
keepalive-time - 2  
hold-time-configured - 6  
keepalive-time-configured - 2  
max-prefix - 12000  
nexthop-self - enable  
originate-def-route - disable  
MD5-authentication - disable  
neighbor-debug - none  
remove-private-as - enable  
route-advertisement-interval - 5  
route-reflector-client - disable  
send-community - disable  
soft-reconfiguration-in - enable  
updt-source-interface - 0.0.0.0
```

- 16** Record the IP addresses of all BGP neighbors and note whether the BGP peer is internal or external using the following table.

BGP neighbor IP address	Type of BGP peer (circle one)	BGP state = Established? (circle one)
	Internal/External	Y/N
	Internal/External	Y/N
	Internal/External	Y/N
	Internal/External	Y/N

- 17** Verify that there is at least one (1) internal BGP peer and one (1) external BGP peer in the output of the command. If this condition is not met, contact your next level of support.
- 18** Verify BGP state = Established on all BGP neighbors. If this condition is not met, contact your next level of support.
- 19** You have completed this procedure. Proceed to [Performing Ethernet Routing Switch 8600 backups on page 107](#) to continue with preparing the Ethernet Routing Switch 8600 for upgrade.

Performing Ethernet Routing Switch 8600 backups

Use the Ethernet Routing Switch 8600 CLI to back up the original software load and configuration files:

- 1 Enter the following command to obtain the name of your current primary image file.

Ensure the config file and image are properly configured on the /flash (primary) and /pcmcia (secondary) by typing

sho sys info

A sample output of the show sys info command follows (only a portion of the output is shown here):


```

Spiderman-C1:6# show sys info
General Info :

SysDescr      : Passport-8610 (3.7.13.0)
SysName       : Spiderman-C1
SysUpTime    : 3 day(s), 18:23:28
SysContact    : support@nortelnetworks.com
SysLocation   : 4655 Great America Parkway, Santa Clara, CA 95054

Chassis Info :

Chassis       : 8010
Serial#       : SSPN6C09LN
HwRev         : 00
NumSlots      : 10
NumPorts      : 242
GlobalFilter   : enable
VlanBySrcMac   : disable
Ecn-Compatib  : enable
WsmDirectMode : disable
BaseMacAddr    : 00:17:65:46:d0:00
MacAddrCapacity : 1024
Temperature    : 27 C

--More-- (q = quit)                                MgmtMacAddr : 00:17:65:46:d3:f6

System MTU    : 1522
clock_sync_time : 60

Power Supply Info :

Ps#1 Status   : up
Ps#1 Type     : Unknown
Ps#1 Description : UNKNOWN
Ps#1 Serial Number: ARTSDG000136
Ps#1 Version   : A
Ps#1 Part Number : 321408

Ps#2 Status   : empty

Ps#3 Status   : up
Ps#3 Type     : Unknown
Ps#3 Description : UNKNOWN
Ps#3 Serial Number: ARTSDG000140
Ps#3 Version   : A
Ps#3 Part Number : 321408

Fan Info :

--More-- (q = quit)                                Fan#1: up, air temp: 29 C

Fan#2: up, air temp: 28 C

Card Info :

Slot#          FrontType  FrontHw  Oper  Admin  BackType  BackHw
                  Version  Status  Status
1      8x1000BaseIC-E      50      up    up      BFM8      50
2      32x100BaseTX-E      50      up    up      BFM6      50
3      48x100BaseTX-E      50      up    up      BFM6      50
4      48x100BaseTX-E      50      up    up      BFM6      50
5              CPU        50  dormant up      FSFM      50
6              CPU        50      up    up      FSFM      50

```

Note: If this does not match the output, copy the loads to /pcmcia. If they are missing from /pcmcia, enter the following commands to copy the files to /pcmcia and to specify the oldload as the secondary file from which to boot.

Perform the following command on each CPU

copy /flash/<oldload> /pcmcia/

Perform the following commands only on the master CPU

**config bootconfig choice secondary image-file
/pcmcia/<oldload>**

**config bootconfig choice secondary config-file
/pcmcia/config.cfg**

where

<oldload> is the original software image filename, where xxxx is the software load version and which must be in lower case, for example p80a3320.img

2

ATTENTION

Do not delete the current software load before successfully completing the upgrade. Current software must remain available as the secondary load to support Ethernet Routing Switch 8600 failback capabilities.

ATTENTION

Refer to section [Text conventions on page 77](#) for brief definitions and examples of the software filenames used in the following command lines.

Verify that any required files are backed up, including

- data encryption standard (DES)
- Triple DES (3DES)
- ATM (if an ATM blade is used)
- Packet over Sonet (POS) (if used)

Back up the current config, bootconfig, and software load files to the /flash and PCMCIA card to ensure the files are synchronized

on the master and slave (if configured) CPU. Enter the following commands:

Note: Before entering the `sav config` command, ensure sufficient free space exists in /flash (20% of total /flash size) to accommodate the configuration file.

sav config

For CS-LANs with a dual CPU configuration to save to primary (/flash), secondary (PCMCIA) and slave CPU, type

sav boot

```
sav config backup /pcmcia/config.cfg standby  
/pcmcia/config.cfg
```

```
sav bootconfig backup /pcmcia/boot.cfg standby  
/pcmcia/boot.cfg
```

For CS-LANs with a single CPU configuration to save to primary (/flash) and secondary (PCMCIA), type

```
sav config backup /pcmcia/config.cfg
```

```
sav bootconfig backup /pcmcia/boot.cfg
```

- 3 You have completed this procedure. Proceed to [Upgrading the Ethernet Routing Switch 8600 on page 111](#) to continue with upgrading the Ethernet Routing Switch 8600.

Upgrading the Ethernet Routing Switch 8600

The following procedure provides the steps you need to execute to upgrade the Ethernet Routing Switch 8600. When applicable, a reference that contains the detailed steps is provided.

This procedure uses a phased approach to upgrade one Ethernet Routing Switch 8600 (ERS 8600) at a time. This approach prevents service interruptions due to CS-LAN failure that will occur if both ERS 8600s are taken out of service at the same time.

This procedure is done in two passes. The first pass upgrades the slave router. The second pass occurs after a SWACT, and the other side of the pair is upgraded.

Note: On the second pass, the master and slave roles are swapped. Take this change into account as you perform the second pass on the repeated steps in this procedure.

Nortel recommends that all unit 0 network elements subtend ERS 8600 Chassis 0. Likewise, all unit 1 network elements must subtend Chassis 1.

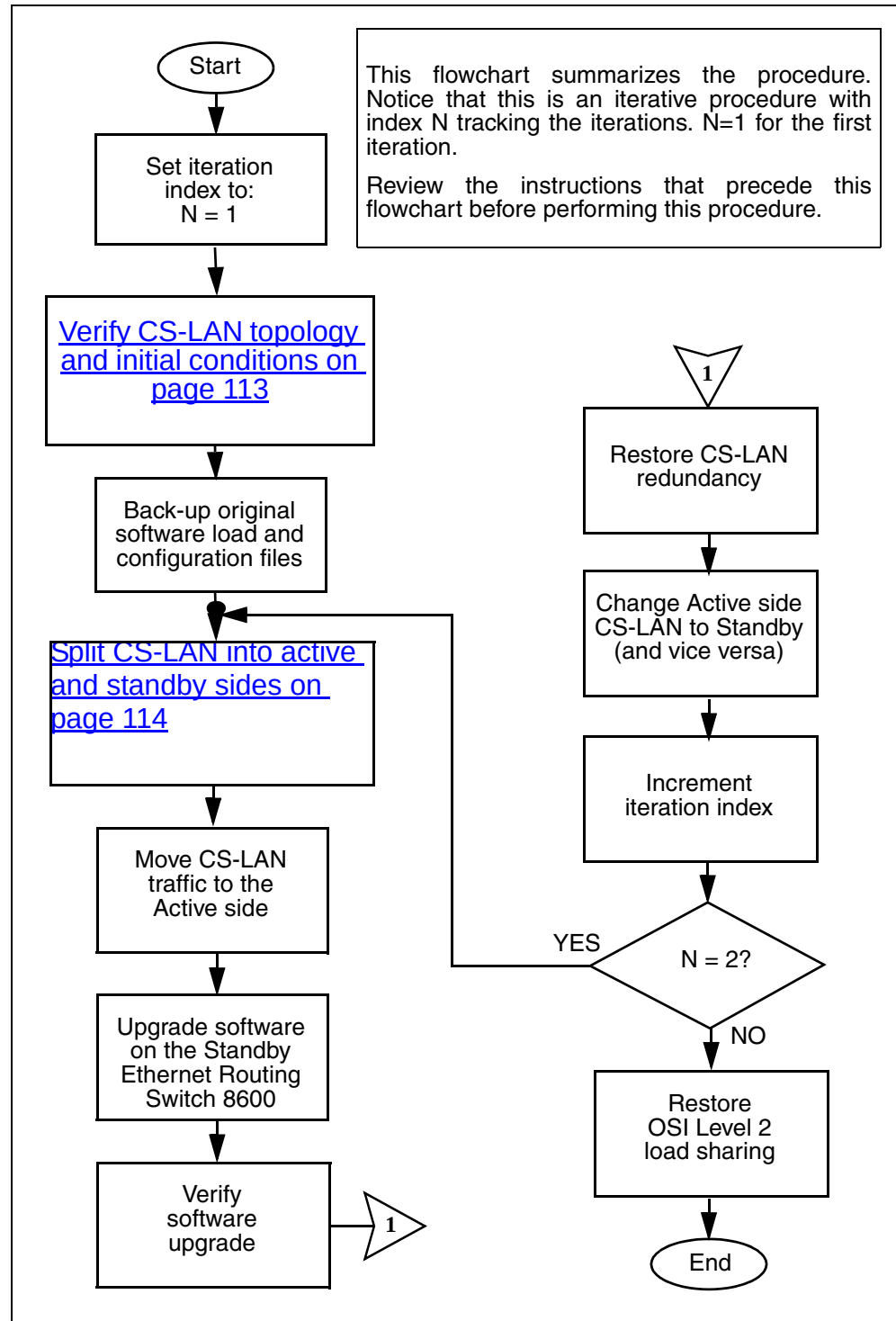
Note 1: If the topology of your CS-LAN does not conform to this recommendation, take this variation into account as you perform this procedure.

Note 2: If your solution includes Media Gateway 15000¹, off load traffic from the slave to the master ERS 8600 before upgrading the slave software. Perform the procedure, [Offloading PVG traffic from the Ethernet Routing Switch 8600 on page 124](#).

¹ Formerly known as the Passport Packet Voice Gateway (PVG)

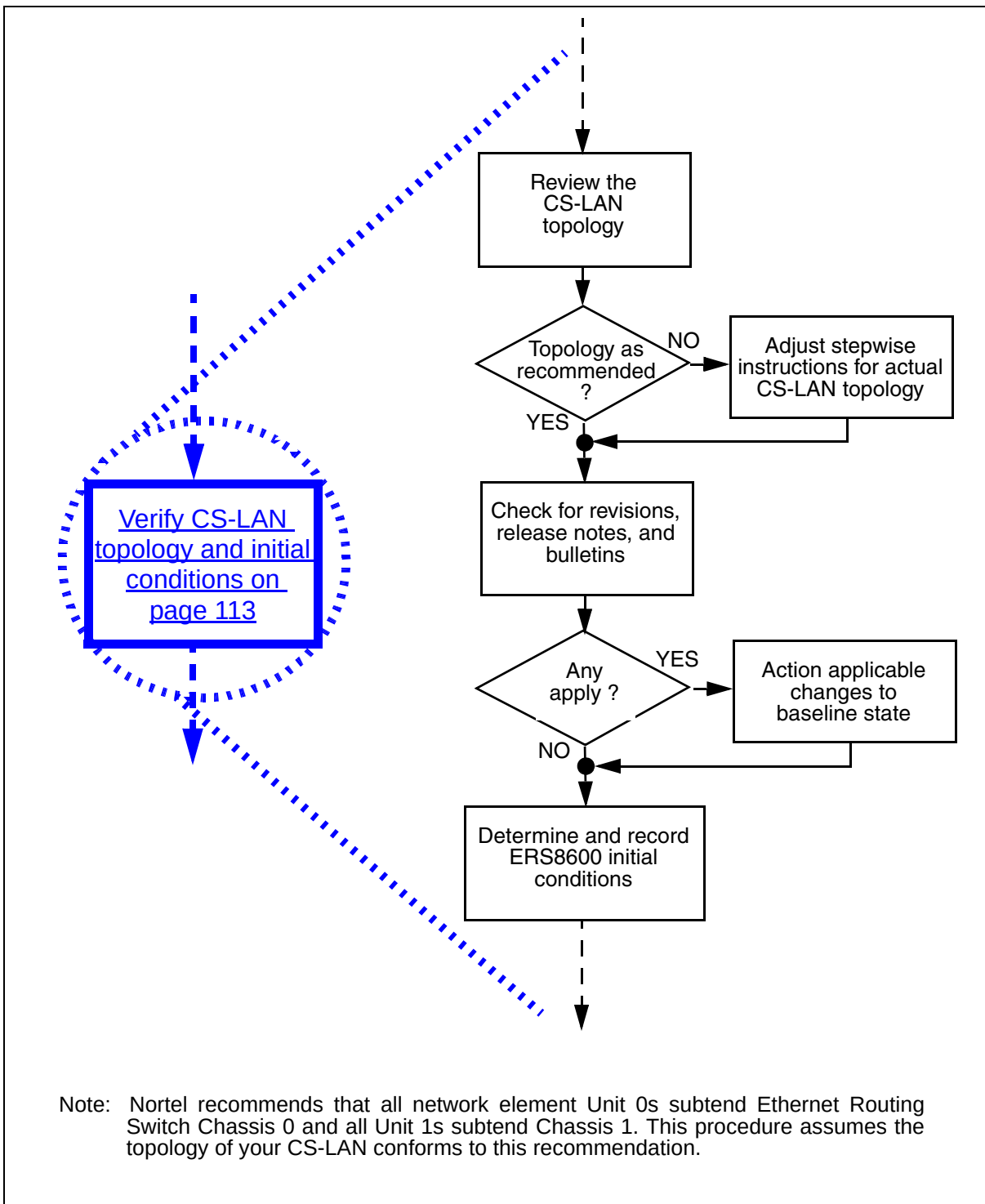
The following flowchart summarizes the overall software upgrade procedure.

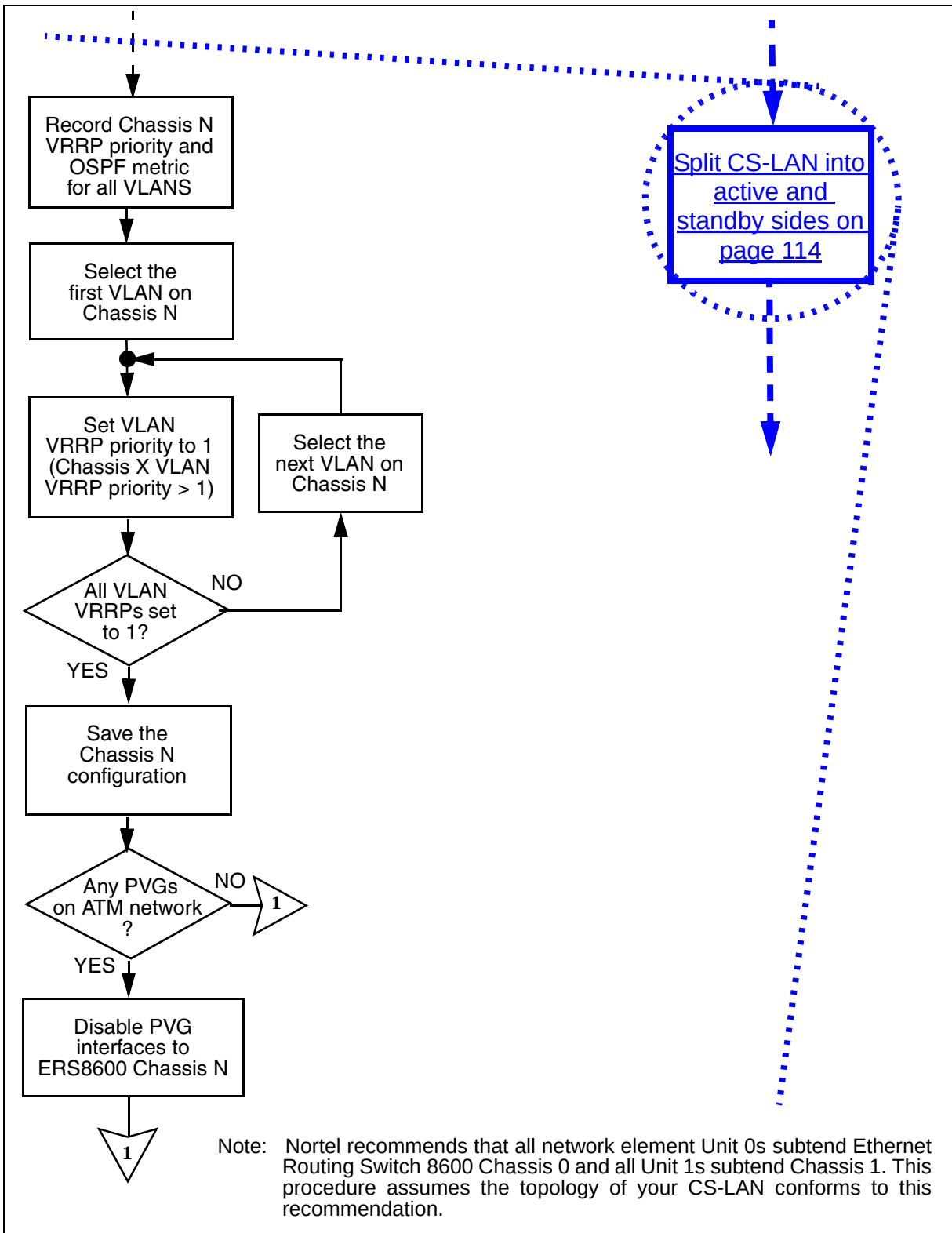
Upgrading Ethernet Routing Switch 8600 software for the CS-LAN

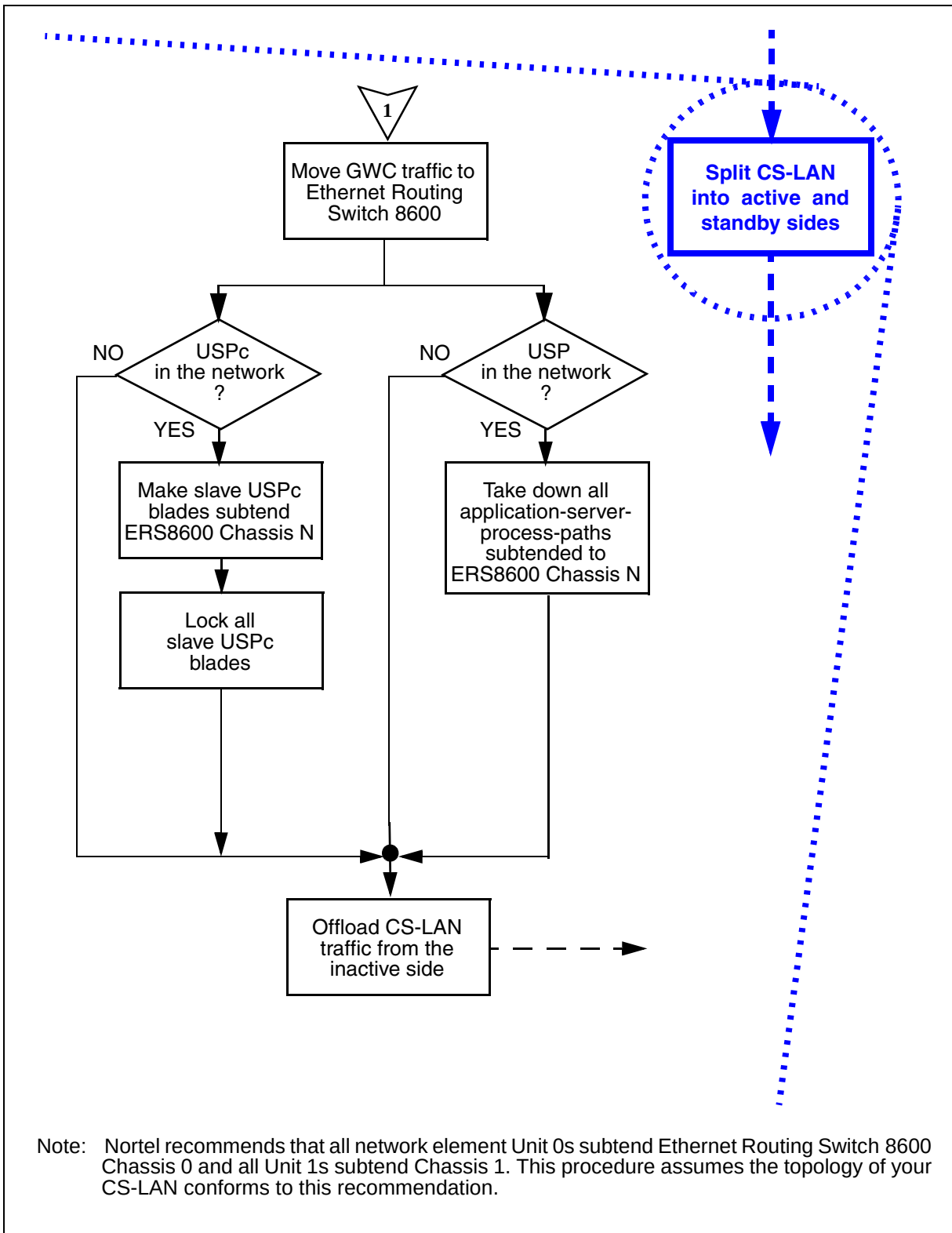


The following flowcharts provide additional detail to the [Upgrading Ethernet Routing Switch 8600 software for the CS-LAN](#) flowchart.

Verify CS-LAN topology and initial conditions



Split CS-LAN into active and standby sides

Split CS-LAN into active and standby sides (cont'd)

Access the ERS 8600s using the serial (console) port. You can use a direct serial connection and a terminal program from an attached PC or a TELNET connection to an appropriately configured IP address on a terminal server connected to the console port.

Note: In dual CPU configurations, after any reset of the master CPU, the slave CPU becomes active. Ensure that you continue the steps on the newly master CPU unless otherwise noted.

Make sure you use READ/WRITE/ALL (RWA) login privileges, password privileges or both when performing this procedure. For more information about RWA privileges, refer to Passport Documentation in the Nortel website.

ATTENTION

The GUI/HMI graphics that support this procedure are current as of (I)SN09U. Although these illustrations differ from the GUI/HMI you are using, perform all stepwise actions by accessing your element managers and making the equivalent choices.

ATTENTION

This upgrade procedure causes alarms to occur on CS-LAN components. These alarms report the loss of certain redundant paths during the upgrade process. These losses are not service affecting and the paths are restored on completion of the upgrade.

ATTENTION

This is an iterative procedure that includes two passes. Make sure you understand the instructions and flowchart that support this procedure before you begin the upgrade. The iterations (passes) proceed as follows:

- common procedures: [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#); [Performing Ethernet Routing Switch 8600 backups on page 107](#),
- first pass (N=0) includes [Splitting the CS-LAN into active and standby sides on page 119](#) to [Enabling the Ethernet links between the XA-Core and the Ethernet Routing Switch 8600 on page 199](#)
- second pass (N=1) includes [Splitting the CS-LAN into active and standby sides on page 119](#) to [Enabling the Ethernet links between the XA-Core and the Ethernet Routing Switch 8600 on page 199](#)

Prerequisites

You have completed procedure [Preparing to upgrade the Ethernet Routing Switch 8600 on page 82](#).

Action

Perform the following high-level procedure to upgrade the Ethernet Routing Switch 8600.

Upgrading the Ethernet Routing Switch 8600 for the CS-LAN

- 1 Perform procedure [Splitting the CS-LAN into active and standby sides on page 119](#).
- 2 If your network configuration contains Border Control Point 7100s directly connected to the Ethernet Routing Switch 8600, perform procedure [Shutting down the Border Control Point 7100 connected to Chassis N on page 122](#) to prevent it from accepting new service requests.
- 3 If your CS-LAN includes any ATM PVGs directly connected to the Ethernet Routing Switch 8600 (that is, a non-VR solution), perform procedure [Offloading PVG traffic from the Ethernet Routing Switch 8600 on page 124](#).
- 4 Perform procedure [Disabling GWCs that subtend the slave Ethernet Routing Switch 8600 on page 134](#).

- 5 If your office uses an XA-Core and HIOPs or HCMICs, perform procedure [Disabling the Ethernet links between an XA-Core and HIOPs and the Ethernet Routing Switch 8600 on page 138](#).
- 6 If your office uses a CS 2000-Compact and a USP-Compact, perform procedure [Locking the USP-Compact on page 140](#).
- 7 If your office uses a Standard USP, perform procedure [Taking down the paths to the Ethernet Routing Switch 8600 Chassis N on page 148](#).
- 8 If your office uses a CS 2000-Compact, perform procedure [Determining if STORM devices require rotating, demounting and busying on page 150](#).
- 9 Perform procedure [Locking the inactive Shelf Controller \(SC\) blade connected to Chassis N on page 155](#).
- 10 If your office is in a Geographic Survivable environment, perform procedure [Disabling Geographic Survivable components on page 160](#).
- 11 Upgrade the Ethernet Routing Switch using procedure [Upgrading the Ethernet Routing Switch 8600 on page 167](#).
- 12 Perform procedure [Verifying all hardware and software on Ethernet Routing Switch 8600 on page 183](#).
- 13 If your configuration includes any Border Control Point 7100s directly connected to the Ethernet Routing Switch 8600, perform procedure [Unlocking the Border Control Point 7100 on page 186](#).
- 14 Perform procedure [Unlocking the inactive SC on page 188](#).
- 15 If the USP-Compact is used, perform procedure [Unlocking the USP-Compact on page 189](#).
- 16 If the Standard USP is used, perform procedure [Returning the paths to the Ethernet Routing Switch 8600 Chassis N to service on page 193](#).
- 17 If your office is in a Geographic Survivable configuration, perform procedure [Enabling Geographic Survivable components on page 194](#).
- 18 If your office uses an XA-Core, perform procedure [Enabling the Ethernet links between the XA-Core and the Ethernet Routing Switch 8600 on page 199](#).
- 19 You have completed this upgrade activity. Proceed to [Completing the Ethernet Routing Switch 8600 upgrade on page 201](#).

Splitting the CS-LAN into active and standby sides

At the Ethernet Routing Switch CLI

- 1 To ensure that Ethernet Routing Switch 8600 Chassis N is the slave, enter the following command to set the VRRP priority to 1.

```
config vlan <vid> ip vrrp <vrid> prio 1
```

Note 1: Setting Ethernet Routing Switch 8600 Chassis N <prio> to 1 makes it slave (Chassis X <prio> is greater than 1 making it the master).

Note 2: VID is obtained by by entering command **sho ip vrrp info** as shown in the following response. P/V is the VLAN ID and should be used for the VID and VRID parameter.

Vrrp Info							
VRID	P/V	IP	MAC	STATE	CONTROL	PRIO	ADV
10	10	47.142.90.1	00:00:5e:00:01:0a	Back Up	Enabled	100	1
20	20	172.19.64.1	00:00:5e:00:01:14	Back Up	Enabled	100	1
30	30	10.26.128.1	00:00:5e:00:01:1e	Back Up	Enabled	100	1
40	40	172.19.68.1	00:00:5e:00:01:28	Back Up	Enabled	100	1
41	41	172.19.68.17	00:00:5e:00:01:29	Back Up	Enabled	100	1
43	42	172.19.68.33	00:00:5e:00:01:2b	Back Up	Enabled	100	1
60	60	172.19.70.1	00:00:5e:00:01:3c	Back Up	Enabled	100	1

VRID	P/V	MASTER	UP TIME	HLD DWN	CRITICAL	IP (ENABLED)
10	10	47.142.90.3	2 day(s), 18:46:07	0	0.0.0.0	(No)
20	20	172.19.64.3	2 day(s), 18:46:07	0	0.0.0.0	(No)
30	30	10.26.128.3	2 day(s), 18:46:07	0	0.0.0.0	(No)
40	40	172.19.68.3	2 day(s), 18:46:07	0	0.0.0.0	(No)
41	41	172.19.68.19	2 day(s), 18:46:07	0	0.0.0.0	(No)
43	42	172.19.68.35	2 day(s), 18:46:07	0	0.0.0.0	(No)

- 2 Repeat step [1](#) for each VLAN provisioned on the router.

- 3 Use the following table to determine the next step.

If	Do
OSPF is enabled	Steps 4 and 5
BGP is enabled	Step 6
both OSPF and BGP are enabled	Steps 4 through 6

- 4 Enter the following command to set the OSPF priority to 1000.

```
config vlan <vid> ip ospf metric 1000
```

- 5 Repeat step 4 for each VLAN provisioned on the router. After this is performed on all VLANs, to verify that all VLANs have a metric of 1000, type

```
sho vlan info ospf
```

After the VRRP priority and OSPF priority have been set for all provisioned VLANs, go to step 8. However if BGP is enabled, continue with the next step.

- 6 Repeat the following command for each external BGP neighbor entry recorded in the BGP neighbor address table in [Performing Ethernet Routing Switch 8600 upgrade pre-checks, step 18](#) on page 106.

```
config ip bgp neighbor <external BGP neighbor IP address> admin-state disable
```

- 7 Check that the default route in the Ethernet Routing Switch 8600 route table correctly points to the master Ethernet Routing Switch 8600 by typing:

```
show ip route info
```

A sample output of the show ip route info command follows:

Ip Route									
DST	MASK	NEXT	COST	VLAN	PORT	PROT	AGE	TYPE	PRF
0.0.0.0	0.0.0.0	172.30.249.12	1	402	-/-	BGP	0	IB	45
10.21.0.0	255.255.255.0	10.21.0.1	1	72	-/-	LOC	0	DB	0
10.22.0.0	255.255.255.0	10.22.0.1	1	73	-/-	LOC	0	DB	0
10.54.0.0	255.255.255.0	10.54.0.1	1	54	-/-	LOC	0	DB	0
10.55.0.0	255.255.255.0	10.55.0.1	1	55	-/-	LOC	0	DB	0
10.240.0.3	255.255.255.255	10.250.0.10	20	100	-/-	STAT	0	IB	5
10.240.0.4	255.255.255.255	10.250.0.26	20	101	-/-	STAT	0	IB	5
10.250.0.0	255.255.255.240	10.250.0.6	1	100	-/-	LOC	0	DB	0
10.250.0.16	255.255.255.240	10.250.0.22	1	101	-/-	LOC	0	DB	0
30.30.30.0	255.255.255.0	30.30.30.1	1	2	-/-	LOC	0	DB	0
172.18.181.0	255.255.255.128	172.18.181.1	1	200	-/-	LOC	0	DB	0
172.30.249.8	255.255.255.248	172.30.249.9	1	402	-/-	LOC	0	DB	0
172.30.254.0	255.255.255.252	172.30.254.1	1	240	-/-	LOC	0	DB	0
172.30.254.192	255.255.255.192	172.30.254.193	1	260	-/-	LOC	0	DB	0
192.168.223.101	255.255.255.255	192.168.223.101	1	0	-/-	LOC	0	DB	0

The IP address in the NEXT field of the default route entry (DST = 0.0.0.0) should be the IP address of the BGP internal peer recorded in the BGP peer address table in [Performing Ethernet Routing Switch 8600 upgrade pre-checks, step 18](#) on page 106. If this condition is not met, contact your next level of support.

- 8 Enter the following command to save the new Ethernet Routing Switch 8600 Chassis N configuration.

Note: Before entering the sav config command, ensure sufficient free space exists in /flash (20% of total /flash size) to accommodate the configuration file. Refer to [Verifying sufficient space exists in directories /flash and /pcmcia on page 88](#) to check the directory size and remove files if necessary.

sav config

This updates the new Ethernet Routing Switch 8600 configuration so that VRRP settings are maintained after any subsequent reboot.

For CS-LANs with a dual CPU configuration to save to primary (/flash), secondary (PCMCIA) and slave CPU, type

```
sav config backup /pcmcia/config.cfg standby  
/pcmcia/config.cfg
```

For CS-LANs with a single CPU configuration to save to primary (/flash) and secondary (PCMCIA), type

```
sav config backup /pcmcia/config.cfg
```

Note: Answer Y to the overwrite question in response to the sav config backup command.

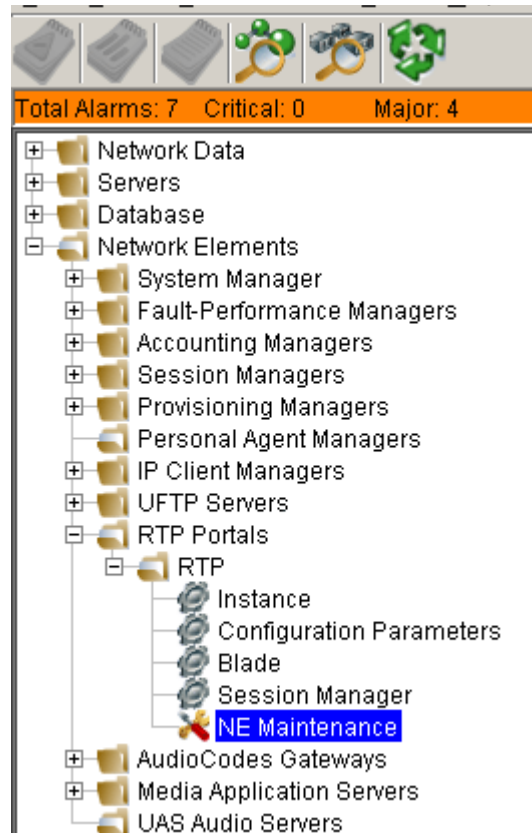
- 9 You have completed this procedure. Return to procedure [Upgrading the Ethernet Routing Switch 8600 for the CS-LAN on page 117](#) that sent you here.

Shutting down the Border Control Point 7100 connected to Chassis N

At the System Management Console

- 1 Ensure that direct connectivity has been established according to the instructions in bulletin *SEB-08-01-009*.
- 2 From the System tree, click the plus sign next to **Network Elements** to expand the view of the folder.

Expanding BCP 7100 window



- 3 Next, click the plus sign next to **RTP Portals** to expand the view of the folder. The contents of this folder lists all BCP 7100s and BCP 7200s configured for the site.
- 4 Continue to expand the view of folders until the target BCP 7100 is selected. Do not modify the state of any BCP 7200s.
- 5 Click the **NE Maintenance** option. A new window opens.
- 6 Click the **Stop** button to initiate shut down.

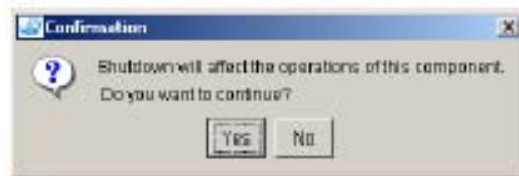
BCP 7100 shutdown



The Stop button shuts down the system. The Kill button locks the BCP 7100, and the Restart button stops and starts the system.

- 7 A confirmation window appears. Click **Yes** to continue.

BCP 7100 shutdown confirmation



- 8 The BCP 7100 component shuts down gracefully and eventually goes into an inactive state when the last active media session ends (as seen in the General Information Area of the System Management Console).
- 9 You have completed this procedure. Return to the procedure that sent you here.

Offloading PVG traffic from the Ethernet Routing Switch 8600

Use the PVG CLI to determine the PVG IP addresses

- 1 Check the provisioning information for the VSPs, NSTA, and VGS subcomponents as follows:
 - a Enter the following command to display media and signaling gateway IP addresses.

d -p nsta/* vgs ctrl/*

The following list provides sample MG and SG IP addresses for a single VSP card provisioned in slot 7.

+=====+-----+-----+-----+			
Nsta	Ctrl	ipAddr	dnsList
+=====+-----+-----+-----+			
7	mg	172.16.201.2	
7	sg	172.16.201.6	

Note: The "nsta/* vgs ctrl/*" portion of this command causes IP addresses for all provisioned VSP cards to be displayed. The example only shows MG and SG IP addresses for a single VSP card provisioned in slot 7.

- b Enter the following command to display the IPmcon IP address.

d -p nsta/* vgs ipmcon

The following list provides a sample IPmcon IP address for a single VSP card provisioned in slot 7.

+=====+-----+-----+-----+			
Nsta	ipAddr	udpBa	Response
		se	
+=====+-----+-----+-----+			
7	172.16.201.10	49152	

Note: The "nsta/* vgs ipmcon" portion of this command causes IP addresses for all provisioned VSP cards to be displayed. The example only shows IPmcon IP address for a single VSP card provisioned in slot 7.

Use each Ethernet Routing Switch 8600 CLI to verify that the PVGs are set up redundantly

- 2** Enter the following command on each Ethernet Routing Switch 8600 chassis to check the VLAN configuration file.

sho config module vlan

This command outputs all VLANs provisioned on the Ethernet Routing Switch 8600 Chassis.

The example that follows shows the output of this command for only one VSP blade.

```
vlan 702 create byport 1 name "PVG40-vsp07-mg"
vlan 702 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8
member portmember
vlan 702 ports add 8/1 member portmember
vlan 702 ip create 172.16.201.1/255.255.255.252 mac_offset 5
vlan 706 create byport 1 name "PVG40-vsp07-sg"
vlan 706 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8
member portmember
vlan 706 ports add 8/1 member portmember
vlan 706 ip create 172.16.201.5/255.255.255.252 mac_offset 14
```

Note: Both Ethernet Routing Switch 8600s display the identical PVG VLAN configuration. The "**vlan <#> ports add**" entry identifies each VSP ATM Sonet connection. This information is required in [step 8](#).

- 3** Check the routing table information for each Ethernet Routing Switch 8600 chassis as follows:
- a** Enter the following command to display IP route information.

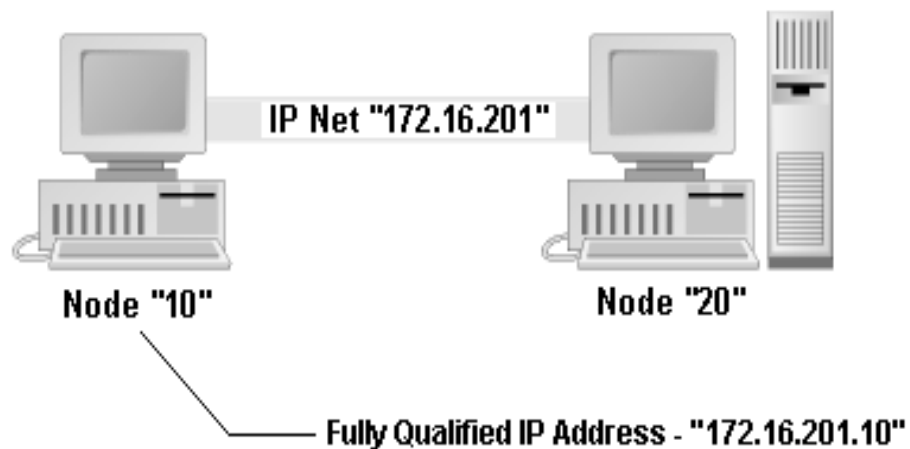
sho ip route info ip x.y.z

where

x.y.z

specifies the IP Net address provided at [step 1](#)

Note: Specifying the x.y.z octets limits the command output to those nodes served by the specified IP Net.



The following list provides an example for the command output for one of the Ethernet Routing Switch 8600s.

```
=====
Ip Route
=====
DSTMASKNEXTCOSTVLANPORTPROTAGETYPEPEPRF
-----
172.16.201.0 255.255.255.252 172.16.201.1 1 702 -/- LOC 0 DB 0
172.16.201.4 255.255.255.252 172.16.201.5 1 706 -/- LOC 0 DB 0
172.16.201.8 255.255.255.252 172.16.201.9 1 710 -/- LOC 0 DB 0

2 out of 360 Total Num of Dest Networks,360 Total Num of Route Entries displayed.
```

The following list provides an example for the command output for the other Ethernet Routing Switch 8600 Chassis.

```
=====
Ip Route
=====
DSTMASKNEXTCOSTVLANPORTPROTAGETYPEPEPRF
-----
172.16.201.0 255.255.255.252 172.30.242.230 20 80 -/- OSPF 0 IB 120
172.16.201.4 255.255.255.252 172.30.242.230 20 80 -/- OSPF 0 IB 120
172.16.201.8 255.255.255.252 172.30.242.230 20 80 -/- OSPF 0 IB 120

2 out of 360 Total Num of Dest Networks,360 Total Num of Route Entries displayed.
```

ATTENTION

The routing information under the PROT column heading must indicate either VSP subnet LOC or OSPF.

If both Ethernet Routing Switch 8600s indicate the same status for the same VSP subnet, this is a non-standard condition. Contact your next level of support.

To prevent service interruption, VSP VLANs on Chassis N of the Ethernet Routing Switch 8600 must be OSPF (LOC for Chassis X). See [step 10](#) for details on forcing compliance to this requirement.

- b** Repeat sub[step 3a](#) for each VSP VLAN on the Ethernet Routing Switch 8600 Chassis N.
- c** Repeat sub[step 3a](#) and [3b](#) for Ethernet Routing Switch 8600 Chassis X.

Use the PVG CLI to verify the correct provisioning of each VSP

- 4** Check the SPVCAP subcomponent of each VSP VGS Ctrl/<mg,sg> and IPmcon as follows:
 - a** Enter the following command to display the provisioning information for each VSP.

d -p -no nsta/* vgs ctrl/* spvcap

The following list shows VSP provisioning information for slot 7. The actual command output lists all VSP information.

```
Nsta/ 7 VGS Ctrl/mediaGateway SpvcAp
atmServiceCategory = nrtVariableBitRate
peakCellRate= 800 cells
sustainedCellRate= 400 cells
maximumBurstSize= 100 cells
retryLimit= 0
localAddress=
45613512123400002F000000010020480D527001
remoteVpiVci= 7.2
addressToCall=
45613512123400002F000000010020480D008D00
Nsta/ 7 VGS Ctrl/signalingGateway SpvcAp
atmServiceCategory = nrtVariableBitRate
peakCellRate= 450 cells
sustainedCellRate= 210 cells
maximumBurstSize= 60 cells
retryLimit= 0
localAddress=
45613512123400002F000000010020480D527002
remoteVpiVci= 7.2
addressToCall=
45613512123400002F000000010020480D008D00
```

b Enter the following command to display IPmcon information.

d -p -no nsta/* vgs ipmcon spvcap

The following list shows information for the IPmcon in slot 7.
The actual command output lists information for all IPmcon
sub-components of the NSTA VGS.

```
Nsta/ 7 VGS IpMcon SpvcAp
atmServiceCategory= rtVariableBitRate
peakCellRate= 336000 cell/s
sustainedCellRate= 336000 cell/s
maximumBurstSize= 1 cells
retryLimit= 0
localAddress=
45613512123400002F000000010020480D517000
remoteVpiVci= 7.10
addressToCall=
45613512123400002F000000010020480D008D00
```

- 5 Confirm that the VSP VGS "addressToCall" (ATMIF UNI address) for Ctrl/mediaGateway, Ctrl/signaling Gateway, and IpMcon are identical.

Note: If they are not identical, contact your next level of support.

- 6 Enter the following command to check the ATMIF UNI addresses provisioned as primary and alternate.

```
1 atmif/* uni addr/*
```

A sample of the command output for the ATMIFs present on the PVG shelf follows.

```
Atmif/141Uni
Addr/45613512123400002F000000010020480D008D00,pri-
mary
```

Note: Make sure the ATMIF UNI provisioning reflects a Primary and Alternate configuration for the same address for each VSP. (Refer to your engineering guidelines for more information.) If they do not match, contact your next level of support.

Use the PVG CLI to verify the PVG ATM (software) connection to the Ethernet Routing Switch 8600s

- 7 Determine which ATMIF the VSP VGS Ctrl/<mg,sg> and IPmcon ATMCON subcomponents point to as follows:

- a Enter the following command to display the VGS Ctrl/<mg,sg> ATMCON subcomponent for all VSPs.

```
d nsta/* vgs ctrl/* atmconn
```

A sample of the command output for a VSP provisioned in slot 7 follows. The actual command output lists all connection states and the ATMIFs they use.

Nsta	Ctrl	nextHop	state
7	mg	AtmIf/141 Vcc/7.2 Ep	connec
7	sg	AtmIf/141 Vcc/7.6 Ep	connec

Note: Make sure the AtmIf information for each VSP is identical to the primary interface information listed in

[step 6](#). If they do not match, contact your next level of support.

- b** Enter the following command to display the NSTA VGS IPmcon ATMCON subcomponent for the VSPs.

d nsta/* vgs ipmcon atmcon

A sample of the command output for a VSP provisioned in slot 7 follows. The actual command output lists all connection states and the ATMIFs they use.

+=====+-----+-----+-----+			
Nsta		nextHop	state Response
+=====+-----+-----+-----+			
7		AtmIf/141 Vcc/7.10	connec

Note: Make sure the AtmIf information for each VSP is identical to the primary interface information listed in [step 6](#). If they do not match, contact your next level of support.

- 8** Check the physical connections between each PVG ATM interface and their related Ethernet Routing Switch 8600s.

Note: See [step 2](#) for the Ethernet Routing Switch 8600 local route tables for the VSPs to be offloaded and verify the fiber connectivity between the PVGs and Ethernet Routing Switch 8600s. Refer to your engineering guidelines for additional information.

Use the PVG CLI to disable the ATM interface to the Ethernet Routing Switch 8600 undergoing the software upgrade

- 9** Select the next step as follows (refer to [step 3](#)):

If all VSP VLANs for Ethernet Routing Switch 8600 Chassis N are **Do**

OSPF (see Note) [step 16](#)

Anything except OSPF [step 10](#)

Note: OSPF routing does not require manual maintenance to reduce the risk of call processing outage, as the link redundancy on PVGs fails over nearly immediately.

- 10** Disable the ATM interface for each VSP as follows:

- a** Enter the following command to identify the ATM interfaces and Sonet layer.

```
d -p -no lp/* sonet/* sts/0
```

A sample of the command output for the first Sonet interface on each card follows. The actual command output lists all Sonet interfaces on the PVG.

```
Lp/14 Sonet/1 Sts/0
applicationFramename = Atmif/141
txPathTrace= ""
expectedReceivePathTrace= ""
concatNumber= 0
customerIdentifier= 0
ifAdminStatus= up
ifIndex= 6
Lp/15 Sonet/1 Sts/0
applicationFramename = Atmif/151
txPathTrace= ""
expectedReceivePathTrace= ""
concatNumber= 0
customerIdentifier= 0
ifAdminStatus= up
ifIndex= 472
```

- b** Enter the following command to lock all Sonet layer connections related to the ATM ports connected to Ethernet Routing Switch 8600 Chassis N.

```
lock -force lp/<slot> sonet/<sonetif>
```

where

<slot>

is the slot number of the ATMIF blade

<sonetif>

is the Sonet interface on the ATM blade

Note: This command results in Sonet layer alarms.

- c** Record all locked Sonet interfaces.
- 11** Confirm the ATM (software) connection switchover is successful as follows:

- a** Enter the following command to display the VGS Ctrl/<mg,sg> ATMCON subcomponent for the VSPs.

```
d nsta/* vgs ctrl/* atmconn
```


A sample of the command output for the switched ATMCON for the Ctrl/* to the ATMIF in slot 7 follows. This example shows a switchover from AtmIf/141 (see [step 7](#)) to AtmIf151.

```

+====+====+-----+-----+
|Nsta |Ctrl|      nextHop      |state
+====+====+-----+-----+
|    7|mg  |AtmIf/151 Vcc/7.2 Ep|connec
|    7|sg  |AtmIf/151 Vcc/7.6 Ep|connec

```

- b** Enter the following command to display the VGS IPmcon ATMCON subcomponent for the VSPs.

d nsta/* vgs ipmcon atmcon

A sample of the command output for the switched ATMCON for the IPmcon in slot 7 follows. This example shows a switchover from AtmIf/141 (see [step 7](#)) to AtmIf/151.

```

+====+-----+-----+-----+-----+
|Nsta |      nextHop      |state |Response
+====+-----+-----+-----+-----+
|    7|AtmIf/151 Vcc/7.10 |connec|

```

Use the Ethernet Routing Switch 8600 CLI to verify the IP route table for the offloaded VSP VLANs

- 12** Enter the following command to display the routing table for both Ethernet Routing Switch 8600s.

```
sho ip route info ip x.y.z
```

where

x.y.z

is the IP Net address (see [step 3](#))

Note: The routing information under the PROT column heading must indicate OSPF for all VSP VLANs on Ethernet Routing Switch 8600 Chassis N.

- 13** Select the next step as follows:

If switchover of all VSPs is	Do
incomplete (that is, not all VSPs switched over)	step 10
complete (that is, all switched over)	step 14

Use the PVG CLI to re-enable all disabled ATM ports

- 14** Enter the following command to unlock all Sonet ports locked at [step 10](#).

```
unlock lp/<slot> sonet/<sonetif>
```

where

<slot>

is the slot number of the ATMIF blade

<sonetif>

is the Sonet interface on the ATM blade

Use the Ethernet Routing Switch 8600 CLIs to check the IP route tables

- 15** Enter the following command to make sure all VSP VLANs remain OSPF on Ethernet Routing Switch 8600 Chassis N, and LOC on Ethernet Routing Switch 8600 Chassis X.

```
sho ip route info ip 172.16.201
```

The routing information under the PROT column heading must indicate OSPF for all VSP VLANs on Ethernet Routing Switch 8600 Chassis N. If it does not, contact your next level of support.

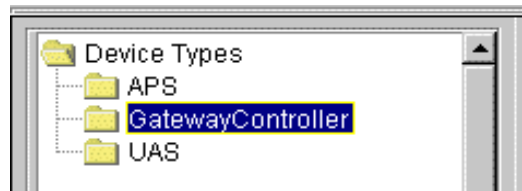
- 16 You have completed this procedure. Return to the procedure that sent you here.

Disabling GWCs that subtend the slave Ethernet Routing Switch 8600

Using your web browser

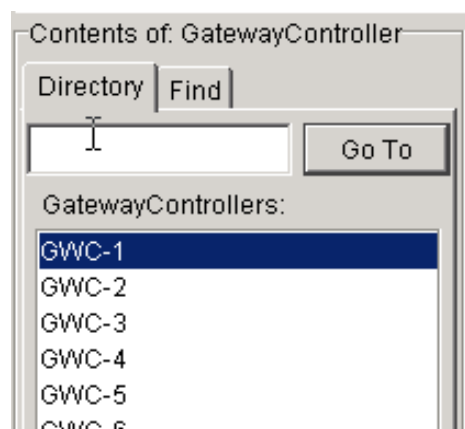
- 1 Launch CS 2000 Management Tools from your web browser. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).
- 2 Access the Maintenance information for the GWCs as follows:
 - a Select **GatewayController** from the **Device Types** field of the CS2000 Management Tools GUI.

The **GatewayController** folder in the **Device Types** field is highlighted.



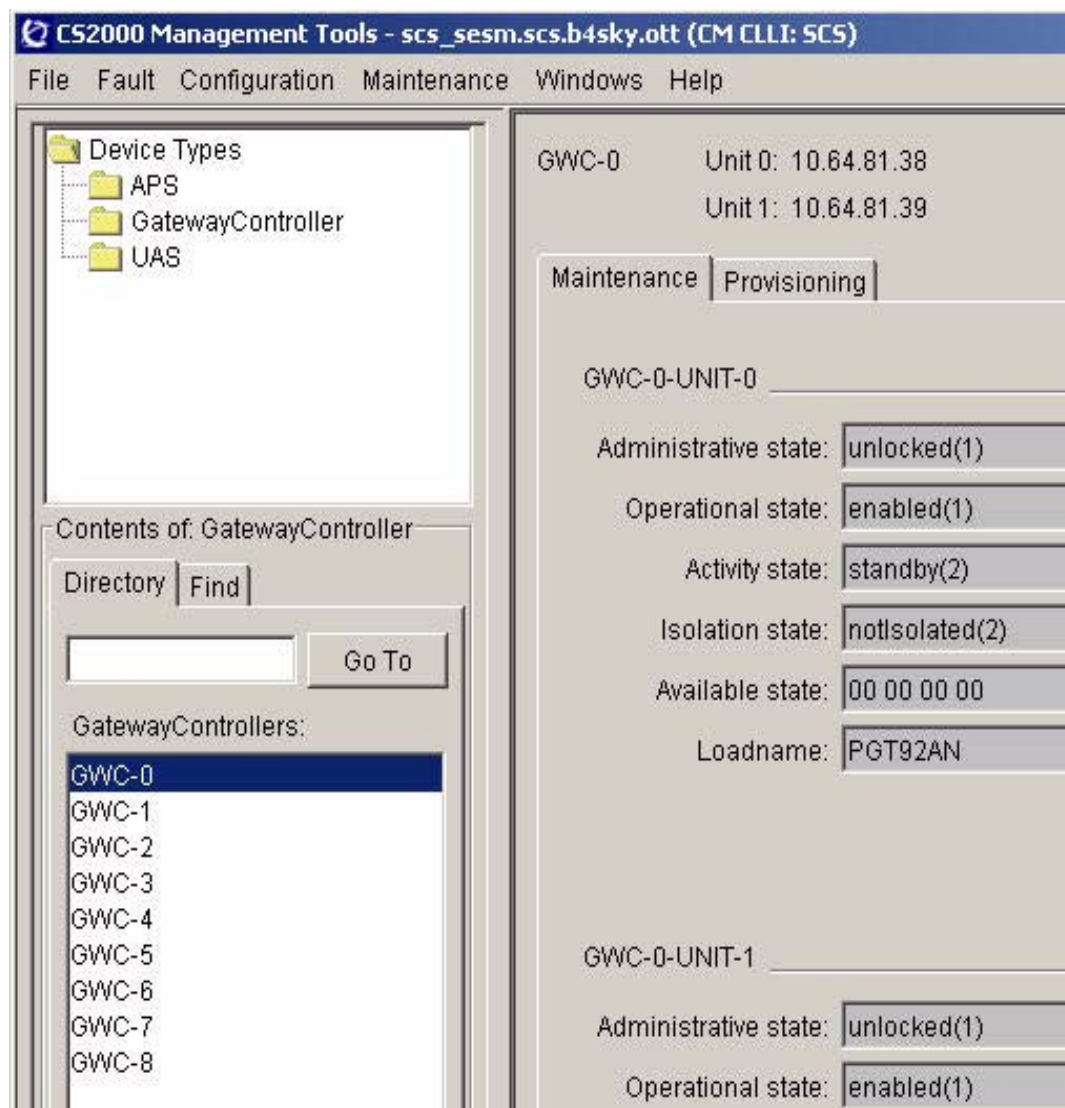
- b Select the **Directory** tab under **Contents of: Gateway Controller**.

The list of Gateway Controllers (GWC) appears.



- c Select the first GWC in the list.

The GWC is highlighted and the related Maintenance or Provisioning information (depending on the active tab) appears in the large right-hand field.



d Select the **Maintenance** tab to make sure the Maintenance information is displayed.

3 Make all GWCs inactive on Ethernet Routing Switch 8600 Chassis **N**.

Note: Recall that the recommendation in procedure [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#) requires that GWC unit 0s subtend Ethernet Routing Switch 8600 Chassis 0. GWC unit 1s subtend Ethernet Routing Switch 8600 Chassis 1. The following table reiterates the Ethernet Routing Switch 8600 Chassis configurations identifying iteration and master/save

status. Remember, this must be checked twice based on the iteration

Iteration		Comment
First Pass	N = 1	Chassis 1 Master
Second Pass	N = 2	Chassis 0 Master

- a** Check the **Activity State** field for GWC Unit N to determine which unit is **active** and which is **standby**

If the Activity State field is Do

active [step 3b](#)

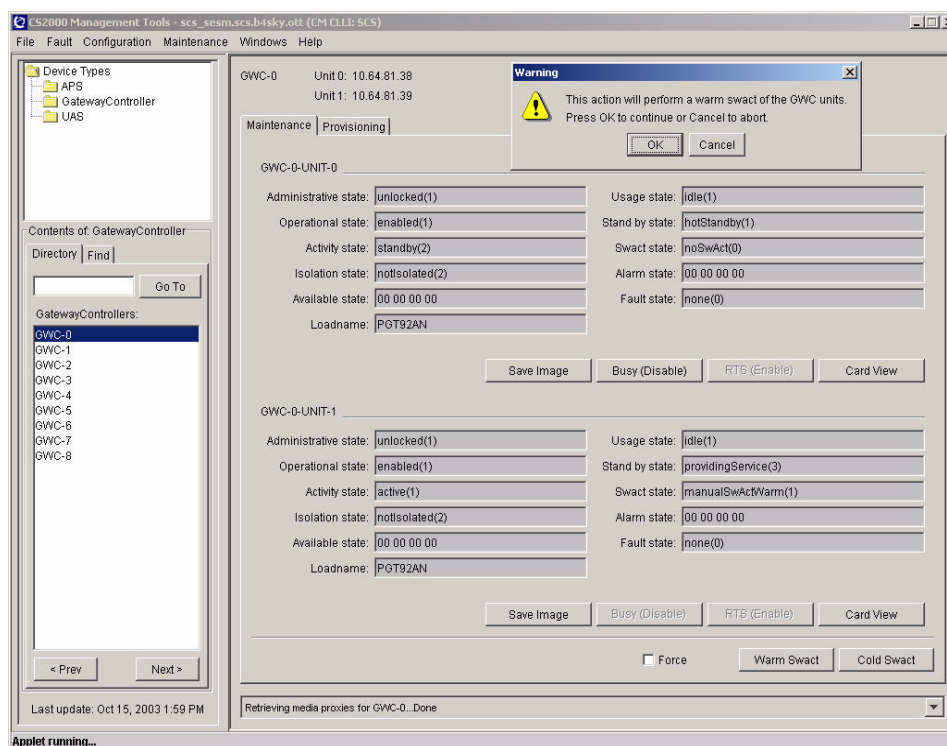
standby, instead of inactive [step 3d](#)

Note: For the first iteration, all GWC 0 units must be standby. For the second iteration, all GWC 1 units are standby.

- b** Click **WarmSwact**.

A warning window appears.

Click OK to continue or Cancel to abort.





- c Click OK, and wait for the activity change to complete.

The selected GWC undergoes a change of activity. The change of activity can take approximately 2 minutes.

- d Select the next GWC in the list, and repeat these substeps until the **Activity State** field for **Unit: N Status** is **standby** for all GWCs.

- 4 You have completed this procedure. Return to the procedure that sent you here.

Disabling the Ethernet links between an XA-Core and HIOPs and the Ethernet Routing Switch 8600

At the MAP terminal

- 1 Log on to the CS 2000 MAP terminal using a valid userid and password.
- 2 Enter the following command to access the ETHR level of the MAP display.

>MAPCI;MTC;XAC;ETHR

The following is a sample MAP display for the ETHR level.

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
ETHR			Front: 11111111	Rear: 111111	SM	PE	IO	PKLT	
0 Quit			123456789012345678	456789012345	SM M	.	HIOPfl	LINKfl	
2			Sta M-- . .		1	0	3	2	
3			Dep F	F FFF F FF					
4			Typ:	** * *					
5			Slot: Side: Packlet: Status: Port Link						
6 Tst_			5 Rear	.	.				
7 Bsy_			14 Rear	.	.				
8 RTS_									
9									
10 LoadFW_									
11									
12 Uneq_									
13									
14 Alarm_									
15 Cntrs_									
16									
17 Indicat_									
18 Query_									

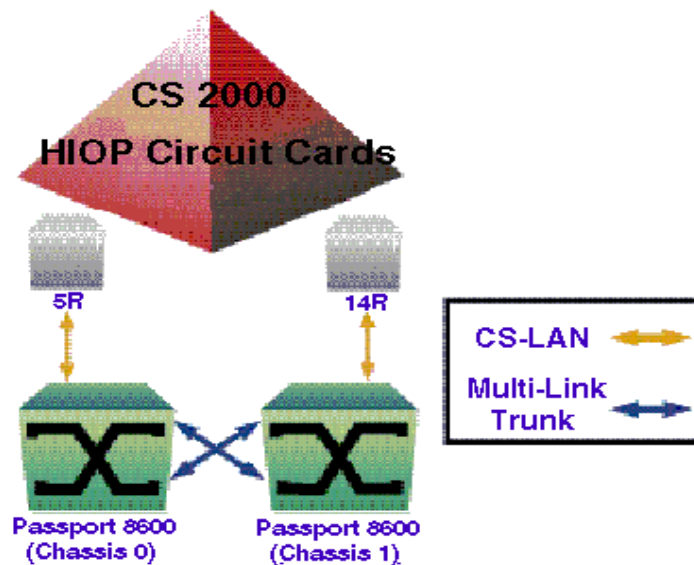
- 3 Refer to the following figure and table. Enter the following command to disable the XA-Core to Ethernet Routing Switch 8600 Chassis N Ethernet link.

bsy <slot> r link force

Accept the state change by typing Y.

Note: Executing this command produces an alarm indicating that the port is down. Ignore this alarm.





HIOPs/HCMICs	N = 1	N = 2
<slot>	5	14

Note: In the previous configuration, one HIOP is connected to each Ethernet Routing Switch 8600.

- 4 You have completed this procedure. Return to the procedure that sent you here.

Locking the USP-Compact

At the USP Compact (USPc) GUI

1

ATTENTION

Prior to adhering to steps [2](#) to [17](#), ensure that the slave USPc blade is being addressed during the first iteration of the Ethernet Routing Switch 8600 software upgrade.

Refer to your network diagram and determine the USPc blade-to-Ethernet Routing Switch 8600 connectivity. The slave USPc blade must connect to Chassis N of the Ethernet Routing Switch 8600; master USPc blade to Chassis X. (This information coincides with the network element-to-Ethernet Routing Switch 8600 assumptions stated in procedure [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100.](#))

Preparing the slave USPc blade for locking consists of the following tasks:

- inhibiting all SS7 links on the slave USPc blade

Note: If only one link is available on a linkset, it cannot be inhibited. If there are other links on the linkset, ensure at least one of the links is available before attempting to inhibit the link.

- deactivating all SS7 links on the slave USPc blade
- bringing down all IPS7 paths on the slave USPc blade
- locking the slave USPc blade from the USPc GUI

Note: Both USPc blades carry traffic and are in service.

2 Launch the USPc GUI.

3 Select **Configuration --> platform --> Node->Search**.

The Administration tab of the USPc GUI displays.

The screenshot shows the Administration tab of the USPc GUI. The interface includes a toolbar with icons for New, Add, Modify, Delete, Lock, Unlock, Load, Offline, Swact, and Restart. Below the toolbar are tabs for Administration, Search, and Graphical View. The main content area is divided into three sections: Provisioning Data, Operational Data, and Boot Data.

Provisioning Data

slot-type	usp-compact			
slot-name	USP1			
slot-description	USP-Compact #1			
shelf	0			
slot	15			
t1-e1-mode	t1			
ext-ip-address	47	131	125	82
ext-subnet-mask	255	255	255	128
ext-gateway	47	131	125	126
front-pec	NTRX51FN			

Operational Data

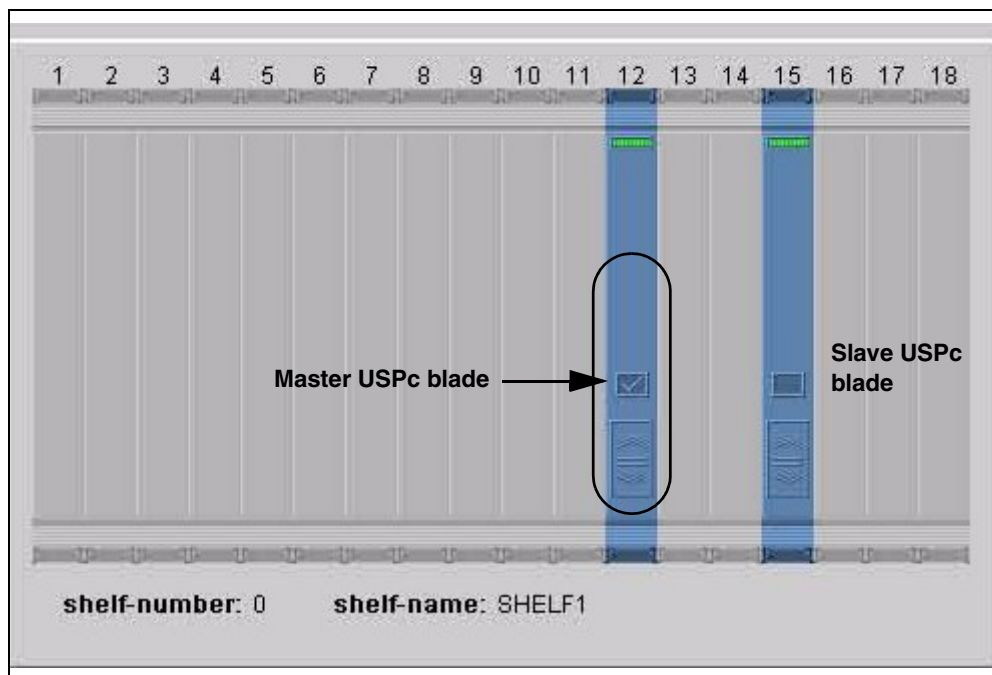
operational-state	enabled
administrative-state	unlocked
procedural-state	null
availability-state	null
activity-state	inactive
rex-status	

Boot Data

status-message	
running-image	samss7_ppc750_10_00_01_06g
ha-running-image	ss7t1e1ha_ppc8260_10_00_01_06g
running-snapshot	current active
boot image	uspc_10_00_01_06g_base
ha-boot-image	uspc_10_00_01_06g_t1e1ha
boot-snapshot	current active
snapshot-description	current active
snapshot-date	
snapshot-version	

loading complete

- 4 Verify the master and slave USPc blade-to-Ethernet Routing Switch 8600 connectivity by selecting the Graphical View tab. The following figure displays the Graphical View of the USPc blades.



The icon with a checkmark identifies the master USPc blade. Slot 12 contains the master USPc blade. Slot 15 contains the slave USPc blade.

- 5 Select the next step as follows.

If the slave USPc blade is	Do
not connected to Chassis N of the ERS 8600	step 6
connected to Chassis N of the ERS 8600	step 7

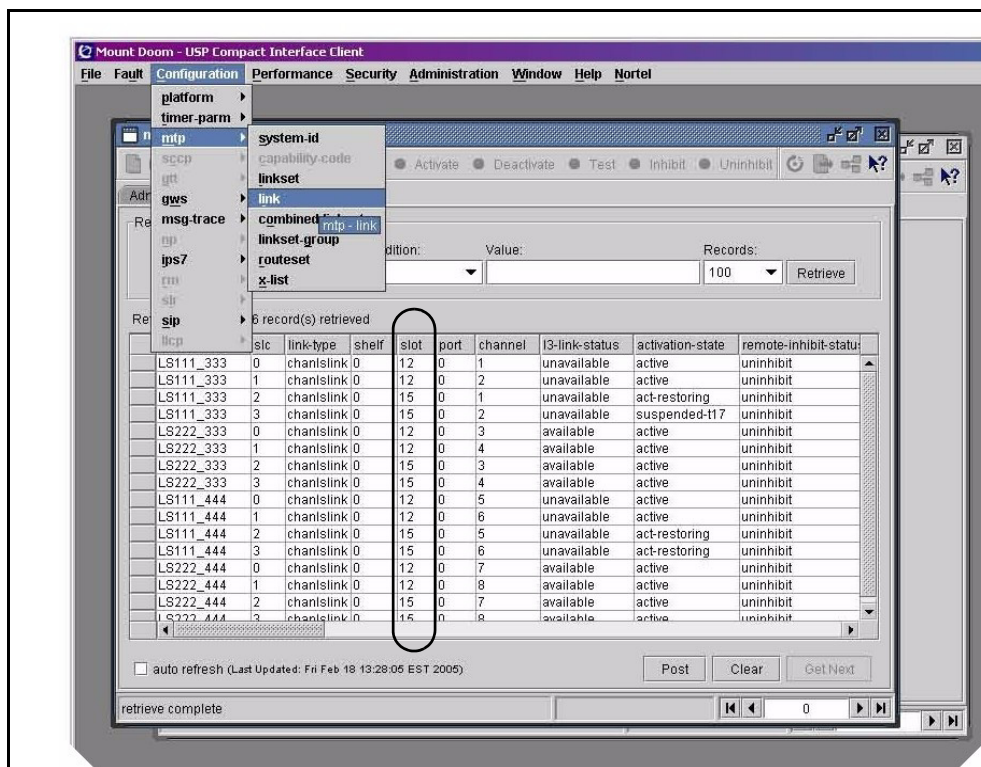
- 6 In the Administration tab, click **Swact** to perform a SWACT on the two USPc blades.

- 7 Turn down the paths and the links associated with the slave blade to be locked.

Select **Configuration --> MTP --> Links** from the pull-down menu.

Select **Search->Retrieve**.

The following screen appears.



- 8 Refer to the Slot column to verify the SS7 links against the USPc blades. Select any SS7 links that are against the slave USPc blade.

Post the link. The following prompt displays:

Execute mtp link inhibit command?

Click **Inhibit** to inhibit the links that apply to the slave USPc blade.

The following prompt displays.

The inhibit command will be executed for all posted records.

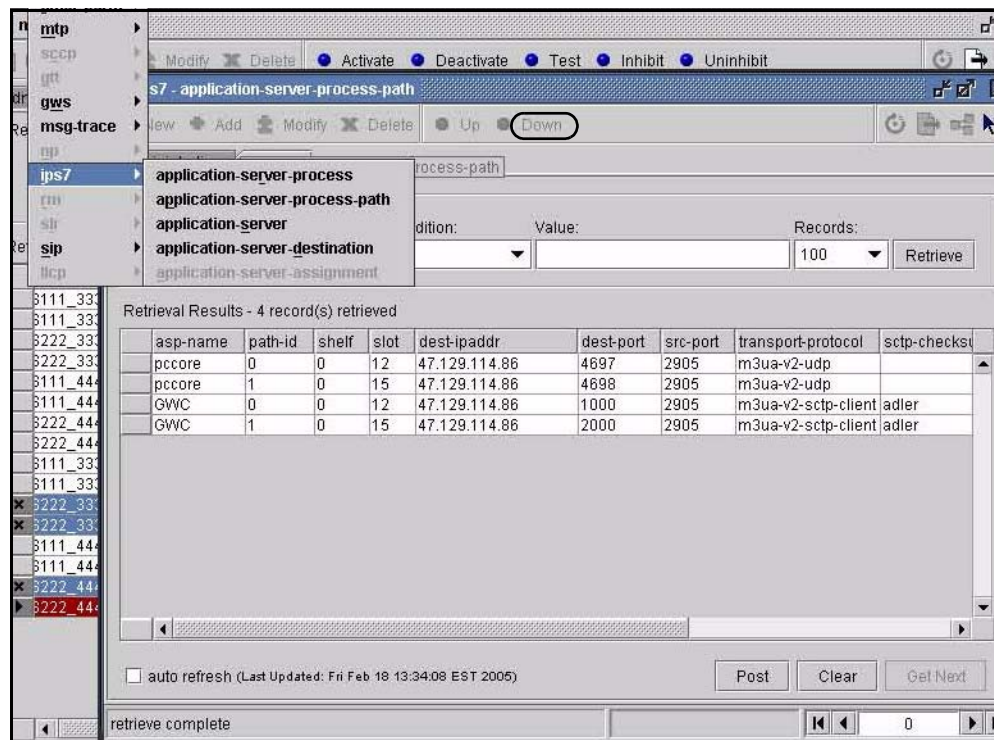
Are you sure you want to continue?

- 9 Click **Yes** to execute the command on the selected links.
- 10 Using the same screen, reselect the links, and click **Deactivate**. The following prompt displays.
- Execute mtp link deactivate command?
- 11 Click **Yes** to execute the command on the selected links.
- 12 Post the IPS7 paths that use the slave USPc blade.

Select **Configuration --> ips7 --> application-server-process-path**.

Select **Search->Retrieve**.

The following screen appears.



- 13** Post the IPS7 paths against the slave USPc blade. The following prompt displays:

Execute ips7 application-serverprocess-path
down command?

Select all the IPS7 paths against the slave USPc blade, and click **Down**.

The following prompt displays:

The down command will be executed for all posted records. Are you sure you want to continue?

- 14** Click **Yes** to execute the command on the IPS7 paths on the slave USPc blade.

The IPS7 paths and SS7 links against the slave USPc blade have been deactivated.

- 15** Lock the slave USPc blade.

Select **Configuration --> platform --> Node**.

The Administration tab, shown in [step 3](#), redisplay.

- 16** Click **Lock**.

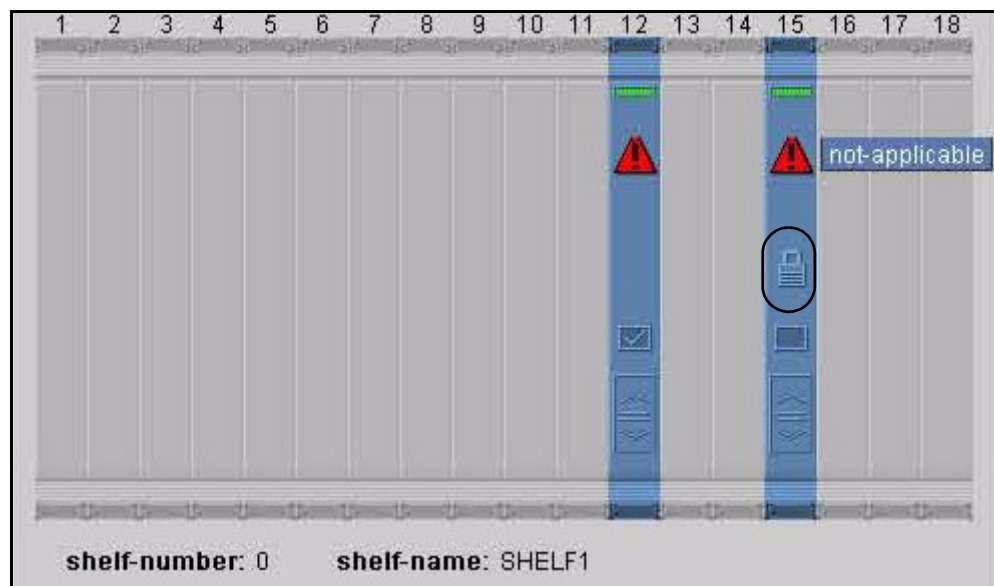
The following prompt displays:

The node lock command will impact the last in-service link in at least 1 linkset and cause at least 1 routeset to become inaccessible which may impact network traffic. Do you want to continue?

- 17** Click **Yes** to lock the USPc blade.

Click the **Graphical View** tab.

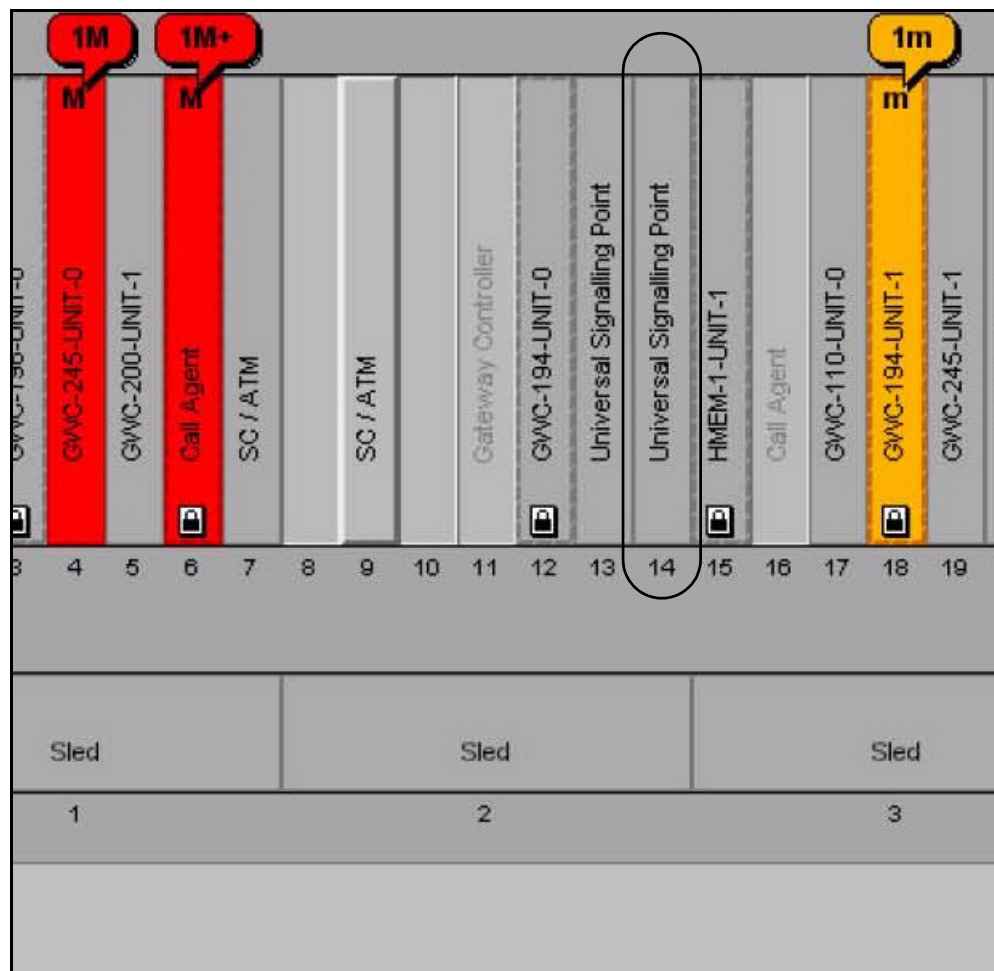
The Graphical View tab shows that the USPc blade has a lock icon next to it, indicating it has been locked.



Use the SAM21 Manager to lock the USPc blade

- 18** Access the SAM21 Manager GUI.
- 19** Select the SAM21 shelf by double-clicking on its icon.

The following figure shows an example of a shelf which contains a slave USPc blade residing on slot 14.



- 20** Right-click on the icon that corresponds to where the slave USPc blade resides.

A sub-window appears with the Card View and Lock selections enabled.



21 Click **Lock**.

The slave USPc blade is locked.

Note 1: This prevents an automatic change of activity from occurring. An automatic SWACT at this point can cause a system outage.

Note 2: An alternative method to lock the blade from the SAM21 Manager is to first open the card by double-clicking on it. Then click Lock in the States tab.

22 You have completed this procedure. Return to the procedure that sent you here.

Taking down the paths to the Ethernet Routing Switch 8600 Chassis N

At the USP GUI

- 1 Launch the USP GUI.

Taking down the paths to the Ethernet Routing Switch 8600 Chassis N consists of the following tasks:

- identifying all IP cards in the USP, and noting which Ethernet Routing Switch Chassis they are connected to
- ensuring that for each path, there is an alternate in-service path through Chassis X
- taking down all IPS7 paths using Chassis N

- 2 Select **Configuration->platform->node->Search**.

- 3 Click **retrieve**, and look for all records that have a slot-type of iplink.

- 4 Note the following information for each IP link card:

- Shelf
- Slot
- IP Address
- ERS8600 unit it is connected to

- 5 Select **Configuration->ips7->application-server-process-path->Search**

- 6 Click **retrieve**, and look for all paths on the cards noted in [step 4](#), that are connected to Chassis N.

- 7 Click on the **asp-name** column to sort the table, and confirm that for each path connected to a card using Chassis N, there is an alternate path using Chassis X that has a path-state of up. Refer to the information you noted in [step 4](#).

- 8



CAUTION

Potential service interruption

If the alternate path to any destination is not in service, performing the step that follows will result in a service interruption.

Select each path connected to Chassis N, and click **Post**, then confirm that only the paths associated with the cards connected

to Chassis N, are selected. Refer to the information you noted in [step 4](#).

- 9** Click **Down** to take the posted paths out of service.
- 10** Click **Yes** to confirm the command execution on the IPS7 paths associated with the cards connected to Chassis N.
- 11** You have completed this procedure. Return to the procedure that sent you here.

Determining if STORM devices require rotating, demounting and busying

At your desk

1

ATTENTION

Before proceeding with the following STORM-related steps, consider if other applications will be affected by the loss of STORM disk volumes.

Select the next step as follows

If	Do
STORM uses a Dothill device	step 2
STORM IA (SAM-XTS) device ¹	step 15

1. The SAM-XTS configuration uses dual-homed split multilink trunks (SMLT). Both STORM volumes are recognized by both Ethernet Routing Switch 8600 routers. Therefore, taking down one router in an SAM-XTS configuration does not affect the STORM volume being addressed.

2

Select the next step as follows.

If	Do
the volumes on any STORM disk (for example, sd01) are actively mounted in Device Independent Recording Package (DIRP) ¹	step 3
the volumes on the STORM disk are not actively mounted DIRP ²	step 15

1. Loss of network connectivity between SOS, the call processing application, and the active STORM disk can cause some or all DIRP volumes to be marked "INERROR," resulting in permanent loss of data.

2. Regardless of whether DIRP volumes are mounted, the procedure can result in an unavailable STORM disk and associated volumes.

3

If needed, enter the following command to check which STORM device is connected to the Ethernet Routing Switch being upgraded. If configured properly, XTS0 should have a lower IP address than XTS1.

```
sho ip arp info <STORM_address>
```

where

<STORM_address>

is the IP address of the STORM device

- 4 Login to the Call Agent as a maintenance user.
- 5 Enter the DF command to map the STORM volumes to XTS IP addresses.

\$ df

Example response

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
tmpfs	51200	36352	14848	71%	/
10.102.16.112:/nfsserv/3pc/mtc/tape1					
	1019200	14216	1004984	2%	/TAPE1
10.102.16.111:/nfsserv/3pc/mtc/tape0					
	1019200	239004	780196	24%	/TAPE
10.102.16.112:/nfsserv/3pc/cs/sd01					
	8187200	1972256	6214944	25%	/3PC/sd01
10.102.16.111:/nfsserv/3pc/cs/sd00					
	8187200	2196124	5991076	27%	/3PC/sd00
10.102.16.112:/nfsserv/3pc/mtc/log1					
	1019200	14216	1004984	2%	/var/log_mate
10.102.16.111:/nfsserv/3pc/mtc/log0					
	1019200	239004	780196	24%	/var/log

- 6 Based on the responses of [step 3](#) and [step 5](#), determine which XTS volume (SD00 or SD01) corresponds with the STORM.
- 7 Logout of the Call Agent.
- 8 From the Core MAP command line, enter the following command to list all available DIRP subsystems (field SYSSNAME in table DIRPSSYS) for the Core.

>table dirpssys; lis all

- 9 Enter the following command to access the DIRP level in SOS.

>mapci nodisp;mtc;iod;dirp

- 10 Enter the following command to query all volumes associated with the subsystem.

>query <subsystem> all

where

<subsystem>

is from the list of available subsystems executed in [step 8](#).

The following figure shows an example of this command for the dlog subsystem with an active file highlighted.

```

>query dlog all
SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL EMERGENCY
DLOG      1      1      3      7  NONE      ***YES***

REGULAR
FILE(S)   STATE VOLUME   RECCOUNT BLOCK E  V  V_B VLID FNUM FRN#
ACTIVE    AVAIL SD00DLG1      1      1 0 71 NO  8448 000D 1014
STANDBY1  AVAIL SD01DLG1      0      0 0 70 NO  8408 0015 3012

PARALLEL
FILE              STATE VOLUME   BLOCK E  V  V_B VLID FNUM FRN#
              NONE

REGULAR VOLUME(S)
VOL# VOLNAME  STATE          IOC CRD PORT VOL FSEG ROOM VLID FILES
  70 SD01DLG1 READY          N/A N/A N/A   8   10   11 8408 S1
  71 SD00DLG1 READY          N/A N/A N/A   8  112  116 8448 A

REGULAR SPACE
VOL# VOLNAME  STATE          SEGS   EXP UNEXP TOTAL
  70 SD01DLG1 READY          10     1     0    11

```

- 11** Enter the following command to rotate the active volume for each subsystem if it is located on a STORM blade connected to the router being upgraded for this iteration. Manually rotate all subsystems until the active files reside on STORM volumes connected to the Ethernet Routing Switch 8600 chassis that is not being upgraded for this iteration.

>rotate <subsystem> <variable>

where

<variable>

is regular, paralel, or both (Enter regular to rotate regular volumes. Enter paralel to rotate parallel volumes. Enter both to rotate both volumes.)

Note 1: Parallel is intentionally misspelled.

Note 2: The volume associated with the slave Ethernet Routing Switch 8600 must not be active. Ensure that no volume is active in each pass which is prefixed with sd0M.

where

M

M = 0 or 1, depending on which volume is connected to the Ethernet Routing Switch 8600, determined in [step 6](#).

(Rotate each subsystem with volumes prefixed with sd0M that are active.)

Note: To minimize risk, rotate and demount the AMA subsystem last. Then restore the AMA subsystem first.

The following figure shows example of input for variable regular.

```
>rotate dlog REGULAR
ACTIVE FILE WILL BE CLOSED IF POSSIBLE (ROTACLOS).
SENDING REQUEST TO SUBSYSTEM
Please confirm ("YES", "Y", "NO", or "N"):
>y
REQUEST SENT TO SUBSYSTEM, CHECK DIRP LOG FOR DETAILS
```

12 Repeat [step 11](#) to ensure that all volumes needing rotating have been rotated successfully.

13 Enter the following command to demount all DIRP volumes connected to the Ethernet Routing Switch 8600 chassis that is to be upgraded.

>dmnt <subsystem> <volume> <variable>

where

<volume>

is the volume on the STORM determined in [step 6](#)

<variable>

is regular or parallel

Note 1: The <variable> parameter is not required when mounting and demounting regular DIRP volumes.

Note 2: Nortel recommends recording all subsystems, volume, and variable information for each volume being demounted in this step.

- 14** Enter the following command to busy all STORM volumes connected to the Ethernet Routing Switch 8600 chassis to be upgraded.

```
>diskadm sd0M; bsy all
```

where

sd0M

is the STORM volume defined in [step 6](#)

Note 1: Nortel does not recommend using option bsy all force.

Note 2: Issuing a bsy all command affects all volumes serviced by that STORM blade, not just those used by DIRP.

- 15** You have completed this procedure. Return to the procedure that sent you here.

Locking the inactive Shelf Controller (SC) blade connected to Chassis N

At the SAM21 Manager

1

ATTENTION

During a SWACT on the SCs, flapping (that is, rapid enabling and disabling of the router port connected to an SC) can result in temporary loss of Ethernet connectivity. This can cause ongoing failures on the newly active SC following the SWACT.

To prevent the possibility of an outage from this condition, monitor ongoing or recent logs for Ethernet instability on the router ports that are associated with the SCs.

Do not SWACT the SCs until all network problems involving flapping are addressed.

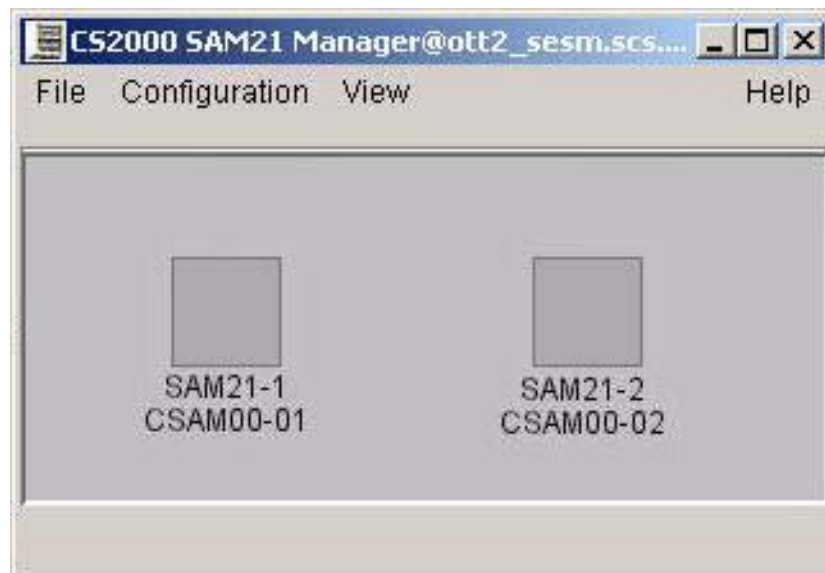
Confirm that SC blade connectivity complies with the recommendations in procedure [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#) for all SAM21 shelves.

Note: Recall that the recommendation at [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#) requires SC unit 0s (in slot 7) subtend Ethernet Routing Switch 8600 Chassis 0, and SC unit 1s (in slot 9) subtend Ethernet Routing Switch 8600 Chassis 1. If the SAM21 shelf varies from this recommendation, adjust this procedure accordingly.

2 Lock the inactive SAM21 SC blade for each SAM21 shelf in turn as follows:

a Launch the SAM21 Manager.

The SAM21 Manager GUI appears with the related shelf icons displayed.

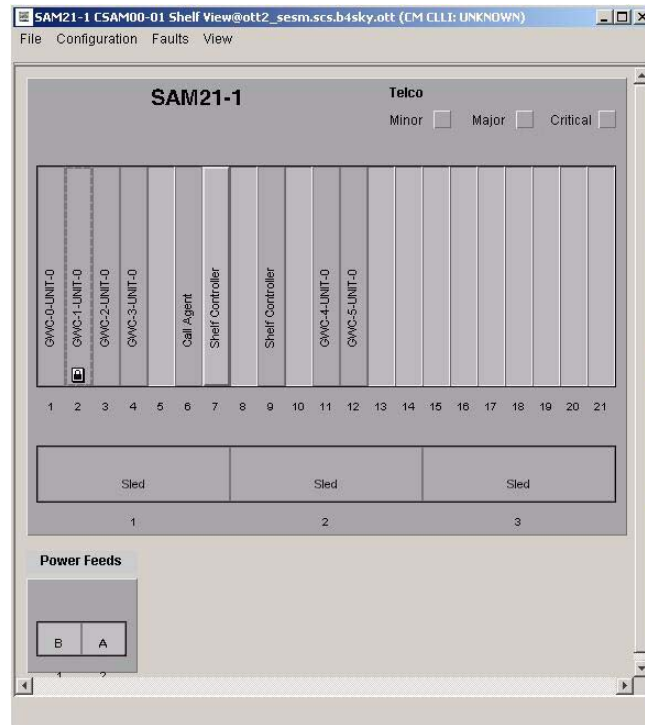


- b** Use the cursor to select the shelf icon for the first SAM21 shelf displayed.

Example

The first shelf in the preceding figure is SAM21-1 CSAM00-01

- c** Double-click the selected shelf icon.
The SAM21 Manager shelf view for the selected shelf appears.



- d Right-click on the icon for the SC blade associated with the inactive Ethernet Routing Switch 8600 Chassis.

Note: The SC blade in slot 7 subtends Ethernet Routing Switch 8600 Chassis 0; slot 9 subtends Chassis 1 (see note to [step 1](#)).

A sub-window appears with the **Card View** and **Lock** selections enabled.



- e Click **Card View**.

The SC Card View appears.

The screenshot shows a web-based configuration interface for a Nortel Networks device. At the top, there are tabs: Alarms, Equip, States, Diags, and Provisioning. The 'States' tab is selected. Below the tabs, there are three main sections: Activity, OSI, and History. The Activity section has a 'Status' dropdown menu set to 'Active' and a 'Swact' button. The OSI section has three rows: 'Administrative' with a dropdown set to 'Unlocked', 'Operational' with a dropdown set to 'Enabled', and 'Availability' with a dropdown set to 'None'. To the right of these dropdowns are 'Lock' and 'Unlock' buttons. The History section is a large empty box with a scrollbar. At the bottom of the interface are 'Save' and 'Clear' buttons.

- f Select the **State** tab and make sure the SC is inactive.
If the SC state is **Active**, click **Swact** to change the activity status to **Inactive**.
- g Close the **Card View**.
The **Shelf View** reappears.
- h Right-click on the icon for the inactive SC blade.
A sub-window appears with the **Card View** and **Lock** selections enabled.
- i Click **Lock**.
The inactive SC blade is locked.
Note: This prevents an automatic change of activity from occurring. An automatic SWACT at this point can cause a system outage.
- j Close the **Shelf View**.
The SAM21 Manager view reappears.

k Select the next step as follows

If the (inactive) SC cards are	Do
locked on all SAM21 shelves	Proceed to step 3
not all locked	select the next SAM21 Shelf and go to sub step 2c

Note: Repeat substeps [2c](#) through [2j](#) until the inactive SCs are all locked.

- 3** You have completed this procedure. Return to the procedure that sent you here.

Disabling Geographic Survivable components

Use the Integrated Element Management System (IEMS) GUI to lock the Media Server 2000 (MS 2000) Series node connected to Chassis N

- 1 Launch the IEMS GUI.
Note: Refer to *IEMS Basics*, NN10329-111, for details on logging into the IEMS GUI.
- 2 Select **Applications ---> Integrated EMS --->Network Elements**.
- 3 Select the MS 2000 Series node to be locked, and right-click on its icon.
- 4 Select the Config and Maintenance Tool from the pop-up menu. The Config and Maintenance Tool launches.
Note: For details, refer to procedure “Launching the Maintenance and Configuration tool” in section Configuring and maintaining MS 2000 devices, in *IEMS Configuration Management*, NN10330-511.
- 5 From the left side of the Config and Maintenance Tool screen, click **Graceful Lock** under the Lock State options to lock the MS 2000 node.
Note: A graceful lock signals to the node that a lock has been requested. The node then stops allocating new audio resources and waits for the last resource to be freed before locking the node. (A forced lock causes the node to immediately free up any resources in use and lock the node.)
- 6 Click **Lock** to gracefully lock short-duration calls from the MS 2000 node.
Note: Since a graceful lock prevents new calls from being originated on the node, existing calls are taken down on their own. For calls still active after an extended period of time, it is up to the discretion of the user to determine whether to issue a forced lock, or to proceed when the Ethernet Routing Switch 8600 is rebooted.

Drop sync the inactive Call Agent

- 7 Before locking the inactive Call Agent card, enter the following commands to drop synchronization on the inactive Call Agent card from the active Call Agent Manager.

 > **ccamt c**

```
> coremtc
```

```
> appl
```

```
> dpsync
```

- 8 Select the next step as follows

If the (active) Call Agent card is	Do
connected to Ethernet Routing Switch 8600 Chassis N	step 9
not connected to Ethernet Routing Switch 8600 Chassis N	step 16

Perform a *LIMITED_PRESWACT*

- 9 At the MAP display, enter the following command to initiate a limited preswact.

```
> BCSUPDATE; LIMITED_PRESWACT
```

Note 1: If a limited preswact process fails to complete, it stops and displays additional information. When this occurs, use the information to investigate and correct the problem.

Note 2: Complete all limited preswact steps prior to SWACTing.

The LIMITED_PRESWACT command displays a warning:

```
Limited_Preswact should not be used for
BCSUPGRADE SWACTs. Do you wish to continue?
Please confirm ("YES", "Y", "NO", "N"):
```

- 10 Enter the following command to confirm you want to continue.

```
> Y
```

A series of steps execute and complete. LIMITED_PRESWACT stops at MATE_RESTART_RELOAD.

```
MATE_RESTART_RELOAD executing
There are users still logged on the Inactive.
Do you want to continue?
MATE_RESTART_RELOAD not complete
ACT - Error: Restart aborted. Type
LIMITED_PRESWACT to continue
Investigate and correct if needed.
```

- 11** If the limited preswact process halts, re-enter the following command to continue.

> LIMITED_PRESWACT

The following warning displays.

```
MATE_RESTART_RELOAD executing
There are users still logged on the Inactive.
Do you want to continue?
Please confirm ("YES", "Y", "NO", "N"):
```

- 12** Enter the following command to confirm you want to continue.

> Y

The inactive unit indicates /restart at the Call Agent Manager. Several more steps execute and complete at the MAP. The following message indicates successful completion:

```
Total execution time for all complete procedures
00:07:31.362
All LIMITED_PRESWACT steps completed
successfully.
```

Perform a NORESTARTSWACT

- 13** If the active Call Agent card is connected to the Ethernet Routing Switch 8600 to be upgraded, minimize the possibility of an outage by performing a NORESTARTSWACT.

- a** Enter the following command to check the status.

> BCSUPDATE;SWACTCI;STATUSCHECK

The following response displays:

```
SWACTCI:
Checking Nodes Status
STATUSCHECK successful
```

- b** Enter the following command to execute the NORESTARTSWACT.

> NORESTARTSWACT

Progress is printed and the process stops to verify that the inactive Call Agent is not jammed.

Beginning SWACT checks:

All the SWACT checks have finished successfully.

The VR_PRESWACT_TRANSFER step completed successfully.

All INSV and ISTB series 1 PMs will have execs loaded after the SWACT.

Device Checking Status:

NOMATCH option is set to OFF <default setting>.

Device matching during CC WARM SWACT Enabled.

Do you wish to continue?

Please confirm ("YES", "Y", "NO", or "N"):

>

- c** If the only alarm is an APPL simplex, enter the following command to confirm you want to continue.

> Y

The final progress follows. Activity also switches at the Call Agent Manager.

All Pre_SWACT checks completed. Starting Warm SWACT now.

**** The cursor will not be returned. ****

**** unless a critical failure occurs.****

**** Now monitoring Warm SWACT messages.****

Pre-initialization done

Communication established

Exchange of data with the mate done

Transfer of data done (FASPECT)

Data estimation done

- d** The telnet session to the active and inactive call processing applications are lost. Re-establish the connection. Refer to the Call Agent upgrade procedure [Interface setup on page 1850](#).

Perform a POSTSWACT

- 14 At the MAP display, enter the following command to run a Postswact through completion.
- > **BCSUPDATE;POSTSWACT**
- 15 Enter the following command when prompted at the CA_SYNC step to leave the switch out of sync.
- > **N**

Lock the inactive Call Agent card

16

**CAUTION****Potential service outage**

Do not attempt to lock the active call agent card. Locking the active unit causes a complete service outage.

To lock the inactive Call Agent, follow these substeps:

- a Access the SAM21 Manager GUI.
- b Select the SAM21 shelf by double-clicking on its icon.
- c From the Shelf View, right-click on the card that corresponds to the inactive Call Agent card.
- d Select the **Lock** option from the context menu.

Note: Lock is also available from the States tab of the Card View window.

- e Wait for the Lock icon to appear on the selected card.

**Demount active DIRP volumes off of SD0M
(where M = 0 or 1, which is connected to the Ethernet Routing
Switch 8600 being upgraded)**

- 17 If needed, enter the following command to check which STORM device is connected to the Ethernet Routing Switch being upgraded. If configured properly, XTS0 should have a lower IP address than XTS1.

sho ip arp info <STORM_address>

where

<STORM_address>

is the IP address of the STORM device

- 18 Login to the Call Agent as a maintenance user.

- 19** Enter the DF command to map the STORM volumes to XTS IP addresses.

\$ df

Example response

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
tmpfs	51200	36352	14848	71%	/
10.102.16.112:/nfsserv/3pc/mtc/tape1	1019200	14216	1004984	2%	/TAPE1
10.102.16.111:/nfsserv/3pc/mtc/tape0	1019200	239004	780196	24%	/TAPE
10.102.16.112:/nfsserv/3pc/cs/sd01	8187200	1972256	6214944	25%	/3PC/sd01
10.102.16.111:/nfsserv/3pc/cs/sd00	8187200	2196124	5991076	27%	/3PC/sd00
10.102.16.112:/nfsserv/3pc/mtc/log1	1019200	14216	1004984	2%	/var/log_mate
10.102.16.111:/nfsserv/3pc/mtc/log0	1019200	239004	780196	24%	/var/log

- 20** Based on the responses of [step 17](#) and [step 19](#), determine if which XTS volume (SD00 or SD01) corresponds with the STORM.
- 21** Logout of the Call Agent.
- 22** At the MAP display, enter the following command to access the DIRP level.
- >MAPCI NODISP;MTC;IOD;DIRP**
- 23** Enter the following commands to query the subsystem and determine which files are active and which are standby.
- >QUERY JF FILES**
- >QUERY DLOG FILES**
- 24** Enter the following commands to demount all volumes on SD0M for the subsystems that are not active.
- >DMNT DLOG SD0MDLG0**
- >DMNT DLOG SD0MDLG1**
- >DMNT DLOG SD0MDLG2**
- Note:** The above command syntax includes reference to SD0M.

where

M

is 0 or 1, which is connected to the Ethernet Routing Switch 8600 being upgraded

- 25** Enter the following commands to rotate the subsystems to a standby volume on the other STORM device.

>ROTATE JF

>ROTATE DLOG

- 26** Enter the following commands to query the subsystem again to verify that the active files are on the other STORM device.

>QUERY JF FILES

>QUERY DLOG FILES

- 27** Enter the following commands to demount any remaining volumes on SD0M.

>DMNT JF SD0MJF

>DMNT DLOG SD0MDLG3

Note: The above command syntax includes reference to SD0M.

where

M

is 0 or 1, which is connected to the Ethernet Routing Switch 8600 being upgraded

- 28** Enter the following commands to query the subsystem again to verify that no volumes on SD0M are used.

>QUERY JF FILES

>QUERY DLOG FILES

- 29** Repeat [step 23](#) for additional DIRP subsystems.

- 30** Enter the following command to quit the DIRP level.

>QUIT ALL

- 31** At the MAP display, enter the following command to busy all STORM disk volumes on device SD0M to ensure that the call processing application does not attempt to access the STORM unit.

>DISKADM SD0M;BSY ALL

If the devices do not pass, determine which application has open files. Perform maintenance on those applications so that the application closes the files.

- 32 You have completed this procedure. Return to the procedure that sent you here.

Upgrading the Ethernet Routing Switch 8600

At the Ethernet Routing Switch 8600 CLI

- 1 Access the Ethernet Routing Switch 8600s using the serial (console) port.

Note 1: Use either a serial connection and terminal program from an attached PC or TELNET session to an appropriately configured IP address on a terminal server.

Note 2: In dual CPU configurations, after any reset of the master CPU, the slave CPU becomes active. Ensure you continue the steps on the newly master CPU unless otherwise noted.

Note 3: If access fails, verify network topology, IP address, and Ethernet Routing Switch 8600 power supply. Try again. If the problem persists, contact your next level of support.

2

ATTENTION

Refer to section [Text conventions on page 77](#) for brief definitions and examples of the software filenames used in the following commands.

Select the next step as follows

If your CS-LAN	Do
is a dual CPU configuration	step 3
is a single CPU configuration	step 14

- 3 For an Ethernet Routing Switch 8600 with a dual-CPU configuration, TFTP the upgrade software to the flash directory on the master CPU. Then copy it to the slave CPU.

Note: Slot 5 is accessed as 127.0.0.5 in each chassis and slot 6 is accessed as 127.0.0.6. The @symbol is used to identify the slave CPU. Therefore the CPU being accessed will appear as:

- <switch_name>:5
- @<switch_name>:6

In the following substeps, both commands must be executed on the master CPU.

Note 1: There is an intentional space between the filename and “/flash/” at the end of the first command syntax in the following substeps.

Note 2: When performing the copy and file transfer through TFTP in the steps that follow, ensure the files were copied successfully. To verify the file transfer was successful, list the directory on the remote device where the files came from, and on the local device to which the files were copied and compare the file sizes.

- a Transfer the new software image file through TFTP using the commands appropriate to your core manager platform.

For the SDM/CS 2000 Core Manager, enter the following commands:

```
copy
<a.b.c.d>:/swd/pp8600/XXX/<p80axxxx.img>
/flash/

copy /flash/<p80axxxx.img>
127.0.0.x:/flash/<p80axxxx.img>
```

For the CBM, enter the following commands:

```
copy <a.b.c.d>:/pp8600/XXX/<p80axxxx.img>
/flash/

copy /flash/<p80axxxx.img>
127.0.0.x:/flash/<p80axxxx.img>
```

where

XXX

is the directory where the new software is located

<a.b.c.d>

is the IP address of the TFTP server

<p80axxxx.img>

is the name of the new software image file, where xxxx is the software load version and which must be in lower case, for example p80a37130.img

127.0.0.x

is the IP address of the slave CPU. If slot 6 is the master, then 127.0.0.5 is where the load is to be copied

Note: If either file transfer fails, verify the TFTP server IP address and connectivity with Ethernet Routing Switch

8600 Chassis N. Enter the following command to confirm Ethernet Routing Switch 8600 TFTP flag is set to true.

config bootconfig flags info

If the tftpd flag is set to false, enter the following command to reset the flag to true.

config bootconfig flags tftpd true

Confirm the flag is now set to true, then retry the transfer. If the problem persists, contact your next level of support.

Note 1: If the transfer completes but the file is corrupted, verify original file and PCMCIA card and transfer the file again. If the problem persists, contact your next level of support.

Note 2: Compare file parameters such as file size to check for possible corruption.

- b** Transfer the new boot monitor image file through TFTP using the commands appropriate to your core manager platform.

For the SDM/CS 2000 Core Manager, enter the following commands:

copy

```
<a.b.c.d>:/swd/pp8600/XXX/<p80bxxxxx.img>  
/flash/
```

```
copy /flash/<p80bxxxxx.img>
```

```
127.0.0.x:/flash/<p80bxxxxx.img>
```

For the CBM, enter the following commands:

```
copy <a.b.c.d>:/pp8600/XXX/<p80bxxxxx.img>  
/flash/
```

```
copy /flash/<p80bxxxxx.img>
```

```
127.0.0.x:/flash/<p80bxxxxx.img>
```

where

<a.b.c.d>

is the IP address of the TFTP server

<p80bxxxxx.img>

is the name of the new boot monitor image file, where xxxx is the software load version and which must be in lower case, for example p80b37130.img

The boot flash image and software image is backed up to the PCMCIA card on the Ethernet Routing Switch 8600 Chassis N.

- c Determine if the Ethernet Routing Switch 8600 has ATM modules installed by typing

sho sys info

Example response:

Card Info :							
Slot#	FrontType	FrontHw Version	Oper Status	Admin Status	BackType	BackHw Version	
1	ATM	4	up	up	BFM3		
2	48x100BaseTX	A	up	up	BFM6	A	
3	8x1000BaseIC	A	up	up	BFM8	A	
4	ATM	04	up	up	BFM3		
5	CPU	05	up	up	SFM		05

- d Only if Chassis N of Ethernet Routing Switch 8600 uses an ATM blade, transfer the ATM Flash image to the Flash card on the Ethernet Routing Switch 8600 Chassis N through TFTP using the commands appropriate to your core manager platform. Otherwise go to [step 5](#).

For the SDM/CS 2000 Core Manager, enter the following commands:

copy

**<a.b.c.d>:/swd/pp8600/XXX/<p80txxxx.dld>
/flash/**

copy /flash/<p80txxxx.dld>

127.0.0.x:/flash/<p80txxxx.dld>

For the CBM, enter the following commands:

**copy <a.b.c.d>:/pp8600/XXX/<p80txxxx.dld>
/flash/**

copy /flash/<p80txxxx.dld>

127.0.0.x:/flash/<p80txxxx.dld>

where

<a.b.c.d>

is the IP address of the TFTP server

<p80txxxx.dld>

is the name of the new ATM file, where xxxx is the software load version and which must be in lower case, for example p80t37130.dld

Note: Notes 1 and 2 from sub[step 3b](#) apply.

- e Determine if the Ethernet Routing Switch 8600 has encryption modules installed by typing

config info

Example response:

```
Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:
```

```
load-encryption-module : DES File p80cXXXXX.des
load-encryption-module : 3DES File p80cXXXXX.img
      setdate : N/A
mac-flap-time-limit : 500
auto-recover-delay : 30
```

- f If the Ethernet Routing Switch 8600 uses DES, transfer the file through TFTP using the commands appropriate to your core manager platform.

For the SDM/CS 2000 Core Manager, enter the following commands:

copy

```
<a.b.c.d>:/swd/pp8600/XXX/<p80cxxxxx.des>
/flash/
```

copy /flash/<p80cxxxxx.des>

```
127.0.0.x:/flash/<p80cxxxxx.des>
```

For the CBM, enter the following commands:

```
copy <a.b.c.d>:/pp8600/XXX/<p80cxxxxx.des>
/flash/
```

copy /flash/<p80cxxxxx.des>

```
127.0.0.x:/flash/<p80cxxxxx.des>
```

where

<a.b.c.d>

is the IP address of the TFTP server

<p80cxxxxx.des>

is the name of the new DES file, where xxxx is the software load version and which must be in lower case, for example p80c37130.des

- g If the Ethernet Routing Switch 8600 uses 3DES, transfer the file through TFTP using the commands appropriate to your core manager platform.

For the SDM/CS 2000 Core Manager, enter the following commands:

```
copy
<a.b.c.d>:/swd/pp8600/XXX/<p80cxxxx.img>
/flash/

copy /flash/<p80cxxxx.img>
127.0.0.x:/flash/<p80cxxxx.img>
```

For the CBM, enter the following commands:

```
copy <a.b.c.d>:/pp8600/XXX/<p80cxxxx.img>
/flash/

copy /flash/<p80cxxxx.img>
127.0.0.x:/flash/<p80cxxxx.img>
```

where

<a.b.c.d>

is the IP address of the TFTP server

<p80cxxxx.img>

is the name of the new 3DES file, where xxxx is the software load version and which must be in lower case, for example p80c37130.img

- h** If POS appeared in response to the sho sys info command in step [c](#) Ethernet Routing Switch 8600 uses POS, transfer the file through TFTP using the commands appropriate to your core manager platform.

For the SDM/CS 2000 Core Manager, enter the following commands:

```
copy
<a.b.c.d>:/swd/pp8600/XXX/<p80pxxxx.dld>
/flash/

copy /flash/<p80pxxxx.dld>
127.0.0.x:/flash/<p80pxxxx.dld>
```

For the CBM, enter the following commands:

```
copy <a.b.c.d>:/pp8600/XXX/<p80pxxxx.dld>
/flash/

copy /flash/<p80pxxxx.dld>
127.0.0.x:/flash/<p80pxxxx.dld>
```

where

<a.b.c.d>

is the IP address of the TFTP server

<p80pxxxx.dld>

is the name of the new POS file, where xxxx is the software load version and which must be in lower case, for example p80p37130.dld

- 4 Transfer all files that were just copied to /flash to /pcmcia by typing.

```
copy /flash/<p80cxxxx.img>
127.0.0.x:/pcmcia/p80cxxxx.img>
```

where

<p80cxxxx.img>

is the name of the new 3DES file, where xxxx is the software load version and which must be in lower case, for example p80p37130.dld

127.0.0.x

is the IP address of the slave CPU. If slot 6 is the master, then 127.0.0.5 is where the load is to be copied

Repeat this step for each file that was transferred and proceed to the next step after all files have been copied. Ensure the files are also copied to the /pcmcia of the slave.

- 5 In both the master and slave CPU sessions, enter the following command to verify that the software has been copied to the master and standby CPUs.

dir

- 6 If running a dual CPU configuration, determine if HA is enabled by typing

sho bootconfig config

Use the following table to determine the next step.

If the response is	Do
flags ha-cpu true	step 7
otherwise	step 8

- 7 Disable HA by typing

config bootconfig flags ha-cpu false

Note: The slave CPU will reset. Wait for the slave CPU to return to service.

On the master CPU, type

reset

Answer "Y" to the prompt "Are you sure you want to reset the switch (y/n)?"

Note: The CPU will switch mastership and the serial cable needs to be moved to the new master CPU.

- 8 Specify the new load as the primary load from which to boot by typing

```
config bootconfig choice primary image-file  
/flash/p80axxxx.img
```

where

<p80axxxx.img>

is the name of the new software image file, and xxxx is the software load version and which must be in lower case, for example p80a37130.img

- 9 Enter the following command to save the bootconfig file.

```
sav bootconfig
```

- 10

ATTENTION

This command upgrades the primary-image file (including the ATM-image, if present) and boot monitor at the same time.



CAUTION

Potential damage to CPU card

Do not interrupt the reboot process. The CPU card can be damaged if the reboot is interrupted incorrectly.

From the serial console to the slave CPU, upgrade the slave CPU by typing

```
boot /flash/p80b37130.img
```

Answer "Y" to the prompt.

A sample output follows:

```
@<switch_name>-C2:6# boot /flash/p80b37130.img
```

- 11 Upgrade the master CPU by typing

```
boot /flash/p80b37130.img
```

Answer "Y" to the prompt.

A sample output follows:

```
<switch_name>-C2:5# boot /flash/p80b37130.img
```

Note: The CPU will switch mastership and the serial cable needs to be moved to the new master CPU.

- 12 Use the following table to determine the next step.

If HA was	Do
enabled in step 6	step 13
not enabled in step 6	step 20

- 13 To enable HA, type

```
config bootconfig flags ha-cpu true
```

Answer “Y” to the prompt.

Note: The slave CPU will reset. Wait for the slave CPU to return to service.

On the master CPU, type

```
reset
```

Answer “Y” to the prompt “Are you sure you want to reset the switch (y/n)?”

Note: The CPU will switch mastership and the serial cable needs to be moved to the new master CPU.

Go to step [20](#).

- 14 For an Ethernet Routing Switch 8600 with a single CPU configuration, transfer the upgrade software to the flash on Chassis N of the Ethernet Routing Switch 8600 through TFTP as follows:

Note 1: There is an intentional space between the filename and “/flash/” at the end of each command syntax in the following substeps.

Note 2: When performing the copy and file transfer through TFTP in the steps that follow, ensure the files were copied successfully. To verify the file transfer was successful, list the directory on the remote device where the files came from, and on the local device to which the files were copied and compare the file sizes.

Note 3: When copying files on the same CPU, the Ethernet Routing Switch 8600 automatically copies files to the flash using the same name as the current file. Therefore, it is not

necessary to enter a new filename in the command for the backup version of the files in substeps [14a](#) through [14g](#).

- a Transfer the new software image file through TFTP using the commands appropriate to your core manager platform.

For the SDM/CS 2000 Core Manager, enter the following command:

```
copy <a.b.c.d>:/swd/pp8600/XXX/<p80axxx.img>
/flash/
```

For the CBM, enter the following command:

```
copy <a.b.c.d>:/pp8600/XXX/<p80axxx.img>
/flash/
```

where

<a.b.c.d>

is the IP address of the TFTP server

<p80axxx.img>

is the name of the new software image file, where xxxx is the software load version and which must be in lower case, for example p80a37130.img

Note: If the file transfer fails, verify the TFTP server IP address and connectivity with Ethernet Routing Switch 8600 Chassis N. Enter the following command to confirm Ethernet Routing Switch 8600 TFTP flag is set to true.

```
config bootconfig flags info
```

If the tftpd flag is set to false, enter the following command to reset the flag to true.

```
config bootconfig flags tftpd true
```

Confirm the flag is now set to true, then retry the transfer. If the problem persists, contact your next level of support.

Note 1: If the transfer completes but the file is corrupted, verify original file and PCMCIA card and transfer the file again. If the problem persists, contact your next level of support.

Note 2: Compare file parameters such as file size to check for possible corruption.

- b** Transfer the new boot monitor image file through TFTP using the commands appropriate to your core manager platform.

For the SDM/CS 2000 Core Manager, enter the following command:

```
copy
<a.b.c.d>:/swd/pp8600/XXX/<p80bxxxxx.img>
/flash/
```

For the CBM, enter the following command:

```
copy <a.b.c.d>:/pp8600/XXX/<p80bxxxxx.img>
/flash/
```

where

<a.b.c.d>

is the IP address of the TFTP server

<p80bxxxxx.img>

is the name of the new boot monitor image file, where xxxx is the software load version and which must be in lower case, for example p80b37130.img

The boot flash image and software image is backed up to the PCMCIA card on the Ethernet Routing Switch 8600 Chassis N.

- c** Determine if the Ethernet Routing Switch 8600 has ATM modules installed by typing

sho sys info

Example response:

Card Info :

Slot#	FrontType	FrontHw Version	Oper Status	Admin Status	BackType	BackHw Version
1	ATM	4	up	up	BFM3	
2	48x100BaseTX	A	up	up	BFM6	A
3	8x1000BaseIC	A	up	up	BFM8	A
4	ATM	04	up	up	BFM3	
5	CPU	05	up	up	SFM	05

- d Only if Chassis N of Ethernet Routing Switch 8600 uses an ATM blade, transfer the ATM Flash image to the Flash card on the Ethernet Routing Switch 8600 Chassis N through TFTP using the commands appropriate to your core manager platform. Otherwise proceed to [step 18](#).

For the SDM/CS 2000 Core Manager, enter the following command:

```
copy
<a.b.c.d>:/swd/pp8600/XXX/<p80txxxx.dld>
/flash/
```

For the CBM, enter the following command:

```
copy <a.b.c.d>:/pp8600/XXX/<p80txxxx.dld>
/flash/
```

where

<a.b.c.d>

is the IP address of the TFTP server

<p80txxxx.dld>

is the name of the new ATM file, where xxxx is the software load version and which must be in lower case, for example p80t37130.dld

Note: Notes 1 and 2 from [step 14](#), sub[step a](#) apply.

- e Determine if the Ethernet Routing Switch 8600 has encryption modules installed by typing

config info

Example response:

```
Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:
```

```
load-encryption-module : DES File p80cXXXXX.des
load-encryption-module : 3DES File p80cXXXXX.img
setdate : N/A
mac-flap-time-limit : 500
auto-recover-delay : 30
```

- f** If the Ethernet Routing Switch 8600 uses DES, transfer the file through TFTP using the commands appropriate to your core manager platform.

For the SDM/CS 2000 Core Manager, enter the following command:

```
copy  
<a.b.c.d>:/swd/pp8600/XXX/<p80cxxxx.des>  
/flash/
```

For the CBM, enter the following command:

```
copy <a.b.c.d>:/pp8600/XXX/<p80cxxxx.des>  
/flash/
```

where

<a.b.c.d>

is the IP address of the TFTP server

<p80cxxxx.des>

is the name of the new DES file, where xxxx is the software load version and which must be in lower case, for example p80c37130.des

- g** If the Ethernet Routing Switch 8600 uses 3DES, transfer the file through TFTP using the commands appropriate to your core manager platform.

For the SDM/CS 2000 Core Manager, enter the following command:

```
copy  
<a.b.c.d>:/swd/pp8600/XXX/<p80cxxxx.img>  
/flash/
```

For the CBM, enter the following command:

```
copy <a.b.c.d>:/pp8600/XXX/<p80cxxxx.img>  
/flash/
```

where

<a.b.c.d>

is the IP address of the TFTP server

<p80cxxxx.img>

is the name of the new 3DES file, where xxxx is the software load version and which must be in lower case, for example p80cxxxx.img

- 15 Transfer all files that were just copied to /flash to /pcmcia by typing.

```
copy /flash/<p80cxxxx.img>
/pcmcia/p80cxxxx.img>
```

where

<p80cxxxx.img>

is the name of the new 3DES file, where xxxx is the software load version and which must be in lower case, for example p80c37130.img

Repeat this step for each file that was transferred and proceed to the next step after all files have been copied.

- 16 Perform the following command on each CPU

```
copy /flash/<oldload> /pcmcia/
```

Perform the following commands only on the master CPU

```
config bootconfig choice secondary image-file
/pcmcia/<oldload>
```

```
config bootconfig choice secondary config-file
/pcmcia/config.cfg
```

where

<oldload> is the original software image filename, where xxxx is the software load version and which must be in lower case, for example p80a3320.img

- 17 Back up the current config, bootconfig, and software load files to the /flash and PCMCIA card to ensure the files are synchronized on the master and slave (if configured) CPU. Enter the following commands

Note: Before entering the sav config command, ensure sufficient free space exists in /flash (20% of total /flash size) to accommodate the configuration file.

```
sav config
```

For CS-LANs with a dual CPU configuration to save to primary (/flash), secondary (PCMCIA) and slave CPU, type

```
sav boot
```

```
sav config backup /pcmcia/config.cfg standby
/pcmcia/config.cfg
```

```
sav bootconfig backup /pcmcia/boot.cfg standby
/pcmcia/boot.cfg
```

For CS-LANs with a single CPU configuration to save to primary (/flash) and secondary (PCMCIA), type

```
sav config backup /pcmcia/config.cfg
```

```
sav bootconfig backup /pcmcia/boot.cfg
```

- 18** Prepare to reboot Ethernet Routing Switch 8600 Chassis N as follows:

Note: There is an intentional space between “image-file” and “/flash/” in the syntax for substep [18a](#).

- a** Enter the following command to specify the newload as the primary file to boot from.

```
config bootconfig choice primary image-file  
/flash/<p80axxxx.img>
```

where

<p80axxxx.img>

is the name of the new software image file, where xxxx is the software load version and which must be in lower case, for example p80a37130.img

- b** Enter the following command to verify the <newload>.

```
sho boot config
```

Make sure the result indicates the primary image file is <newload>.

- c** Enter the following command to save the bootconfig file.

```
sav bootconfig
```

The Ethernet Routing Switch 8600 Chassis N is ready to reboot.

19

ATTENTION

The command that follows upgrades the primary-image file (including the ATM-image, if present) and boot monitor at the same time.

**CAUTION**

Potential damage to CPU card

Do not interrupt the reboot process. The CPU card can be damaged if the reboot is interrupted incorrectly.

Enter the following command to reboot Ethernet Routing Switch 8600 Chassis N to upgrade the software image with the new software load.

```
boot /flash/<p80bxxxx.img>
```

where

<p80bxxxx.img>

is the name for the new monitor image file, where xxxx is the software load version and which must be in lower case, for example p80b37130.img



Serial connectivity is maintained between the terminal server and Ethernet Routing Switch 8600 Chassis N during the 60 to 90 seconds required to load the new software image.

20

You have completed this procedure. Return to the procedure that sent you here.

Verifying all hardware and software on Ethernet Routing Switch 8600

At Ethernet Routing Switch 8600 CLI

- 1 Make sure Ethernet Routing Switch 8600 Chassis X (for N=0, X=1; for N=1, X=0) is still operating correctly. To check the configuration file on the master CPU, type.

sho config

Example of output

```
#<output date and time info>
#boxtype : Passport-8010
#software version : W.X.Y.Z
#monitor version : W.X.Y.Z
#<output continues>
```

where

W.X.Y.Z

is the release number (Ignore the NNN.)

- 2 To check the slave CPU (console port) configuration file, type

more /flash/config.cfg

Compare the output of the master and slave CPU configuration files.

Review the configuration file (showing network topology and configuration) and correct any incorrect configurations.

Note: Software version is the load or image version. Monitor version is the bootflash version. The software version of the configuration displayed on the slave CPU is the version prior to the upgrade. If the configuration file on the master CPU is smaller or different than that displayed on the slave CPU, contact your next level of support.

3 Select the next step as follows.

If	Do
an inservice CPU memory upgrade for an Ethernet Routing Switch 8600 chassis is anticipated for future expansion	Power down the shelf of the Ethernet Routing Switch 8600 before pulling out the CPU card. OTHERWISE AN OUTAGE CAN RESULT! Refer to the appropriate CPU installation method or contact Nortel Global Product Support.
an inservice CPU memory upgrade for an Ethernet Routing Switch 8600 is not anticipated	step 5

4 If using an XA-Core, skip to [step 9](#).**5** Select the next step as follows.

If	Do
STORM uses a Dothill device	step 6
STORM IA (SAM-XTS) device ¹	step 9

1. The SAM-XTS configuration uses dual-homed split multilink trunks (SMLT). Both STORM volumes are recognized by both Ethernet Routing Switch 8600 routers. Therefore, taking down one router in an SAM-XTS configuration does not affect the STORM volume being addressed.

6 Select the next step as follows.

If	Do
the volumes on any STORM disk (for example, sd01) are actively mounted in DIRP ¹	step 7
the volumes on the STORM disk are not actively mounted in DIRP ²	step 9

1. Loss of network connectivity between SOS, the call processing application, and the active STORM disk can cause some or all DIRP volumes to be marked "INER-ROR," resulting in permanent loss of data.

2. Regardless of whether DIRP volumes are mounted, the procedure can result in an unavailable STORM disk and associated volumes.

- 7 From the Core MAP command line, return to service all disk volumes connected to the Ethernet Routing Switch 8600 chassis that were upgraded.

```
>diskadm sd0M; rts all
```

where

sd0M

is the STORM volume defined in procedure [Determining if STORM devices require rotating, demounting and busying on page 150](#)

- 8 Enter the following command to individually remount all volumes in DIRP. (Ensure you are at the nodisp;mtc;iod;dirp level of the MAPCI for this step.)

```
>mnt <subsystem> <volume> <variable>
```

Note 1: The <variable> parameter is not required when mounting and demounting regular DIRP volumes.

Note 2: Nortel recommends recording all subsystems, volume, and variable information for each volume remounted in this step.

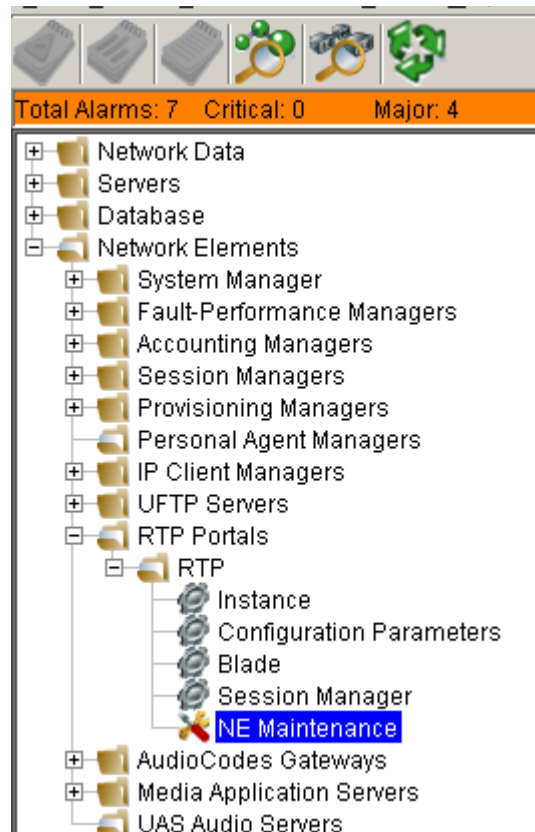
- 9 You have completed this procedure. Return to the procedure that sent you here.

Unlocking the Border Control Point 7100

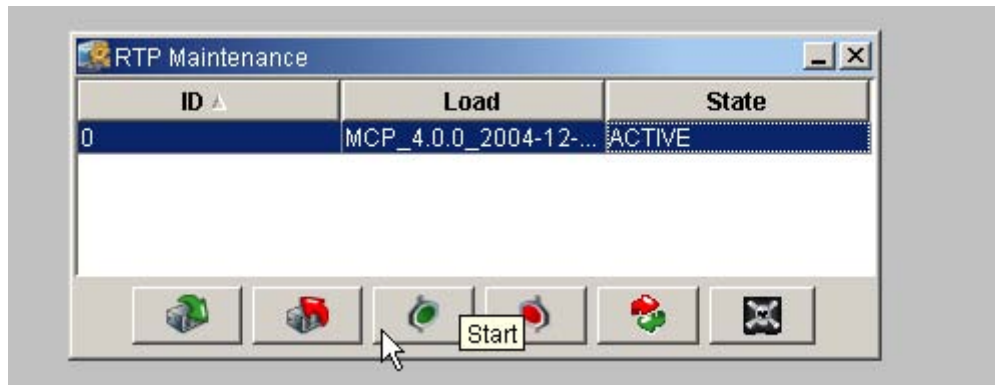
Use the System Management Console to start the Border Control Point 7100 connected to Chassis N

- 1 From the System tree, click the plus sign next to **Network Elements** to expand the view of the folder.

Expanding BCP 7100 windows



- 2 Next, click the plus sign next to **RTP Portals** to expand the view of the folder. The contents of this folder lists all BCP 7100s and BCP 7200s configured for the site.
- 3 Continue to expand the view of folders until the target BCP 7100 is selected. Do not modify the state of any BCP 7200s.
- 4 Click the **NE Maintenance** option. A new window opens.
- 5 Click the **Start** button to restart the previously shut down BCP 7100.

Start the BCP 7100

- 6 You have completed this procedure. Return to the procedure that sent you here.

Unlocking the inactive SC

At the SAM21 Manager

- 1 Launch the SAM21EM client.
The SAM21 Manager GUI appears.
 - 2 Unlock each locked SC blade as follows:
 - a Right-click on each locked SC blade.
 - b Select **Unlock** from the drop-down menu that appears.
 - c Repeat sub[step a](#) and sub[step b](#) until all units are unlocked.
- Note:** A padlock icon identifies locked SC blades.
- 3 You have completed this procedure. Return to the procedure that sent you here.

Unlocking the USP-Compact

At the SAM21 Manager

- 1 Re-access the SAM21 Manager. Unlock the locked slave USPc blade.

Note 1: Unlocking the slave USPc blade from the SAM21 Manager enables the USPc GUI.

Note 2: An alternative method to unlock the blade from the SAM21 Manager is to open the card by double-clicking on it. Click **Unlock** in the States tab.

At the USPc GUI

- 2 Re-access the USPc GUI, waiting to ensure that the inactive blade is enabled and locked.

Note: Re-accessing the USPc GUI can take several minutes.

- 3 Select **Configuration --> platform --> Node**.

The Administration tab of the USPc GUI displays.

The screenshot shows the Administration tab of the USPc GUI. The interface includes a toolbar at the top with buttons for New, Add, Modify, Delete, Lock, Unlock (highlighted), Load, Offline, Swact, and Restart. Below the toolbar are tabs for Administration, Search, and Graphical View. The main content area is divided into three sections:

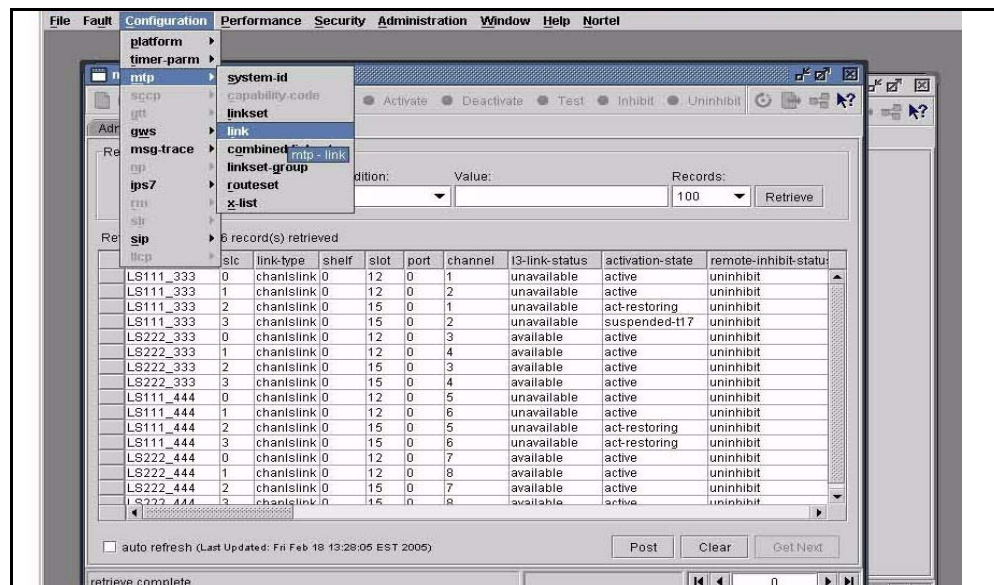
- Provisioning Data:**
 - slot-type: usp-compact
 - slot-name: USP1
 - slot-description: USP-Compact #1
 - shelf: 0
 - slot: 15
 - t1-e1-mode: t1
 - ext-ip-address: 47.131.125.82
 - ext-subnet-mask: 255.255.255.128
 - ext-gateway: 47.131.125.126
 - front-pec: NTRX51FN
- Operational Data:**
 - operational-state: enabled
 - administrative-state: unlocked
 - procedural-state: null
 - availability-state: null
 - activity-state: inactive
 - rex-status:
- Boot Data:**
 - status-message:
 - running-image: samss7_ppc750_10_00_01_06g
 - ha-running-image: ss7t1e1ha_ppc8260_10_00_01_06g
 - running-snapshot: current active
 - boot image: uspc_10_00_01_06g_base
 - ha-boot-image: uspc_10_00_01_06g_t1e1ha
 - boot-snapshot: current active
 - snapshot-description: current active
 - snapshot-date:
 - snapshot-version:

The bottom status bar shows "loading complete" and a page number "1".

- 4 Click **Unlock** to unlock the slave USPc blade.
- 5 Reactivate the SS7 links and the paths associated with the slave USPc blade.

From the Administration tab, select **Configuration --> MTP --> Links** from the pull-down menu.

The following screen appears.

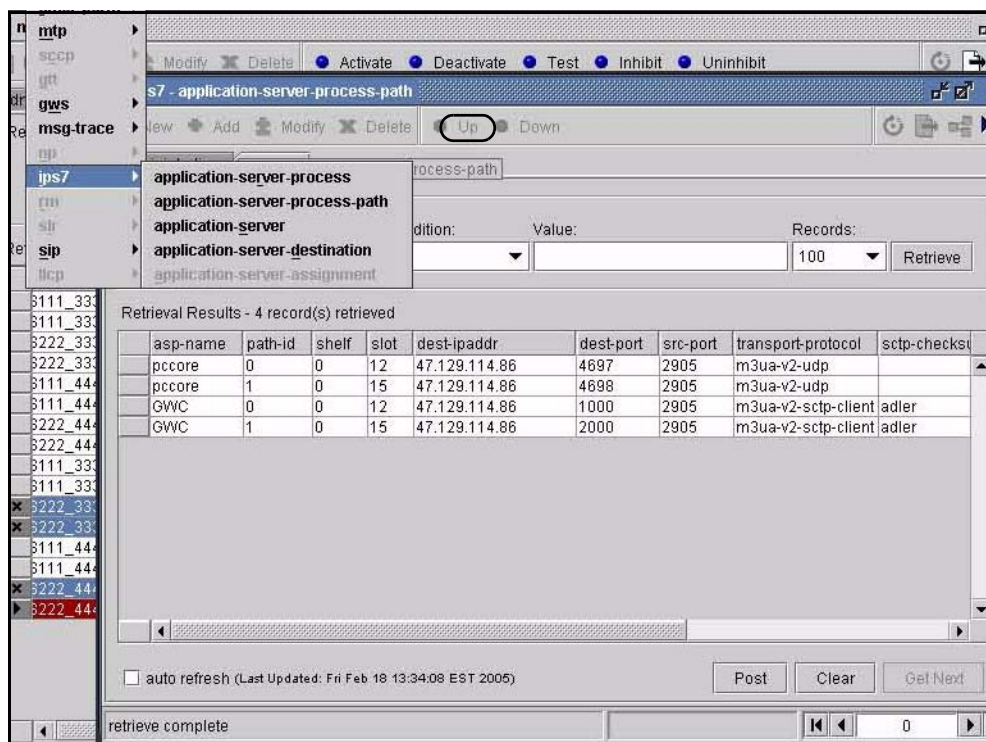


- 6 Select any SS7 links displayed in the form that are against the slave blade, and click **Activate**.
- 7 Select Yes to execute the command on the selected links.
- 8 Using the same screen, reselect the links, and click **Uninhibit**.
- 9 Select Yes to execute the command on the selected links.

- 10** Post the IPS7 paths that use the slave USPc blade.

From the menu, select **Configuration --> ips7 --> application-server-process-path** from the pull-down menu.

The following screen appears.



- 11** Select all the IPS7 paths against the slave USPc blade, and click **Up**.

The following prompt displays:

```
execute ips7 application-serverprocess-path up
command ?
```

- 12** Select Yes to execute the command on the IPS7 paths on the slave USPc blade.
- 13** If desired, perform an optional SWACT on the USPc blades to restore initial mastership states.

To perform a SWACT, redisplay the Administration tab, as shown in [step 3](#). Press the Swact button in the upper-right portion of the screen.

- 14 Select the next step as follows:

If your office is	Do
in a Geographic Survivability environment	step 15
not in a Geographic Survivability environment	step 17

Use the SAM21 Manager to unlock the inactive slave USP Compact blade

- 15 Launch the SAM21EM client.
The SAM21 Manager GUI appears.
- 16 Unlock each locked USPc blade as follows:
- a Right-click on each locked USPc blade.
 - b Select **Unlock** from the drop-down menu that appears.
 - c Repeat sub[a](#) and sub[b](#) until all units are unlocked.
- Note:** A padlock icon identifies locked USPc blades.
- 17 You have completed this procedure. Return to the procedure that sent you here.

Returning the paths to the Ethernet Routing Switch 8600 Chassis N to service

At the USP GUI

- 1** Post the IPS7 paths that use nodes connected to Chassis N by selecting Configuration->ips7->application-server-process-path.
- 2** Select each path connected to Chassis N and click Post, then confirm that only the paths associated with the cards connected to Chassis N, are selected.
- 3** Click Up to bring the posted paths back into service.
- 4** Click Yes to confirm the command execution on the IPS7 paths associated with the cards connected to Chassis N.
- 5** You have completed this procedure. Return to the procedure that sent you here.

Enabling Geographic Survivable components

At the SAM21 Manager

- 1 Re-access the SAM21 Manager. Unlock the locked inactive Call Agent card.

Note: An alternative method to unlock the blade from the SAM21 Manager is to open the card by double-clicking on it. Click **Unlock** in the States tab.

- 2 Wait for the lock icon to disappear.
- 3 At the Call Agent Manager, verify that the call processing application loads successfully and waits for synchronization.

Use the MAP display to perform a LIMITED_PRESWACT on the inactive Call Agent

- 4 If the switch is in sync, enter the following command to execute a drop synchronization from the ccamtc apply level.

```
> ccamtc
> coremtc
> appl
> dpsync
```

- 5 Select the next step as follows

If the (inactive) Call Agent card is	Do
not connected to the ERS 8600 being upgraded	step 6
connected to the ERS 8600 being upgraded	step 12

- 6 At the MAP display, enter the following command to initiate a limited preswact.

```
> BCSUPDATE; LIMITED_PRESWACT
```

Note 1: If a limited preswact process fails to complete, it stops and displays additional information. When this occurs, use the information to investigate and correct the problem.

Note 2: All limited preswact steps must be completed prior to SWACTing.

The LIMITED_PRESWACT command displays a warning:

Limited_Preswact should not be used for
BCSUPGRADE SWACTs. Do you wish to continue?
Please confirm ("YES", "Y", "NO", "N"):

7 Enter the following command to confirm you want to continue.

> Y

- 8 If the limited preswact process halts, re-enter the following command to continue.

> LIMITED_PRESWACT

The inactive unit indicates /restart at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated by display of the following message:

```
Total execution time for all complete procedures
00:07:31.362
All LIMITED_PRESWACT steps completed
successfully.
```

Perform a NORESTARTSWACT

- 9 If the active Call Agent card is connected to the Ethernet Routing Switch 8600 to be upgraded, minimize the possibility of an outage by performing a NORESTARTSWACT as follows:

- a Enter the following command to check the status.

> BCSUPDATE:SWACTCI;STATUSCHECK

The following response displays:

```
SWACTCI:
Checking Nodes Status
STATUSCHECK successful
```

- b** Enter the following command to execute the NORESTARTSWACT.

> NORESTARTSWACT

Progress is printed and the process stops to verify that the inactive Call Agent is not jammed.

Beginning SWACT checks:

All the SWACT checks have finished successfully.

The VR_PRESWACT_TRANSFER step completed successfully.

All INSV and ISTB series 1 PMs will have execs loaded after the SWACT.

Device Checking Status:

NOMATCH option is set to OFF <default setting>.

Device matching during CC WARM SWACT Enabled.

Do you wish to continue?

Please confirm ("YES", "Y", "NO", or "N"):

>

- c** If the only alarm is an APPL simplex, enter the following command to confirm you want to continue.

> Y

The final progress follows. Activity also switches at the Call Agent Manager.

All Pre_SWACT checks completed. Starting Warm SWACT now.

**** The cursor will not be returned. ****

**** unless a critical failure occurs.****

**** Now monitoring Warm SWACT messages.****

Pre-initialization done

Communication established

Exchange of data with the mate done

Transfer of data done (FASPECT)

Data estimation done

- d** The telnet session to the active and inactive call processing applications are lost. Re-establish the connection. Refer to the Call Agent upgrade procedure [Interface setup on page 1850](#).

Perform a POSTSWACT

- 10 At the MAP display, enter the following command to run a Postswact through completion.
- > **BCSUPDATE;POSTSWACT**
- 11 Enter the following command when prompted at the CA_SYNC step.
- > **Y**

Verify availability of NFS mounts on STORM

- 12 At the Call Agent Manager, enter the following commands to query the NFS mounts and ensure that they are accessible on STORM 1.
- > **ccamtc**
- > **coremtc**
- > **sys**
- > **querynfs**
- 13 From the resulting screen display, verify that all mounts are accessible.

Return to service disk volumes on SD0M

- 14 Enter the following command to return to service all disk volumes connected to the Ethernet Routing Switch 8600 chassis that were upgraded.
- >**diskadm sd0M; rts all**
- where
- sd0M**
- is the STORM volume defined in procedure [Determining if STORM devices require rotating, demounting and busying on page 150](#)

Mount DIRP volumes

- 15 Enter the following command to individually remount all volumes in DIRP. (Ensure you are at the nodisp;mtc;iod;dirp level of the MAPCI for this step.)

```
>mnt <subsystem> <volume> <variable>
```

Note 1: The <variable> parameter is not required when mounting and demounting regular DIRP volumes.

Note 2: Nortel recommends recording all subsystems, volume, and variable information for each volume remounted in this step.

Use the IEMS GUI to unlock the MS 2000 node

- 16 Launch the IEMS GUI.
- Note:** Refer to *IEMS Basics*, NN10329-111, for details on logging into the IEMS GUI.
- 17 Select **Applications ---> Integrated EMS --->Network Elements**.
- 18 Select the MS 2000 Series node to be unlocked and right-click on its icon.
- 19 Select the Config and Maintenance Tool from the pop-up menu. The Config and Maintenance Tool launches.
- 20 Click **Unlock** under the Lock State options to unlock the MS 2000 node.
- 21 You have completed this procedure. Return to the procedure that sent you here.

Enabling the Ethernet links between the XA-Core and the Ethernet Routing Switch 8600

At the MAP display

- 1 Enter the following command to access the ETHR level of the MAP display.
- ```
>MAPCI;MTC;XAC;ETHR
```
- 2 Refer to the following table and enable the Ethernet link between the XA-Core and Ethernet Routing Switch 8600 Chassis N by executing the following command to enable the link.
- ```
rts <slot> r link
```



HIOPs/HCMICs	N = 1	N = 2
<slot>	5	14

- 3 You have completed this procedure. Proceed to procedure [Completing the Ethernet Routing Switch 8600 upgrade on page 201](#) to continue with the upgrade process.

Completing the Ethernet Routing Switch 8600 upgrade

The following procedure provides the tasks to complete the Ethernet Routing Switch 8600 upgrade. These tasks include verifying the Ethernet Routing Switch 8600 chassis is working properly and re-routing traffic to the Ethernet Routing Switch 8600 device you upgraded.

Prerequisites

Ensure you have completed procedure [Upgrading the Ethernet Routing Switch 8600 on page 111](#).

Action

Perform the following procedure to complete the upgrade of the component.

Using the Ethernet Routing Switch 8600 CLI to reset the VRRP priority settings and OSPF and/ or BGP cost metrics

At the Ethernet Routing Switch 8600 CLI

- 1 Check the IP route information.

sho ip route info

The IP route information file appears. Review the file and verify that the route information is correct.

- 2 Check the IP VRRP information.

sho ip vrrp info

Note: P/V is the VLAN ID and should be used for the VID and VRID parameter.

The IP VRRP information file appears as shown in the following response. Review the file and verify that the information is correct.

Vrrp Info							
VRID	P/V	IP	MAC	STATE	CONTROL	PRIO	ADV
10	10	47.142.90.1	00:00:5e:00:01:0a	Back Up	Enabled	100	1
20	20	172.19.64.1	00:00:5e:00:01:14	Back Up	Enabled	100	1
30	30	10.26.128.1	00:00:5e:00:01:1e	Back Up	Enabled	100	1
40	40	172.19.68.1	00:00:5e:00:01:28	Back Up	Enabled	100	1
41	41	172.19.68.17	00:00:5e:00:01:29	Back Up	Enabled	100	1
43	42	172.19.68.33	00:00:5e:00:01:2b	Back Up	Enabled	100	1
60	60	172.19.70.1	00:00:5e:00:01:3c	Back Up	Enabled	100	1

VRID	P/V	MASTER	UP TIME	HLD DWN	CRITICAL	IP (ENABLED)
10	10	47.142.90.3	2 day(s), 18:46:07	0	0.0.0.0	(No)
20	20	172.19.64.3	2 day(s), 18:46:07	0	0.0.0.0	(No)
30	30	10.26.128.3	2 day(s), 18:46:07	0	0.0.0.0	(No)
40	40	172.19.68.3	2 day(s), 18:46:07	0	0.0.0.0	(No)
41	41	172.19.68.19	2 day(s), 18:46:07	0	0.0.0.0	(No)
43	42	172.19.68.35	2 day(s), 18:46:07	0	0.0.0.0	(No)

3 Reset the VRRP priority.

config vlan <vid> ip vrrp <vrid> prio <setting>

The VRRP priority metric is reset to its operational value.

Note: P/V is the VLAN ID and should be used for the VID and VRID parameter.

Use the VRRP priority metric recorded in the VID and metric table in procedure [Performing Ethernet Routing Switch 8600 upgrade pre-checks](#) in step [6](#) on page [101](#).

4 Repeat step [3](#) for each VLAN prioritized on Chassis N.

5 Use the following table to determine the next step.

If	Do
OSPF is enabled	step 6
otherwise	step 8

6 Reset the OSPF metric by typing

config vlan <vid> ip ospf metric <value>

Use the original metric value recorded in the VID and metric table in procedure [Performing Ethernet Routing Switch 8600 upgrade pre-checks](#) in step [6](#) on page [101](#).

The OSPF metrics reset to their original value.

- 7 Repeat step [6](#) for each VLAN on Chassis X recorded in the VID and metric table in procedure [Performing Ethernet Routing Switch 8600 upgrade pre-checks](#) in step [6](#) on page [101](#).

- 8 Use the following table to determine the next step.

If	Do
BGP is configured	step 9
otherwise	step 10

- 9 For each external BGP peer in the table above, execute the following command on the ERS 8600:

```
config ip bgp neighbor <external peer IP address> admin-state enable
```

Refer to the BGP neighbor internal/external table in procedure [Performing Ethernet Routing Switch 8600 upgrade pre-checks](#) in step [16](#) on page [106](#).

- 10 To delete the previous files, excluding the current image files, from the /flash directory, type

```
remove /flash/<filename>
```

where

filename

is the name of the old image, log or bootconfig file, for example, p80aXXXX.img and p80bXXXX.img, where XXXX is the version of the software

- 11 To delete the previous files, excluding the current image files, from the /pcmcia directory, type

```
remove /pcmcia/<filename>
```

where

filename

is the name of the old image, log, or bootconfig file, for example, p80aXXXX.img and p80bXXXX.img, where XXXX is the version of the software

- 12 Ensure the bootconfig file is properly configured on the /flash (primary) and /pcmcia (secondary). Select the next step as follows

If your CS-LAN	Do
is a dual CPU configuration	step 13
is a single CPU configuration	step 14

- 13** For a dual-CPU configuration, use the following commands to backup the bootconfig file that was just modified to the flash and pcmcia memory locations of both CPUs:

```
sav bootconfig backup /pcmcia/boot.cfg standby  
/pcmcia/boot.cfg  
  
config bootconfig choice secondary image-file  
/pcmcia/<newload>
```

A sample output follows:

```
Save config to file /flash/boot.cfg successful.  
File [/pcmcia/boot.cfg] already existing,  
overwrite (y/n) ?  
Respond Y to overwrite
```

y

```
Save bootconfig to backupfile /pcmcia/boot.cfg  
successful.  
Save to standby file /pcmcia/boot.cfg
```

Go to step [15](#)

- 14** For a single-CPU configuration, use the following command to backup the bootconfig file that was just modified to the flash and pcmcia memory locations for the single CPU:

```
sav bootconfig backup /pcmcia/boot.cfg  
  
config bootconfig choice secondary image-file  
/pcmcia/<newload>
```

A sample output follows:

```
Save config to file /flash/boot.cfg successful.  
File [/pcmcia/boot.cfg] already existing,  
overwrite (y/n) ?  
Respond Y to overwrite
```

y

```
Save bootconfig to backupfile /pcmcia/boot.cfg  
successful.
```

- 15** Ensure the config file and image are properly configured on the /flash (primary) and /pcmcia (secondary). Select the next step as follows

If your CS-LAN	Do
is a dual CPU configuration	step 16
is a single CPU configuration	step 17

- 16** For a dual-CPU configuration, use the following commands to save to primary and secondary, and to the slave CPU:

sav config

A sample output follows:

```
Save config to file /flash/config.cfg
successful.
Save to standby file /flash/config.cfg
successful.
```

sav config backup /pcmcia/config.cfg standby /pcmcia/config.cfg

A sample output follows:

Respond Y to overwrite

Y

```
Save config to backupfile /pcmcia/config.cfg
successful.
Save to standby file /pcmcia/config.cfg
successful.
```

Telnet to the slave CPU and login and copy the files to /flash by typing

```
copy /flash/<new_load>
127.0.0.6:/flash/<new_load>
```

Go to step [18](#)

- 17** For a single-CPU configuration, use the following command to save to both primary and secondary:

sav config backup /pcmcia/config.cfg

A sample output follows:

```
save config backup /pcmcia/config.cfg
Save config to file /flash/config.cfg
successful.
File [/pcmcia/config.cfg] already existing,
overwrite (y/n) ?
```

Type Y to confirm the intent to save the config file.

```
Save config to backupfile /pcmcia/config.cfg
successful.
```

- 18** Increment the iteration index ($N = N+1$), and select the next step as follows:

If the iteration index is	Do
$N = 1$	Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100 (to start the second pass)
$N = 2$	step 19

Note: In the second iteration (where $N=2$), use Chassis X in place of Chassis N. Ethernet Routing Switch 8600 Chassis 1 (identified as Chassis N) is the slave and Ethernet Routing Switch 8600 Chassis 0 (identified as Chassis X) is the master.

- 19** Go to the Release Notes and identify any post-upgrade requirements.

- 20** To save the new Ethernet Routing Switch 8600 configuration, type

Note: Before entering the sav config command, ensure sufficient free space exists in /flash (20% of total /flash size) to accommodate the configuration file. Refer to [Verifying sufficient space exists in directories /flash and /pcmcia on page 88](#) to check the directory size and remove files if necessary.

sav config

This updates the new Ethernet Routing Switch 8600 configuration so that VRRP settings are maintained after any subsequent reboot.

- 21** Delete any old files that are no longer needed.

List the contents of the /flash and /pcmcia directories by typing

dir

Examine the output and identify previous files that can be removed. If upgrading a dual-CPU Ethernet Routing Switch 8600, remove any old files from the slave CPU as well.

Note: Delete the following files after the upgrade has been completed successfully:

- all files in the /swd directory on the core manager
- software load file in the /tmp directory on the CS 2000 Management Tools server (applies just to the SDM/CS 2000 Core Manager)

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



IEMS upgrade

This section provides information on how to upgrade the SPFS-based server that is hosting the Integrated Element Management System (IEMS). The upgrade consists of upgrading the following software:

- Server Platform Foundation Software (SPFS)
- Network Patch Manager (NPM)
- Patching server Element (PSE)
- Integrated Element Management System (IEMS)

Note: If the IEMS resides on the same SPFS-based server as the CS 2000 Management Tools, refer to section [CS 2000 Management Tools upgrade on page 272](#).

The supported platforms for the IEMS are as follows:

- a simplex server (Sun Netra t1400 or Sun Netra 240)
- a high-availability server pair (Sun Netra 240)

What's new in IEMS upgrades in (I)SN09U

IEMS backward compatibility and upgrade

This feature provides backward compatibility in IEMS so that all the (I)SN09U device versions and the previous device versions (n – 2) are supported in IEMS.

Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U
- SN09U to SN09U MNCL

Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade/rollback
- the service impacts of a software upgrade
- other information affecting a software upgrade

Time to complete an upgrade/rollback

The following table lists the estimated times to upgrade/rollback the IEMS on a SPFS-based server.

Estimated time to complete a software upgrade/rollback

Task	Upgrade/rollback path	Time
Upgrading the IEMS software (includes the upgrade of platform SPFS)	SN08 to SN09U HA upgrade	6 hours (IEMS out of service for 33 minutes)
	SN09 to SN09U HA upgrade	3 hours 30 minutes (IEMS out of service for 26 minutes)
	SN09 to SN09U Simplex	3 hours 30 minutes (IEMS out of service for 1 hour 15 minutes)
	SN09 to SN09U Simplex with co-resident CS2M	3 hours 50 minutes (IEMS out of service for 1 hour 15 minutes)
	SN09U to SN09U HA maintenance release	2 hours 15 minutes (IEMS out of service for 19 minutes)
	SN09 to SN09U HA upgrade with ~100 managed objects and max events (~900000)	4 hours (IEMS out of service for 28 minutes)
Performing a rollback	SN09U to SN09 HA after point of no return	3 hours 40 minutes. (IEMS out of service for 2 hours 45 minutes)
	SN09U to SN08 HA after point of no return	2 hours 50 minutes (IEMS out of service for 2 hours)
	SN09U to SN09 Simplex after point of no return	1 hour 45 minutes (IEMS out of service for 1 hour 45 minutes)
	SN09U to SN09U HA prior to point of no return	50 minutes (IEMS out of service for 2 minutes)

Service impacts

The upgrade of the SPFS-based server that is hosting the IEMS creates the following service impacts:

- OAM and security services outage occurs for the combined SPFS and IEMS upgrade times.
- For HA configurations (N240 server pair), the switch of activity (SWACT) between the active and inactive server requires approximately 7 minutes.
- An HA configuration SWACT can result in up to a
 - 4-minute alarm and log notification delay if generated during the SWACT
 - 5-minute inability to access a component GUI through the IEMS

Additional information

The following additional information applies to the upgrade of an SPFS-based server that is hosting the IEMS:

- Nortel engineering recommends using N240 servers for IEMS performance collection with intervals less than 30 minutes.
- If this server is in a geographically-redundant configuration, the standby server must also be upgraded.
- For the SPFS upgrade, new logs and alarms are not processed during the required reboot. However, the status of those logs and alarms are resynchronized after the reboot to ensure accurate status.

System capacity

The software upgrade procedure can impact the system capacity. This means that additional disk space on the OAMP workstation are required for converting existing databases.

System performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade.

System limitations during upgrade

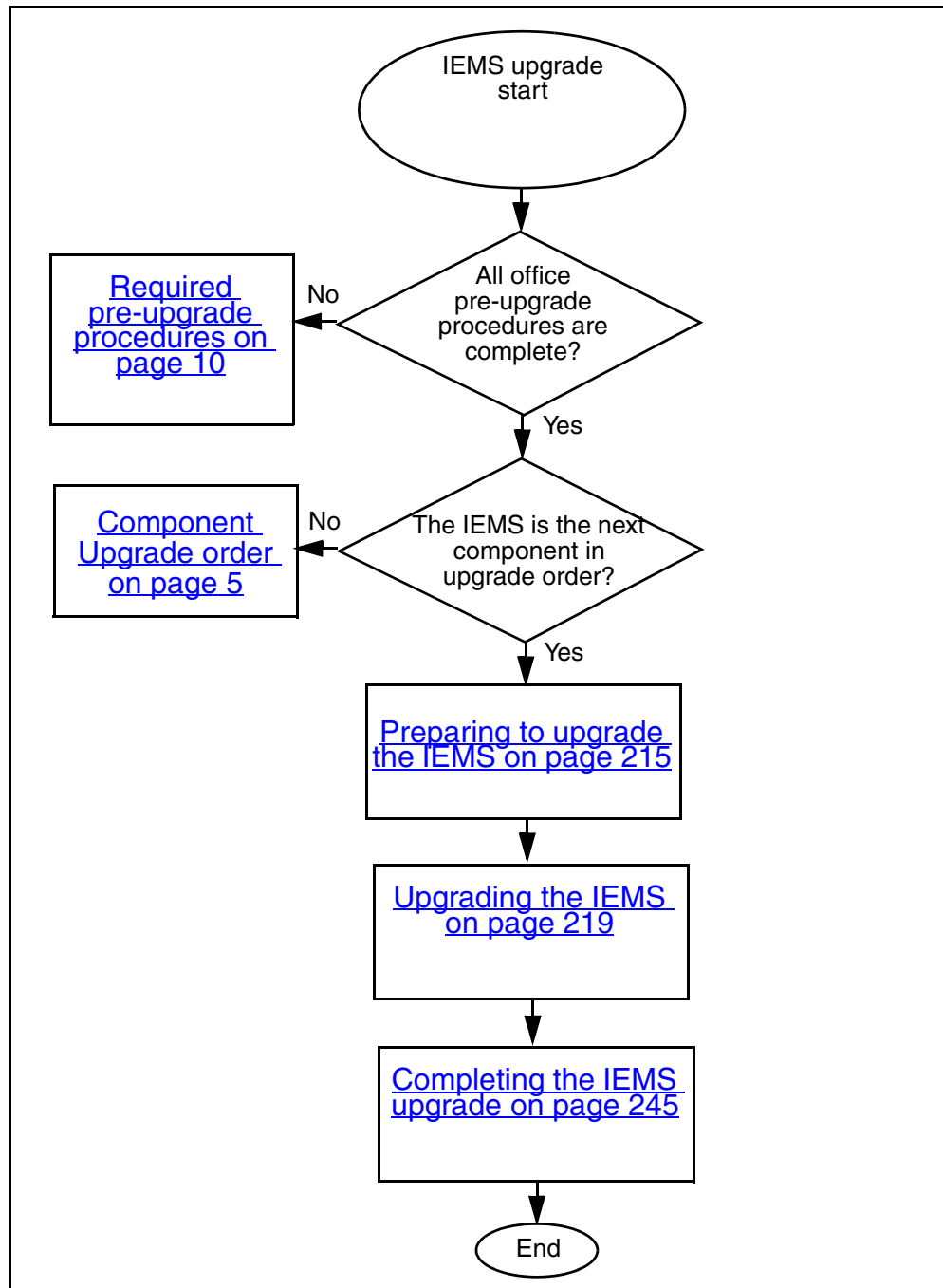
Do not perform the following actions during an upgrade or you risk corrupting the entire system:

- System administration
 - adding, deleting, or modifying users
 - setting the time of day
 - changing passwords
- System management
 - modifying the system name
 - adding or deleting system nodes
 - modifying the IP addresses

IEMS upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

IEMS upgrade tasks



Preparing to upgrade the IEMS

The following procedure provides the steps you need to execute prior to upgrading the SPFS-based server that is hosting the Integrated Element Management System (IEMS) software. When applicable, a reference to the procedure that contains the detailed steps is provided.

Prerequisites

This procedure has the following prerequisites:

- you have completed the tasks under [Preparing to upgrade the Carrier Voice over IP Network on page 9](#)
- you have upgraded all components that precede the IEMS under [Component Upgrade order on page 5](#)

Action

Follow the link associated with the type of server you are preparing to upgrade.

- [Preparing to upgrade a simplex server on page 215](#)
- [Preparing to upgrade an HA server pair on page 217](#)

Preparing to upgrade a simplex server

At your workstation

- 1 Ensure your server meets the hardware requirements.
For details, refer to “System requirements” in *IEMS Overview*, NN10329-111.
- 2 Establish a connection to the server and log in using the root user ID and password.
For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

At the server

- 3 Ensure the SPFS and the IEMS software are at the latest maintenance release (MNCL) for the release you are currently running, and are patch-current.
For detailed steps viewing the SPFS release on the server, refer to the procedure [Determining the SPFS software MNCL level on page 424](#).
- 4 Run the IEMS precheck script.

Do not proceed with the upgrade until the IEMS precheck test passes and indicates that the upgrade can proceed.

For detailed steps, refer to procedure [Running the IEMS pre-check script on page 251](#)

- 5 Ensure the domain name service (DNS) is enabled on the server by typing

```
# nslookup <hostname>
```

and pressing the enter key.

The system will return the DNS information for this server when DNS is enabled. For detailed steps to configure DNS for a server, refer to the procedure “Configuring Domain Name Service” in *ATM/IP Solution-level Configuration Management*, NN10409-500.

- 6 Verify whether an HTTPS certificate is installed on the server, and whether it is valid.

For detailed steps, refer to procedure [Verifying the presence and validity of an HTTPS certificate on an SPFS-based server on page 329](#).

- 7 Back up the oracle data.

For detailed steps, refer to procedure [Performing a backup of oracle data on an SPFS-based server on page 374](#).

- 8 Back up the file systems.

For detailed steps, refer to procedure [Performing a backup of file systems on an SPFS-based server on page 379](#).

- 9 Save NPM user-defined data.

For detailed steps, refer to procedure [Archiving the NPM database into a file on page 383](#).

- 10 Save NPM patch files.

For detailed steps, refer to procedure [Saving the NPM patch and database files on page 385](#).

- 11 You have completed this procedure. Proceed to [Upgrading the IEMS on page 219](#).

Preparing to upgrade an HA server pair

At your workstation

- 1 Ensure your server meets the hardware requirements.
For details, refer to “System requirements” in *IEMS Basics*, NN10329-111.
- 2 Establish a connection to the active and inactive servers and log in using the root user ID and password.
For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

On the inactive server

- 3 Ensure the SPFS and the IEMS software are at the latest maintenance release (MNCL) for the release you are currently running, and are patch-current.
For detailed steps viewing the SPFS release on the server, refer to the procedure [Determining the SPFS software MNCL level on page 424](#).
- 4 Run the IEMS precheck script.
Do not proceed with the upgrade until the IEMS precheck test passes and indicates that the upgrade can proceed.
For detailed steps, refer to procedure [Running the IEMS pre-check script on page 251](#).
- 5 Ensure the domain name service (DNS) is enabled on the server by typing

```
# nslookup <hostname>
```


and pressing the enter key.
The system will return the DNS information for this server when DNS is enabled. For detailed steps to configure DNS, refer to procedure “Configuring Domain Name Service” in *ATM/IP Solution-level Configuration Management*, NN10409-500.
- 6 Verify the state of the cluster.
For detailed steps, refer to procedure [Verifying the state of a cluster on page 400](#).

On the active server

- 7** Verify whether an HTTPS certificate is installed on the server, and whether it is valid.
For detailed steps, refer to procedure [Verifying the presence and validity of an HTTPS certificate on an SPFS-based server on page 329](#).
- 8** Back up the oracle data.
For detailed steps, refer to procedure [Performing a backup of oracle data on an SPFS-based server on page 374](#).
- 9** Back up the file systems.
For detailed steps, refer to procedure [Performing a backup of file systems on an SPFS-based server on page 379](#).
- 10** Save NPM user-defined data.
For detailed steps, refer to procedure [Archiving the NPM database into a file on page 383](#).
- 11** Save NPM patch files.
For detailed steps, refer to procedure [Saving the NPM patch and database files on page 385](#).
- 12** You have completed this procedure. Proceed to [Upgrading the IEMS on page 219](#).

Upgrading the IEMS

The following procedure provides the steps you need to execute to upgrade the SPFS-based server that is hosting the IEMS software application. When applicable, a reference to the procedure that contains the detailed steps is provided.

Note: If the IEMS application resides on the same SPFS-based server that hosts the CS 2000 Management Tools application, refer to section [CS 2000 Management Tools upgrade on page 272](#).

Prerequisites

You have completed procedure [Preparing to upgrade the IEMS on page 215](#).

Action

Follow the link associated with the release you are upgrading from.

- [Upgrading from \(I\)SN08 or \(I\)SN09 to \(I\)SN09U on page 220](#)
- [Upgrading from \(I\)SN09U to \(I\)SN09U \(maintenance release\) on page 236](#)

Upgrading from (I)SN08 or (I)SN09 to (I)SN09U

Follow the link associated with the type of server you are upgrading.

- [Upgrading a simplex server on page 220](#)
- [Upgrading an HA server pair on page 228](#)

Upgrading a simplex server

ATTENTION

At any point from [step 3](#) up to and including [step 13](#) in this procedure, executing a fallback will involve performing procedure “Executing a fallback during an SPFS-based server upgrade” for a [One-server configuration on page 419](#).

At any point after [step 13](#) in this procedure, executing a fallback will involve a full system restore. Refer to “Performing a full system restore on an SPFS-based server” in *ATM/IP Fault Management*, NN10408-900.

ATTENTION

During the upgrade of a simplex server, you may see the following console message:

```
/opt/resmon/Hardware/disk_check.ksh: Disk or disk mirroring errors:
```

This is an expected and normal part of the simplex upgrade.

At your workstation

- 1 Establish a connection to the server and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#)

On the server

- 2 Back up the central security server. Failure to back up the central security server will result in the loss of all the current IEMS user and password information.

For detailed steps, refer to [Backing up the central security server](#).

3

**CAUTION****Potential for operational problems**

Once you have upgraded the SPFS, continue until you have upgraded all applications on this server. Failing to upgrade an application to the same release as the SPFS will result in operational problems.

In order for this server to be completely upgraded, the entire procedure must be followed. Do not subdivide this upgrade procedure into separate maintenance windows.

Upgrade the SPFS.

For detailed steps, refer to procedure [Upgrading SPFS software on page 403](#).

4

Use the following table to determine your next step.

If	Do
you received a notification bulletin that an SPFS MNCL is available for the release you just upgraded to	step 5
otherwise	step 6

5

Install the SPFS MNCL.

For detailed steps, refer to the instructions provided with the MNCL.

6

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be transferred to NPM, if not already available on NPM.

Obtain any patches applicable to the components that are on the server, such as, PSE, NPM, SPFS, IEMS, IEMSCSS,

IEMSCSS_DS, COREM, CSMONITOR, PKMGR_SERVER, and transfer them to the NPM database.

If you received patches	Do
as an ISO image file	step 7
on a CD	step 11

- 7** Transfer and mount the ISO image on the server.
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 8** Transfer the patches from the ISO image file to the NPM database.
For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).
- 9** Unmount and remove the ISO image from the server.
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 10** Proceed to [step 12](#).
- 11** Transfer the patches from the CD to the NPM database.
For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).
- 12** Use the following table to determine your next step.
-
If	Do
you have SPFS patches for the release you just upgraded to	step 13
otherwise	step 14
-
- 13** Apply the SPFS patches.
For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#)

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

If	Do
you have NPM patches for the release you just upgraded to	step 15
otherwise	step 16

- 15 Apply the NPM patches and restart the NPM.

For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#).

Note: If you have a large network, abort any NPM tasks that are queued ahead of the NPM restart tasks. In a large network, the list of NPM tasks queued ahead of the NPM restart task can be long and can take many hours to complete. Therefore, aborting NPM tasks is recommended in large networks to shorten the upgrade time.

For detailed steps, refer to procedure [Prioritizing or aborting a patching maintenance request using the NPM on page 2421](#)

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

If	Do
you have PSE patches for the release you just upgraded to	step 17
otherwise	step 18

- 17 Apply the PSE patches and restart PSE.

For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#)

- 18 Enable the health monitors by typing

```
# cfigsplxck enable
```

and pressing the Enter key.

Example response

```
NOTE: Enabling health monitor...Success.
```

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

If you are upgrading IEMS using	Do
ESD	step 20
CD	step 21

- 20 Transfer the IEMS iso image to the server and mount the iso image on the server.

For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)

- 21 Upgrade IEMS.

For detailed steps, refer to procedure [Upgrading the IEMS software on page 254](#).

- 22

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be applied the SN09U IEMS load.

Use the following table to determine your next step.

If	Do
you have IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, or PKMGR_SERVER patches for the release you just upgraded to	step 23
otherwise	step 24

- 23 Apply the IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, PKMGR_SERVER patches, and restart the components.

For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#)

- 24 Restore the central security server backup file.

For detailed steps, refer to [Restoring the central security server](#).

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

If you upgraded IEMS using	Do
ESD	step 26
CD	step 29

- 26 For an ESD upgrade, run the Config Swap script by typing
/tmpmnt/bin/switch09conf.ksh
and pressing the Enter key.
When prompted, confirm you want to continue by typing
y
and pressing the Enter key.
- 27 Unmount and remove the IEMS iso image from the server.
For detailed steps, refer to [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 28 Proceed to [step 31](#).
- 29 For a CD upgrade, run the Config Swap script by typing
/cdrom/cdrom0/bin/switch09conf.ksh
and pressing the Enter key.
When prompted, confirm you want to continue by typing
y
and pressing the Enter key.
- 30 Eject the CD from the drive as follows:

- a** Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- b** Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

- c** Remove the CD or DVD from the drive.

- 31** If you have not started IEMS yet, start the IEMS server application by typing

```
# servstart IEMS
```

and pressing the Enter key.

- 32** Verify that IEMS, WEBSERVER, WEBSERVICES, DATABASE, RADSVR and IS are running by typing

```
servquery -status all
```

and pressing the Enter key.

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

If	Do
all applications are running	step 36
otherwise	step 34

- 34** Start each application indicated in [step 32](#) that is not running by typing

```
# servstart <app_name>
```

and pressing the Enter key.

where

app_name

is the name of the application that is not in a RUNNING state, for example, IEMS

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

If	Do
all applications started	step 36
otherwise	contact your next level of support

- 36** Verify the IEMS upgrade was successful.

For detailed steps, refer to procedure [Verifying the IEMS upgrade was successful on page 472](#).

- 37** Use the following table to determine the next step.

If	Do
you choose to accept the upgraded environment	step 38
you choose to rollback to the state prior to the upgrade	step 39

- 38** Accept the upgraded environment by typing

/SSPFS_Upgrade.accept

and pressing the Enter key.

The execution of this step takes approximately 20 minutes to complete depending on system configuration.

Proceed to [step 40](#).

- 39** If you choose to fallback, refer to the procedure “Performing a full system restore on an SPFS-based server” in the document *ATM/IP Fault Management*, NN10408-900.

After a full system restore, if the IEMS is configured with a central security server, you will need to restore the central security server. For detailed steps, refer to [Restoring the central security server](#).

- 40** You have completed this procedure. Proceed to [Completing the IEMS upgrade on page 245](#).

Upgrading an HA server pair

ATTENTION

A fallback can be executed at any point from [step 9](#) to [step 29](#) in this procedure, by performing procedure “Executing a fallback during an SPFS-based server upgrade” for a [Two-server configuration on page 419](#).

If you choose to fallback after executing [step 29](#), refer to procedure “Performing a full system restore on an SPFS-based server” in document *ATM/IP Fault Management*, NN10408-900. After the full system restore, if the IEMS is configured with a central security server, you will need to restore the central security server. For detailed steps, refer to [Restoring the central security server](#).

At your workstation

- 1 Establish a connection to the active and inactive servers and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

On the active server

- 2 Back up the central security server. Failure to back up the central security server will result in the loss of all the current IEMS user and password information.

For detailed steps, refer to [Backing up the central security server](#).

- 3

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be transferred to NPM, if not already available on NPM.

Obtain any patches applicable to the components that are on the server, such as, PSE, NPM, SPFS, IEMS, IEMSCSS,

IEMSCSS_DS, CSMONITOR, PKMGR_SERVER, COREM, and transfer them to the NPM database.

If you received patches**Do**

on a CD

[step 8](#)

as an ISO image file

[step 4](#)

- 4** Transfer and mount the ISO image on the server.
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 5** Transfer the patches from the ISO image file to the NPM database.
For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).
- 6** Unmount and remove the ISO image from the server.
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 7** Proceed to [step 9](#).
- 8** Transfer the patches from the CD to the NPM database.
For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).

On the inactive server**9****CAUTION****Potential for operational problems**

Once you have upgraded the SPFS, continue until you have upgraded all applications on this server. Failing to upgrade an application to the same release as the SPFS will result in operational problems.

In order for this server to be completely upgraded, the entire procedure must be followed. Do not subdivide this upgrade procedure into separate maintenance windows.

Upgrade the SPFS.

For detailed steps, refer to procedure [Upgrading SPFS software on page 403](#).

10 Use the following table to determine your next step.

If	Do
you received a notification bulletin that an SPFS MNCL is available for the release you just upgraded to	step 11
otherwise	step 12

11 Install the SPFS MNCL.

For detailed steps, refer to the instructions provided with the MNCL.

12 Apply the SPFS, NPM, and PSE patches to the inactive server by typing

patchUpToDate

and pressing the Enter key.

Enter yes when prompted for any of the following (entering no stops the process):

- to confirm the NPM host name
If the NPM host is incorrect, then either re-configure the PSE to point to the NPM or contact next level of support to do this. Then run patchUpToDate again.
- to confirm you want to apply the patches listed
- to confirm you want to continue when patches have special application instructions
- to confirm you want to restart of any devices that require a restart
- to confirm the you want to continue when a reboot is required
After a reboot, you will have to log back into the server as root once the reboot is complete.

The patchUpToDate session generates a report called *patchUpToDate.report* and places it in the directory from where the command was executed.

The report contains all the console output from the patchUpToDate session and a summary of the patching actions that occurred and any errors. The summary includes patches applied, any patches that were already applied when the patchUpToDate utility started, any patches that have been applied and removed when the patchUpToDate utility started, and any patches that were not applied because their prerequisite patches were not available.

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

If you are upgrading IEMS using	Do
ESD	step 14
CD	step 15

- 14** Transfer the IEMS iso image to the active server and mount the iso image on the inactive server.
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)
- 15** Upgrade IEMS.
For detailed steps, refer to procedure [Upgrading the IEMS software on page 254](#).

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

If	Do
you have IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, or PKMGR_SERVER patches for the release you just upgraded to	step 17
otherwise	step 25

- 17** Apply the IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, PKMGR_SERVER patches to the inactive server by typing

patchUpToDate

and pressing the Enter key.

Enter yes when prompted for any of the following (entering no stops the process):

- to confirm the NPM host name
If the NPM host is incorrect, then either re-configure the PSE to point to the NPM or contact next level of support to do this. Then run patchUpToDate again.
- to confirm you want to apply the patches listed
- to confirm you want to continue when patches have special application instructions
- to confirm you want to restart of any devices that require a restart
- to confirm the you want to continue when a reboot is required
After a reboot, you will have to log back into the server as root once the reboot is complete.

The patchUpToDate session generates a report called *patchUpToDate.report* and places it in the directory from where the command was executed.

The report contains all the console output from the patchUpToDate session and a summary of the patching actions that occurred and any errors. The summary includes patches applied, any patches that were already applied when the patchUpToDate utility started, any patches that have been applied and removed when the patchUpToDate utility started, and any patches that were not applied because their prerequisite patches were not available.

- 18** Restore the central security server backup file.
For detailed steps, refer to [Restoring the central security server](#).

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

If you upgraded IEMS using	Do
ESD	step 20
CD	step 23

- 20** For an ESD upgrade, run the Config File Swap script as follows:

- a** Run the script by typing
`# /tmpmnt/bin/switch09conf.ksh`
and pressing the Enter key.
- b** When prompted, confirm you want to continue by typing
`y`
and pressing the Enter key.

- 21** Unmount and remove the IEMS iso image from the server.

For detailed steps, refer to [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).

- 22** Proceed to [step 16](#).

- 23** For a CD upgrade, run the Config File Swap script as follows:

- a** Run the script by typing
`# /cdrom/cdrom0/bin/switch09conf.ksh`
and pressing the Enter key.
- b** When prompted, confirm you want to continue by typing
`y`
and pressing the Enter key.

24 Eject the CD from the drive as follows:

- a**
- Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- b**
- Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

- c**
- Remove the CD or DVD from the drive.

On the active server**25** Stop the cluster.

For detailed steps, refer to procedure [Stopping a cluster on page 457](#).

On the newly active server with the (I)SN09U software**26** Verify the IEMS upgrade was successful.

For detailed steps, refer to procedure [Verifying the IEMS upgrade was successful on page 472](#).

27 Execute the amldap user password script as follows:

- a**
- Change directories by typing (there is no space between security/ and current_core)

```
# cd /opt/nortel/applications/security/  
current_core/bin
```

and pressing the Enter key.

- b**
- Run the update_am_pwd_exp.sh script by typing

```
# ./update_am_pwd_exp.sh
```

and pressing the Enter key.

- c**
- When prompted, confirm you want to continue by typing

```
# y
```

and pressing the Enter key.

- 28** Use the following table to determine the next step.

If	Do
you choose to accept the upgraded environment	step 29
you choose to rollback to the state prior to the upgrade	step 30

- 29**

ATTENTION

At this point, you can easily revert this upgraded server back to the previous release. Continuing with this procedure, clones the image of the upgraded server onto the server running the previous release, and once both servers are upgraded, reverting back to the previous release will require a full system restore.

Accept the upgraded environment by typing

/SSPFS_Upgrade.accept

and pressing the Enter key.

The execution of this step takes approximately 20 minutes to complete depending on system configuration.

Proceed to [step 31](#).

- 30** If you choose to fallback, refer to procedure “Executing a fallback during an SPFS-based server upgrade” for a [Two-server configuration on page 419](#).
- 31** Clone the image of the upgraded server onto the other server. For detailed steps, refer to procedure [Cloning the image of one server in a cluster to the other server on page 478](#)
- 32** You have completed this procedure. Proceed to [Completing the IEMS upgrade on page 245](#).

Upgrading from (I)SN09U to (I)SN09U (maintenance release)

Follow the link associated with the type of server you are upgrading.

- [Upgrading a simplex server \(maintenance release\) on page 236](#)
- [Upgrading an HA server pair \(maintenance release\) on page 240](#)

Upgrading a simplex server (maintenance release)***At your workstation***

- 1 Establish a connection to the server and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

At the server

- 2 Verify whether other users are logged on to the system by typing

```
# who
```

and pressing the Enter key.

- 3 The presence of other users logged on to the system can have adverse effects on the upgrade process and can cause the upgrade to fail. Therefore, request that all users log out before you proceed using the wall command:

```
# wall
```

```
The system is coming down for maintenance.  
Please log off immediately in order to save your  
files. Any user logged in with the "nortel"  
userid MUST log out now.
```

and pressing the Enter key.

Then hit the Ctrl and D keys simultaneously to send the message to all users.

- 4 Back up the central security server. Failure to back up the central security server will result in the loss of all the current IEMS user and password information.

For detailed steps, refer to [Backing up the central security server](#).

5

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be transferred to NPM, if not already available on NPM.

Obtain any patches applicable to IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, or PKMGR_SERVER.

For detailed steps, refer to one of the following procedures:

- [Transferring patches delivered on CD to the NPM database on page 2297](#)
- [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#)

6 Stop the IEMS server application by typing

```
# servstop IEMS
```

and pressing the Enter key.

7 Use the following table to determine your next step.

If you are upgrading IEMS using	Do
ESD	step 8
CD	step 9

8 Transfer the IEMS iso image to the server and mount the iso image on the server.

For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)

9 Upgrade IEMS.

For detailed steps, refer to procedure [Upgrading the IEMS software on page 254](#).

10 Use the following table to determine your next step.

If you upgraded IEMS using	Do
ESD	step 11
CD	step 13

- 11 Unmount and remove the IEMS iso image from the server.
For detailed steps, refer to [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 12 Proceed to [step 14](#).
- 13 Eject the CD from the drive as follows:
 - a Ensure you are at the root directory level by typing
cd /
and pressing the Enter key.
 - b Eject the CD by typing
eject cdrom
and pressing the Enter key.

Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:
 # **/etc/init.d/volmgt stop**
 # **/etc/init.d/volmgt start**
 Then, press the eject button located on the front of the DVD drive.
 - c Remove the CD or DVD from the drive.

14

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be applied the SN09U IEMS load.

Use the following table to determine your next step.

If	Do
you have IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, or PKMGR_SERVER patches for the release you just upgraded to	step 15
otherwise	step 19

- 15 Apply the IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, PKMGR_SERVER patches, and restart the components.
For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#).
- 16 If you have not started IEMS yet, start the IEMS server application by typing

```
# servstart IEMS
```

and pressing the Enter key.
- 17 Restore the central security server backup file.
For detailed steps, refer to [Restoring the central security server](#).
- 18 Verify the IEMS upgrade was successful.
For detailed steps, refer to procedure [Verifying the IEMS upgrade was successful on page 472](#).
- 19 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Upgrading an HA server pair (maintenance release)

At your workstation

- 1 Establish a connection to the active and inactive servers and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

On the active server

- 2 Verify whether other users are logged on to the system.

```
# ssh unit1-priv0 who
```

```
# ssh unit0-priv0 who
```

- 3 The presence of other users logged on to the system can have adverse effects on the upgrade process and can cause the upgrade to fail. Therefore, request that all users log out before you proceed using the wall command:

```
# wall
```

```
The system is coming down for maintenance.  
Please log off immediately in order to save your  
files. Any user logged in with the "nortel"  
userid MUST log out now.
```

and pressing the Enter key.

Then hit the Ctrl and D keys simultaneously to send the message to all users.

- 4 Back up the central security server. Failure to back up the central security server will result in the loss of all the current IEMS user and password information.

For detailed steps, refer to [Backing up the central security server](#).

- 5

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be transferred to NPM, if not already available on NPM.

Obtain any patches applicable to IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, or PKMGR_SERVER.

For detailed steps, refer to one of the following procedures:

- [Transferring patches delivered on CD to the NPM database on page 2297](#)
- [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#)

On the inactive server

- 6** Remove the inactive server from the cluster.

For detailed steps, refer to procedure [Removing a server from a cluster on page 438](#).

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

If you are upgrading IEMS using	Do
ESD	step 8
CD	step 9

- 8** Transfer the IEMS iso image to the server and mount the iso image on the server.

For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)

- 9** Stop the IEMS server application by typing

```
# servstop IEMS
```

and pressing the Enter key.

- 10** Upgrade IEMS.

For detailed steps, refer to procedure [Upgrading the IEMS software on page 254](#).

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

If you upgraded IEMS using	Do
ESD	step 12
CD	step 14

- 12** Unmount and remove the IEMS iso image from the server.

For detailed steps, refer to [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).

- 13 Proceed to [step 15](#).
- 14 Eject the CD from the drive as follows:
 - a Ensure you are at the root directory level by typing
`# cd /`
 and pressing the Enter key.
 - b Eject the CD by typing
`# eject cdrom`
 and pressing the Enter key.

Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

`# /etc/init.d/volmgt stop`

`# /etc/init.d/volmgt start`

Then, press the eject button located on the front of the DVD drive.

- c Remove the CD or DVD from the drive.

15

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be applied the SN09U IEMS load.

Use the following table to determine your next step.

If	Do
you have IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, or PKMGR_SERVER patches for the release you just upgraded to	step 16
otherwise	step 18

- 16 Apply the IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, PKMGR_SERVER patches, and restart the components.
For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#)
- 17 Restore the central security server backup file.
For detailed steps, refer to [Restoring the central security server](#).
- 18 Return the inactive server to the cluster.
For detailed steps, refer to procedure [Returning a server to a cluster on page 456](#).

On the active server

- 19 Stop the cluster.
For detailed steps, refer to procedure [Stopping a cluster on page 457](#)

On the newly active server with the (I)SN09U maintenance release software

- 20 Verify the IEMS upgrade was successful.
For detailed steps, refer to procedure [Verifying the IEMS upgrade was successful on page 472](#).
- 21 Execute the amlsap user password script as follows:
 - a Change directories by typing (there is no space between security/ and current_core)

```
# cd /opt/nortel/applications/security/  
current_core/bin
```

and pressing the Enter key.
 - b Run the update_am_pwd_exp.sh script by typing

```
# ./update_am_pwd_exp.sh
```

and pressing the Enter key.
 - c When prompted, confirm you want to continue by typing

```
# y
```

and pressing the Enter key.

22**ATTENTION**

At this point, you can easily revert this upgraded server back to the previous release. Continuing with this procedure, clones the image of the upgraded server onto the server running the previous release, and once both servers are upgraded, reverting back to the previous release will require a full system restore.

Clone the image of the upgraded server onto the other server.

For detailed steps, refer to procedure [Cloning the image of one server in a cluster to the other server on page 478](#)

23

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

Completing the IEMS upgrade

The following procedure provides the high-level steps to complete the component upgrade. When applicable, a reference to the procedure that contains the detailed steps is provided.

Prerequisites

You have completed procedure [Upgrading the IEMS on page 219](#)

Action

Follow the link associated with the type of server you just upgraded.

- [Completing the upgrade on a simplex server on page 245](#)
- [Completing the upgrade on an HA server pair on page 248](#)

Completing the upgrade on a simplex server

At your workstation

- 1 Establish a connection to the IEMS server and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

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

If	Do
the Media Server 2000 is in the network	step 3
otherwise	step 8

At your workstation

- 3 Establish a connection to the CMT server and log in using your user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

At the CMT server

- 4 Determine if the bootptab file is present on the CMT server by typing

```
# ls -l /data/sspfs/etc/bootp/bootptab
```

and pressing the Enter key.

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

If	Do
the bootptab file is present and the file size is greater than 0	step 7
otherwise	step 6

- 6 Set up the BootP file on the CMT server using procedure [Setting up the BootP file on SPFS on page 269](#).
- 7 Log out of the CMT server.

At the IEMS server

- 8 If, before the upgrade, you determined through your system administrator that your site is using a third-party security application as opposed to the IEMS security application, have your system administrator re-edit the NSCD, PAM and NSSwitch configuration files.
- Refer to your system administrator.
- 9 Update the CEM documentation if not already updated.
- For detailed steps, refer to procedure [Updating the CEM documentation on page 261](#).
- 10 Start the Core Element Manager (CEM).
- For detailed steps, refer to procedure [Starting and stopping the Core Element Manager \(CEM\) on page 543](#)
- 11 Through the IEMS GUI, update the Device version field in the object properties of the IEMS SPFS platform under EMS platforms, to reflect the new software version you just upgraded to.
- For detailed steps on how to update the software version in the Device Version field, refer to one of the following procedures:
- [Editing and viewing object properties using Java Web Start Client](#)
 - [Editing and viewing object properties using Web Client](#)
- 12 Configure and start the Client Session Monitor.
- For detailed steps, refer to procedure [Configuring the Client Session Monitor on page 534](#).

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

If	Do
you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS)	step 14
otherwise	step 15

- 14** Configure NPM for automatic patch file delivery.
For detailed steps, refer to procedure [Configuring NPM for automatic patch file delivery on page 493](#).
- 15** Back up the oracle data.
For detailed steps, refer to procedure [Performing a backup of oracle data on an SPFS-based server on page 374](#).
- 16** Back up the file systems.
For detailed steps, refer to procedure [Performing a backup of file systems on an SPFS-based server on page 379](#).
- 17** Back up the central security server.
For detailed steps, refer to [Backing up the central security server](#).
- 18** If this is a geographically-redundant configuration, upgrade the standby IEMS server. Refer to procedures “Installing the remote backup server” and “Scheduling automatic backups on the remote server”, in *Carrier Voice over IP, Disaster Recovery Procedures*, NN10450-900.
- 19** Upgrade the next component in the end-to-end upgrade. Refer back to [Component Upgrade order on page 5](#).

Completing the upgrade on an HA server pair

At your workstation

- 1 Establish a connection to the active IEMS server and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

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

If	Do
the Media Server 2000 is in the network	step 3
otherwise	step 8

At your workstation

- 3 Establish a connection to the active CMT server and log in using your user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

At the active CMT server

- 4 Determine if the bootptab file is present on the CMT server by typing

```
# ls -l /data/sspfs/etc/bootp/bootptab
```

and pressing the Enter key.

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

If	Do
the bootptab file is present and the file size is greater than 0	step 7
otherwise	step 6

- 6 Set up the BootP file on the CMT server using procedure [Setting up the BootP file on SPFS on page 269](#).

- 7 Log out of the CMT server.

At the at IEMS active server

- 8** If, before the upgrade, you determined through your system administrator that your site is using a third-party security application as opposed to the IEMS security application, have your system administrator re-edit the NSCD, PAM and NSSwitch configuration files.
Contact your system administrator.
- 9** Update the CEM documentation if not already updated.
For detailed steps, refer to procedure [Updating the CEM documentation on page 261](#).
- 10** Start the Core Element Manager (CEM).
For detailed steps, refer to procedure [Starting and stopping the Core Element Manager \(CEM\) on page 543](#)
- 11** Through the IEMS GUI, update the Device version field in the object properties of the IEMS SPFS platform under EMS platforms, to reflect the new software version you just upgraded to.
For detailed steps on how to update the software version in the Device Version field, refer to one of the following procedures:
- [Editing and viewing object properties using Java Web Start Client](#)
 - [Editing and viewing object properties using Web Client](#)
- 12** Configure and start the Client Session Monitor.
For detailed steps, refer to procedure [Configuring the Client Session Monitor on page 534](#).
- 13** Use the following table to determine your next step.

If	Do
you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS). Note: if the NPM was configured for automatic patch delivery before the upgrade it is still configured.	step 14
otherwise	step 13

- 14** Configure NPM for automatic patch file delivery.
For detailed steps, refer to procedure [Configuring NPM for automatic patch file delivery on page 493](#).
- 15** Back up the oracle data.
For detailed steps, refer to procedure [Performing a backup of oracle data on an SPFS-based server on page 374](#).
- 16** Back up the file systems.
For detailed steps, refer to procedure [Performing a backup of file systems on an SPFS-based server on page 379](#).
- 17** Back up the central security server.
For detailed steps, refer to [Backing up the central security server](#).
- 18** If this is a geographically-redundant configuration, upgrade the standby IEMS server. Refer to procedures “Installing the remote backup server” and “Scheduling automatic backups on the remote server”, in *Carrier Voice over IP, Disaster Recovery Procedures*, NN10450-900.
- 19** Upgrade the next component in the end-to-end upgrade. Refer back to [Component Upgrade order on page 5](#).

Running the IEMS pre-check script

Application

Use this procedure to run the IEMS script prior to upgrading the Server Platform Foundation Software (SPFS) or IEMS software on an SPFS-based server. The script determines which devices are not supported with the higher version.

ATTENTION

Do not proceed with the upgrade until the IEMS pre-check test passes and indicates that the upgrade can proceed. If unsupported device versions are configured in the IEMS inventory, the IEMS software upgrade will fail.

Prerequisites

You need root user privileges.

Action

Perform the steps that follow to complete this procedure.

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

At the server

- 2 Change directory by typing

```
# cd /opt/nortel/iems/current/bin
```

and pressing the Enter key.

3 Run the IEMS pre-check script by typing

```
# sh IEMSupgradePreCheck.sh <to version>  
<supported version 1> <supported version 2>
```

and pressing the Enter key.

where

<to version> is the version that you are upgrading to

<supported version 1> and <supported version 2> are the versions that the <to version> supports

Example

To upgrade from (I)SN08 or (I)SN09 to (I)SN09FF, enter:

```
hostname:/opt/nortel/iems/current/bin> sh  
IEMSupgradePreCheck.sh 9FF 9.0 8.0
```

Example response

```
IEMS Upgrade Pre-Check Test:
```

```
*****
```

```
The IEMS upgrade pre-check test passed. The  
IEMS upgrade may proceed.
```

4 Use the following table to determine your next step.

If the pre-check test	Do
fails	step 5
passes	step 7

- 5 If any device versions are not supported by the version you are upgrading to, the pre-check step fails, and the following warning message appears.

Example response

```
IEMS Upgrade Pre-Check Test:
*****
The IEMS upgrade pre-check test Failed. The IEMS
upgrade should not proceed.
```

```
Device version check failed. The following
devices must be upgraded prior to proceeding
with the IEMS Upgrade to SN09.0:-
```

```
=====
|S.No.| Device Name          | Version |
=====
| 1    | wcarslqf-MDM-Mgr      | 6.2     |
| 2    | wcarsljk-MG9K-Mgr_9   | 6.2     |
-----
```

If the IEMS pre-check upgrade fails, upgrade the device version in the IEMS, for the devices that appear in the list, before proceeding with the IEMS upgrade.

Note: Any devices that appear in the list must be running the target software version. If they are not, the devices must be upgraded to the target software version.

- 6 Repeat this procedure to run the IEMS pre-check script.

If the pre-check test	Do
fails	contact your next level of support
passes	step 7

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

Upgrading the IEMS software

Use this procedure to upgrade IEMS software in simplex and high availability configurations.

Prerequisites

This procedure has the following prerequisites:

- Ensure all console and telnet sessions used during the upgrade, are recorded to a file.
- If upgrading from CD, ensure you have the CD that contains the IEMS software for the release you are upgrading to. If upgrading through Electronic Software Delivery (ESD), ensure the software has been transferred and mounted onto the server. If required, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- Ensure no other users are logged on to the system. If Nortel is assisting in the upgrade, they must not log in using the nortel userid.

Action

Perform the following steps to complete this procedure.

At the server console

- 1 Obtain the password for user nortel prior to upgrading the IEMS software, as the password will be changed during the upgrade, and you will need to reset it following the upgrade.
- 2



CAUTION

Potential for upgrade problems

Do not log in with the nortel userid when performing the IEMS upgrade. The use of the nortel userid will result in upgrade errors.

Log in to the IEMS server through the console (port A) using the root user ID and password. In a two-server configuration, log in to the inactive server.

Note: In a two-server configuration, ensure you are on the inactive server by typing ubmstat. If ClusterIndicatorACT is displayed in the response, which indicates you are on the active server, log out of that server and log in to the other

server. The response must display ClusterIndicatorSTBY, which indicates you are on the inactive server.

3

**CAUTION****Potential for upgrade problems**

The presence of other users will result in upgrade errors for IEMS sub-components. Do not proceed until ALL other users have logged off.

Ensure no other users are logged on the system by typing

who

and pressing the Enter key.

Example response:

```
# who
nortel      pts/2          Aug 22 11:35
maint      pts/3          Aug 22 11:37
```

If another user is present, proceed to [step 4](#) otherwise go to [step 5](#).

4

Use the wall command to request all other users log out before you proceed by typing:

wall

The system is coming down for maintenance. Please log off immediately in order to save your files. Any user logged in with the "nortel" userid MUST log out now.

and pressing the enter key.

Then hit the Ctrl and D keys simultaneously to send the message to all users. Repeat [step 3](#) until all other users have logged out.

5

Use the following table to determine your next step.

If upgrading from a	Do
CD	step 6
directory	step 9

At the server

- 6 Insert the CD that contains the IEMS software into the drive. In a two-server configuration, insert the CD into the inactive server.

At the server console

- 7 Upgrade the IEMS software from the CD by typing

```
# cd /cdrom/cdrom0/bin/
```

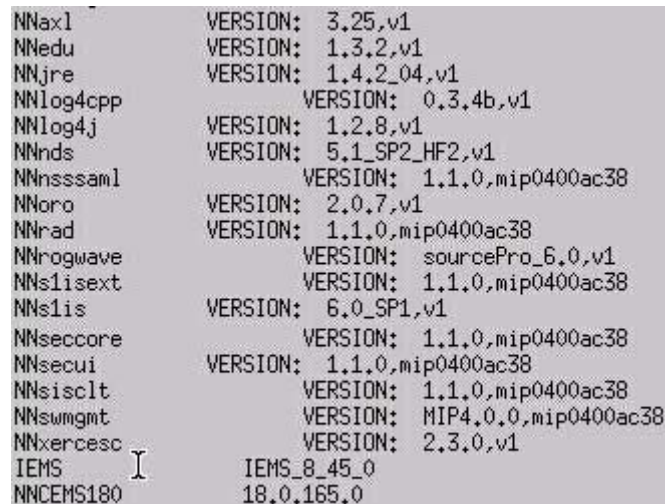
and pressing the Enter key.

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

The screen output lists the currently installed packages and confirms the upgrade.

The screen output then lists the contents of the IEMS software package to be installed, similar to the following screen shot:



```
NNaxl      VERSION: 3.25,v1
NNedu      VERSION: 1.3.2,v1
NNjre      VERSION: 1.4.2_04,v1
NNlog4cpp  VERSION: 0.3.4b,v1
NNlog4j    VERSION: 1.2.8,v1
NNnds      VERSION: 5.1_SP2_HF2,v1
NNnssaml   VERSION: 1.1.0,mip0400ac38
NNoro      VERSION: 2.0.7,v1
NNrad      VERSION: 1.1.0,mip0400ac38
NNrogwave  VERSION: sourcePro_6.0,v1
NNslisext  VERSION: 1.1.0,mip0400ac38
NNslis     VERSION: 6.0_SP1,v1
NNseccore  VERSION: 1.1.0,mip0400ac38
NNsecui    VERSION: 1.1.0,mip0400ac38
NNsisclt   VERSION: 1.1.0,mip0400ac38
NNswmgmt   VERSION: MIP4.0.0,mip0400ac38
NNxercesc  VERSION: 2.3.0,v1
IEMS      IEMS_8_45_0
NNCEMS180  18.0.165.0
```

- 8 Proceed to [step 10](#).
- 9 Upgrade the IEMS software from the directory by typing

```
# cd /tmpmnt/bin/
```

and pressing the Enter key.

Run the appl_mgr script by typing

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

The screen output lists the currently installed packages and confirms the upgrade.

The screen output then lists the contents of the IEMS software package to be installed, similar to the following screen shot:

```

NNaxl      VERSION: 3.25,v1
NNedu      VERSION: 1.3.2,v1
NNjre      VERSION: 1.4.2_04,v1
NNlog4cpp  VERSION: 0.3.4b,v1
NNlog4j    VERSION: 1.2.8,v1
NNnds      VERSION: 5.1_SP2_HF2,v1
NNnssaml   VERSION: 1.1.0,mip0400ac38
NNoro      VERSION: 2.0.7,v1
NNrad      VERSION: 1.1.0,mip0400ac38
NNrogwave  VERSION: sourcePro_6.0,v1
NNs1isext  VERSION: 1.1.0,mip0400ac38
NNs1is     VERSION: 6.0_SP1,v1
NNseccore  VERSION: 1.1.0,mip0400ac38
NNsecui    VERSION: 1.1.0,mip0400ac38
NNsisclt   VERSION: 1.1.0,mip0400ac38
NNswgmt    VERSION: MIP4.0.0,mip0400ac38
NNxercesc  VERSION: 2.3.0,v1
IEMS       IEMS_8_45_0
NNCEMS180  18.0.165.0

```

- 10 When prompted, confirm you want to upgrade by typing

y

and pressing the Enter key.

A message appears, similar to the following screen shot:

Note: The upgrade can take 30 minutes or more depending on the user data.

```

Installing the new security server components...
Done installing the new security server components.

=====
Checking version of IEMS package...

Installing IEMS Package...
Done Installing IEMS Package.

Installing the CEM ...

=====
Upgrade of the IEMS software package completed successfully

Exporting data for migration
Configuring ... this will take 30 minutes or more depending on user data

```

- 11 Reset the password for user nortel by typing

passwd -r files nortel

and pressing the Enter key.

- 12 When prompted, enter the password for user nortel that you obtained prior to the upgrade.

- 13** When prompted, enter the password again to confirm it.
- 14** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Backing up the central security server

Application

Use this procedure to back up the central security server. When the Security Services component is installed, the generic backup and restore script (brr_security.sh) are registered with servman (bkmgr).

The NDS database and all files under the following directories are backed up using this procedure:

- /opt/nortel/config/3rd_party/netscape
- /opt/nortel/config/3rd_party/security/s1is
- /opt/nortel/config/applications/security
- /opt/nortel/data/3rd_party/netscape
- /opt/nortel/data/3rd_party/security/s1is
- /opt/nortel/data/applications/security

Prerequisites

You must have root user privileges to perform this procedure.

Action

At your workstation

- 1 Establish a connection to the server where IEMS resides through telnet or SSH, using the host name or IP address of the server, and log in using the root user ID and password.

In a two-server configuration, establish the connection to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

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

If	Do
this server is hosting the CMT and IEMS	step 3
this server is only hosting the IEMS	step 6

- 3 Verify the status of the SESM server application by typing **servman query -status -group SESMService** and pressing the Enter key.

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

If	Do
the SESM server application is running	step 6
otherwise	step 5

- 5 Start the SESM server application by typing **servstart SESMService** and pressing the Enter key.

- 6 Enter the backup manager utility by typing **/opt/bkresmgr/cbm/bkmgr** and pressing the Enter key.

- 7 Start the backup by typing **backup full** and pressing the Enter key.

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

If response is	Do
Backup succeeded.	step 9
Backup failed. For more detailed errors, refer to log file at ...	Contact your next level of support.

- 9 Exit the backup manager utility by typing **quit** and pressing the Enter key.

The Security Services configuration settings and data are backed up to the following file:

/data/bkresmgr/<date><time>backupSS1.1<host_name>.tar

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

Updating the CEM documentation

Application

Use this procedure to update the CEM documentation.

Note: To configure CEM, see Integration of Core Element Manager with IEMS in *IEMS Basics*, NN10329-111.

Prerequisites

No prerequisites are required for this procedure.

Action

At the active server console

- 1 Determine if a previous version of the SScemhelp package is installed by typing
pkginfo -l SScemhelp
- 2 Use the information in the following table to determine the next step.

If a previous version of SScemhelp is	Do
installed	step 3
not installed	step 6

- 3 Remove the previous version of the SScemhelp package by typing
pkgrm <SScemhelp_package_name>
and pressing the Enter key.
- 4 When prompted, confirm you want to remove the previous version of the SScemhelp package by typing
y
and pressing the Enter key.
- 5 When prompted, confirm the removal by typing
y
and pressing the Enter key.

- 6 Select your next step.
- | If | Do |
|----------------------------|-------------------------------|
| you are using a CD | go to step 7 |
| you are using an ISO image | go to step 12 |
- 7 Insert the Integrated Element Mgmt System (IEMS) Version 9 Docs CD (CD2) containing the CEM documentation into the drive.
- 8 Change directories by typing
cd /cdrom/cdrom0
and pressing the Enter key.
- 9 Upgrade the CEM documentation by typing
pkgadd -d SScemhelp.pds
and pressing the Enter key.
The installation process prompts you to select the package(s) and to confirm you want to proceed with the installation. Enter the default responses (**a**ll, **y**).
- 10 Eject the CD from the drive as follows:
- a Ensure you are at the root directory level by typing
cd /
and pressing the Enter key.
 - b Eject the CD by typing
eject cdrom
and pressing the Enter key.
Note: If the drive tray will not open after you have determined that the drive is not busy and is not being read from or written to, enter the following commands:
/etc/init.d/volmgt stop
/etc/init.d/volmgt start
Then, press the eject button located on the front of the drive.
 - c Remove the CD from the drive.
- 11 Go to [step 16](#).
- 12 Mount the CEM help file.

For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

- 13** Change directories by typing

```
# cd /tmpmnt
```

and pressing the Enter key.

- 14** Upgrade the CEM documentation by typing

```
# pkgadd -d SScemhelp.pds
```

and pressing the Enter key.

The installation process prompts you to select the package(s) and to confirm you want to proceed with the installation. Enter the default responses (all, y).

- 15** Unmount and remove the CEM help file from the server.

For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).

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

Restoring the central security server

Application

Use this procedure to restore the security server from a backup file.

ATTENTION

SSL uses certificates. Certificates from one server cannot be used on another server. If you want to take a back up file from a server where SSL is implemented and restore to a different server, you must perform the procedure “Replacing HTTPS certificate on security server for SunOne component” in *ATM/IP Solution-level Administration and Security*, NN10402-600 after the restore is completed. This script is run to set up IS authentication, session, and policy traffic to operate under SSL.

Note that servers in the same high availability cluster can use the same SSL certificate.

Note that if the restored IS SSL certificate has expired, you must perform the procedure in “Replacing HTTPS certificate on security server for SunOne component” in *ATM/IP Solution-level Administration and Security*, NN10402-600 after the restore is completed.

Prerequisites

This procedure has the following prerequisites:

- You must have root user privileges.
- You must have a backup tar file created using the procedure for [Backing up the central security server](#).

Action

Perform the following steps to restore central security server data.

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 server

Note: If you are upgrading the active server, telnet to the active server. If you are upgrading the inactive server, telnet to the inactive 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.

If	Do
you are performing this procedure during an upgrade on the inactive server of a two-server configuration	step 7
otherwise	step 5

5 Stop the security services by doing the following:

a Type:

```
servstop RADSVR
```

and press the Enter key.

b Type:

```
servstop IS
```

and press the Enter key.

c Type:

```
servstop WEBSERVICES
```

and press the Enter key.

6 List the available security server backup files and determine the backup file to be restored by typing:

```
ls /data/bkresmgr
```

and pressing the Enter key.

The format of the security server backup files are
<date><time>backupSS1.1<host_name>.tar

Note the name of the security server backup file you intend to restore. You will need this information in a later step.

- 7 Change directories by typing:
- ```
cd /opt/nortel/applications/security/current_s
l1sxt/swmgmt/bin
```
- and pressing the Enter key.
- 8 Determine if SAML is enabled on the workstation by looking at the `nsswitch.conf` file.
- ```
vi /etc/nsswitch.conf
```
- and pressing the Enter key.
- if the following is seen:
- ```
passwd: files
group: files
```
- do: continue to [step 10](#)
- if: `saml` is seen in the two lines, for example:
- ```
passwd:  saml files  
group:   saml files
```
- do: continue to [step 9](#)
- 9 Disable SAML by typing:
- ```
vi /etc/nsswitch.conf
```
- and pressing the Enter key.
- replace the "passwd:" & "group:" lines with the following:
- ```
passwd:  files  
group:   files
```
- save and close the file
- 10 Perform the restore operation by typing:
- ```
./brr_security.sh -restore /data/bkresmgr/
<date><time>backupSS1.1<host_name>.tar
```
- where `<date><time>backupSS1.1<host_name>.tar` is the backup file you determined in [step 6](#) should be restored.
- Press the Enter key.

**If****Do**

you are performing this procedure during an upgrade on the inactive server of a two-server configuration

step [13](#)

|           | <b>If</b>                                                                                                                                                                                                                                                                                                                                                                      | <b>Do</b>               |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
|           | otherwise                                                                                                                                                                                                                                                                                                                                                                      | step <a href="#">11</a> |
| <b>11</b> | Restart the security services by doing the following:                                                                                                                                                                                                                                                                                                                          |                         |
|           | <b>a</b> Type:<br><b>servstart WEBSERVICES</b><br>and press the Enter key.                                                                                                                                                                                                                                                                                                     |                         |
|           | <b>b</b> Type:<br><b>servstart IS</b><br>and press the Enter key.                                                                                                                                                                                                                                                                                                              |                         |
|           | <b>c</b> Type:<br><b>servstart RADSVR</b><br>and press the Enter key.                                                                                                                                                                                                                                                                                                          |                         |
| <b>12</b> | Enable SAML by typing:<br><b>vi /etc/nsswitch.conf</b><br>and pressing the Enter key.<br>replace the "passwd: and " group:" lines with the following:<br>passwd: saml files<br>group: saml files<br>save and close the file                                                                                                                                                    |                         |
| <b>13</b> | If the restored image was backed up from a different server with a different certificate or if the restored certificate has expired, follow the procedure in "Replacing HTTPS certificate on security server for SunOne component" in <i>ATM/IP Solution-level Administration and Security</i> , NN10402-600 to replace the invalid or expired certificate on the IEMS Server. |                         |
| <b>14</b> | Select your next step.                                                                                                                                                                                                                                                                                                                                                         |                         |
|           | <b>If you are restoring a server</b>                                                                                                                                                                                                                                                                                                                                           | <b>Do</b>               |
|           | in a simplex configuration                                                                                                                                                                                                                                                                                                                                                     | <a href="#">step 17</a> |
|           | in a high-availability configuration                                                                                                                                                                                                                                                                                                                                           | <a href="#">step 15</a> |



**15** Select your next step.

| <b>If</b>                                                                                                | <b>Do</b>               |
|----------------------------------------------------------------------------------------------------------|-------------------------|
| you are performing this procedure during an upgrade on the inactive server of a two-server configuration | step <a href="#">17</a> |
| otherwise                                                                                                | step <a href="#">16</a> |

**16** Clone the active server to the inactive server. For details, see “Cloning the image of one node in a cluster to the other node” in *ATM/IP Solution-level Administration and Security*, NN10402-600.**17** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Setting up the BootP file on SPFS

---

### Application

Use this procedure to set up the Server Platform Foundation Software (SPFS-based server as the bootp master and migrate the bootp entries from the core manager to the SPFS-based server.

**Note:** The term core manager is used to mean either SDM, CS 2000 Core Manager, or Core and Billing Manager.

### Prerequisites

This procedure has the following prerequisites:

- the OpenSSH fileset on the CS 2000 Core Manager version of the core manager must be APPLIED. Since OpenSSH is part of the SPFS platform, however, nothing must be done for the Core and Billing Manager (CBM) version of the core manager.

**Note:** You can verify whether the OpenSSH fileset is APPLIED on the CS 2000 Core Manager version of the core manager by using command “sdmmtc details” at the core manager. If it is not applied, refer to procedure “Installing or upgrading OpenSSH” in document Upgrading a Carrier Voice over IP Network, NN10440-450.

- you need the password for the root user on the core manager
- you need the IP address of the core manager

**Note:** You can obtain the IP address of the CS 2000 Core Manager version of a core manager by using the command “sdmmtc eth”. Use the IP address associated with the host name of the core manager, which is the first one.

You can obtain the IP address of the Core and Billing Manager (CBM) version of a core manager by using command “cbmmtc core”. Use the IP address that is printed beneath the node address.

## Action

Perform the following steps to complete this procedure.

### *At your workstation*

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Access the command line interface to configure the IP address of the core manager by typing

```
cli
```

and pressing the Enter key.

- 3 Enter the number next to the “Configuration” option in the menu.
- 4 Enter the number next to the “OAMP Application Configuration” option in the menu.
- 5 Enter the number next to the “sdm\_conf” option in the menu.
- 6 When prompted, enter the IP address of the core manager.
- 7 When prompted, confirm the current settings by typing

```
ok
```

and pressing the Enter key.

The system generates the ssh key pair needed for data transmission between the SPFS-based server and the core manager.

#### *Example response with no change in IP address*

```
SDM IP and CM CLLI have been Successfully
Configured
```

#### *Example response with change in IP address*

```
Re-Generate the SSH key using the new SDM IP <IP
address>
Checking if SDM IP address is configured
Enter file in which to save the key
(/export/home/sam21em/.ssh/id_rsa):
```

- 8 When prompted, press the Enter key to accept the default location and filename “/export/home/sam21em/.ssh/id\_rsa” for the key.  
**Note 1:** If the default location and filename is not provided, enter “/export/home/sam21em/.ssh/id\_rsa”.  
**Note 2:** If the location and filename “/export/home/sam21em/.ssh/id\_rsa” already exists and you wish to overwrite, type **y** and press the Enter key. Otherwise, type **n**.
- 9 When prompted, confirm you want to continue connecting by typing  
**yes**  
and pressing the Enter key.
- 10 When prompted, enter the password for the core manager root user.
- 11 When prompted, enter the password for the core manager root user again.  
*Example response 1:*  
Successfully performed bootptab manipulation  
Synchronizing files IF clustered node  
*Example response 2:*  
The bootptab file is NOT empty, no need to transfer it from SDM...  
Synchronizing files IF clustered node  
*Example response 3:*  
bootptab file size is 0, will get copy from SDM  
**Note:** If you receive the second response, take no action. It means that the script has detected changes have been made to the bootptab file and is not overwriting it.  
Once complete, access to the needed directories and files on the core manager will be provided.
- 12 Exit each menu level of the command line interface to eventually exit the command line interface, by typing  
**select - x**  
and pressing the Enter key.
- 13 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.



## CS 2000 Management Tools upgrade

This section provides information on how to upgrade the SPFS-based server that is hosting the CS 2000 Management Tools. The upgrade consists of upgrading the following software:

- Server Platform Foundation Software (SPFS)
- Network Patch Manager (NPM) if present on this server
- Patching server Element (PSE)
- CS 2000 Management (CS2M) components, which include SESM, SAM21 Manager, QCA
- Integrated Element Management System (IEMS) if present on this server

**Note:** If the IEMS application resides on a separate SPFS-based server, refer to section [IEMS upgrade on page 208](#).

- Audio Provisioning Server (APS) if present on the server
- Alternate Boot Server (ABS)

The supported platforms for the CS 2000 Management Tools are as follows:

- a simplex server (Sun Netra t1400 or Sun Netra 240)
- a high-availability server pair (Sun Netra 240)

In the event you need or want to downgrade the CS 2000 Management Tools, refer to procedure “Downgrading the CS 2000 Management Tools software” in *ATM/IP Fault Management*, NN10408-900.

### What's new in CS 2000 Management Tools upgrades in (I)SN09U

There are no feature changes in the CS 2000 Management Tools upgrade.

## Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U
- SN09U to SN09U

## Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

**Time to complete an upgrade**

The following table lists the tasks to upgrade the SPFS-based server that is hosting the CS 2000 Management Tools and other applications, and the estimated time to complete each task.

**Estimated time to complete a software upgrade**

| Task                         | Application                                                                                          | Time                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Preparing for the upgrade    |                                                                                                      | 120 minutes                                           |
| Upgrading the software       | SPFS<br>(Disk 2 is for a Solaris OS upgrade and is used only when upgrading from a pre SN08 release) | Disk 1: 60 min.<br>Disk 2: 30 min.<br>Disk 3: 75 min. |
|                              | SPFS (for GEO survivability standby server)                                                          | Disk 1: 25 min.<br>Disk 2: 20 min.<br>Disk 3: 50 min. |
|                              | IEMS (if present on this server)                                                                     | 45 min. to 2 hrs depending on size of oracle database |
|                              | CS2M                                                                                                 | 30 min.                                               |
|                              | APS (if present on the server)                                                                       | 110 min.                                              |
|                              | ABS                                                                                                  | 6 min.                                                |
|                              | Total time for upgrade components                                                                    | 4 - 8.75 hours (depending on configuration)           |
| Completing the upgrade       |                                                                                                      | 1.5 - 3.5 hours depending on configuration            |
| Total estimated upgrade time |                                                                                                      | 7.5 - 14.25 hours depending on configuration          |
| Performing a rollback        |                                                                                                      | 120 minutes                                           |

**Service impacts**

The upgrade of the SPFS-based server that is hosting the CS 2000 Management Tools creates the following service impacts:

- During the SWACT between active and inactive servers, a network loss of visibility occurs. For an N240, this outage can last for up to 40 minutes.
- The APS application will be out of service for approximately 110 minutes.
- The ABS application and USP GUI will be out of service for approximately 121 minutes.
- N240 cluster configurations run in a simplex configuration until the clone takes place. The clone can take 60 to 90 minutes to complete.
- In a simplex configuration, the CS2M application will be out of service during the entire CMT upgrade. In a HA configuration, the CS2M application will be out of service from the SWACT between the active and inactive servers until the completion of the CMT upgrade.

**Additional information**

The following additional information applies to the upgrade of an SPFS-based server that is hosting the CS 2000 Management Tools:

- Nortel engineering recommends limiting t1400 servers in IEMS co-resident configurations capacity to less than 16 Gateway Controllers (GWC), and that systems with a higher capacity move to N240 servers.
- IEMS co-resident with the CS 2000 Management Tools on a t1400 simplex server, requires 4GB of RAM.
- Nortel engineering recommends using N240 servers for IEMS performance collection with intervals less than 30 minutes.
- If this server is in a geographically-redundant configuration, the standby server must also be upgraded.
- For the SPFS upgrade, new logs and alarms are not processed during the required reboot. However, the status of those logs and alarms are resynchronized after the reboot to ensure accurate status.

**System capacity**

The software upgrade procedure can impact the system capacity. This means that additional disk space on the OAMP workstation are required for converting existing databases.



## System performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade.

## System limitations during upgrade

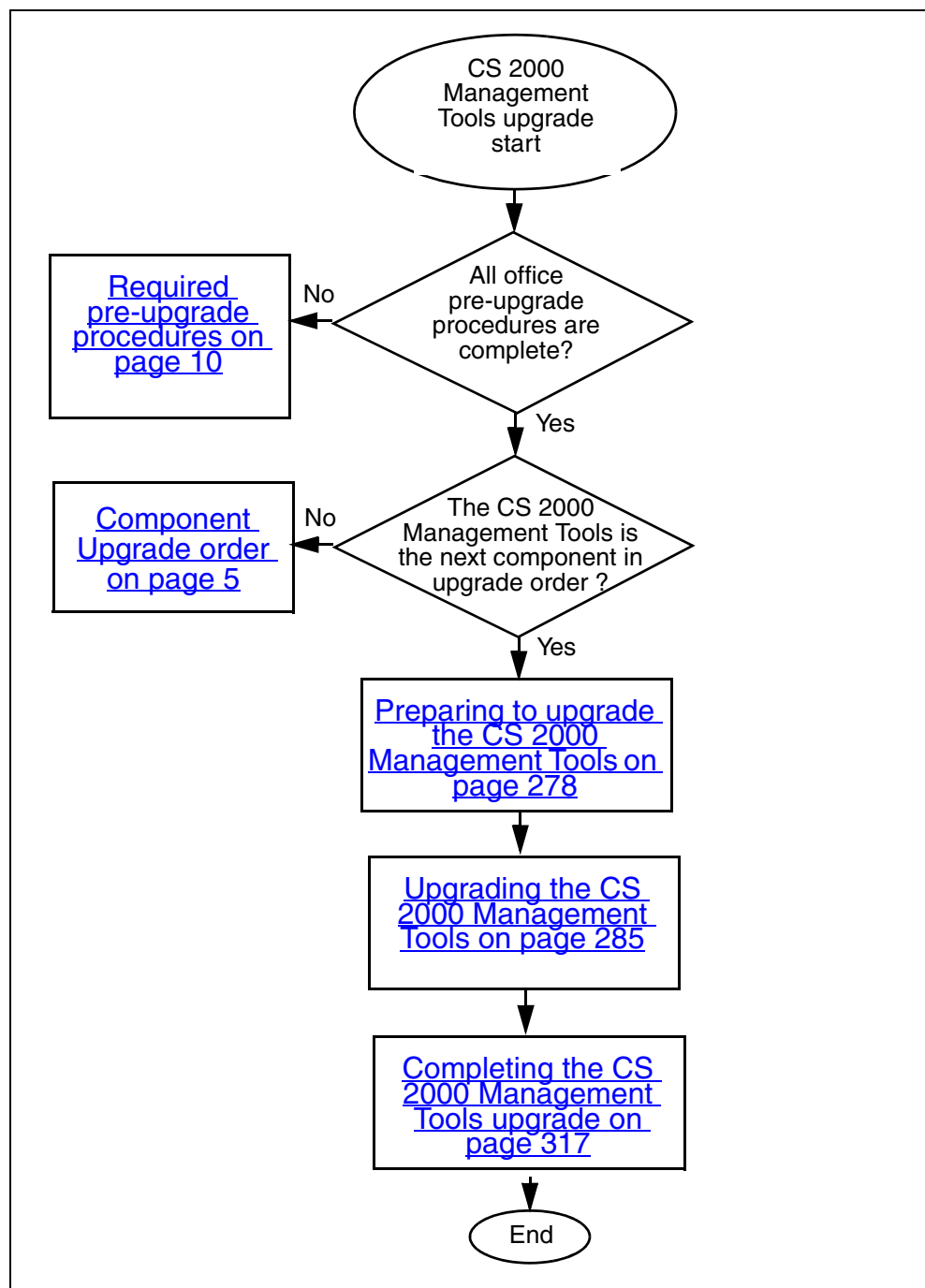
The following limitations apply:

- Migrating from a Sun Netra t1400 to a Sun Netra 240 one-server or two-server configuration is not supported as part of an upgrade to (I)SN09U.
- Migrating from a Sun Netra 240 one-server configuration to a Sun Netra 240 two-server configuration is not supported as part of an upgrade to (I)SN09U.

## CS 2000 Management Tools upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade the CS 2000 Management Tools.

### CS 2000 Management Tools upgrade tasks



---

## Preparing to upgrade the CS 2000 Management Tools

---

The following procedure provides the steps you need to execute prior to upgrading the SPFS-based server that is hosting the CS 2000 Management Tools software. When applicable, a reference to the procedure that contains the detailed steps is provided.

### Prerequisites

This procedure has the following prerequisites:

- you have completed the tasks under [Preparing to upgrade the Carrier Voice over IP Network on page 9](#)
- you have upgraded all components that precede the CS 2000 Management Tools under [Component Upgrade order on page 5](#)
- ensure that you have an RJ-45 to DB-9 Serial Cable on hand. This cable is necessary when you log in to the server through the console port.

### Action

Follow the link associated with the type of server you are preparing to upgrade.

- [Preparing to upgrade a simplex server on page 278](#)
- [Preparing to upgrade an HA server pair on page 281](#)

#### Preparing to upgrade a simplex server

##### *At your workstation*

- 1 Establish a connection to the server and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

##### *At the server*

- 2 Verify which applications are present on the server by typing  

```
servquery -registered all
```

and pressing the Enter key.

- 3 Note whether the following applications are present on the server:

| Application | Present (yes or no) |
|-------------|---------------------|
| APS         |                     |
| NPM         |                     |
| IEMS        |                     |

- 4 Ensure the SPFS and all applications on the server are at the latest maintenance release (MNCL) for the release you are currently running, and are patch-current.
- For detailed steps on viewing the SPFS release on the server, refer to procedure [Determining the SPFS software MNCL level on page 424](#).
- For detailed steps on patch currency, refer to procedure [Ensuring patch currency on page 12](#).
- 5 Verify whether an HTTPS certificate is installed on the server, and whether it is valid.
- For detailed steps, refer to procedure [Verifying the presence and validity of an HTTPS certificate on an SPFS-based server on page 329](#).
- 6 Perform all applicable audits on the server using the CS 2000 Management Tools Audit System.
- For detailed steps, refer to procedure [Performing an audit on page 332](#).
- 7 Back up the oracle data.
- For detailed steps, refer to procedure [Performing a backup of oracle data on an SPFS-based server on page 374](#).
- 8 Back up the file systems.
- For detailed steps, refer to procedure [Performing a backup of file systems on an SPFS-based server on page 379](#).
- 9 If the APS is present on the server (determined in [step 3](#)), proceed to [step 10](#), otherwise, proceed to [step 12](#).

- 10 Back up the APS audio files.  
For detailed steps, refer to one of the following procedures:
  - For a Sun Netra t1400, refer to procedure [Performing a backup of APS audio files to tape on page 392](#).
  - For a Sun Netra 240, refer to procedure [Performing a backup of APS audio files to CD or DVD on page 394](#).
- 11 Back up the APS oracle data.  
For detailed steps, refer to one of the following procedures:
  - For a Sun Netra t1400, refer to procedure [Performing a backup of APS oracle data to tape on page 396](#).
  - For a Sun Netra 240, refer to procedure [Performing a backup of APS oracle data to CD or DVD on page 398](#).
- 12 If the NPM is present on this server (determined in [step 3](#)), proceed to [step 13](#), otherwise proceed to [step 15](#).
- 13 Save NPM user-defined data.  
For detailed steps, refer to procedure [Archiving the NPM database into a file on page 383](#).
- 14 Save NPM patch files.  
For detailed steps, refer to procedure [Saving the NPM patch and database files on page 385](#).
- 15 If the IEMS is present on this server (determined in [step 3](#)), proceed to [step 18](#), otherwise proceed to [step 16](#).
- 16 Determine if PAM Radius is configured on this server by typing  

```
grep pam_radius /etc/pam.conf
```

  
and pressing the Enter key.  
  
If any output is displayed, then PAM Radius is configured. Record this information. The information is required to reconfigure PAM Radius after the server upgrade.
- 17 Proceed to [step 23](#).
- 18 Run the IEMS pre-check script.  
For detailed steps, refer to procedure [Running the IEMS pre-check script on page 251](#).

- 19** Determine if a third-party security application is used on this server by typing
- ```
# grep pam_dce /etc/pam.conf
```
- and pressing the Enter key.
- ```
grep pam_ldap /etc/pam.conf
```
- and pressing the Enter key.
- 20** If you received a response from the commands you entered in the previous step ([step 19](#)), proceed to [step 21](#), otherwise, proceed to [step 22](#).
- 21** This server is using a third-party security application, and the NSCD, PAM and NSSwitch configuration files (nscd.conf, pam.conf and nsswitch.conf) have special edits in them. Those special edits will need to be put back following the upgrade, since during the upgrade, the configuration files are replaced with new configuration files that use the IEMS security application.
- Inform your system administrator before you proceed with the upgrade, that the files will be replaced during the upgrade.
- 22** Determine the status of the QCA server application by typing
- ```
# servquery -status -g QCA
```
- and pressing the Enter key.
- Example response when QCA is running*
- ```
A QCA instance is registered with PMFADN as Qca
and running on the portNumber=20000
```
- Example response when QCA is not running*
- ```
A QCA instance is not registered with PMFADM as
Qca
```
- Record the status of QCA as running or not running. You will have to set the QCA to this same status after the upgrade.
- 23** You have completed this procedure. Proceed to [Upgrading the CS 2000 Management Tools on page 285](#).

Preparing to upgrade an HA server pair

At your workstation

- 1** Establish a connection to the active and inactive servers and log in using the root user ID and password.
- For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

On the inactive server

- 2 Verify which applications are present on the server by typing
`# servquery -registered all`
and pressing the Enter key.
- 3 Note whether the following applications are present on the server:

Application	Present (yes or no)
APS	
NPM	
IEMS	

- 4 Ensure the SPFS and all applications on the server are at the latest maintenance release (MNCL) for the release you are currently running, and are patch-current. Contact your system administrator if required.

For detailed steps on viewing the SPFS release on the server, refer to procedure [Determining the SPFS software MNCL level on page 424](#).

For detailed steps on patch currency, refer to procedure [Ensuring patch currency on page 12](#).
- 5 Verify the state of the cluster.

For detailed steps, refer to procedure [Verifying the state of a cluster on page 400](#).

On the active server

- 6 Verify whether an HTTPS certificate is installed on the server, and whether it is valid.

For detailed steps, refer to procedure [Verifying the presence and validity of an HTTPS certificate on an SPFS-based server on page 329](#).
- 7 Perform all applicable audits on the server using the CS 2000 Management Tools Audit System.

For detailed steps, refer to procedure [Performing an audit on page 332](#).
- 8 Back up the oracle data.

For detailed steps, refer to procedure [Performing a backup of oracle data on an SPFS-based server on page 374](#).

- 9 Back up the file systems.
For detailed steps, refer to procedure [Performing a backup of file systems on an SPFS-based server on page 379](#).
- 10 If the APS is present on the server (determined in [step 3](#)), proceed to [step 11](#), otherwise proceed to [step 13](#).
- 11 Back up the APS audio files.
For detailed steps, refer to procedure [Performing a backup of APS audio files to CD or DVD on page 394](#).
- 12 Back up the APS oracle data.
For detailed steps, Refer to procedure [Performing a backup of APS oracle data to CD or DVD on page 398](#).
- 13 If the NPM is present on this server (determined in [step 3](#)), proceed to [step 14](#), otherwise proceed to [step 16](#).
- 14 Save NPM user-defined data.
For detailed steps, refer to procedure [Archiving the NPM database into a file on page 383](#).
- 15 Save NPM patch files.
For detailed steps, refer to procedure [Saving the NPM patch and database files on page 385](#).
- 16 If the IEMS is present on this server (determined in [step 3](#)), proceed to [step 19](#), otherwise proceed to [step 17](#).
- 17 Determine if PAM Radius is configured on this server by typing

```
# grep pam_radius /etc/pam.conf
```

and pressing the Enter key.
If any output is displayed, then PAM Radius is configured.
Record this information. The information is required to reconfigure PAM Radius after the server upgrade.
- 18 Proceed to [step 24](#).
- 19 Run the IEMS pre-check script.
For detailed steps, refer to procedure [Running the IEMS pre-check script on page 251](#).
- 20 Determine if a third-party security application is used on this server by typing

```
# grep pam_dce /etc/pam.conf
```

and pressing the Enter key.

```
# grep pam_ldap /etc/pam.conf
```


and pressing the Enter key.

- 21** If you received a response from the commands you entered in the previous step ([step 20](#)), proceed to [step 22](#), otherwise, proceed to [step 23](#).
- 22** This server is using a third-party security application, and the NSCD, PAM and NSSwitch configuration files (nscd.conf, pam.conf and nsswitch.conf) have special edits in them. Those special edits will need to be put back following the upgrade, since during the upgrade, the configuration files are replaced with new configuration files that use the IEMS security application.
- Inform your system administrator before you proceed with the upgrade, that the files will be replaced during the upgrade.
- 23** Determine the status of the QCA server application by typing
- ```
servquery -status -g QCA
```
- and pressing the Enter key.
- Example response when QCA is running*
- ```
A QCA instance is registered with PMFADN as Qca
and running on the portNumber=20000
```
- Example response when QCA is not running*
- ```
A QCA instance is not registered with PMFADM as
Qca
```
- Record the status of QCA as running or not running. You will have to set the QCA to this same status after the upgrade.
- 24** You have completed this procedure. Proceed to [Upgrading the CS 2000 Management Tools on page 285](#).

---

## Upgrading the CS 2000 Management Tools

---

The following procedure provides the steps you need to execute to upgrade the SPFS-based server that is hosting the CS 2000 Management Tools software application. When applicable, a reference to the procedure that contains the detailed steps is provided.

### Prerequisites

You have completed procedure [Preparing to upgrade the CS 2000 Management Tools on page 278](#).

### Action

Follow the link associated with the upgrade path release you are on:

- [Upgrading from \(I\)SN08 or \(I\)SN09 to \(I\)SN09U on page 286](#)
- [Upgrading from \(I\)SN09U to \(I\)SN09U \(maintenance release\) on page 306](#)

## Upgrading from (I)SN08 or (I)SN09 to (I)SN09U

Follow the link associated with the type of server you are upgrading.

- [Upgrading a simplex server on page 286](#)
- [Upgrading an HA server pair on page 295](#)

### Upgrading a simplex server

#### ATTENTION

At any point from [step 8](#) up to and including [step 16](#) in this procedure, executing a fallback will involve performing procedure “Executing a fallback during an SPFS-based server upgrade” for a [One-server configuration on page 419](#).

At any point after [step 16](#) in this procedure, executing a fallback will involve a full system restore. Refer to “Performing a full system restore on an SPFS-based server” in *ATM/IP Fault Management*, NN10408-900.

### At your workstation

- 1 Establish a connection to the server and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

### On the server

- 2 If IEMS is present on this server, proceed to [step 3](#), otherwise, proceed to [step 4](#).
- 3 Back up the central security server. Failure to back up the central security server will result in the loss of all the current IEMS user and password information.  
For detailed steps, refer to [Backing up the central security server](#).
- 4 Verify whether other users are logged on to the system by typing  

```
who
```

and pressing the Enter key.
- 5 The presence of other users logged on to the system can have adverse effects on the upgrade process and can cause the upgrade to fail. Therefore, request that all users log out before you proceed.  

```
wall
```

**The system is coming down for maintenance. Please log off immediately in order to save your files.**

and pressing the Enter key.

Then hit the Ctrl and D keys simultaneously to send the message to all users.

6

**CAUTION****Potential for operational problems**

Once you have upgraded the SPFS, continue until you have upgraded all applications on this server. Failing to upgrade an application to the same release as the SPFS will result in operational problems.

In order for this server to be completely upgraded, the entire procedure must be followed. Do not subdivide this upgrade procedure into separate maintenance windows.

Upgrade the SPFS.

For detailed steps, refer to procedure [Upgrading SPFS software on page 403](#).

7

If you received a notification bulletin that an SPFS MNCL is available for the SPFS release you just upgraded to, proceed to [step 8](#), otherwise, proceed to [step 9](#).

8

Install the SPFS MNCL.

For detailed steps, refer to the instructions provided with the MNCL.

9

**ATTENTION**

The SN08 Central Security Server (IEMSCSS and IEMSCSS\_DS) patches remain applicable to the SN09U IEMS load and must be transferred to NPM, if not already available on NPM.

Obtain any patches you received with your software release, that are applicable to the components on the server, such as, PSE, SESM, SAM21EM, NPM, SPFS, QCA, IEMS, IEMSCSS,

IEMSCSS\_DS, CSMONITOR, PKMGR\_SERVER, COREM, and transfer them to the NPM database.

If you received patches in ISO image file(s), proceed to [step 10](#), otherwise, proceed to [step 13](#).

- 10 Transfer and mount the patch ISO image on the server.  
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 11 Transfer the patches from the ISO image file to the NPM database.  
For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).
- 12 Unmount and remove the patch ISO image from the server.  
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).  
If there is another patch ISO image file to transfer to the NPM database return to [step 10](#), otherwise, proceed to [step 13](#).
- 13 If you received patches on one or more CDs, proceed to [step 14](#), otherwise, proceed to [step 15](#).
- 14 For each CD with patches, transfer the patches from the CD to the NPM database.  
For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).
- 15 If you have SPFS patches for the SPFS release you just upgraded to, proceed to [step 16](#), otherwise, proceed to [step 17](#).
- 16 Audit the upgraded device, and apply the SPFS patches.  
For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#).
- 17 If the NPM is present on this server, proceed to [step 18](#), otherwise, proceed to [step 20](#).
- 18 If you have NPM patches for the SPFS/NPM release you just upgraded to, proceed to [step 19](#), otherwise, proceed to [step 20](#).
- 19 Apply the NPM patches and restart the NPM.  
For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#).

**Note:** If you have a large network, abort any NPM tasks that are queued ahead of the NPM restart tasks. In a large network, the list of NPM tasks queued ahead of the NPM

restart task can be long and can take many hours to complete. Therefore, aborting NPM tasks is recommended in large networks to shorten the upgrade time.

For detailed steps, refer to procedure [Prioritizing or aborting a patching maintenance request using the NPM on page 2421](#).

- 20 If you have PSE patches for the SPFS/PSE release you just upgraded to, proceed to [step 21](#), otherwise, proceed to [step 22](#).
- 21 Audit the upgraded device, apply the PSE patches and restart PSE.

For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#).

- 22 Import the security certificates by typing

```
import_certs.ksh
```

and pressing the Enter key.

- 23 If IEMS is on a separate SPFS-based server, proceed to [step 24](#), otherwise, proceed to [step 27](#).
- 24 If PAM Radius was configured on this server prior to the SPFS upgrade, proceed to [step 25](#), otherwise, proceed to [step 46](#).
- 25 Reconfigure PAM Radius. PAM Radius uses the Integrated Element Management System (IEMS) central security server for authentication. This step configures this server as a radius client of the IEMS centralized security server.

For detailed steps, refer to procedure [Configuring an SPFS-based client server to use PAM Radius on page 443](#).

- 26 Proceed to [step 46](#).
- 27 Enable the health monitors by typing

```
cfgsplxck enable
```

and pressing the Enter key.

Example response

```
NOTE: Enabling health monitor...Success.
```

- 28 If you are upgrading IEMS using ESD, proceed to [step 29](#), or if you are upgrading IEMS using a CD, proceed to [step 30](#).
- 29 Transfer the IEMS ISO image file to the server and mount the ISO image file on the server.

For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

**30** Upgrade IEMS.

For detailed steps, refer to procedure [Upgrading the IEMS software on page 254](#).

**31****ATTENTION**

The SN08 Central Security Server (IEMSCSS and IEMSCSS\_DS) patches remain applicable to the SN09U IEMS load and must be applied the SN09U IEMS load.

If you have IEMS, IEMSCSS, IEMSCSS\_DS, COREM, CSMONITOR, or PKMGR\_SERVER patches for the IEMS release you just upgraded to, proceed to [step 32](#), otherwise, proceed to [step 33](#).

**32** Apply the IEMS, IEMSCSS, IEMSCSS\_DS, COREM, CSMONITOR, PKMGR\_SERVER patches, and restart the components.

For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#)

**33** Restore the central security server backup file.

For detailed steps, refer to [Restoring the central security server](#).

**34** If you upgraded IEMS using ESD, proceed to [step 35](#), or if you upgraded IEMS using a CD, proceed to [step 38](#).**35** For an ESD upgrade, run the Config Swap script by typing

```
/tmpmnt/bin/switch09conf.ksh
```

and pressing the Enter key.

When prompted, confirm you want to continue by typing

**y**

and pressing the Enter key.

**36** Unmount and remove the IEMS ISO image file from the server.

For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).

**37** Proceed to [step 40](#).**38** For a CD upgrade, run the Config Swap script by typing

```
/cdrom/cdrom0/bin/switch09conf.ksh
```

and pressing the Enter key.

When prompted, confirm you want to continue by typing

**y**

and pressing the Enter key.

- 39** Eject the CD by typing

# **cd /**

and pressing the Enter key.

# **eject cdrom**

and pressing the Enter key.

**Note:** If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

# **/etc/init.d/volmgt stop**

# **/etc/init.d/volmgt start**

Then, press the eject button located on the front of the DVD drive.

Remove the CD or DVD from the drive.

- 40** If, before the upgrade, you determined that this server is using a third-party security application as opposed to the IEMS security application, have your system administrator re-edit the NSCD, PAM and NSSwitch configuration files.

Contact your system administrator.

- 41** Start the IEMS server application if you have not already started by typing

# **servstart IEMS**

and pressing the Enter key.

- 42** Verify that IEMS, WEBSERVER, WEBSERVICES, DATABASE, RADSVR and IS are running by typing

# **servquery -status all**

and pressing the Enter key.

- 43** If the applications indicated in the previous step ([step 42](#)) are running, proceed to [step 46](#), otherwise, proceed to [step 44](#).



- 44 Start each application, indicated in [step 42](#), that is not running by typing

```
servstart <app_name>
```

and pressing the Enter key.

where

**app\_name**

is the name of the application that is not in a RUNNING state, for example, IEMS

- 45 If all applications you started in the previous step ([step 44](#)) are now running, proceed to [step 46](#), otherwise, contact your next level of support.
- 46 If you are upgrading CS2M using ESD, proceed to [step 47](#), or if you are upgrading CS2M using a CD, proceed to [step 48](#).
- 47 Transfer the CS2M ISO image file to the server and mount the ISO image file on the server.
- For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 48 Upgrade CS2M.
- For detailed steps, refer to procedure [Upgrading the CS2M software on page 446](#).
- 49 If you upgraded CS2M using ESD, proceed to [step 50](#), or if you upgraded CS2M using a CD, proceed to [step 52](#).
- 50 Unmount and remove the CS2M ISO image file.
- For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 51 Proceed to [step 54](#).
- 52 Eject the CD by typing
- ```
# cd /
```
- and pressing the Enter key.
- ```
eject cdrom
```
- and pressing the Enter key.
- Note:** If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:
- ```
# /etc/init.d/volmgt stop
```
- ```
/etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

- 53** Remove the CD or DVD from the drive.
- 54** If you have SESM, SAM21EM, QCA patches for the CS2M release you just upgraded to, proceed to [step 55](#), otherwise, proceed to [step 56](#).
- 55** Apply the SESM, SAM21EM, QCA patches, and restart each component.
- For detailed steps, refer to table [Patching procedures checklist for the CS 2000 Management Tools components on page 2277](#).
- 56** Start the SESM server application if you have not already started by typing
- ```
# servstart SESMSERVICE
```
- and pressing the Enter key.
- 57** Start the SAM21EM server application if you have not already started by typing
- ```
servstart SAM21EM
```
- and pressing the Enter key.
- 58** Set the QCA server application to the same status it was before the upgrade, as determined in [Preparing to upgrade the CS 2000 Management Tools on page 278](#) by using the procedure [Starting and stopping the QoS Collector Application on page 539](#).

| If QCA status was | Do            |
|-------------------|---------------|
| running           | Start the QCA |
| not running       | Stop the QCA  |

- 59** If APS is present on the server, proceed to [step 60](#), otherwise, proceed to [step 70](#).
- 60** If you are upgrading the APS from SN08, proceed to [step 61](#), otherwise, proceed to [step 70](#) as no upgrade is required for the APS from SN09 to SN09U.
- 61** If you are upgrading APS using ESD, proceed to [step 62](#), or if you are upgrading APS using a CD, proceed to [step 63](#).
- 62** Transfer the APS ISO image file to the server and mount the ISO image file on the server.

For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)

- 63** Upgrade APS.  
For detailed steps, refer to procedure [Upgrading APS software on page 466](#).
- 64** If you upgraded APS using ESD, proceed to [step 65](#), or if you upgraded APS using a CD, proceed to [step 67](#).
- 65** Unmount and remove the APS ISO image file.  
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 66** Proceed to [step 69](#).
- 67** Eject the CD by typing  
`# cd /`  
and pressing the Enter key.  
`# eject cdrom`  
and pressing the Enter key.  
**Note:** If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:  
`# /etc/init.d/volmgt stop`  
`# /etc/init.d/volmgt start`  
Then, press the eject button located on the front of the DVD drive.
- 68** Remove the CD or DVD from the drive.
- 69** Configure the SNMP agent. For detailed instructions, refer to procedure “Configuring the SNMP agent” in document *Media Server 2000 Configuration Management*, NN10340-511.
- 70** If IEMS was upgraded on this server, proceed to [step 71](#), otherwise, proceed [step 72](#).
- 71** Verify the IEMS upgrade was successful.  
For detailed steps, refer to procedure [Verifying the IEMS upgrade was successful on page 472](#).
- 72** Verify the CS2M upgrade was successful.  
For detailed steps, refer to procedure [Verifying the CS2M upgrade was successful on page 506](#).
- 73** Verify the APS upgrade was successful.  
For detailed steps, refer to procedure [Verifying the APS upgrade was successful on page 510](#).

- 74 Use the following table to determine the next step.

| If                                                       | Do                      |
|----------------------------------------------------------|-------------------------|
| you choose to accept the upgraded environment            | <a href="#">step 75</a> |
| you choose to rollback to the state prior to the upgrade | <a href="#">step 76</a> |

- 75 Accept the upgraded environment by typing  
**# /SSPFS\_Upgrade.accept**  
and pressing the Enter key.  
The execution of this step takes approximately 20 minutes to complete depending on system configuration.  
Go to [step 77](#).
- 76 If you choose to fallback, refer to the procedure “Performing a full system restore on an SPFS-based server” in the document *ATM/IP Fault Management*, NN10408-900.
- 77 You have completed this procedure. Proceed to [Completing the CS 2000 Management Tools upgrade on page 317](#).

### Upgrading an HA server pair

#### ATTENTION

A fallback can be executed at any point from [step 12](#) onward in this procedure, by performing procedure “Executing a fallback during an SPFS-based server upgrade” for a [Two-server configuration on page 419](#).

#### *At your workstation*

- 1 Establish a connection to the active and inactive servers and log in using the root user ID and password.  
For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

#### *On the active server*

- 2 If the IEMS is present on this server, proceed to [step 3](#), otherwise, proceed to [step 4](#).

- 3 Back up the central security server. Failure to back up the central security server will result in the loss of all the current IEMS user and password information.  
For detailed steps, refer to [Backing up the central security server](#).
- 4 Verify whether other users are logged on to the system by typing

```
ssh unit1-priv0 who
ssh unit0-priv0 who
```
- 5 The presence of other users logged on to the system can have adverse effects on the upgrade process and can cause the upgrade to fail. Therefore, request that all users log out before you proceed.

```
wall
```

**The system is coming down for maintenance.  
Please log off immediately in order to save your files.**

and pressing the Enter key.

Then hit the Ctrl and D keys simultaneously to send the message to all users.
- 6

**ATTENTION**

The SN08 Central Security Server (IEMSCSS and IEMSCSS\_DS) patches remain applicable to the SN09U IEMS load and must be transferred to NPM, if not already available on NPM.

Obtain any patches you received with your software release, that are applicable to the components that are on the server, such as, PSE, SESM, SAM21EM, NPM, SPFS, QCA, IEMS, IEMSCSS, IEMSCSS\_DS, CSMONITOR, PKMGR\_SERVER, COREM, and transfer them to the NPM database.

If you received patches in ISO image file(s), proceed to [step 7](#), otherwise, proceed to [step 10](#).
- 7 Transfer and mount a patch ISO image file on the active server.  
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 8 Transfer the patches from the ISO image file to the NPM database.

For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).

- 9 Unmount and remove the patch ISO image file from the server.

For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).

If there is another patch ISO image file to transfer to the NPM database return to [step 7](#). Otherwise, proceed to [step 10](#).

- 10 If you received patches on one or more CDs, proceed to [step 11](#). Otherwise, proceed to [step 12](#).

- 11 For each CD with patches, transfer the patches from the CD to the NPM database.

For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).

### ***On the inactive server***

- 12



#### **CAUTION**

##### **Potential for operational problems**

Once you have upgraded the SPFS, continue until you have upgraded all applications on this server. Failing to upgrade an application to the same release as the SPFS will result in operational problems.

In order for this server to be completely upgraded, the entire procedure must be followed. Do not subdivide this upgrade procedure into separate maintenance windows.

Upgrade the SPFS.

For detailed steps, refer to procedure [Upgrading SPFS software on page 403](#).

- 13 If you received a notification bulletin that an SPFS MNCL is available for the SPFS release you just upgraded to, or received a CD for an SPFS MNCL upgrade, proceed to [step 14](#), otherwise, proceed to [step 15](#).
- 14 Install the SPFS MNCL.

For detailed steps, refer to the instructions provided with the MNCL.

- 15 If you have SPFS, NPM and PSE patches for the release you just upgrade to, proceed to [step 16](#), otherwise, proceed to [step 21](#).
- 16 If the NPM is present on this server, proceed to [step 19](#), otherwise, proceed to [step 17](#).
- 17 When the NPM is on another SPFS-based server, apply the SPFS, NPM and PSE patches using procedure [Applying patches using the NPM on page 2319](#).
- 18 Proceed to [step 20](#).
- 19 Apply the SPFS, NPM and PSE patches to the inactive server by typing

**# patchUpToDate**

and pressing the Enter key.

Enter yes when prompted for any of the following (entering no stops the process):

- to confirm the NPM host name  
If the NPM host is incorrect, then either re-configure the PSE to point to the NPM or contact next level of support to do this. Then run patchUpToDate again.
- to confirm you want to apply the patches listed
- to confirm you want to continue when patches have special application instructions
- to confirm you want to restart any of the devices that require a restart
- to confirm you want to continue when a reboot is required  
Following a reboot, you will have to log back into the server as root.

The patchUpToDate session generates a report called *patchUpToDate.report* and places it in the directory from where the command was executed.

The report contains all the console output from the patchUpToDate session and a summary of the patching actions that occurred and any errors. The summary includes patches applied, any patches that were already applied when the patchUpToDate utility started, any patches that have been applied and removed when the patchUpToDate utility started,

- and any patches that were not applied because their prerequisite patches were not available.
- 20** Import the security certificates by typing
- ```
# import_certs.ksh
```
- and pressing the Enter key.
- 21** If IEMS is present on this server, proceed to [step 24](#), otherwise, proceed to [step 22](#).
- 22** If PAM Radius was configured on this server prior to the SPFS upgrade, proceed to [step 23](#), otherwise, proceed to [step 38](#).
- 23** Reconfigure PAM Radius. PAM Radius uses the Integrated Element Management System (IEMS) central security server for authentication. This step configures this server as a radius client of the IEMS centralized security server.
- For detailed steps, refer to procedure [Configuring an SPFS-based client server to use PAM Radius on page 443](#).
- Proceed to [step 38](#).
- 24** If you are upgrading IEMS using ESD, proceed to [step 25](#), or if you are upgrading IEMS using a CD, proceed to [step 26](#).
- 25** Transfer the IEMS ISO image file to the active server and mount the ISO image file on the inactive server.
- For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 26** Upgrade IEMS.
- For detailed steps, refer to procedure [Upgrading the IEMS software on page 254](#).
- 27** If you have IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, or PKMGR_SERVER patches for the IEMS release you just upgraded to, proceed to [step 28](#), otherwise, proceed to [step 29](#).
- 28** Apply the IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, PKMGR_SERVER patches by typing
- ```
cd /
```
- and pressing the enter key.
- ```
# patchUpToDate
```
- and pressing the Enter key.

Enter yes when prompted for any of the following (entering no stops the process):

- to confirm the NPM host name
If the NPM host is incorrect, then either re-configure the PSE to point to the NPM or contact next level of support to do this. Then run patchUpToDate again.
- to confirm you want to apply the patches listed
- to confirm you want to continue when patches have special application instructions
- to confirm you want to restart any of the devices that require a restart
- to confirm you want to continue when a reboot is required
Following a reboot, you will have to log back into the server as root.

The patchUpToDate session generates a report called *patchUpToDate.report* and places it in the directory from where the command was executed (in this case, in the root directory).

The report contains all the console output from the patchUpToDate session and a summary of the patching actions that occurred and any errors. The summary includes patches applied, any patches that were already applied when the patchUpToDate utility started, any patches that have been applied and removed when the patchUpToDate utility started, and any patches that were not applied because their prerequisite patches were not available.

- 29 Restore the central security server backup file.
For detailed steps, refer to [Restoring the central security server](#).
- 30 If you upgraded IEMS using ESD, proceed to [step 31](#), or if you upgraded IEMS using a CD, proceed to [step 34](#).
- 31 For an ESD upgrade, run the Config File Swap script as follows:
 - a Run the script by typing

```
# /tmpmnt/bin/switch09conf.ksh
```

and pressing the Enter key.
 - b When prompted, confirm you want to continue by typing

```
y
```

and pressing the Enter key.
- 32 Unmount and remove the IEMS ISO image file from the server.

For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).

- 33 Proceed to [step 37](#).
- 34 For a CD upgrade, run the Config File Swap script as follows:
 - a Run the script by typing

```
# /cdrom/cdrom0/bin/switch09conf.ksh
```

and pressing the Enter key.
 - b When prompted, confirm you want to continue by typing

```
y
```

and pressing the Enter key.
- 35 Eject the CD by typing

```
# cd /
```

and pressing the Enter key.

```
# eject cdrom
```

and pressing the Enter key.

Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.
- 36 Remove the CD or DVD from the drive.
- 37 If, before the upgrade, you determined that this server is using a third-party security application as opposed to the IEMS security application, have your system administrator re-edit the NSCD, PAM and NSSwitch configuration files.

Contact your system administrator.
- 38 If you are upgrading CS2M using ESD, proceed to [step 39](#), or if you are upgrading CS2M using a CD, proceed to [step 40](#).
- 39 Transfer the CS2M ISO image file to the active server and mount the ISO image file on the inactive server.

For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

- 40** Upgrade CS2M.
For detailed steps, refer to procedure [Upgrading the CS2M software on page 446](#).
- 41** If you upgraded CS2M using ESD, proceed to [step 42](#), or if you upgraded CS2M using a CD, proceed to [step 44](#).
- 42** Unmount and remove the CS2M ISO image file from the server.
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 43** Proceed to [step 46](#).
- 44** Eject the CD by typing
`# cd /`
and pressing the Enter key.
`# eject cdrom`
and pressing the Enter key.
Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:
`# /etc/init.d/volmgt stop`
`# /etc/init.d/volmgt start`
Then, press the eject button located on the front of the DVD drive.
- 45** Remove the CD or DVD from the drive.
- 46** If you have SESM, SAM21EM, QCA patches for the CS2M release you just upgraded to, proceed to [step 47](#), otherwise, proceed to [step 51](#).
- 47** If the NPM is present on this server, proceed to [step 50](#), otherwise, proceed to [step 48](#).
- 48** When the NPM is on a another SPFS-based server, apply the SESM, SAM21EM, and QCA patches using procedure [Applying patches using the NPM on page 2319](#).
- 49** Proceed to [step 51](#).

- 50 Apply the SESM, SAM21EM, QCA patches by typing

patchUpToDate

and pressing the Enter key.

Example response:

Obtaining the list of devices that can be patched.

According to the current PSE configuration, 'wnc0s00z' is the NPM host.

Is this correct? [yes]

Press the Enter key to confirm that you want the patches applied.

Note: Typing no and pressing the Enter key causes the processing to stop.

A report is generated which contains all the console output from the patchUpToDate session.

The report that is produced contains a summary of the patching actions that occurred as well as any errors. The summary includes patches applied, any patches that were already applied when the patchUpToDate utility started, any patches that have been applied and removed when the patchUpToDate utility started, and any patches that were not applied because their prerequisite patches were not available.

On the active server

- 51 Stop the cluster.

For detailed steps, refer to procedure [Stopping a cluster on page 457](#).

On the newly active server with the (I)SN09U software

- 52 If the APS is present on the server, proceed to [step 53](#) , otherwise, proceed to [step 63](#) .
- 53 If you are upgrading the APS from SN08, proceed to [step 54](#), otherwise, proceed to [step 63](#) as no upgrade is required for the APS from SN09 to SN09U.
- 54 If you are upgrading the APS using ESD, proceed to [step 55](#), or if you are upgrading APS using a CD, proceed to [step 56](#).
- 55 Transfer the APS ISO image file to the active server and mount the ISO image file on the active server.

For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

- 56 Upgrade APS.
For detailed steps, refer to procedure [Upgrading APS software on page 466](#).
- 57 If you upgraded APS using ESD, proceed to [step 58](#), or if you upgraded APS using a CD, proceed to [step 60](#).
- 58 Unmount and remove the APS ISO image file from the server.
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 59 Proceed to [step 62](#).
- 60 Eject the CD by typing
`# cd /`
and pressing the Enter key.
`# eject cdrom`
and pressing the Enter key.
Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:
`# /etc/init.d/volmgt stop`
`# /etc/init.d/volmgt start`
Then, press the eject button located on the front of the DVD drive.
- 61 Remove the CD or DVD from the drive.
- 62 Configure the SNMP agent. For detailed instructions, refer to procedure “Configuring the SNMP agent” in document *Media Server 2000 Configuration Management*, NN10340-511.
- 63 If IEMS was upgraded on this server, proceed to [step 64](#), otherwise, proceed to [step 68](#).
- 64 Verify the IEMS upgrade was successful.
For detailed steps, refer to procedure [Verifying the IEMS upgrade was successful on page 472](#).
- 65 Verify all services are up by typing
`# servquery -status all`
and pressing the Enter key.
- 66 Set the QCA server application to the same status it was before the upgrade, as determined in [Preparing to upgrade the CS 2000 Management Tools on page 278](#) by using the procedure

[Starting and stopping the QoS Collector Application on page 539.](#)

If QCA status was	Do
running	Start the QCA
not running	Stop the QCA

- 67** Execute the amldap user password script as follows:
- a** Change directories by typing (there is no space between security/ and current_core)


```
# cd /opt/nortel/applications/security/current_core/bin
```

 and pressing the Enter key.
 - b** Run the update_am_pwd_exp.sh script by typing


```
# ./update_am_pwd_exp.sh
```

 and pressing the Enter key.
 - c** When prompted, confirm you want to continue by typing


```
# y
```

 and pressing the Enter key.
- 68** Verify the CS2M upgrade was successful.
For detailed steps, refer to procedure [Verifying the CS2M upgrade was successful on page 506](#).
- 69** Verify the APS upgrade was successful.
For detailed steps, refer to procedure [Verifying the APS upgrade was successful on page 510](#).
- 70** Use the following table to determine the next step.

If	Do
you choose to accept the upgraded environment	step 71
you choose to rollback to the state prior to the upgrade	step 72

71

ATTENTION

At this point, you can easily revert this upgraded server back to the previous release. Continuing with this procedure, clones the image of the upgraded server onto the server running the previous release, and once both servers are upgraded, reverting back to the previous release will require a full system restore.

Accept the upgraded environment by typing

```
# /SSPFS_Upgrade.accept
```

and pressing the Enter key.

The execution of this step takes approximately 20 minutes to complete depending on system configuration.

Go to [step 73](#).

- 72 If you choose to fallback, refer to procedure “Executing a fallback during an SPFS-based server upgrade” [Two-server configuration on page 419](#).
- 73 You have completed this procedure. Proceed to [Completing the CS 2000 Management Tools upgrade on page 317](#).

Upgrading from (I)SN09U to (I)SN09U (maintenance release)

Follow the link associated with the type of server you are upgrading.

- [Upgrading a simplex server \(maintenance release\) on page 306](#)
- [Upgrading an HA server pair \(maintenance release\) on page 311](#)

Upgrading a simplex server (maintenance release)***At your workstation***

- 1 Establish a connection to the server and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

At the server

- 2** Verify whether other users are logged on to the system by typing
who
and pressing the Enter key.

The presence of other users logged on to the system can have adverse effects on the upgrade process and can cause the upgrade to fail. Therefore, request that all users log out before you proceed.

- 3** If IEMS is present on this server and you have a maintenance release for the IEMS, proceed to [step 4](#), otherwise, proceed to [step 21](#).

- 4** Back up the central security server. Failure to back up the central security server will result in the loss of all the current IEMS user and password information.

For detailed steps, refer to [Backing up the central security server](#).

5

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be transferred to NPM, if not already available on NPM.

Obtain any patches you received after the maintenance release, that are applicable to the IEMS components (IEMS, IEMSCSS, IEMSCSS_DS, CSMONITOR, PKMGR_SERVER, COREM).

For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).

- 6** Stop the IEMS server application by typing
servstop IEMS
and pressing the Enter key.

- 7** Stop the CEM server application by typing
servstop CEM
and pressing the Enter key.

- 8** If you are upgrading IEMS using ESD, proceed to [step 9](#), or if you are upgrading IEMS using a CD, proceed to [step 10](#).

- 9 Transfer the IEMS ISO image file to the server and mount the ISO image file on the server.
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)
- 10 Upgrade IEMS.
For detailed steps, refer to procedure [Upgrading the IEMS software on page 254](#).
- 11 If you upgraded IEMS using ESD, proceed to [step 12](#), or if you upgraded IEMS using a CD, proceed to [step 14](#).
- 12 Unmount and remove the IEMS ISO image file from the server.
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 13 Proceed to [step 16](#).
- 14 Eject the CD by typing

```
# cd /
```

and pressing the Enter key.

```
# eject cdrom
```

and pressing the Enter key.
Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.
- 15 Remove the CD or DVD from the drive.
- 16

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be applied the SN09U IEMS load.

If you have IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, or PKMGR_SERVER patches for the IEMS release you just upgraded to, proceed to [step 17](#), otherwise, proceed to [step 19](#).

- 17 Apply the IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, PKMGR_SERVER patches.
For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#).
- 18 Restore the central security server backup file.
For detailed steps, refer to [Restoring the central security server](#).
- 19 Start the IEMS server application by typing
servstart IEMS
and pressing the Enter key.
- 20 Start the CEM server application by typing
servstart CEM
and pressing the Enter key.
- 21 Obtain any patches you received after the maintenance release, that are applicable to the CS2M components (SESM, SAM21EM, and QCA).
For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).
- 22 Stop the SESM server application by typing
servstop SESMSERVICE
and pressing the Enter key.
- 23 Stop the SAM21EM server application by typing
servstop SAM21EM
and pressing the Enter key.
- 24 Stop the QCA server application by typing
servstop QCA
and pressing the Enter key.
- 25 If you are upgrading CS2M using ESD, proceed to [step 26](#), or if you are upgrading CS2M using a CD, proceed to [step 27](#).
- 26 Transfer the CS2M ISO image file to the server and mount the ISO image file on the server.
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)

- 27** Upgrade CS2M.
For detailed steps, refer to procedure [Upgrading the CS2M software on page 446](#).
- 28** If you upgraded CS2M using ESD, proceed to [step 29](#), or if you upgraded CS2M using a CD, proceed to [step 31](#).
- 29** Unmount and remove the CS2M ISO image file from the server.
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 30** Proceed to [step 33](#).
- 31** Eject the CD by typing
`# cd /`
and pressing the Enter key.
`# eject cdrom`
and pressing the Enter key.
Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:
`# /etc/init.d/volmgt stop`
`# /etc/init.d/volmgt start`
Then, press the eject button located on the front of the DVD drive.
- 32** Remove the CD or DVD from the drive.
- 33** If you have SESM, SAM21EM, QCA patches for the CS2M release you just upgraded to, proceed to [step 34](#), otherwise, proceed to [step 35](#).
- 34** Apply the SESM, SAM21EM, and QCA patches.
For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#).
- 35** Start the SESM server application by typing
`# servstart SESMSERVICE`
and pressing the Enter key.
- 36** Start the SAM21EM server application by typing
`# servstart SAM21EM`
and pressing the Enter key.

- 37** Set the QCA server application to the same status it was before the upgrade, as determined in [Preparing to upgrade the CS 2000 Management Tools on page 278](#) by using the procedure [Starting and stopping the QoS Collector Application on page 539](#).

If QCA status was	Do
running	Start the QCA
not running	Stop the QCA

Upgrading an HA server pair (maintenance release)

At your workstation

- 1** Establish a connection to the active and inactive servers and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

On the active server

- 2** Verify whether other users are logged on to the system by typing

```
# ssh unit1-priv0 who
# ssh unit0-priv0 who
```

- 3** The presence of other users logged on to the system can have adverse effects on the upgrade process and can cause the upgrade to fail. Therefore, request that all users log out before you proceed.

```
# wall
```

**The system is coming down for maintenance.
Please log off immediately in order to save your files.**

and pressing the Enter key.

Then hit the Ctrl and D keys simultaneously to send the message to all users.

- 4** If the IEMS is present on this server and you have a maintenance release for the IEMS, proceed to [step 5](#), otherwise, proceed to [step 7](#).
- 5** Back up the central security server. Failure to back up the central security server will result in the loss of all the current IEMS user and password information.

For detailed steps, refer to [Backing up the central security server](#).

6

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be transferred to NPM, if not already available on NPM.

Obtain any patches applicable to the IEMS components (IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, PKMGR_SERVER), that were delivered after the delivery of the the IEMS maintenance release.

For detailed steps, refer to one of the following procedures:

- [Transferring patches delivered on CD to the NPM database on page 2297](#)
- [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#)

7

Obtain any patches applicable to the CS2M components (SESM, SAM21EM, QCA), that were delivered after the delivery of the CS2M maintenance release.

For detailed steps, refer to one of the following procedures:

- [Transferring patches delivered on CD to the NPM database on page 2297](#)
- [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#)

On the inactive server

8

Remove the inactive server from the cluster.

For detailed steps, refer to procedure [Removing a server from a cluster on page 438](#).

9

If IEMS is present on this server and you have a maintenance release for the IEMS, proceed to [step 10](#), otherwise, proceed to [step 21](#).

10

If you are upgrading IEMS using ESD, proceed to [step 11](#), or if you are upgrading IEMS using a CD, proceed to [step 12](#).

- 11 Transfer the IEMS ISO image file to the server and mount the ISO image file on the server.
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)
- 12 Upgrade IEMS.
For detailed steps, refer to procedure [Upgrading the IEMS software on page 254](#).
- 13 If you upgraded IEMS using ESD, proceed to [step 14](#), or if you upgraded IEMS using a CD, proceed to [step 16](#).
- 14 Unmount and remove the IEMS ISO image file from the server.
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 15 Proceed to [step 18](#).
- 16 Eject the CD by typing

```
# cd /
```

and pressing the Enter key.

```
# eject cdrom
```

and pressing the Enter key.
Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.
- 17 Remove the CD or DVD from the drive.
- 18

ATTENTION

The SN08 Central Security Server (IEMSCSS and IEMSCSS_DS) patches remain applicable to the SN09U IEMS load and must be applied the SN09U IEMS load.

If you have IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, or PKMGR_SERVER patches for the IEMS release you just upgraded to, proceed to [step 19](#), otherwise, proceed to [step 20](#).

- 19 Apply the IEMS, IEMSCSS, IEMSCSS_DS, COREM, CSMONITOR, PKMGR_SERVER patches.
For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#).
- 20 Restore the central security server backup file.
For detailed steps, refer to [Restoring the central security server](#).
- 21 If you are upgrading CS2M using ESD, proceed to [step 22](#), or if you are upgrading CS2M using a CD, proceed to [step 23](#).
- 22 Transfer the CS2M ISO image file to the active server and mount the ISO image file on the inactive server.
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)
- 23 Upgrade CS2M.
For detailed steps, refer to procedure [Upgrading the CS2M software on page 446](#).
- 24 If you upgraded CS2M using ESD, proceed to [step 25](#), or if you upgraded CS2M using a CD, proceed to [step 27](#).
- 25 Unmount and remove the CS2M ISO image file from the server.
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 26 Proceed to [step 29](#).
- 27 Eject the CD by typing
`cd /`
and pressing the Enter key.
`eject cdrom`
and pressing the Enter key.
Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:
`/etc/init.d/volmgt stop`
`/etc/init.d/volmgt start`
Then, press the eject button located on the front of the DVD drive.
- 28 Remove the CD or DVD from the drive.

- 29** If you have SESM, SAM21EM, and QCA patches for the CS2M release you just upgraded to, proceed to [step 30](#), otherwise, proceed to [step 31](#).
- 30** Apply the SESM, SAM21EM, and QCA patches.
For detailed steps, refer to procedure [Applying patches using the NPM on page 2319](#).
- 31** Return the inactive server to the cluster.
For detailed steps, refer to procedure [Returning a server to a cluster on page 456](#).

On the active server

- 32** Stop the cluster.
For detailed steps, refer to procedure [Stopping a cluster on page 457](#).

On the newly active server with the (I)SN09U maintenance release software

- 33** Set the QCA server application to the same status it was before the upgrade, as determined in [Preparing to upgrade the CS 2000 Management Tools on page 278](#) by using the procedure [Starting and stopping the QoS Collector Application on page 539](#).

If QCA status was	Do
running	Start the QCA
not running	Stop the QCA

- 34** If IEMS is present on the server, execute the amldap user password script below, otherwise, proceed to [step 35](#):
- a** Change directories by typing (there is no space between security/ and current_core)

```
# cd /opt/nortel/applications/security/current_core/bin
```

 and pressing the Enter key.
 - b** Run the update_am_pwd_exp.sh script by typing

```
# ./update_am_pwd_exp.sh
```

 and pressing the Enter key.
 - c** When prompted, confirm you want to continue by typing

```
# y
```


and pressing the Enter key.

35

ATTENTION

At this point, you can easily revert this upgraded server back to the previous release. Continuing with this procedure, clones the image of the upgraded server onto the server running the previous release, and once both servers are upgraded, reverting back to the previous release will require a full system restore.

Clone the image of the upgraded server onto the other server.

For detailed steps, refer to procedure [Cloning the image of one server in a cluster to the other server on page 478](#).

You have completed this procedure.

Completing the CS 2000 Management Tools upgrade

The following procedure provides the steps you need to execute following an upgrade of the SPFS-based server that is hosting the CS 2000 Management Tools software application. When applicable, a reference to the procedure that contains the detailed steps is provided.

Prerequisites

You have completed procedure [Upgrading the CS 2000 Management Tools on page 285](#).

Action

Follow the link associated with the type of server you just upgraded.

- [Completing the upgrade on a simplex server on page 317](#)
- [Completing the upgrade on an HA server pair on page 320](#)

Completing the upgrade on a simplex server

At your workstation

- 1 Establish a connection to the server and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

On the server

- 2 Configure the user inactivity timeout setting, which is set to 10 minutes by default, and requires a user to re-login after periods of 10 minutes of inactivity. This setting can be disabled or changed based on office preferences.

For detailed steps, refer to procedure “Modifying login session timeouts on an SPFS-based server” in *Carrier VoIP ATM/IP Solution-level Security and Administration*, NN10402-600.

- 3 If the NPM is present on this server, proceed to [step 4](#), otherwise, proceed to [step 6](#).
- 4 If you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS), proceed to [step 5](#), otherwise, proceed to [step 6](#).

If the NPM was configured for automatic patch delivery before the upgrade it is still configured.

- 5 Configure NPM for automatic patch file delivery.
For detailed steps, refer to procedure [Configuring NPM for automatic patch file delivery on page 493](#).
- 6 If you are using QCA redundancy in your network, refer to procedure [Installing the QCA software package on a separate server on page 504](#), otherwise proceed to [step 7](#).
- 7 Upgrade the ABS application.
ABS is the Alternate Boot Server for the USP. It resides on the CMT server and updates some of the bootp tab files so that the USP can boot off of the CMT server. The USP has the ability to take an image of its load and place it in a directory on the CMT server so that if needed, it can boot off of the CMT server.
For detailed steps, refer to procedure [Upgrading the ABS software on the CS 2000 Management Tools server on page 519](#).
- 8 Back up the oracle data.
For detailed steps, refer to procedure [Performing a backup of oracle data on an SPFS-based server on page 374](#).
- 9 Back up the file systems.
For detailed steps, refer to procedure [Performing a backup of file systems on an SPFS-based server on page 379](#).
- 10 If the APS is present on the server, proceed to [step 11](#), otherwise, proceed to [step 13](#).
- 11 Back up the APS audio files.
For detailed steps, refer to one of the following procedures:
 - For a Sun Netra t1400, refer to procedure [Performing a backup of APS audio files to tape on page 392](#)
 - For a Sun Netra 240, refer to procedure [Performing a backup of APS audio files to CD or DVD on page 394](#)
- 12 Back up the APS oracle data.
For detailed steps, refer to one of the following procedures:
 - For a Sun Netra t1400, refer to procedure [Performing a backup of APS oracle data to tape on page 396](#)
 - For a Sun Netra 240, refer to procedure [Performing a backup of APS oracle data to CD or DVD on page 398](#)
- 13 If the IEMS is present on this server, proceed to [step 14](#), otherwise, proceed to [step 18](#).

- 14** If, before the upgrade, you determined through your system administrator that your site is using a third-party security application as opposed to the IEMS security application, have your system administrator re-edit the NSCD, PAM and NSSwitch configuration files.

Contact your system administrator.
- 15** Update the CEM documentation if not already updated.

For detailed steps, refer to procedure [Updating the CEM documentation on page 261](#).
- 16** Start the Core Element Manager (CEM).

For detailed steps, refer to procedure [Starting and stopping the Core Element Manager \(CEM\) on page 543](#)
- 17** Configure and start the Client Session Monitor.

For detailed steps, refer to procedure [Configuring the Client Session Monitor on page 534](#).
- 18** Using the IEMS GUI, update the Device version field of the managed objects hosted on the CMT server to reflect the new software version. The hosted managed objects are as follows:

 - under EMS platforms: CS 2000 Management Tools SPFS platform
 - under Element Managers: APS Mgr, GWC Mgr and SAM21 Mgr
 - under EMS Applications: LMM, TMM, OSSGate, QoS Collector, SBRM, and NPM

For detailed steps on how to update the software version in the Device Version field, refer to one of the following procedures:

 - [Editing and viewing object properties using Java Web Start Client](#)
 - [Editing and viewing object properties using Web Client](#)
- 19** If this is a geographically-redundant configuration, upgrade the standby CS 2000 Management Tools server. Refer to procedures “Installing the remote backup server” and “Scheduling automatic backups on the remote server”, in *Carrier Voice over IP, Disaster Recovery Procedures*, NN10450-900.
- 20** Upgrade the next component in the end-to-end upgrade. Refer back to [Component Upgrade order on page 5](#).

Completing the upgrade on an HA server pair

At your workstation

- 1 Establish a connection to the active server and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

On the active server

- 2 Configure the user inactivity timeout setting, which is set to 10 minutes by default, and requires a user to re-login after periods of 10 minutes of inactivity. This setting can be disabled or changed based on office preferences.

For detailed steps, refer to procedure “Modifying login session timeouts on an SPFS-based server” in *Carrier Voice over IP Security and Administration*, NN10402-600.

- 3 If the NPM is present on this server, proceed to [step 4](#), otherwise, proceed to [step 6](#).
- 4 If you want to enable automatic patch file delivery to the NPM through the Patch File Receipt System (PFRS), proceed to [step 5](#), otherwise, proceed to [step 6](#).
If the NPM was configured for automatic patch delivery before the upgrade it is still configured.
- 5 Configure NPM for automatic patch file delivery.
For detailed steps, refer to procedure [Configuring NPM for automatic patch file delivery on page 493](#).
- 6 If you are you using QCA redundancy in your network, refer to procedure [Installing the QCA software package on a separate server on page 504](#), otherwise proceed to [step 7](#).
- 7 Upgrade the ABS application.

ABS is the Alternate Boot Server for the USP. It resides on the CMT server and updates some of the bootp tab files so that the USP can boot off of the CMT server. The USP has the ability to take an image of its load and place it in a directory on the CMT server so that if needed, it can boot off of the CMT server.

For detailed steps, refer to procedure [Upgrading the ABS software on the CS 2000 Management Tools server on page 519](#).

- 8 If the IEMS is present on this server, proceed to [step 9](#), otherwise, proceed to [step 14](#).

- 9 If, before the upgrade, you determined through your system administrator that your site is using a third-party security application as opposed to the IEMS security application, have your system administrator re-edit the NSCD, PAM and NSSwitch configuration files.
Contact your system administrator.
- 10 Update the CEM documentation if not already updated.
For detailed steps, refer to procedure [Updating the CEM documentation on page 261](#).
- 11 Start the Core Element Manager (CEM).
For detailed steps, refer to procedure [Starting and stopping the Core Element Manager \(CEM\) on page 543](#).
- 12 Using the IEMS GUI, update the Device version field of the managed objects hosted on the CMT server to reflect the new software version. The hosted managed objects are as follows:
 - under EMS platforms: CS 2000 Management Tools SPFS platform
 - under Element Managers: APS Mgr, GWC Mgr and SAM21 Mgr
 - under EMS Applications: LMM, TMM, OSSGate, QoS Collector, SBRM, and NPMFor detailed steps on how to update the software version in the Device Version field, refer to one of the following procedures:
 - [Editing and viewing object properties using Java Web Start Client](#)
 - [Editing and viewing object properties using Web Client](#)
- 13 Configure and start the Client Session Monitor.
For detailed steps, refer to procedure [Configuring the Client Session Monitor on page 534](#).
- 14 If this is a geographically-redundant configuration, upgrade the standby CS 2000 Management Tools server. Refer to procedures “Installing the remote backup server” and “Scheduling automatic backups on the remote server”, in *Carrier Voice over IP, Disaster Recovery Procedures*, NN10450-900.
- 15 Clone the image of the upgraded server onto the other server.
For detailed steps, refer to procedure [Cloning the image of one server in a cluster to the other server on page 478](#).

- 16** Back up the oracle data.
For detailed steps, refer to procedure [Performing a backup of oracle data on an SPFS-based server on page 374](#).
- 17** Back up the file systems.
For detailed steps, refer to procedure [Performing a backup of file systems on an SPFS-based server on page 379](#).
- 18** If APS is present on the server, proceed to [step 19](#), otherwise, proceed to [step 21](#).
- 19** Back up the APS audio files.
For detailed steps, refer to one of the following procedures:
 - For a Sun Netra t1400, refer to procedure [Performing a backup of APS audio files to tape on page 392](#)
 - For a Sun Netra 240, refer to procedure [Performing a backup of APS audio files to CD or DVD on page 394](#)
- 20** Back up the APS oracle data.
For detailed steps, refer to one of the following procedures:
 - For a Sun Netra t1400, refer to procedure [Performing a backup of APS oracle data to tape on page 396](#)
 - For a Sun Netra 240, refer to procedure [Performing a backup of APS oracle data to CD or DVD on page 398](#)
- 21** Upgrade the next component in the end-to-end upgrade. Refer back to [Component Upgrade order on page 5](#).

Logging in to an SPFS-based server

Application

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

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

Prerequisites

This procedure requires the following information:

- the IP address or host name of the server

Note: In a two-server configuration, you need the physical IP address of the active or inactive server.

- a valid user id and password
- the root password if you need to perform a task on the server that requires root user privileges

Action

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

- [Logging in using SSH on page 323](#)
- [Logging in using Telnet on page 326](#)
- [Logging in through the console on page 328](#)

Logging in using SSH

At your workstation

- 1 Establish an SSH session.

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

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

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

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

where

user_id

is root or your user id

server

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

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

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

- 3**

ATTENTION

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

Continue the connection by typing

y

and pressing the Enter key.

- 4** Enter the password for root or your user id.

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

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

- 6** Ensure you are on the correct server by typing

ubmstat

and pressing the Enter key.

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

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 8
inactive server and the response is ClusterIndicatorACT	step 8
active server and the response is ClusterIndicatorACT	step 9
inactive server and the response is ClusterIndicatorSTBY	step 9

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

Logging in using Telnet

At your workstation

- 1 Establish a telnet session to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

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

- 2 When prompted, enter your userid.

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

- 3 When prompted, enter your password.

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

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

- 5 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- 6 When prompted, enter the root password.

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

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

- 8 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

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

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

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

Logging in through the console

At the console connected to the server

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

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

- 3 Ensure you are on the correct server by typing
`# ubmstat`
and pressing the Enter key.

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

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

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

Verifying the presence and validity of an HTTPS certificate on an SPFS-based server

Application

Use this procedure to verify whether an HTTPS certificate is installed on the server, and if one is installed, ensuring it has not expired.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

At your workstation

- 2 Access the apache directory by typing

```
# cd /opt/apache
```

and pressing the Enter key.

- 3 Determine whether a certificate file (.crt) and a key file (.key) exist on the server by typing the following commands:

```
# find conf -type f -name *.crt
```

and pressing the Enter key.

```
# find conf -type f -name *.key
```

and pressing the Enter key.

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

If	Do
the response to the commands in the previous step (step 3) displayed a .crt and a .key file, then an HTTPS certificate exists on the server	step 5
otherwise, you need to install a certificate	step 9

- 5 Change directories by typing

```
# cd conf
```

and pressing the Enter key.

- 6 Verify the certificate dates by typing

```
# keytool -printcert -file ssl.crt/server.crt
```

and pressing the Enter key.

Example response

```
Owner: EMAILADDRESS=znc0s0jh.us.nortel.com,
CN=znc0s0jh.us.nortel.com, OU=
jh.us.nortel.com, O=Nortel, L=RTP, ST=NC, C=US
Issuer: EMAILADDRESS=znc0s0jh.us.nortel.com,
CN=znc0s0jh.us.nortel.com, OU=
0jh.us.nortel.com, O=Nortel, L=RTP, ST=NC, C=US
Serial number: c5aa63a60d80bf96
Valid from: Thu Oct 27 02:51:50 EDT 2005 until: Sun Oct
26 01:51:50 EST 2008
Certificate fingerprints:
    MD5:
B1:1D:F6:17:7B:95:3D:7C:61:48:9E:78:6A:D5:22:29
    SHA1:
D8:06:0B:73:9A:46:76:A3:E9:52:65:96:16:95:E6:A5:E6:54:53
:BC
```

- 7 From the response, locate the certificate dates next to Valid from.
- 8 Use the following table to determine your next step.

If	Do
the certificate has reached its expiry date	step 9
otherwise	step 10
- 9 Install or replace the HTTPS certificate.
For detailed steps, refer to procedure [Installing or replacing an HTTPS certificate on an SPFS-based server on page 358](#).
- 10 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to 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 *ATM/IP Configuration Management*, NN10409-500.

CS 2000 data audit

For a CS2K data audit, the system compares the GWC element manager (EM) database (part of the CS 2000 GWC Manager database) with the CS 2000 XA-Core database and flags any mismatches between the two databases. You need to take action in order to correct a data mismatch. The XA-Core is considered to hold the ‘master’ database. The system also audits IP-VPN (NAT) datafill internal to Succession Element and Sub-element Manager (SESM) and its CS2KSS EM equivalent. This audit attempts to automatically correct the datafill on CS2K SS EM when a problem is detected. Whether the audit succeeded or failed to correct the problem is indicated in the problem report.

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

Line audit

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

- DNINV
- LGRPINV
- LNINV
- LNENDPT (if DQOS gateway has been provisioned)
- HUNTMEM (if hunt groups have been provisioned)
- MDNMEM (if MADN groups have been provisioned)

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

Trunk audit

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

- SERVRINV
- TRKMEM
- LTMAP
- TRKSGRP

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

V5.2 audit

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

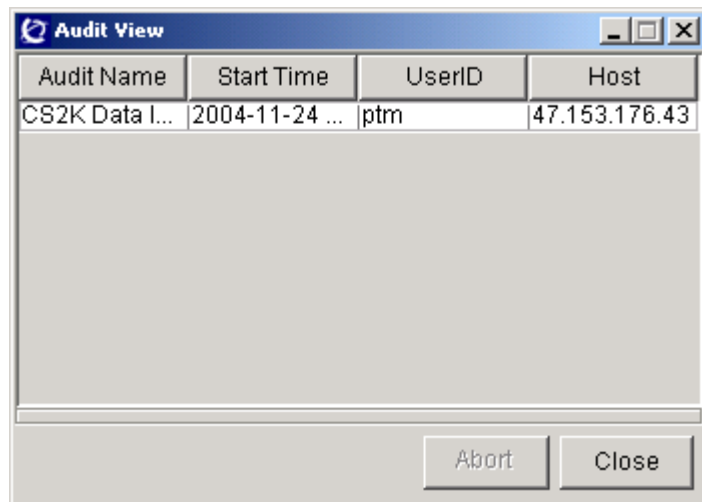
- V5.2 interface data stored in the Network View database
- V5.2 endpoint data stored in the CS 2000 GWC Manager database
- V5.2 interface data stored in the table GPPTRNSL in the CS 2000 XA-Core database

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

Aborting audits

All four types of audits can be aborted when running by selecting the View Current Audits option from the Maintenance menu of the CS 2000 Management Tools GUI.

Select the audit you want from the Audit View window and click Abort in order to end an audit currently in progress.



Prerequisites

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

You must be assigned to user group "mgcadm" to run an audit. If required, refer to procedure "Setting up local user accounts on an SPFS-based server" in *ATM/IP Security and Administration*, NN10402-600.

Action

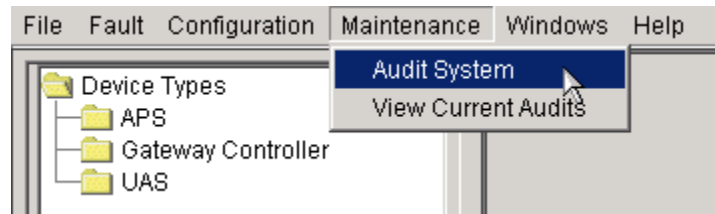
Perform the following steps to complete this procedure.

At your workstation

- 1 Launch the CS2000 Management Tools GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

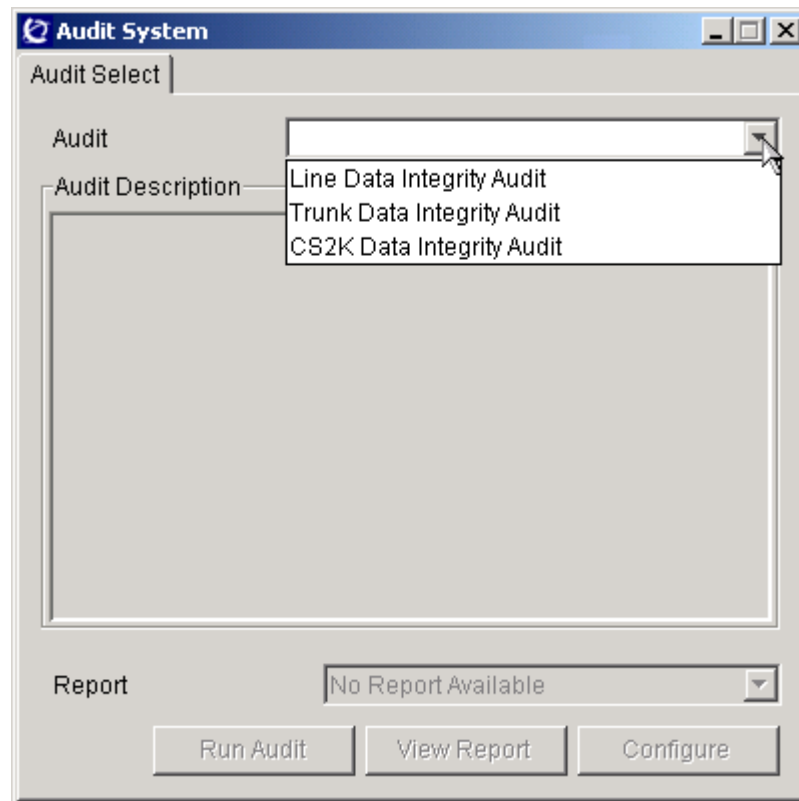
At the CS2000 Management Tools GUI

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



The Audit System window opens.

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



Note: In addition to the audit types shown in the preceding example, the international version of the software also contains the V5.2 audit.

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

If you selected the	Do
CS2K Data Integrity Audit	step 5
Line Data Integrity Audit	step 9
Trunk Data Integrity Audit	step 13
V5.2 Data Integrity Audit	step 13

- 5 Click **Run Audit**.
- 6 Select the type of CS2K audit to be run by clicking one or both of the check boxes.



Note: The CS2KSS EM Data Integrity Audit option is only available when the CS2KSS EM is provisioned with SESM.

Choosing the first option runs an audit that compares the GWC manager with the CS 2000 XA-Core database and flags mismatches. Choosing the second option runs an audit that compares the IP-VPN (NAT) datafill internal to SESM and its CS2KSS EM equivalent. Both options can be selected at the same time as well.

- 7 Click **Run Audit**.

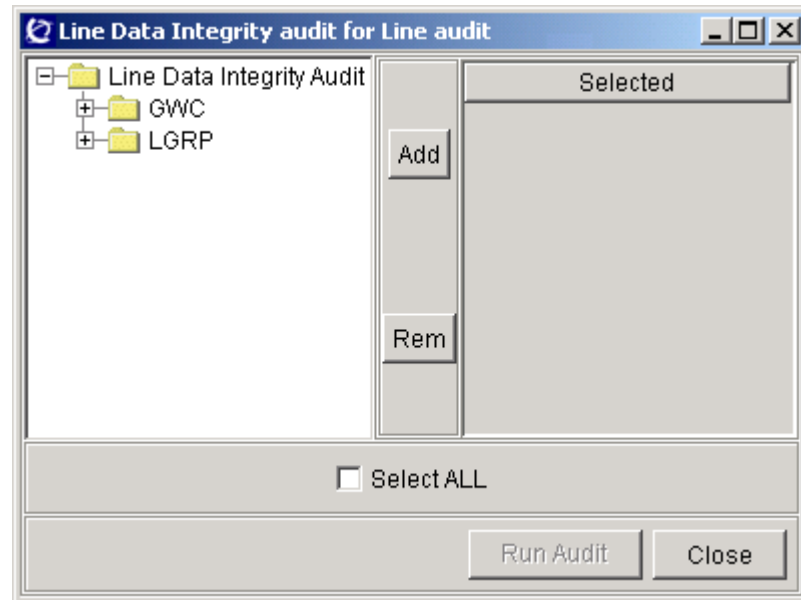
During the audit, an Audit Status window is displayed to indicate the audit is in progress. The Audit Status window indicates when the audit is complete.

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.

- 8 Proceed to step [14](#).
- 9 Click **Run Audit**.

- 10 Select the elements you want audited and click Add, or click the Select ALL checkbox to audit the entire call server.

Note: You cannot select GWCs and LGRPs for the same audit.



The Line Data Integrity Audit list on the left displays all the small and large line GWCs and the associated gateways, as well as the logical line groups of these small line or large line gateways.

- 11 Click **Run Audit**.

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

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.

- 12 Proceed to step [14](#).
- 13 Click **Run Audit**.
- 14 Click **Close** to close the Audit Status window once the audit completes.

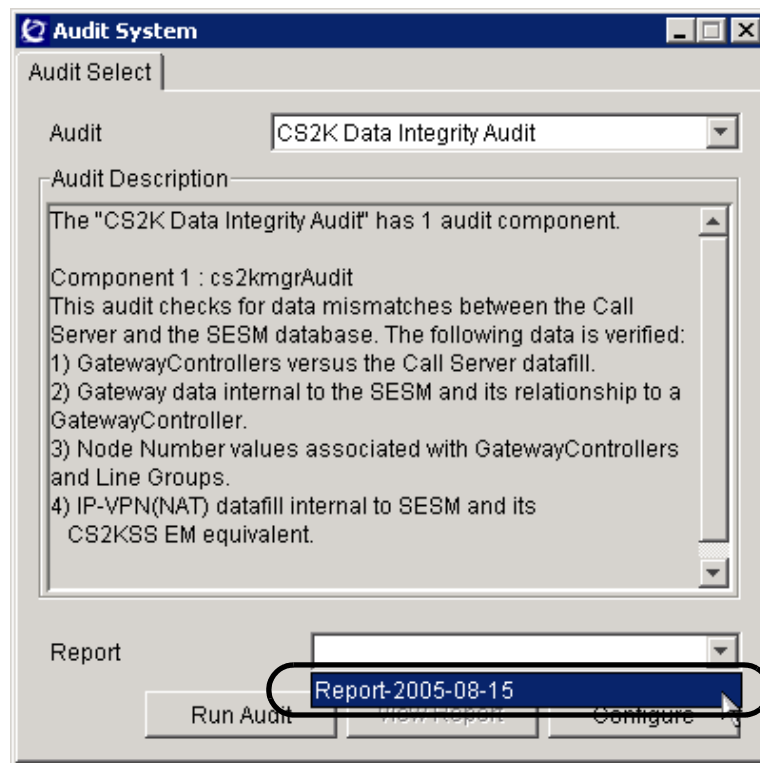
- 15 Use the following table to determine your next step.

If additional audits	Do
need to be run	step 3
do not need to be run	step 16

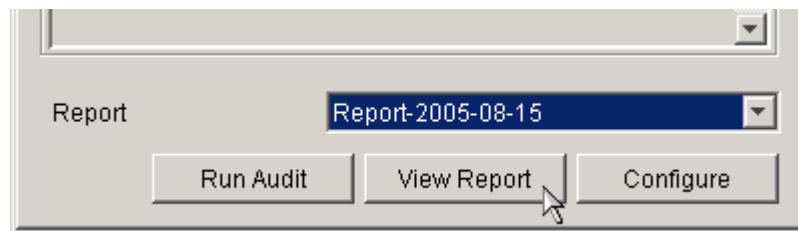
- 16 Use the following table to determine your next step.

If you performed a	Do
CS2K Data Integrity Audit	step 17
Line Data Integrity Audit	step 21
Trunk Data Integrity Audit	step 24
V5.2 Data Integrity Audit	step 27

- 17 Proceed as follows for a CS2K Data Integrity Audit:
- 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.
 - Select **Report** <date> from the pull-down menu in the Report field at the bottom of the dialog box.
The file name has the following format:
Report-<date>
where
<date> is the date in yyyy-mm-dd format, for example, 2005-07-14.



c Click View Report.



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

CS2K Data Integrity Audit Report		
File		Last Audit Date: 2005-08-11 14:24:17
Index	Problem Description	Current Status
17	The LGRP node 'MG9K 00 3' in Call Server is not used in SESM	Problem Exists
18	The LGRP node 'KEYM 06 0' in Call Server is not used in SESM	Problem Exists
19	The LGRP node 'PTGM 00 0' in Call Server is not used in SESM	Problem Exists
20	The LGRP node 'KEYM 00 0' in Call Server is not used in SESM	Problem Exists
21	The LGRP node 'KEYM 01 0' in Call Server is not used in SESM	Problem Exists
22	The LGRP node 'KEYM 02 0' in Call Server is not used in SESM	Problem Exists
23	The LGRP node 'MG9K 00 1' in Call Server is not used in SESM	Problem Exists
24	The LGRP node 'MUXS 00 0' in Call Server is not used in SESM	Problem Exists
25	The LGRP node 'REM1 00 0' in Call Server is not used in SESM	Problem Exists
26	The LGRP node 'PHNX 00 0' in Call Server is not used in SESM	Problem Exists
27	The LGRP node 'PLG 00 0' in Call Server is not used in SESM	Problem Exists
28	The LGRP node 'KEYM 04 0' in Call Server is not used in SESM	Problem Exists
29	Network Zone deneme2 not present on Session Server	Problem Corrected
30	Wrong ID for Network Zone deneme on Session Server	Problem Corrected

Problem Detail:	
Problem Number:	
Problem Description:	
Current Status:	
Possible Actions	
Actions:	
Description	
Take Action	

This example report is the result of the user running both the CS2K Call Server Data Integrity Audit and CS2KSS EM Data Integrity Audit. The problems labelled with the status of

'Problem Corrected' were automatically corrected as part of the CS2KSS EM Data Integrity Audit.

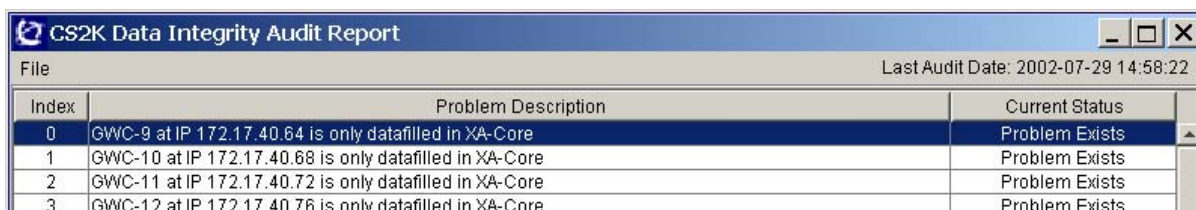
Note 1: The CS 2000 Management Tools server retains the most recent CS 2000 audit report. When a new audit occurs, the server deletes the previous report.

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.

- 18** Review the results of the audit and click on a problem with the status of 'Problem Exists' that needs to be resolved.

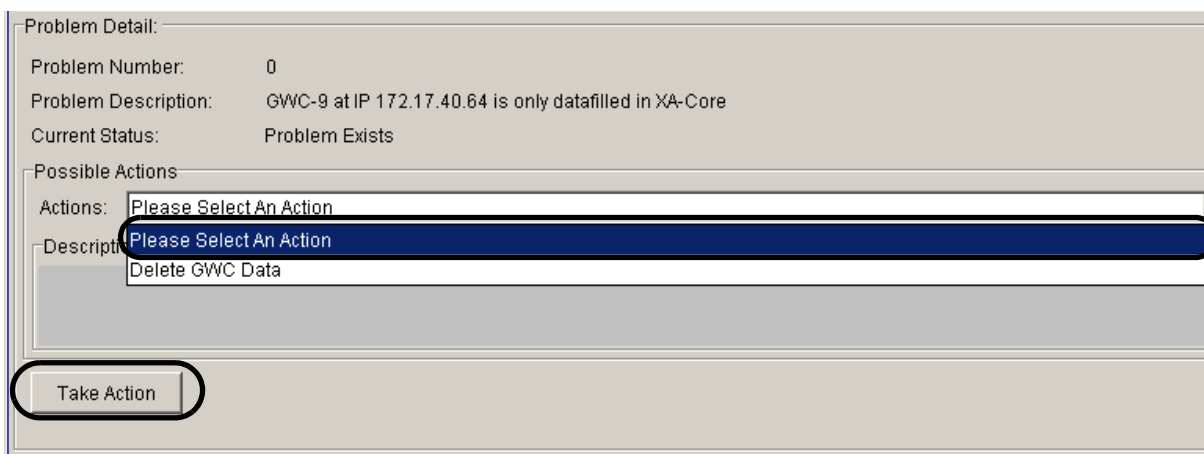
Note: If necessary, resize the entire window to completely view the Problem Description field.



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

- 19** Evaluate actions to resolve a problem and take action.

- Click and hold on the Action pull-down menu near the bottom of the screen to assess any possible actions.
- If appropriate, select an action. Read the description of the action and ensure that you observe any recommended steps or cautions.



Problem Detail:

Problem Number: 0

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

Current Status: Problem Exists

Possible Actions

Actions: Please Select An Action

Describe: Please Select An Action

Delete GWC Data

Take Action

c Click 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 Proceed as follows for a Line Data Integrity Audit:

If you want to view	Do
the line valid-data report	step 22
the line problem-data report	step 23

22 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.

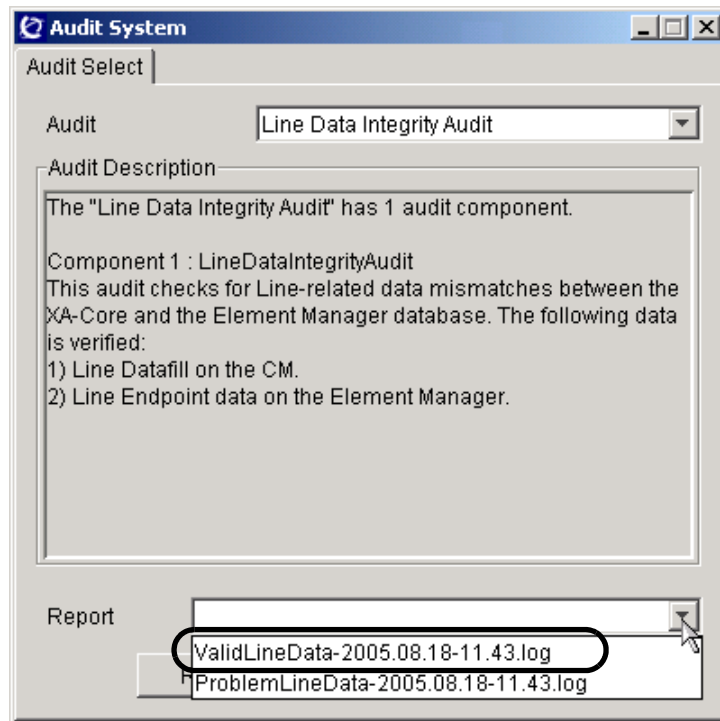
The file name has the following format:

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.



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.

23 View the line problem-data report as follows:

- a** Ensure that you have selected **Line Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.
- b** Select **ProblemLineData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ProblemLineData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

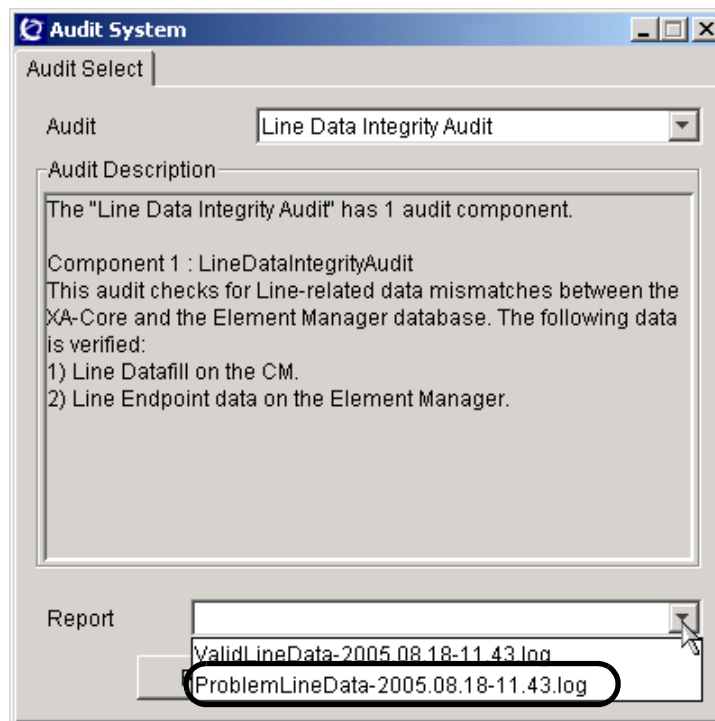
The file name has the following format:

ProblemLineData-<date>-<time>.log

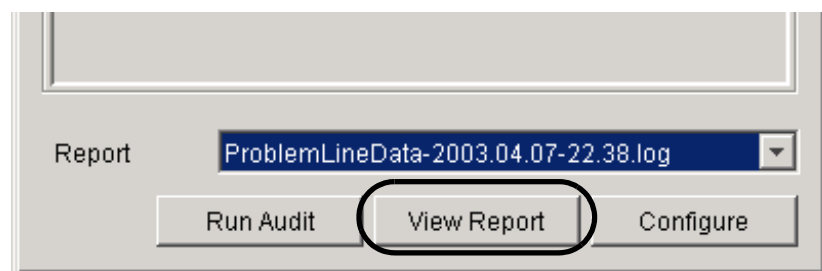
where

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

<time> is the time in hh.mm format, for example 17.30.



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



The system displays the selected report.

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

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

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

Following is an example of a "ProblemLineData" report:

ProblemLineData-2005.02.17-14.52.log

Page: 1/1 Go to

```

EndPoint aaln/48 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/5 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/6 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/7 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/8 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/9 on Gateway mgikv2007.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/2 on Gateway mindytest.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/3 on Gateway mindytest.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/1 on Gateway natl.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/2 on Gateway natl.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/3 on Gateway natl.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/4 on Gateway natl.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/1 on Gateway natla.nortel.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/10 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/11 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/3 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/4 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/5 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/6 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/7 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/8 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/9 on Gateway test.gdnt.com on GWC GWC-100 has no associated LEN on CM
EndPoint aaln/1 on Gateway ambitlp4217nat.nortel.com on GWC GWC-116 has no associated LEN on CM

Invalid Data (For Event Messaing Supported Line Data Integrity)
EndPoint aaln/1 on Gateway isp33199.nortel.com on GWC GWC-100 has no event messaging associated LEN on CM
EndPoint aaln/2 on Gateway isp33199.nortel.com on GWC GWC-100 has no event messaging associated LEN on CM
LEN LG 00 0 08 56 for EndPoint aaln/1 on Gateway moto2pl.nortel.com has no associated endpoint on GWCEM
LEN LG 00 0 08 57 for EndPoint aaln/2 on Gateway moto2pl.nortel.com has no associated endpoint on GWCEM
LEN LG 00 0 10 17 for EndPoint aaln/1 on Gateway hobdqos.gdnt.com has no associated endpoint on GWCEM
LEN LG 00 1 03 50 for EndPoint aaln/1 on Gateway HOBDQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 51 for EndPoint aaln/2 on Gateway HOBDQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 52 for EndPoint aaln/3 on Gateway HOBDQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 53 for EndPoint aaln/4 on Gateway HOBDQOS1 has no associated endpoint on GWCEM
LEN LG 00 1 03 64 for EndPoint aaln/1 on Gateway HOBDQOS2 has no associated endpoint on GWCEM
LEN LG 00 1 03 65 for EndPoint aaln/2 on Gateway HOBDQOS2 has no associated endpoint on GWCEM
LEN LG 00 1 03 66 for EndPoint aaln/3 on Gateway HOBDQOS2 has no associated endpoint on GWCEM
LEN LG 00 1 03 67 for EndPoint aaln/4 on Gateway HOBDQOS2 has no associated endpoint on GWCEM
LEN LG 00 9 00 67 for EndPoint aaln/1 on Gateway lab3ncsgw2.nortel.com has no associated endpoint on GWCEM
LEN LG 00 9 00 68 for EndPoint aaln/2 on Gateway lab3ncsgw2.nortel.com has no associated endpoint on GWCEM

```

Prev Next Save as Exit

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

Note 2: The system places problem data audit reports in the following directory on the CS 2000 Management Tools server:

/opt/nortel/ptm/current/www/Audit/LineDataIntegrityAudit/.

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

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

24 Proceed as follows for a Trunk Data Integrity Audit:

If you want to view	Do
the trunk valid-data report	step 25
the trunk problem-data report	step 26

25 View the trunk valid-data report as follows:

- a Ensure that you have selected **Trunk Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit System dialog box.
- b Select **ValidTrunkData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ValidTrunkData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

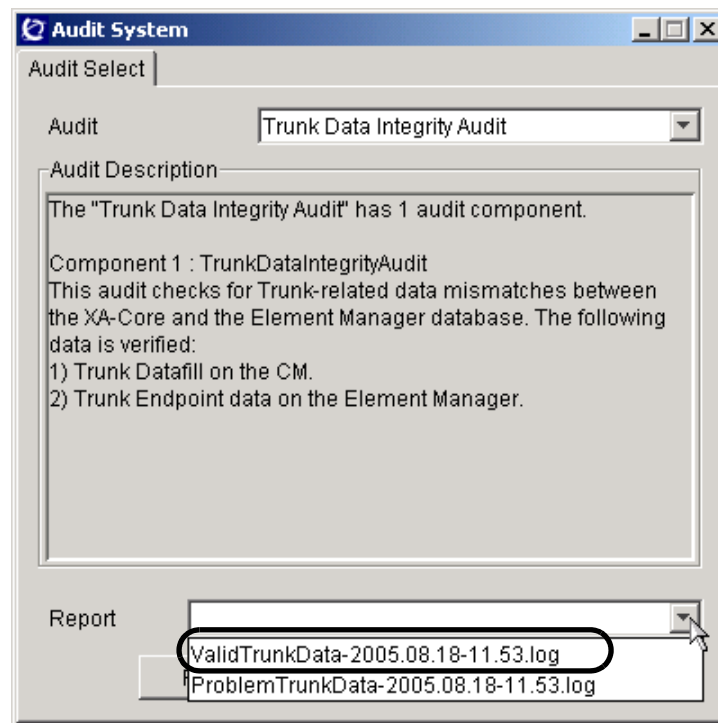
The file name has the following format:

ValidTrunkData-<date>-<time>.log

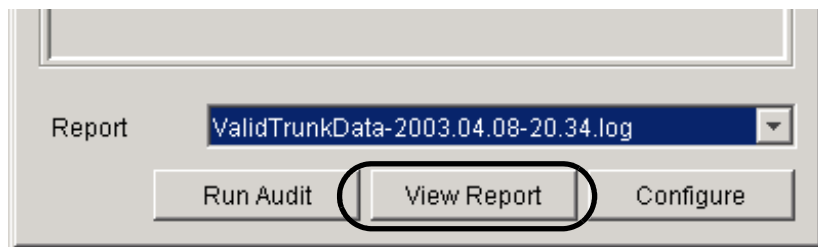
where

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

<time> is the time in hh.mm format, for example 17.30.



- c** Click **View Report**.



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

ValidTrunkData-2003.09.23-11.32.log

Page: 1/1

Go to page: 1

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

Prev Next Save as Exit

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

Note 2: The system places trunk audit reports in the following directory on the CS 2000 Management Tools server:

/opt/nortel/ptm/current/www/Audit/TrunkDataIntegrityAudit/.

- d If you want to retain one of these reports for a longer time, or if you want to print a report, click **Save as** at the bottom of the screen. Then, save the report under a file name of your choice.
- e To print a report you have saved, open the file using a text editor and print the file.
- f After viewing the valid-data report, click **Exit** at the bottom of the screen.

- 26 View the trunk problem-data report as follows:
- Ensure that you have selected **Trunk Data Integrity Audit** from the Audit field pull-down menu at the top of the Audit system dialog box.
 - Select **ProblemTrunkData** from the pull-down menu in the Report field at the bottom of the dialog box. If there is more than one ProblemTrunkData report, assess the date and time information in the report names to guide you in selecting the report you want to view.

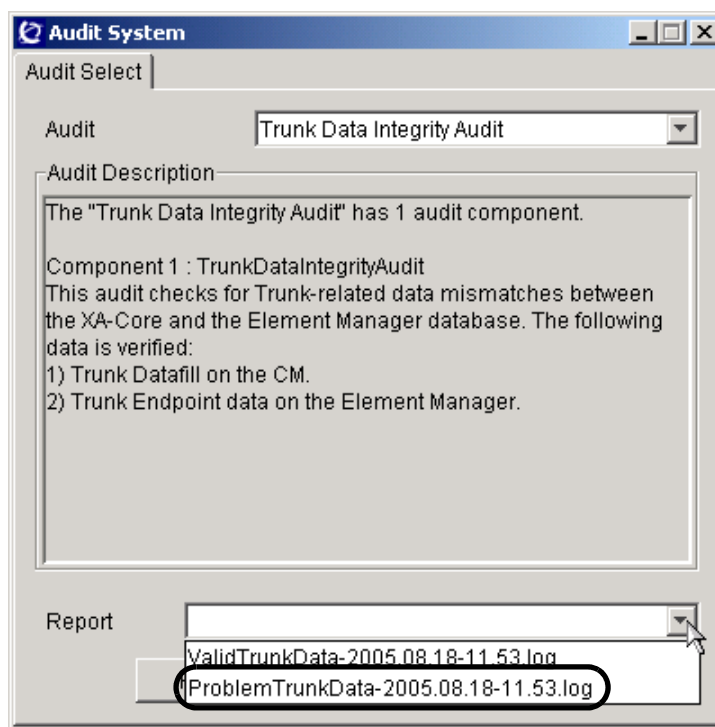
The file name has the following format:

ProblemTrunkData-<date>-<time>.log

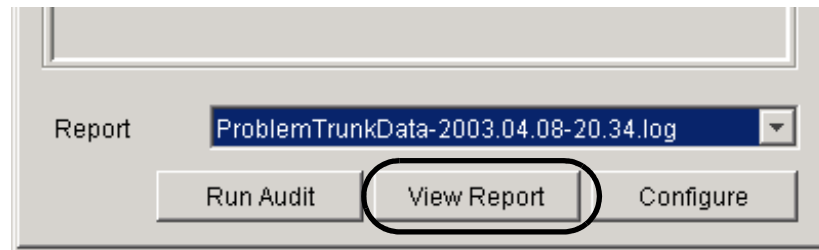
where

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

<time> is the time in hh.mm format, for example 17.30.



- Click the **View Report** button.



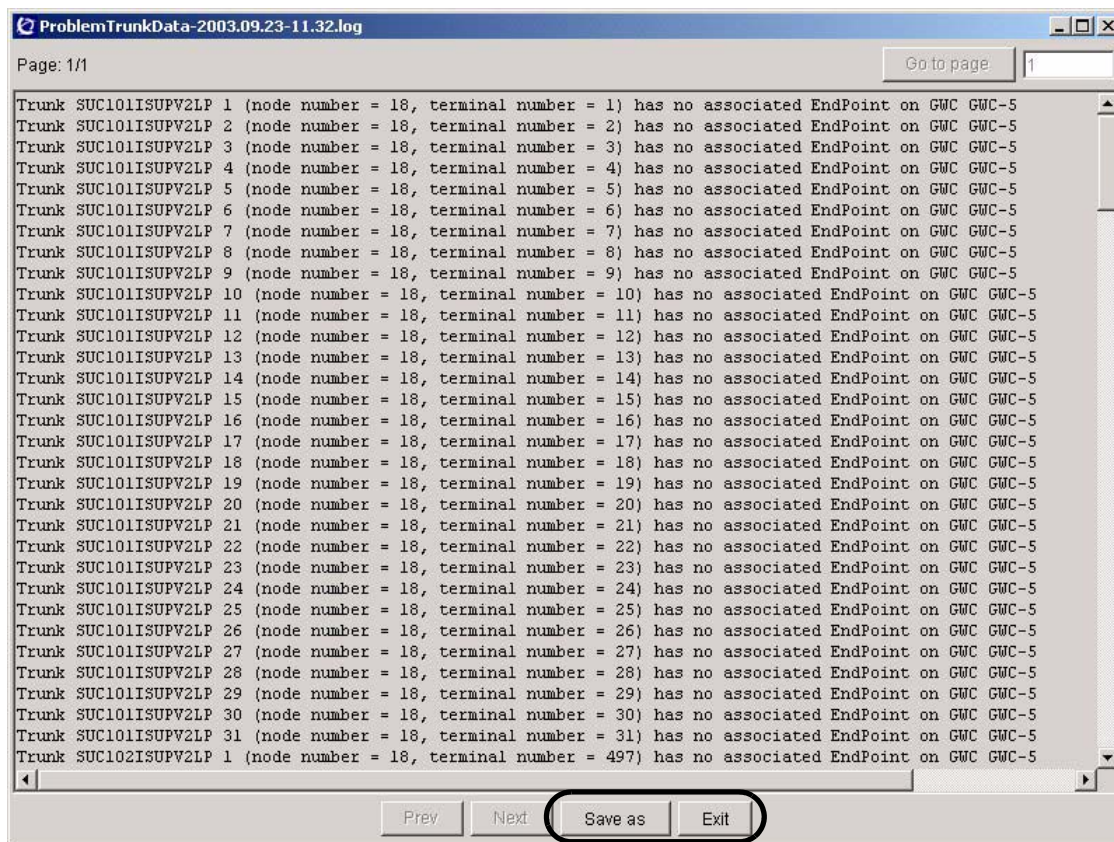
The system displays the selected report.

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

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

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

Here is an example of a “ProblemTrunkData” report:



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

Note 2: The system places trunk audit reports in the following directory on the CS 2000 Management Tools server:

/opt/nortel/ptm/current/www/Audit/TrunkDataIntegrityAudit/.

- d If you want to retain one of these reports for a longer time, or print a report, click **Save as** at the bottom of the screen. Then, save the report under a file name of your choice.
- e To print a report you have saved, open the file using a text editor and print the file.

c Click View Report.



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

V5.2 Data Integrity Audit Report		
File		Last Audit Date: 2003-04-11 16:50:33
Index	Problem Description	Current Status
0	A V5.2 Link with Interface ID 23456 and Link ID 1 is datafilled in GPPTNSL table but there is no matching entry in GWC-EM	Problem Exists
1	A V5.2 Link with Interface ID 23456 and Link ID 2 is datafilled in GPPTNSL table but there is no matching entry in GWC-EM	Problem Exists
Problem Detail: Problem Number: Problem Description: Current Status: Possible Actions Actions: Description Take Action		

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.

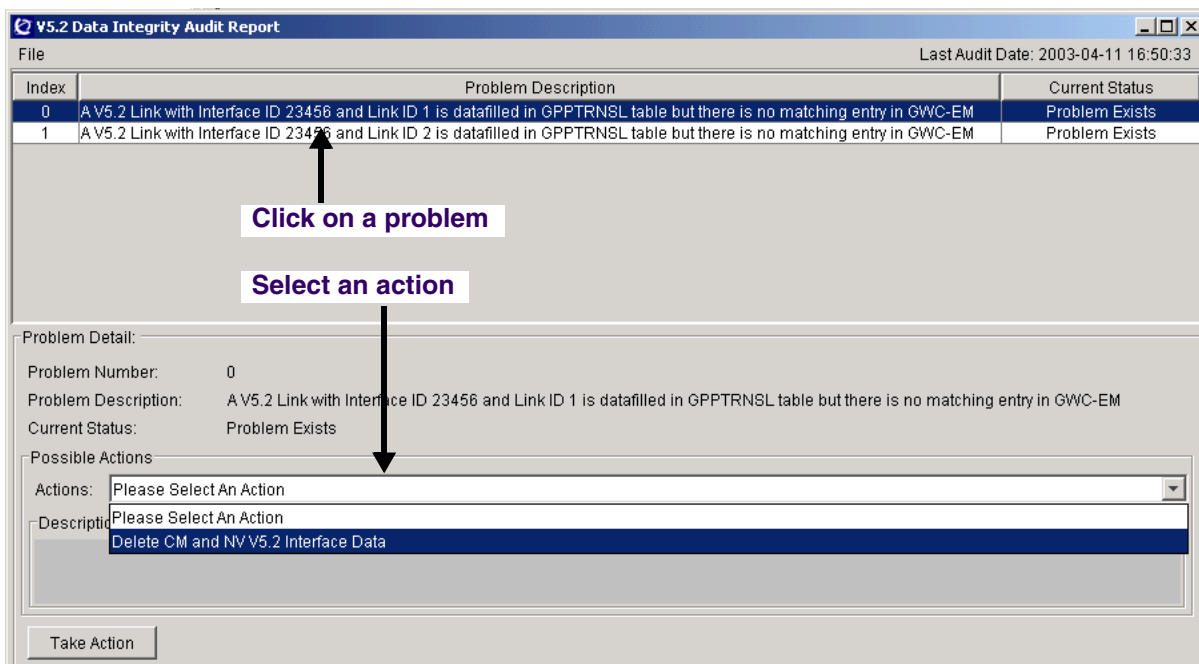
Note 3: The CS 2000 GWC Manager does not provide an option to save a V5.2 audit report to local disk.

28 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.

29 Evaluate actions to resolve a problem and take action.

- a Click and hold on the Action pull-down menu near the bottom of the screen to assess any possible actions.
- b If appropriate, select an action. Read the description of the action and ensure that you observe any recommended steps or cautions.



c Click Take Action.

Possible Actions

Actions: Delete CM and NV V5.2 Interface Data

Description

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

Take Action

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

- 30** Return to [step 28](#) to review another problem.
- 31** You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Installing or replacing an HTTPS certificate on an SPFS-based server

Application

Use this procedure to install or replace an HTTPS certificate on a Server Platform Foundation Software (SPFS)-based server. An HTTPS certificate enables secure transmission of communications, and is required from the (I)SN07 release onward.

The steps to create a self-signed certificate are included in this procedure if you choose to use a self-signed certificate (see [Types of certificates](#)).

Types of certificates

You can use any one of the following three types of security certificates:

- a certificate granted from a well known certificate authority (CA): Used when the server is used in a public way, such as for e-commerce web sites.
- a company-generated certificate: Used when the server is used internally, and the operating company has its own internal CA.
- a self-signed certificate created locally on the server: Used when the server is used in a more restricted manner.

Note: When a server with a self-signed certificate is accessed, the browser presents the certificate and asks whether the certificate can be trusted. If the user answers “yes”, the server can be accessed. If the user answers “no”, nothing further will be received from the server.

The certificates differ in the level of trust that needs to be assigned to a server.

Prerequisites

This procedure has the following prerequisites:

- The domain name service (DNS) must be enabled on the server to allow the security certificate to work, and must be enabled prior to the installation of the certificate. Refer to procedure “Configuring Domain Name Service” in *ATM/IP Configuration Management*, NN10409-500.
- If purchasing a certificate from a third-party certificate authority (CA), such as VeriSign, obtain a PEM-encoded X.509 certificate, but without a passcode.

Note: The common name portion of the certificate must match the fully qualified domain name (FQDN) of the server. Nortel recommends the installation of a unique certificate for each host. A separate file contains the key, and must not have an associated password.

- Make sure all GUI screens are closed before you install the certificate.
- The RSA key for the HTTPS certificate must not have a password.
- The certificate must be created with the fully qualified domain name (FQDN) of the server on which the certificate will be installed.
- Sub-directories “ssl.crt” and “ssl.key” must already exist in the “/opt/apache/conf” directory.

Action

Use one of the methods below to install the certificate according to your office configuration:

- [Simplex configuration \(one server\) on page 359](#)
- [High-availability configuration \(two servers\) on page 364](#)

Simplex configuration (one server)

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

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

If	Do
you are using a self-signed certificate	step 3
otherwise	step 4

- 3 Create the self-signed certificate as follows:

- a Access the “conf” directory by typing

```
# cd /opt/apache/conf
```

and pressing the Enter key.

- b Generate the key file (server.key) by typing

```
# /opt/openssl/bin/openssl genrsa -rand  
/var/log/sspfslog 1024 > server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -rand and /var/log/sspfslog entries.

- c Generate the certificate file (server.crt) by typing

```
# /opt/openssl/bin/openssl req -new -key  
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -key and server.key entries.

Example response:

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank.

For some fields there will be a default value. If you enter '.', the field will be left blank.

- d** When prompted for the Country Name, enter a two-letter code for the country where the server is located.
 - e** When prompted for the State or Province Name, enter the full name of the State or Province where the server is located.
 - f** When prompted for the Locality Name, enter the city where the server is located.
 - g** When prompted for the Organization Name, enter the name of the company that owns the server.
 - h** When prompted for the Organizational Unit Name, enter the name of the department that owns the server.
 - i** When prompted for the Common Name, enter the fully qualified domain name (FQDN) of the server.
 - j** When prompted for the Email Address, enter the email address of the organization that owns the server.
- 4** Place the certificate file (server.crt) you obtained in “/opt/apache/conf/ssl.crt”.
Note: If directory “ssl.crt” does not exist, you need to create it.
- 5** Place the key file (server.key) you obtained in “/opt/apache/conf/ssl.key”.
Note: If directory “ssl.key” does not exist, you need to create it.
- 6** Change the ownership and group for the certificate file by typing
chown root:other /opt/apache/conf/ssl.crt/server.crt
and pressing the Enter key.
Note: Enter the command on one line with a space between “other” and the directory path.
- 7** Change the ownership and group for the key file by typing
chown root:other /opt/apache/conf/ssl.key/server.key
and pressing the Enter key.
Note: Enter the command on one line with a space between “other” and the directory path.
- 8** Set the permissions for the certificate file by typing
chmod 600 /opt/apache/conf/ssl.crt/server.crt
and pressing the Enter key.

- 9 Set the permissions for the key file by typing
chmod 600 /opt/apache/conf/ssl.key/server.key
and pressing the Enter key.
- 10 Restart the WEBSERVER as follows:
- a Stop the WEBSERVER by typing
servstop WEBSERVER
and pressing the Enter key.
 - b Start the WEBSERVER by typing
servstart WEBSERVER
and pressing the Enter key.
- 11 Restart the WEBSERVICES as follows:
- a Stop the WEBSERVICES by typing
servstop WEBSERVICES
and pressing the Enter key.
 - b Start the WEBSERVICES by typing
servstart WEBSERVICES
and pressing the Enter key.
- 12 Use the following table to determine your next step.
- | If | Do |
|--------------------------------|-------------------------|
| the server is hosting the IEMS | step 13 |
| otherwise | step 22 |
- 13 Use the following table to determine your next step.
- | If | Do |
|------------------------------------|-------------------------|
| you replaced an HTTPS certificate | step 14 |
| you installed an HTTPS certificate | step 22 |
- 14 Stop the IEMS server application by typing
servstop IEMS
and pressing the Enter key.

- 15 Disable the SSL utility by typing

```
# /opt/nortel/iems/current/bin/SSLUtil.sh Disable
```

and pressing the Enter key.
- 16 Enable the SSL utility by typing

```
# /opt/nortel/iems/current/bin/SSLUtil.sh Enable
```

and pressing the Enter key.
- 17 Start the IEMS server application by typing

```
# servstart IEMS
```

and pressing the Enter key.
- 18 Reconfigure the SunOne IS client environment on the system to use SSL by typing

```
#/opt/nortel/applications/security/  
current_slisext/swmgmt/bin/configure_slisext.s  
h -ssl
```

and pressing the Enter key.
Note: The above command is entered on one line.
- 19 Restart the Web Server as follows:
 - a Stop the Web Server by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.
 - b Start the Web Server by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.
- 20 Restart the Web Services as follows:
 - a Stop Web services by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.
 - b Start Web Services by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.

- 21 Restart the Radius server as follows:
 - a Stop the Radius server by typing

```
# servstop RADSVR
```

and pressing the Enter key.
 - b Start the Radius server by typing

```
# servstart RADSVR
```

and pressing the Enter key.
- 22 If the CS 2000 Management Tools software is installed prior to installing the HTTPS certificate, you need to reconfigure SESM. If required, refer to procedure “Configuring the SESM server application” in *ATM/IP Configuration Management*, NN10409-500.
- 23 If you installed an HTTPS certificate on an existing SPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure “Clearing the JWS cache on a client workstation” in *ATM/IP Configuration Management*, NN10409-500.
- 24 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

High-availability configuration (two servers)

At your workstation

- 1 Establish a connection to the active server through telnet or SSH, log in using the root user ID and password, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Use the following table to determine your next step.

If	Do
you are using a self-signed certificate	step 3
otherwise	step 6

3 Create the self-signed certificate as follows:

a Access the “conf” directory by typing

```
# cd /opt/apache/conf
```

and pressing the Enter key.

b Generate the key file (server.key) by typing

```
# /opt/openssl/bin/openssl genrsa -rand  
/var/log/sspfsllog 1024 > server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -rand and /var/log/sspfsllog entries.

c Generate the certificate file (server.crt) by typing

```
# /opt/openssl/bin/openssl req -new -key  
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -key and server.key entries.

Example response:

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank.

For some fields there will be a default value. If you enter '.', the field will be left blank.

d When prompted for the Country Name, enter a two letter code for the country where the server is located.

e When prompted for the State or Province Name, enter the full name of the State or Province where the server is located.

f When prompted for the Locality Name, enter the city where the server is located.

g When prompted for the Organization Name, enter the name of the company that owns the server.

h When prompted for the Organizational Unit Name, enter the name of the department that owns the server.

- i When prompted for the Common Name, enter the fully qualified domain name (FQDN) of the server.
 - j When prompted for the Email Address, enter the email address of the organization that owns the server.
- 4 Determine if the “ssl.crt” directory exists:

```
ls /opt/apache/conf/ssl.crt
```

If the ssl.crt directory	Do
exists	step 6
does not exist	step 5
- 5 Create the “ssl.crt” directory:

```
mkdir /opt/apache/conf/ssl.crt
```
- 6 Place the certificate file (server.crt) you obtained in “/opt/apache/conf/ssl.crt”.

```
cp server.crt /opt/apache/conf/ssl.crt
```
- 7 Determine if the “ssl.key” directory exists:

```
ls /opt/apache/conf/ssl.key
```

If the ssl.key directory	Do
exists	step 9
does not exist	step 8
- 8 Create the “ssl.key” directory:

```
mkdir /opt/apache/conf/ssl.key
```
- 9 Place the key file (server.key) in “/opt/apache/conf/ssl.key”.

```
cp server.key /opt/apache/conf/ssl.key
```
- 10 Change the ownership and group for the certificate file by typing

```
# chown root:other /opt/apache/conf/ssl.crt/server.crt
```

 and pressing the Enter key.

Note: Enter the command on one line with a space between “other” and the directory path.
- 11 Change the ownership and group for the key file by typing

```
# chown root:other /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between “other” and the directory path.

- 12 Set the permissions for the certificate file by typing
 # **chmod 600 /opt/apache/conf/ssl.crt/server.crt**
 and pressing the Enter key.
- 13 Set the permissions for the key file by typing
 # **chmod 600 /opt/apache/conf/ssl.key/server.key**
 and pressing the Enter key.
- 14 Restart the WEBSERVER as follows:
 - a Stop the WEBSERVER by typing
 # **servstop WEBSERVER**
 and pressing the Enter key.
 - b Start the WEBSERVER by typing
 # **servstart WEBSERVER**
 and pressing the Enter key.
- 15 Restart the WEBSERVICES as follows:
 - a Stop the WEBSERVICES by typing
 # **servstop WEBSERVICES**
 and pressing the Enter key.
 - b Start the WEBSERVICES by typing
 # **servstart WEBSERVICES**
 and pressing the Enter key.
- 16 Use the following table to determine your next step.

If	Do
the server is hosting the IEMS	step 17
otherwise	step 26

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

If	Do
you replaced an HTTPS certificate	step 18

	If	Do
	you installed an HTTPS certificate	step 26
18	Stop the IEMS server application by typing # servstop IEMS and pressing the Enter key.	
19	Disable the SSL utility by typing # /opt/nortel/iems/current/bin/SSLUtil.sh Disable and pressing the Enter key.	
20	Enable the SSL utility by typing # /opt/nortel/iems/current/bin/SSLUtil.sh Enable and pressing the Enter key.	
21	Start the IEMS server application by typing # servstart IEMS and pressing the Enter key.	
22	Reconfigure the SunOne IS client environment on the system to use SSL by typing # /opt/nortel/applications/security/current_slisext/swmgmt/bin/configure_slisext.sh -ssl and pressing the Enter key. Note: The above command is entered on one line.	
23	Restart the Web Server as follows: a Stop the Web Server by typing # servstop WEBSERVER and pressing the Enter key. b Start the Web Server by typing # servstart WEBSERVER and pressing the Enter key.	
24	Restart the Web Services as follows: a Stop Web services by typing # servstop WEBSERVICES and pressing the Enter key.	

- b** Start Web Services by typing
servstart WEBSERVICES
and pressing the Enter key.
- 25** Restart the Radius server as follows:
 - a** Stop the Radius server by typing
servstop RADSVR
and pressing the Enter key.
 - b** Start the Radius server by typing
servstart RADSVR
and pressing the Enter key.
- 26** If the CS 2000 Management Tools software is installed prior to installing the HTTPS certificate, you need to reconfigure SESM. If required, refer to procedure “Configuring the SESM server application” in *ATM/IP Configuration Management*, NN10409-500.
- 27** Clone the image of the node with the HTTPS certificate onto the other node using procedure [Cloning the image of one server in a cluster to the other server on page 478](#).
- 28** If you installed an HTTPS certificate on an existing SPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure “Clearing the JWS cache on a client workstation” in *ATM/IP Configuration Management*, NN10409-500.
- 29** You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Configuring the security server SunOne component to use a new HTTPS certificate

Application

Use this procedure to make the SunOne component use the new server certificate to run in secure mode on the central security server and central security clients.

Note: The activation of SunOne SSL mode is now automatic (part of install/upgrade).

Prerequisites

An HTTPS certificate must already be installed on the Integrated Element Management System (IEMS) server. If required, refer to procedure [Installing or replacing an HTTPS certificate on an SPFS-based server on page 358](#) to install the Apache server's certificate.

Action

Use one of the procedures below according to your office configuration:

- [Simplex configuration \(one server\) on page 370](#)
- [High-availability configuration \(two servers\) on page 372](#)

Simplex configuration (one server)

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the IEMS server on which you want to configure the security SunOne component
- 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 Reconfigure the SunOne IS client environment on the system to use SSL by typing

```
#/opt/nortel/applications/security/  
current_slisext/swmgmt/bin/configure_slisext.s  
h -ssl
```

and pressing the Enter key.

Note: The above command is entered on one line.
- 6 Restart the Web Server as follows:
 - a Stop the Web Server by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.
 - b Start the Web Server by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.
- 7 Restart the Web Services as follows:
 - a Stop Web services by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.
 - b Start Web Services by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.
- 8 Restart the Radius server as follows:
 - a Stop the Radius server by typing

```
# servstop RADSVR
```

and pressing the Enter key.
 - b Start the Radius server by typing

```
# servstart RADSVR
```

and pressing the Enter key.
- 9 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

High-availability configuration (two servers)

At your workstation

- 1 Log in to the active server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the active IEMS server on which you want to configure the security SunOne component
- 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 Reconfigure the SunOne IS client environment on the system to use SSL by typing

```
#/opt/nortel/applications/security/  
current_slisext/swmgmt/bin/configure_slisext.s  
h -ssl
```

and pressing the Enter key.
Note: The above command is entered on one line.
- 6 Initiate a failover by typing

```
# swact /Y
```

and pressing the Enter key.
- 7 Reconfigure the SunOne IS client environment on the system to use SSL on the newly active server by typing

```
#/opt/nortel/applications/security/  
current_slisext/swmgmt/bin/configure_slisext.s  
h -ssl
```

and pressing the Enter key.
Note: The above command is entered on one line.

- 8 Restart the Web Server on the newly active server as follows:
 - a Stop the Web Server by typing
servstop WEBSERVER
and pressing the Enter key.
 - b Start the Web Server by typing
servstart WEBSERVER
and pressing the Enter key.
- 9 Restart Web Services on the newly active server as follows:
 - a Stop Web services by typing
servstop WEBSERVICES
and pressing the Enter key.
 - b Start Web Services by typing
servstart WEBSERVICES
and pressing the Enter key.

You have completed this procedure.
- 10 Restart the Radius server as follows:
 - a Stop the Radius server by typing
servstop RADSVR
and pressing the Enter key.
 - b Start the Radius server by typing
servstart RADSVR
and pressing the Enter key.
- 11 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Performing a backup of oracle data on an SPFS-based server

Application

Use this procedure to perform a backup of oracle data on a Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240).

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager

Note: An oracle data backup is not required when the SPFS-based server is hosting the MG 9000 Manager.

- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

Note: An oracle data backup is not required when the SPFS-based server is hosting the CBM.

Refer to the procedure “Configuring dark office backups on an SPFS-based server” in *ATM/IP Solution-level Configuration Management*, NN10409-500.

ATTENTION

It is recommended that provisioning activities be put on hold during the time of the data backup.

Prerequisites

This procedure has the following prerequisites:

- For a Sun Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data.
- For a Sun Netra 240, you need one or more blank CD-R, DVD-R, CD-RW or DVD-RW to store the data. Backups have been successfully tested on a Maxwell 4x DVD-RW and Memorex 4 x DVD-RW.

Note: The backup utility limits the storage to 4 GB on a DVD-R and DVD-RW.

If you are using a new CD-RW or DVD-RW, or want to reuse a CD-RW or DVD-RW by erasing the contents, perform procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

ATTENTION

The database must be in sync with the Communication Server 2000 and the MG 9000 Manager (if present). Therefore, ensure you have the appropriate images before you proceed. Performing a restore from the Oracle database alone can cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

Action

At the server

- 1 Insert the blank tape, CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the active server.

At your workstation

- 2 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 3 If the server is hosting the IEMS, and you want to purge the event and performance data, do [step 4](#), otherwise proceed to [step 10](#).

Note: It is highly recommended to purge the IEMS event and performance data prior to executing the data backup. This reduces the size of the oracle space used by the IEMS, and therefore, reduces the backup time, and possibility of a backup failure.

4

ATTENTION

This step stops the IEMS server application. Ensure it is acceptable at this time to stop the IEMS server application.

Stop the IEMS server by typing

```
# servstop IEMS
```

and pressing the Enter key.

- 5 Run the script to purge the data by typing

```
# /opt/nortel/iems/current/bin/purgeTempData.sh
```

and pressing the Enter key.

Example response

```
This will purge all Events, Alarms and
Performance data in the IEMS Database. Do you
want to continue ?[yes | No] :
```

- 6 When prompted, indicate you want to continue by typing

```
yes
```

- 7 Start the IEMS server by typing

```
# servstart IEMS
```

and pressing the Enter key.

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

If you are using	Do
a tape for backup	step 9
a CD or DVD for backup	step 10

- 9 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

- 10** Back up the data by typing
/opt/nortel/sspfs/bks/bkdata
and pressing the Enter key.

Example response:

Backup behavior is set to 1 ...

*** Note: 8X or higher DVD-RW media may result
in a lower success rate. ***

*** DVD will be ejected after the backup is
complete ***

Do you wish to continue the backup (yes or no)?

In response to the prompt, enter either yes or no.

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

If you are using	Do
a tape for backup	step 12
a CD or DVD for backup	step 14

- 12** List the content of the tape by typing

tar tvf /dev/rmt/0

and pressing the Enter key.

Example response:

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:16 2005  
backup/oracle.dmp.gz  
-rw-rw-rw- 0/1 1007616 Mar 2 10:16 2005  
opt/critdata.cpio
```

- 13** Remove the tape from the drive, label it, write-protect it, and
store it in a safe place.

Proceed to [step 19](#).

- 14** The CD or DVD was ejected after backup. Reinsert the backup
CD or DVD into the drive.

- 15 List the content of the CD or DVD by typing

```
# tar tvf /cdrom/*bkdata*/*.tar
```

and pressing the Enter key.

Example response:

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:17 2005
backup/oracle.dmp.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:17 2005
opt/critdata.cpio
```

When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.

- 16 Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- 17 Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

If the DVD drive tray does not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands in the order listed:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then press the eject button located on the front of the DVD drive.

- 18 Remove the CD or DVD from the drive, label it, and store it in a safe place.
- 19 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Note: To restore the data from this backup tape, CD or DVD, refer to procedure “Restoring the oracle data on an SPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.

Performing a backup of file systems on an SPFS-based server

Application

Use this procedure to perform a backup of the file systems on a Server Platform Foundation Software (SPFS)-based server(Sun Netra t1400 or Sun Netra 240.

The server can be hosting one or more of the following components:

- Multiservice Data Manager (MDM)
- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

Prerequisites

This procedure has the following prerequisites:

- You must perform a backup of oracle data prior to performing this procedure. Refer to procedure [Performing a backup of oracle data on an SPFS-based server on page 374](#) to complete this task.

Note: A backup of oracle data is not required prior to this procedure for the Core and Billing Manager (CBM) or the MG 9000 Manager.

- For a Sun Netra t1400, use a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data.
- For a Sun Netra 240, use one or more blank DVD-R or DVD-RW disks to store the data. Backups have been successfully tested on a Maxwell 4x DVD-RW and Memorex 4 x DVD-RW.

Note 1: The backup utility limits the storage to 2 GB on a DVD-R and DVD-RW.

Note 2: If you are using a new DVD-RW, or want to reuse a used DVD-RW and need to erase the contents, complete procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

Action

ATTENTION

In a two-server configuration, execute this procedure on the active server.

If unit 0 is backed up, any ensuing restore should be on the same unit.

Use a media safe marker to write a label on each disk (1 of N, 2 of N etc , hostname, date, unit 0 /1).

At the server

- 1 Insert the blank tape or DVD into the drive. In a two-server configuration, insert the blank DVD into the active server.

At your workstation

- 2 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

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

If you are using	Do
a tape for backup	step 4
a DVD for backup	step 5

- 4 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

- 5 Back up the file systems by typing

```
# /opt/nortel/sspfs/bks/bkfullsys
```

and pressing the Enter key.

Note: If you are using DVD, the system will prompt you to insert another blank disk if more than one is needed.

The backup can take between one and four hours depending on system configuration.

Example response:

Backup Completed Successfully

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

If you are using	Do
a tape for backup	step 7
a DVD for backup	step 9

- 7** List the contents of the tape by typing
- ```
gtar -tvMf /dev/rmt/0
```
- and pressing the Enter key.
- 8** Eject and remove the tape from the drive, label it, write-protect it, and store it in a safe place.
- Proceed to [step 17](#).
- 9** The DVD was ejected after backup. Insert the backup DVD into the drive. If the backup resides on multiple DVDs, insert the first backup DVD.
- 10** Access the command line interface by typing
- ```
cli
```
- and pressing the Enter key.
- 11** Enter the number next to the Other option in the menu.
- 12** Enter the number next to the bklist option in the menu to list the content of the DVD.
- 13** Exit each level of the command line interface to eventually return to the command line prompt by typing
- ```
select - x
```
- and pressing the Enter key.
- 14** Ensure you are at the root directory level by typing
- ```
# cd /
```
- and pressing the Enter key.

- 15** Eject the DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

If the disk drive tray will not open after you have determined that the disk drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the disk drive.

- 16** Remove the DVD from the drive, label it, and store it in a safe place.

If the backup	Do
resides on multiple DVDs	Insert the next backup DVD in the disk drive and go to step 10
resides on a single DVD	step 17

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

Archiving the NPM database into a file

Application

Before performing an upgrade of the Network Patch Manager (NPM) to a new release, it is recommended that you preserve any user-defined data in the current release. Examples are user-defined sets, reports, alarms, tasks and plans.

Under normal circumstances this is not required since these user-defined sets and reports are automatically preserved across the upgrade. In the event of a fallback however they will be lost. This procedure creates a file to be used in the case of a fallback such that the user-defined sets and reports can be restored.

Prerequisites

The SPFS software has not been upgraded yet.

Action

ATTENTION

In a two-server configuration, execute this procedure on the active server.

At the server

- 1 Log in to the server if not already logged in by typing
 > **telnet <server>**
 and pressing the Enter key.
 where
 server
 is the IP address or hostname of the SPFS-based server
 where NPM resides
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing
 \$ **su -**
 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directory to the data directory by typing
 # **cd /data**

- and pressing the Enter key.
- 6 Make a directory to store the old NPM files by typing
`# mkdir npm_old`
and pressing the Enter key.
 - 7 Change directory to the directory you just created by typing
`# cd npm_old`
and pressing the Enter key.
 - 8 Archive the NPM database into a file by typing
`# tar -cvf old_npm_db.tar /data/npm/database/*`
and pressing the Enter key.
 - 9 Return to the home directory by typing
`# cd`
and pressing the Enter key.
 - 10 Proceed to procedure [Saving the NPM patch and database files on page 385](#) to complete this procedure.
 - 11 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Saving the NPM patch and database files

Application

Use this procedure prior to upgrading the Network Patch Manager (NPM) software. This procedure provides instructions on how to copy patch and database file information to one of the following locations:

- to disk
- to tape (Sun Netra t1400 only)
- to CD (Sun Netra 240 only)

NPM patch files saved to a location on disk are preserved over an upgrade. However, if for some reason you need to restore those patch files, contact your next level of support. If you save the NPM patch files on tape (Sun Netra t1400), or CD or DVD (Sun Netra 240), you can restore them using procedure “Restoring NPM patch files” in *ATM/IP Fault Management*, NN10408-900.

NPM user-defined functions and schedules are automatically preserved over an upgrade. However, they are lost if a fallback has to be performed (see [Executing a fallback during an SPFS-based server upgrade on page 418](#)). Having a saved NPM database allows you to restore any user-defined functions and schedules in the NPM if a fallback to the old NPM is required.

Prerequisites

This procedure has the following prerequisites:

- For a Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data.
- For a Netra 240, you need one or more blank CD-R, CD-RW, DVD-R or DVD-RW to store the data.

Note 1: The backup utility limits the storage to 4 GB on a DVD-R and DVD-RW.

Note 2: If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600, if required.

Action

Perform the steps using one of the following methods to complete this procedure:

- [Saving NPM patch files to disk](#)
- [Saving NPM patch files to CD \(Sun Netra 240 only\)](#)
- [Saving NPM database files to tape \(Sun Netra t1400 only\)](#)
- [Saving NPM patch files to tape \(Sun Netra t1400 only\)](#)
- [Saving NPM database files to CD \(Sun Netra 240 only\)](#)

Saving NPM patch files to disk

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Verify whether any NPM patch files exist as follows:
 - a Change directory to the NPM's patch file directory by typing


```
# cd /data/npm/Au
```

 and pressing the Enter key.
 - b List the content of the directory by typing


```
# ls
```

 and pressing the Enter key.

If	Do
patch files exist	step 3
otherwise	step 9

- 3 Access the data directory by typing


```
# cd /data
```

 and pressing the Enter key.
- 4 Make a directory to store the old NPM files by typing


```
# mkdir <npm_old>
```

where

npm_old

is a valid Unix directory name

- 5 Change directory to the directory you just created by typing

```
# cd <npm_old>
```

where

npm_old

is a valid Unix directory name

- 6 Create a temporary directory to hold the NPM backup data by typing

```
# mkdir <directory_name>
```

and pressing the Enter key.

where

directory_name

is a valid UNIX directory name

Example

```
# mkdir patch_data
```

7

ATTENTION

This step copies all or selected NPM patch files to a temporary location. If it is preferable to download the required patch files after the upgrade, then skip this step.

Save a copy of the needed patch files as follows:

Note: The NPM upgrade process does not remove the patch files present in the patch file repository. However, in some instances the NPM server cannot locate and utilize all the files. The NPM server and database will remain unaware of any patches present that are not yet applied to any working device.

- a Change directory to the NPM's patch file directory by typing

```
# cd /data/npm/Au
```

and pressing the Enter key.

- b Copy all patch files to the backup directory by typing

```
# cp *.ptch* <directory_path>
```

and pressing the Enter key.

where

directory_path

is the path to the directory you created in [step 6](#)

Example

```
# cp *.ptch* /data/npm_old/patch_data
```

Watch for any errors during the copy.

- c Ensure the backup directory contains the patches by typing

```
# ls <directory_path>
```

and pressing the Enter key.

where

directory_path

is the path to the directory where you copied the patch files

Example

```
# ls /data/npm_old/patch_data
```

- 8 Return to the home directory by typing

```
# cd
```

and pressing the Enter key.

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

Saving NPM patch files to tape (Sun Netra t1400 only)

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Insert a blank tape into the drive.

Note: Ensure the write-protect tab is set to allow writing.

- 3 Rewind the tape by typing

```
# mt rewind
```

and pressing the Enter key.

- 4 Copy the patch files to tape by typing

```
# tar cv /data/npm/Au
```

and pressing the Enter key.
- 5 Rewind and eject the tape by typing

```
# mt offline
```

and pressing the Enter key.
- 6 Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

```
mt -f /dev/rmt/0 rewoff
```
- 7 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Saving NPM patch files to CD (Sun Netra 240 only)

At the server

- 1 Insert a blank CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the active server.

At your workstation

- 2 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 3 Create a temporary directory by typing

```
# mkdir /tmp/.iso
```

and pressing the Enter key.

Note: The directory may already exist.

- 4 Make an ISO image of the patch files and write this image to the CD or DVD by typing

```
# /opt/nortel/sspfs/bks/cdwrite /data/npm/Au  
PATCHES
```

and pressing the Enter key.

Note 1: This step is mandatory for an N240 simplex configuration. However, it is optional for an N240 HA (cluster)

configuration and can be performed outside the upgrade window.

Note 2: Ensure there is a space between the directory /data/npm/Au and PATCHES.

Note 3: The CD or DVD is automatically ejected.

- 5 Remove the CD or DVD from the drive, label it, and store it in a safe place.
- 6 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Saving NPM database files to tape (Sun Netra t1400 only)

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Insert a blank tape into the drive.

Note: Ensure the write-protect tab is set to allow writing.
- 3 Rewind the tape by typing

`# mt rewind`

and pressing the Enter key.
- 4 Copy the database files to tape by typing

`# tar cv /data/npm_old/old_NPM_db.tar`

and pressing the Enter key.
- 5 Rewind and eject the tape by typing

`# mt offline`

and pressing the Enter key.
- 6 Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

`mt -f /dev/rmt/0 rewoff`
- 7 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Saving NPM database files to CD (Sun Netra 240 only)

At the server

- 1 Insert a blank CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the active server.

At your workstation

- 2 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 3 Create a temporary directory by typing

```
# mkdir /tmp/.iso
```

and pressing the Enter key.

Note: The directory may already exist.

- 4 Make an ISO image of the database files and write this image to the CD or DVD by typing

```
# /opt/nortel/sspfs/bks/cdwrite  
/data/npm_old/old_npm_db.tar
```

and pressing the Enter key.

Note 1: This step is mandatory for an N240 simplex configuration. However, it is optional for an N240 HA (cluster) configuration and can be performed outside the upgrade window.

Note 2: There is a space after the word cdwrite.

Note 3: The CD or DVD is automatically ejected.

- 5 Remove the CD or DVD from the drive, label it, and store it in a safe place.
- 6 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Performing a backup of APS audio files to tape

Application

Use this procedure to back up APS audio files to a 4mm Digital Audio Tape (DAT).

ATTENTION

This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure [Performing a backup of APS audio files to CD or DVD on page 394](#).

Prerequisites

You need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the audio files.

Action

Perform the following steps to complete this procedure.

At the server

- 1 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) digital audio tape (DAT) tape into the DAT drive on the server where the APS resides.

At the server console

- 2 Log in to the server through the console (port A) using the root user ID and password.
- 3 Rewind the tape:
mt -f /dev/rmt/0c rewind
- 4 Change directories to the root filesystem:
cd /
- 5 Back up the APS audio files:
/usr/ntdb/uas/scripts/backup_appl_data.sh
Note: This command backs up file systems /PROV_data, /audio_files, and /user_audio_files.
- 6 Rewind the backup tape:
mt -f /dev/rmt/0c rewind

- 7 To ensure that the backup was successful, list the content of the tape:

```
tar tvf /dev/rmt/0c | more
```
- 8 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen) to prevent the data on the tape from being accidentally over-written. Store the tape for later use.
- 9 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Performing a backup of APS audio files to CD or DVD

Application

Use this procedure to back up APS audio files to CD or DVD, or move the backup of audio files to another server if the backup is more than 4 GB.

Prerequisites

You need one blank CD-R, DVD-R, CD-RW or DVD-RW to store the data if the data is less than 4 GB. Otherwise you need a server accessible through FTP with adequate space to hold the data.

Note 1: The backup utility limits the storage to 4 GB on a DVD-R, or DVD-RW.

Note 2: If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

Action

Perform the steps that follow to complete this procedure.

At the server

- 1 Insert a blank CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the active server.

At your workstation

- 2 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 3 Change directories to the root file system:
`cd /`

- 4 Create a “tar” file of the APS audio files:

```
tar cvf AudioFiles.tar /audio_files  
/user_audio_files /opt/uas/uas_conf_backup
```

Note: The above command is entered on one line, and includes a space between each directory.
- 5 Verify the size of the “AudioFiles.tar” file:

```
ls -l AudioFiles.tar
```

If the “AudioFiles.tar” file is	Do
under 4 GB	step 7
over 4 GB	step 6
- 6 Move the “AudioFiles.tar” file onto another server using File Transfer Protocol (FTP).
Proceed to step [10](#)
- 7 Create a temporary directory:

```
mkdir /tmp/.iso
```

Note: The directory may already exist.
- 8 Backup the tar file of the APS audio files onto the CD or DVD:

```
/opt/nortel/sspfs/bks/cdwrite AudioFiles.tar
```
- 9 Remove the CD or DVD from the drive, label it, and store it in a safe place.
- 10 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Performing a backup of APS oracle data to tape

Application

Use this procedure to back up APS oracle data to a 4mm Digital Audio Tape (DAT).

ATTENTION

This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure [Performing a backup of APS oracle data to CD or DVD on page 398](#).

Prerequisites

You need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the oracle data.

Action

Perform the following steps to complete this procedure.

At the server console

- 1 Log in to the server through the console (port A) using the root user ID and password.
- 2 Back up the APS oracle data to hard disk by typing

```
# ips_export_db.sh -diskonly
```

and pressing the Enter key.
- 3 Change directories to where the backup is by typing

```
# cd /audio_files/aps_db_backup
```

and pressing the Enter key.

At the server

- 4 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) digital audio tape (DAT) tape into the DAT drive on the server where the APS resides. In a two-server configuration, insert the tape into the drive of the active server.

At the server console

- 5 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

- 6 Create a tar file of the APS oracle files onto tape by typing

```
# tar cvf /dev/rmt/0 ./*.dmp
```

and pressing the Enter key.
- 7 Rewind the backup tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.
- 8 To ensure the backup was successful, list the content of the tape by typing

```
# tar tvf /dev/rmt/0c | more
```

and pressing the Enter key.
- 9 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen) to prevent the data on the tape from being accidentally over-written. Store the tape for later use.
- 10 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Performing a backup of APS oracle data to CD or DVD

Application

Use this procedure to back up APS oracle data onto a CD or DVD, or move the backup of oracle data onto another server if the backup is over 4 GB.

Prerequisites

You need one blank CD-R, DVD-R, CD-RW or DVD-RW to store the data

Note 1: The backup utility limits the storage to 4 GB on a DVD-R, or DVD-RW.

Note 2: If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

Action

Perform the steps that follow to complete this procedure.

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Back up the APS oracle data to hard disk:

```
ips_export_db.sh -diskonly
```

- 3 Change directories to where the backup is:

```
cd /audio_files/aps_db_backup
```

- 4 Create a tar file of the APS oracle files:

```
tar cvf aps_oracle_bkup.tar *
```

- 5 Verify the size of the “aps_oracle_bkup.tar ” file:

```
ls -l aps_oracle_bkup.tar
```

If “aps_oracle_bkup.tar” file is	Do

under 4 GB	step 7

over 4 GB	step 6

- 6 Move the “aps_oracle_bkup.tar” file onto another server using File Transfer Protocol (FTP).
Proceed to step [11](#).

- 7 Create a temporary directory:

```
mkdir /tmp/.iso
```

Note: The directory may already exist.

At the server

- 8 Insert a blank CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the active server.

At your workstation

- 9 Backup the tar file of the APS oracle data onto the CD or DVD:

```
/opt/nortel/sspfs/bks/cdwrite aps_oracle_bkup.tar
```

At the server

- 10 Remove the CD or DVD from the drive, label it, and store it in a safe place.
- 11 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Verifying the state of a cluster

Application

Use this procedure to verify the state of a cluster, which involves verifying the status of replicated disk volumes, the cluster indicator, and the cluster configuration. A cluster refers to a Sun Netra 240 server pair.

When a cluster node is out of sync, log SPFS310 is generated. You can view log SPFS310 through the IEMS GUI or in file `/var/log/customerlog` on the server.

For more information on logs, refer to *Carrier Voice over IP Networks Fault Management Logs Reference*, NN10275-909. For information on how to configure log reporting, route customer logs to a remote host and view customer logs, refer to *ATM/IP Fault Management*, NN10408-900.

Prerequisites

You need the root user ID and password for the inactive server.

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Establish a connection to the inactive server through telnet or SSH, log in using the root user ID and password, and ensure you are on the inactive server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Verify the status of replicated disk volumes by typing
`# udfstat`
and pressing the Enter key.

If	Do
the system response for each filesystem is STANDBY normal UP clean	step 3
otherwise	step 4

- 3 Verify the status of the cluster configuration by typing
`# CheckConfiguration`

and pressing the Enter key.

If	Do
the system response is Checking local configuration against unit0-priv0 #	the cluster is in a good state and you can proceed to step 9
otherwise	step 4

Note: There will be some discrepancy between the (I)SN08 and (I)SN09 responses to the CheckConfiguration command. In (I)SN09, the system returns an additional response if the verification passes and the cluster nodes are in sync. This response is not returned in (I)SN08. This discrepancy is normal.

- 4 Reboot the inactive server by typing
init 6
and pressing the Enter key.
- 5 Following the reboot, establish a connection to the inactive server through telnet or SSH, log in using the root user ID and password, and ensure you are on the inactive server.
For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 6 Verify the status of replicated disk volumes by typing
udstat
and pressing the Enter key.

If	Do
the system response for each filesystem is STANDBY normal UP clean	step 7
otherwise	step 8

- 7 Verify the status of the cluster configuration by typing
CheckConfiguration

and pressing the Enter key.

If	Do
the system response is Checking local configuration against unit0-priv0 #	the cluster is in a good state and you can proceed to step 9
otherwise	step 8

Note: There will be some discrepancy between the (I)SN08 and (I)SN09 responses to the CheckConfiguration command. In (I)SN09, the system returns an additional response if the verification passes and the cluster nodes are in sync. This response is not returned in (I)SN08. This discrepancy is normal.

- 8 Contact your next level of support.
- 9 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Upgrading SPFS software

Application

Use this procedure to upgrade the Server Platform Foundation Software (SPFS) on a Sun Netra t1400 or Sun Netra 240.

The SPFS must be upgraded prior to upgrading the software for any one of the following components that reside on an SPFS-based server.

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Media Gateway 9000 Manager
- Core and Billing Manager (CBM)
- Multiservice Data Manager (MDM) on a Sun Netra 240

Prerequisites

This procedure has the following prerequisites:

- If upgrading from ESD, ensure you have the CD *Server Platform Foundation Software Ver SN09.1 Disk 1* (order code SPFR0091). ESD users require this CD to perform a full system restore of a SPFS based server.
- If upgrading from CD, ensure you have SPFS Disk 1 (ordercode SPFR0091) and SPFS Disk 3 (ordercode SPFS0091) for the (I)SN09U release. SPFS Disk 2 is only used to upgrade the Solaris OS from a pre SN08 release, and is not used in the SPFS upgrade procedure documented here.
- If upgrading from ESD, ensure the ESD file has been uncompressed to platform_disk_1.iso, platform_disk_2.iso, and platform_disk_3.iso files on the repository server prior to performing this procedure. An SPFS MNCL ISO file may also exist.

- Ensure you have backed up your Oracle data and file systems before proceeding with this procedure. If required, refer to the following procedures:
 - [Performing a backup of oracle data on an SPFS-based server on page 374](#)
 - [Performing a backup of file systems on an SPFS-based server on page 379](#)

Note 1: Backing up the Oracle data is not applicable on an SPFS-based server that is hosting the Core and Billing Manager (CBM).

Note 2: Backing up file systems is not required on an SPFS-based server that is hosting an MG 9000 Manager since the file system back up was performed as part of the MG 9000 Manager pre-upgrade activity.

- Verify there are no faults on the system that will interfere with the upgrade by executing the queryflt command after logging onto the server. In a two-server configuration, execute this command on both nodes. The system response to the command displays any local faults on the node or nodes that could interfere with the upgrade process. If alarms are present, contact the next level of support.
- Nortel recommends verifying that the SPFS console ports are accessible for Nortel Support in advance of starting this upgrade. For information about console access, refer to [Configuring SPFS console access on page 51](#)

Action

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

- [Upgrading SPFS software using CDROM disks on page 405](#)
- [Upgrading SPFS software using ESD on page 410](#)

ATTENTION

A fallback can be executed at any point from [step 8](#) onward in this procedure, by performing procedure “Executing a fallback during an SPFS-based server upgrade” for a [One-server configuration on page 419](#).

ATTENTION

The pre_upgrade and liveupgrade scripts perform an alarm check for any Major/Critical alarms upon execution. If any major or critical alarms are present, you will be receive the following prompt to review the alarm(s) and either continue or terminate the upgrade.

WARNING: There are major or critical alarms on this unit. It is recommended to review the alarms before proceeding with the upgrade. Type "ok" when ready to continue or "abort" to terminate:

You may clear the alarm and enter "ok" to continue or enter "abort" to terminate. It is not recommended to continue an upgrade while Major/Critical alarms are present. If you terminate execution of the script at this point, you can re-execute the script once you clear the alarm, or contact your next level of support.

Another alarm check is performed by SPFS before the maintenance reboots take place. If any major or critical alarms are generated during the upgrade, you are prompted to clear the alarm and continue or terminate the upgrade. You can review/clear the alarm and enter "ok" to resume, contact your next level of support, or terminate by entering "abort".

If you enter "abort", the upgrade is terminated and you will get the "#" prompt. Run the SSPFS_Upgrade.fallback command and then clone the unit using the procedure [Cloning the image of one server in a cluster to the other server on page 478](#) to return it to its preupgrade state.

Upgrading SPFS software using CDROM disks**ATTENTION**

On a simplex server, a fallback can be executed at any point from [step 8](#) up to and including [step 12](#) in this procedure, by running the fallback command `/SSPFS_Upgrade.fallback`. At any point after [step 12](#) in this procedure, executing a fallback will involve performing procedure "Executing a fallback during an SPFS-based server upgrade" for a [One-server configuration on page 419](#).

On an HA server pair, a fallback can be executed at any point from [step 8](#) onward in this procedure, by performing procedure "Executing a fallback during an SPFS-based server upgrade" for a [Two-server configuration on page 419](#).

At the server console

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

In a two-server configuration, log in to the inactive server and ensure you are on the inactive server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

At the server

- 2 Insert SPFS Disk 1 into the drive. In a two-server configuration, insert the disk into the inactive server.

At the server console

- 3 Verify whether other users are logged on to the system
who

- 4 The presence of other users logged on to the system can have adverse effects on the upgrade process and can cause the upgrade to fail. Therefore, request that all users log out before you proceed using the wall command:

wall

**The system is coming down for maintenance.
Please log off immediately in order to save your files.**

- 5 Then hit the Ctrl and D keys simultaneously to send the message to all users.
- 6 Verify the available disk space

df -k

Ensure the file systems on the following mount points have the specified minimum of available disk space:

Note: The value under the avail column is the amount of available kilobytes. If the do not have enough disk space, contact your next level of support.

- /opt must have a minimum of 1800000 kilobytes of available disk space
- /var must have a minimum of 1200000 kilobytes of available disk space

- /tmp must have a minimum of 200000 kilobytes of available disk space
 - / (root) must have a minimum of 1550000 kilobytes of available disk space
- 7** Ensure you are at the root directory level
- cd /**
- 8** Run the pre-upgrade script
- /cdrom/cdrom0/s0/pre_upgrade**
- The pre-upgrade script prepares the server for the upgrade, and begins the upgrade of the Sun Solaris operating system.
- The execution of this step takes approximately 5 minutes to complete on a Netra t1400, and 3 minutes on a Netra 240. The execution time can vary depending on system configuration.
- 9** Start the upgrade process
- /liveupgrade.ksh**
- Example response
- All Three Required ISO Image Files Were NOT Found In The /Upgrade Directory.
Type "cdrom" for CDROM Upgrade, Or "exit" To Abort.
- 10** Confirm you want to continue with the CDROM install
- cdrom**
- Example response
- Creating initial configuration for primary boot environment <old_sspfs>.
WARNING: The device </dev/md/dsk/d2> for the root file system mount point </> is not a physical device.
Is the physical device </dev/dsk/clt0d0s1> the boot device for the logical device </dev/md/dsk/d2>? (yes or no)
- 11** Accept the specified device as the boot device
- yes**
- The execution of this step takes approximately 120 minutes to complete on a Netra t1400, and 60 minutes on a Netra 240. The execution time can vary depending on system configuration.

During this time, the server is fully functional and applications can be used.

Note 1: Once the liveupgrade process starts, the disks will no longer be in redundant mode, and log SPFS310 will be generated indicating disk or disk mirroring errors. This is an expected condition during an upgrade, and no action is required.

Note 2: During the execution of this step, the system displays a warning message stating that <n> packages failed to install properly on boot environment SN09U. This message is expected and does not indicate a problem.

Once this step completes, the system ejects SPFS Disk 1 and prompts you to insert Disk 3.

At the server

- 12 Remove SPFS Disk 1 from the CDROM drive, and insert SPFS Disk 3.

At the server console

- 13 When ready, indicate you want to proceed

ok

The execution of this step takes approximately 165 minutes to complete on a Netra t1400, and 75 minutes on a Netra 240. The execution time can vary depending on system configuration.

Note 1: During the execution of this step, the system displays a warning message stating that <n> packages failed to install properly on boot environment SN09U. This message is expected and does not indicate a problem.

Note 2: During the execution of this step, you may receive the following warnings or errors:

```
Installation of 114332-15 failed:  
Attempt to apply a patch that's already been  
applied
```

```
Installation of 113135-03 failed: Attempting  
to patch a package that is not installed
```

```
Installation of 112954-11 failed: An  
incompatible patch is applied
```

No action is necessary if you receive this warning. It only means that the patch has already been applied.

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

If	Do
you are upgrading a CBM and you have received a prompt to select the software delivery method for the upgrade	You have completed this procedure. Return to Upgrading the CBM on page 767
otherwise	step 15

- 15 Wait until the upgraded server fully reboots, which consists of two reboots.

On simplex SPFS-based servers hosting the CMT, IEMS, or both, data migration starts once the server has rebooted. The time required for data migration depends on the configuration.

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

If	Do
the server you are upgrading starts data migration	step 17
otherwise	step 18

- 17 Wait until data migration completes and the prompt returns before you proceed.

Note: Data migration is complete when the prompt returns. To check the status of the data migration, refer to [Verifying the completion of data migration on page 422](#).

- 18 Log back in to the server through the console (port A) using the root user ID and password.

In a two-server configuration, log back in to the upgraded (inactive) server and ensure you are on the inactive server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

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

If	Do
the SPFS-based server is hosting the IEMS	step 20
otherwise	step 22

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

If	Do
you are upgrading a simplex server	step 21
otherwise	step 22

- 21 Disable the health monitors and ensure WEBSERVICES is started

cfigsplxck disable

Example response

NOTE: Disabling health monitor...Success.

NOTE: Starting WEBSERVICES...Success.

- 22 Remove SPFS Disk 3 from the CDROM drive.

- 23 Verify the version of the SPFS software.

For detailed steps, refer to the procedure [Verifying the SPFS software load on page 416](#).

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

Upgrading SPFS software using ESD

ATTENTION

On a simplex server, a fallback can be executed at any point from [step 6](#) up to and including [step 23](#) in this procedure, by running the fallback command **/SSPFS_Upgrade.fallback**. At any point after [step 23](#) in this procedure, executing a fallback will involve performing procedure “Executing a fallback during an SPFS-based server upgrade” for a [One-server configuration on page 419](#).

On an HA server pair, a fallback can be executed at any point from [step 6](#) onward in this procedure, by performing procedure “Executing a fallback during an SPFS-based server upgrade” for a [Two-server configuration on page 419](#).

At the server console

- 1 Transfer and mount the ISO image of SPFS Platform Disk 1 (platform_disk_1.iso) onto the SPFS based server.
In a two-server configuration, transfer and mount the image on the inactive server.
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 2 Log in to the server through the console (port A) using the root user ID and password.
In a two-server configuration, log in to the inactive server and ensure you are on the inactive server.
For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 3 Verify whether other users are logged on to the system
who
- 4 The presence of other users logged on to the system can have adverse effects on the upgrade process and can cause the upgrade to fail. Therefore, request that all users log out before you proceed by using the wall command:
wall
The system is coming down for maintenance. Please log off immediately in order to save your files.
Then hit the Ctrl and D keys simultaneously to send the message to all users.
- 5 Verify the available disk space
df -k
Ensure the file systems on the following mount points have the specified minimum of available disk space.
Note: The value under the avail column is the amount of available kilobytes. If the do not have enough disk space, contact your next level of support.
 - /opt must have a minimum of 1800000 kilobytes of available disk space
 - /var must have a minimum of 1200000 kilobytes of available disk space

- /tmp must have a minimum of 200000 kilobytes of available disk space
- / (root) must have a minimum of 1550000 kilobytes of available disk space

6 Run the pre-upgrade script

/tmpmnt/pre_upgrade

The pre-upgrade script prepares the server for the upgrade, and begins the upgrade of the Sun Solaris operating system.

The execution of this step takes approximately 5 minutes to complete on a Netra t1400, and 3 minutes on a Netra 240. The execution time can vary depending on system configuration.

7

ATTENTION

You must unmount the image file using the umount command before removing the image file. If the file is deleted while it is mounted by the operating system, it can interfere with normal operation of runtime applications running on this server.

Access the command line interface to unmount the iso image

cli

- 8** Enter the number next to the Other option in the menu.
- 9** Enter the number next to the umount_image option in the menu.
- 10** Exit each menu level of the command line interface to eventually return to the root level prompt

select - x

- 11** Copy the platform_disk_1.iso image to the /Upgrade directory.

cp /data/esd_iso/platform_disk_1.iso /Upgrade

- 12** Remove the platform_disk_1.iso from the /data/esd_iso directory.

rm /data/esd_iso/platform_disk_1.iso

- 13** Change to the Upgrade directory.

cd /Upgrade

- 14** Establish an FTP session to the repository server where the ESD software is located.

ftp <repository_server>

where

repository_server

is the host name or IP address of the server owned by the operating company that was selected to be the destination for ESD software.

- 15** Log in to the repository server.

- 16** Change directory to where the SPFS iso files are located on the repository server.

cd <esd_directory>

where

esd_directory

is the directory that contains the SPFS iso files, for example, SPFS0091.91.R.NCL.NAP.VAULT.1.D

- 17** Change the transfer mode to binary

bin

- 18** Transfer the platform_disk_2.iso image to the SPFS-based server

get platform_disk_2.iso

- 19** Transfer the platform_disk_3.iso image to the SPFS-based server

get platform_disk_3.iso

- 20** End the FTP session

bye

- 21** Ensure you are in the root directory

cd /

- 22** Run the SPFS upgrade script

/liveupgrade.ksh

Example response

All Three Required ISO Image Files Found Present
In The /Upgrade Directory.
Type "esd" For ESD Upgrade, "cdrom" For CDROM
Upgrade, Or "exit" To Abort:

23 Confirm you want to continue with the ESD install**esd**

Example response

Creating initial configuration for primary boot environment <old_sspfs>.

WARNING: The device </dev/md/dsk/d2> for the root file system mount point </> is not a physical device.

WARNING: The system boot prom identifies the physical device </dev/dsk/clt0d0s1> as the system boot device.

Is the physical device </dev/dsk/clt0d0s1> the boot device for the logical device </dev/md/dsk/d2>? (yes or no)

24 Accept the specified device as the boot device**yes**

Note 1: The warnings that display are expected and can be ignored.

Note 2: Once the liveupgrade process starts, the disks will no longer be in redundant mode, and log SPFS310 will be generated indicating disk or disk mirroring errors. This is an expected condition during an upgrade, and no action is required.

The execution of this step takes approximately three-and-a-half hours to complete on a Netra t1400, and two hours on a Netra 240. The execution time can vary depending on system configuration. During this time, the server is fully functional and applications can be used.

25 Use the following table to determine your next step.

If	Do
you are upgrading a CBM	You have completed this procedure. Return to Upgrading the CBM on page 766
otherwise	step 26

26 Wait until the upgraded server fully reboots, which consists of two reboots.

On simplex SPFS-based servers hosting the CMT, IEMS, or both, data migration starts once the server has rebooted. The time required for data migration depends on the configuration.

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

If	Do
the server you are upgrading starts data migration	step 28
otherwise	step 29

- 28 Wait until data migration completes and the prompt returns before you proceed.

Note: Data migration is complete when the prompt returns. To check the status of the data migration, refer to [Verifying the completion of data migration on page 422](#).

- 29 Log back in to the server through the console (port A) using the root user ID and password.

In a two-server configuration, log back in to the upgrade (inactive) server and ensure you are on the inactive server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

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

If	Do
the SPFS-based server is hosting the IEMS	step 31
otherwise	step 33

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

If	Do
you are upgrading a simplex server	step 32
otherwise	step 33

- 32 Disable the health monitors and ensure WEBSERVICES is started

cfigsplxck disable

Example response

NOTE: Disabling health monitor...Success.

NOTE: Starting WEBSERVICES...Success.

- 33 Verify the version of the SPFS software.
For detailed steps, refer to the procedure [Verifying the SPFS software load on page 416](#).
- 34 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Verifying the SPFS software load

At the server console

- 1 Verify that your system is running the SN09U version of the SPFS through the command line interface
cli
- 2 Enter the number next to the View option in the menu.
- 3 Enter the number next to the sspfs_soft option in the menu.
- 4 Note the SPFS version.
- 5 Exit each menu level of the command line interface to eventually return to the command prompt

select - **x**

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

If	Do
the SPFS version you noted is 09.1	step 7
any other version	stop and contact your next level of support

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

If	Do
you upgraded an HA server	step 8
otherwise	step 9

- 8 Verify the status of replicated disk volumes

udstat

All filesystems must have a state of STANDBY normal UP clean. Repeat this command until the state of all filesystems is STANDBY normal UP clean.

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

Executing a fallback during an SPFS-based server upgrade

Application

Use this procedure to roll back (fall back) to the state prior to the upgrade. One or more of the following components can be hosted on the server:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)
- Multiservice Data Manager (MDM) on a Sun Netra 240

ATTENTION

Only use this procedure when directed to do so.

Prerequisites

You can only perform this procedure on the newly upgraded node.

Action

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

- [One-server configuration on page 419](#)
- [Two-server configuration on page 419](#)

ATTENTION

The following error messages are expected during a fallback:

ERROR: No boot environments are configured on this system
ERROR: cannot determine list of all boot environment names
ERROR: No boot environments are configured on this system
ERROR: cannot determine list of all boot environment names
ERROR: Unable to determine the previous Boot Environment

One-server configuration

At the server console

- 1 Log in to the server through the console (port A) using the root user ID and password if not already logged in.
- 2 Rollback to the state prior to the upgrade by typing
/SSPFS_Upgrade.fallback
and pressing the Enter key.
- 3 Use the following table to determine your next step. If server is hosting the:

If your server is hosting the	Do
Core and Billing Manager (CBM) or MG 9000 Element Manager	step 5
CS 2000 Management Tools, CS 2000 SAM21 Manager, Audio Provisioning Server (APS), or Integrated Element Management System (IEMS)	step 4

- 4 Restore the oracle data on the server. If required, refer to procedure “Restoring the oracle data on an SPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.
- 5 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Two-server configuration

At the server console

- 1 Log in to the upgraded server through the console (port A) using the root user ID and password if not already logged in.
- 2 Rollback to the state prior to the upgrade by typing
/SSPFS_Upgrade.fallback
and pressing the Enter key.
Note: This may take some time to execute.
- 3 Connect to the console port of the nonupgraded server that has the previous software on it.

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

If the nonupgraded server is	Do
at the "OK" prompt	Type: boot and go to step 5
not at the "OK" prompt	step 5

- 5 Log in using the root user ID and password once the login prompt is available if not already logged in.

- 6 Verify the status of replicated disk volumes by typing
udstat
and pressing the Enter key.

If	Do
all the file systems are ACTIVE and none are reporting "operator" or "nodaemon"	step 7
otherwise	contact your next level of support

Note: On the active side, it is normal for the udstat command to show the status of the replicated filesystems as "DOWN dirty" while the inactive side is at the OK prompt.

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

If	Do
server is hosting the MG 9000 EM Server	step 10
server is hosting the IEMS or CS2M	refer to procedure "Restoring the oracle data on an SPFS-based server" in <i>ATM/IP Security and Administration</i> , NN10402-600

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

If	Do
server is hosting the NPM	step 9
otherwise	step 10

- 9** Restore the NPM patch files using the procedure [Restoring NPM patch files on page 501](#).
- 10** Clone the image of the active (non-upgraded) server onto the upgraded server. If required, refer to procedure [Cloning the image of one server in a cluster to the other server on page 478](#).
- 11** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Verifying the completion of data migration

Application

Use this procedure to verify if the database upgrade is still in progress or if it has been completed. This procedure applies to SPFS upgrades from SN08 where connection to the console is lost and there is a need to check the data migration progress.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Access the scripts directory by typing
cd /opt/nortel/sspfs/Scripts
and pressing the Enter key.

- 3 Type
./checkdb_upgrade
to check the progress of the database upgrade.

Note: This script can be executed multiple times to check the progress of the database upgrade.

- 4 Use the output of the script to determine the current status of the database upgrade.

Example response if the database upgrade was completed

```
Database upgrade completed.  
Verifying database version ....
```

```
Sun Microsystems Inc.   SunOS 5.9           Generic  
May 2002
```

```
Database version 9.2.0.7.0  
Oracle Instance is UP.  
Oracle Listener is UP.
```

Example response if the database upgrade is still in progress

```
Database upgrade in progress
```

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

Determining the SPFS software MNCL level

Purpose of this procedure

Use this procedure to determine the MNCL level of a SPFS software load.

To verify if SPFS is at the latest Maintenance Release (MNCL), compare the MNCL load displayed using this procedure with the latest load on the Electronic Software Delivery (ESD) server or against the technical bulletins for SPFS. When a new MNCL is released, a technical bulletin is issued with a Notification of Availability.

To view bulletins, please visit Nortel Technical Support on the web at: <http://www.nortel.com/support>.

Prerequisites

You are logged onto a SPFS-based server.

Action

at the server console

- 1 Access the SPFS command line interface (CLI) by typing
`# cli`
and pressing the Enter key.
- 2 Enter the number next to the View option in the menu.
- 3 Enter the number next to the sspfs_soft option in the menu.
- 4 Review the output.

The system returns the SSPFS version showing the release, build ID, and server profile. For a maintenance release (MNCL), the release value is appended with the MNCL identifier.

Example response for MNCL load

SSPFS version: 09.1MA Build: 200613103 Server
Profile: cs2kmt

Example response for a non MNCL load

SSPFS version: 09.1 Build: 200613103 Server
Profile: cs2kmt
- 5 Exit each menu level of the command line interface to eventually return to the command prompt by typing
`select - x`

and pressing the Enter key.

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

Transferring and mounting an ISO image on an SPFS-based server

Application

Use this procedure to perform the following tasks:

- uncompress the software load on your ESD load repository server
- transfer an iso image file from your ESD load repository server to the SSPFS-based server
- mount the image on the SSPFS-based server

Nortel delivers a software load in a compressed file through Electronic Software Delivery (ESD) to a local ESD load repository server. Once the file is uncompressed, the software load and patches are then available as International Standard of Organization (ISO) 9660-compliant images for transfer to an SSPFS-based server.

Only the files with a .iso extension need to be transferred to the SSPFS-based server. The other files contained in the uncompressed file are for information purposes and do not need to be transferred to the SSPFS-based server.

The patch iso image file contains a P in its name, for example, CS2MP080, when delivered with an NCL, or an X, for example, CS2MX080.iso, when delivered with an MNCL.

Prerequisites

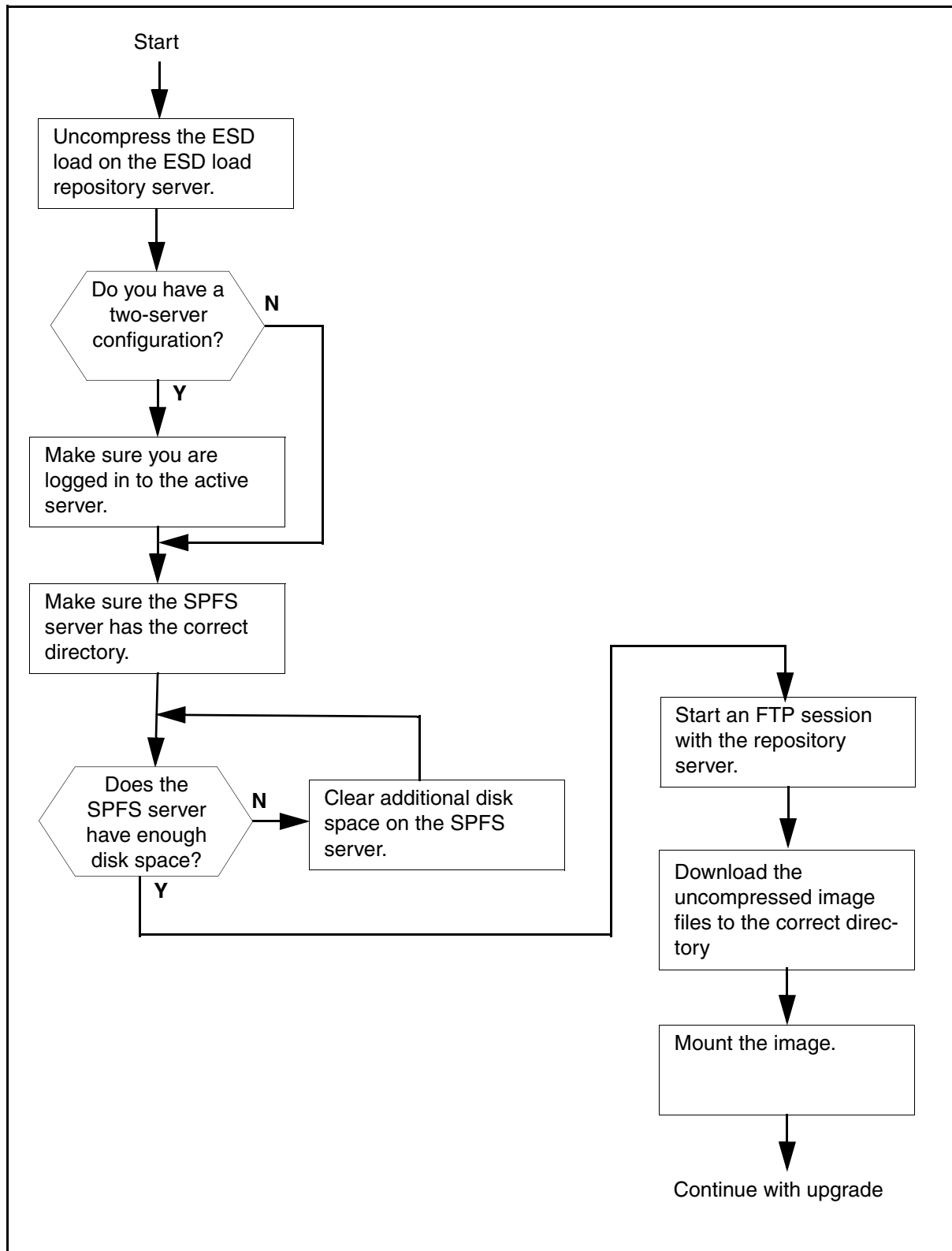
This procedure has the following prerequisites:

- The ESD load must be available on your ESD load repository server.
- You must know the name or IP address of the load repository server and the location of the dropbox directory on the server.
- You must know the name or IP address of the SPFS-based server.
- You must know the root password to the SPFS-based server.

This procedure requires you to confirm the availability of disk space on the SPFS-based server. If the server does not have the required amount of available disk space, follow your local office policy to clear space. If you do not know your policy or cannot clear the required amount of available disk space, contact your next level of support.

Action

Use the flowchart as an overview of the tasks required to complete this procedure. Use the step-by-step instructions to complete the procedure.

Overview of steps to transfer and mount an ISO image to an SPFS-based server

Uncompressing the load on the ESD load repository server

At the ESD load repository server

- 1 Log in to the ESD load repository server, and change directory to the drop box location.

Note: Ensure you log in with a user ID that has permission to uncompress files.

- 2 List the contents of the drop box:

```
ls *.gz
```

- 3 Locate the file you want to uncompress.

- 4 Uncompress the file:

```
gzip -d <esd_filename>.tar.gz
```

where

esd_filename

is the name of the ESD software load, for example:

SPFS0091.91.LAB.NCL.NAP.VAULT.1.D, which is the esd_filename for SPFS

IEMS0091.91.LAB.NCL.NAP.VAULT.2.D, which is the esd_filename for IEMS

UCBM0010.10.LAB.NCL.NAP.VAULT.5.D, which is the esd_filename for CBM

CS2M0091.91.LAB.NCL.NAP.VAULT.1.D, which is the esd_filename for CS 2000 Management Tools

- 5 List the uncompressed file:

```
ls *.tar
```

- 6 Unpack the file:

```
tar -xvf <esd_filename>.tar
```

where

esd_filename

is the name of the ESD software load, for example:

SPFS0091.91.LAB.NCL.NAP.VAULT.1.D, which is the esd_filename for SPFS

IEMS0091.91.LAB.NCL.NAP.VAULT.2.D, which is the esd_filename for IEMS

UCBM0010.10.LAB.NCL.NAP.VAULT.5.D, which is the esd_filename for CBM

CS2M0091.91.LAB.NCL.NAP.VAULT.1.D, which is the esd_filename for CS 2000 Management Tools

The unpacked file is a directory that contains the iso image files.

- 7 Log out of the ESD load repository server.
- 8 Perform the steps under [Transferring an ISO image to an SPFS-based server on page 430](#) to continue with this procedure.

Transferring an ISO image to an SPFS-based server

ATTENTION

In a two-server configuration, you will transfer the ISO image to the active server.

At your workstation

- 1 Establish a connection to the SPFS-based server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Make sure the server has the correct directories. Use the following table as reference to identify the directory required for the SPFS-based server type (component) to which the ISO image is to be transferred.

Component	Directory path
ERS 8600	/swd
GWC	/gwc
All other components	/data/esd_iso

List the directory for your component:

ls <directory>

where

directory

is /swd, /gwc, or /data/esd_iso

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

If the response	Do
indicates no such directory exists	step 4
displays the name of the directory	step 5

- 4 Create the directory:

mkdir <directory>

where

directory

is /swd, /gwc, or /data/esd_iso

- 5 Display the available disk space in the directory:

df -k <directory>

where

directory

is /swd, /gwc, or /data

Example response

```
# df -k /data
```

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/md/dsk/d2	3082223	144125	2876454	5%	/data

- 6 Record the amount of available disk space, which is provided in kilobytes. You will need the information later in this procedure.

- 7 Change directory:

cd <directory>

where

directory

is /swd, /gwc, or /data/esd_iso

- 8 Start an FTP session with the ESD repository server:
ftp <ESD_repository_server_ip>
where
ESD_repository_server_ip
is the machine owned by the operating company that was selected to be the destination for ESD software.
- 9 When prompted, enter your user ID and password.
- 10 List the directories on the ESD repository server:
ftp> ls
- 11 Change directory to the drop box directory:
ftp> cd <dropbox_directory>
where
dropbox_directory
is the name of the your dropbox directory.
- 12 List the contents of the drop box:
ftp> ls -l
- 13 Change to the directory that contains the iso image files:
ftp> cd <esd_filename_directory>
where
esd_filename_directory
is the directory that contains the iso image files, for example:

SPFS0091.91.LAB.NCL.NAP.VAULT.1.D, for SPFS

IEMS0091.91.LAB.NCL.NAP.VAULT.2.D, for IEMS

UCBM0010.10.LAB.NCL.NAP.VAULT.5.D, for CBM

CS2M0091.91.LAB.NCL.NAP.VAULT.1.D, for CS 2000 Management Tools
- 14 Locate the load or patch iso image file you want to transfer, and identify the size of the file, which is provided in bytes.
Note 1: Divide the number of bytes by 1024 to convert the size to kilobytes.
Note 2: The patch iso image file contains a P in its name, for example, CS2MP080, when delivered with an NCL, or an X, for example, CS2MX080.iso, when delivered with an MNCL.

- 15** Compare the size of the iso image file with the amount of available space you recorded in [step 6](#).
- 16** Use the following table to determine your next step.
- | If | Do |
|--|-------------------------|
| the server has enough available disk space | step 18 |
| otherwise | step 17 |
- 17** Clear additional disk space following local office policy, before you continue with this procedure. If necessary, contact your next level of support.
- 18** Change the transfer mode to binary:
- ```
ftp> bin
```
- 19** Transfer the iso image file to the SPFS-based server:
- ```
ftp> get <iso_image>
```
- where
- iso_image**
is the full name of the iso image file
- Note:** Do not transfer any file with a .tar.gz extension.
- 20** End the FTP session:
- ```
ftp> bye
```
- 21** List the contents of the directory to ensure the files successfully transferred to the server:
- ```
ls -l
```
- You are now ready to mount the iso image on the server.
- 22** Perform the steps under [Mounting an ISO image on an SPFS-based server on page 433](#) to complete this procedure.

Mounting an ISO image on an SPFS-based server

ATTENTION

In a two-server configuration, you will mount the ISO image on the inactive server with the exception of the APS, CEM, Media Server 2000, GWC, SAM21, MG 9000 nodes (cards) ISO images, and Patch Media ISO images, which you will mount on the active server.

At your workstation

- 1 Use the following table to determine your first step.

If	Do
you have a two-server configuration	step 2
otherwise	step 4

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

If	Do
you are mounting the APS, CEM, Media Server 2000, GWC, SAM21, MG 9000 nodes (cards) ISO image, or Patch Media ISO image	step 4
otherwise	step 3

- 3 Establish a connection to the inactive server through telnet or SSH using the physical IP address of the inactive server, log in using the root user ID and password, and ensure you are on the inactive server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 4 Start the command line interface:

c1i

- 5 Enter the number next to the Other option in the menu.
- 6 Enter the number next to the mount_image option in the menu.
- 7 Use the following table to determine your next step.

If the system response is	Do
Enter full path to ISO image	step 9
ISO image Already Mounted	step 8

- 8 Enter the number next to the umount_image option in the menu and retry [step 6](#).

Note: If either command is unsuccessful a second time, contact your next level of support.

- 9 When prompted, enter the full path name of the iso image on the server:

<directory_path>/<iso_image>

where

directory_path

is /swd, /gwc, or /data/esd_iso

iso_image

is the full name of the ISO image file

Note 1: Do not attempt to change directories to the /tmpmnt directory until the mount command is complete.

Note 2: Record the path of the ISO image file for ISO image file removal.

10 Use the following table to determine your next step.

If the response is	Do
It is very important for the user of this command to know that if you mount an iso image, you must unmount the image before removing the image file. If the file is deleted while the operating system has it mounted, it can be harmful to the runtime applications on this unit.	step 11
Provided full path to ISO image does not exist	Verify the location and name of the image and retry step 8 .
Error creating the image device location	Retry step 8 . An operating system error with the loopback file driver occurred. If the command fails a second time, contact your next level of support.
ERROR MOUNTING <ESD_filename>	This response indicates that either the iso file is corrupt, or the /tmpmnt directory has been deleted. Exit each menu level of the command line interface to eventually return to the root level prompt by typing select - x Repeat the steps under Transferring an ISO image to an SPFS-based server on page 430. If the procedure fails a second time, contact your next level of support.

11 Exit each menu level of the command line interface:

select - x

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

Removing a server from a cluster

Application

Use this procedure to remove a server from a cluster. A cluster refers to a Sun Netra 240 server pair.

ATTENTION

Only perform this procedure when directed to do so.

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you need access to the inactive server of the cluster

Action

Perform the steps that follow to complete this procedure.

At your workstation

- 1 Establish a connection to the inactive server through telnet or SSH using the physical IP address of the inactive server, log in using the root user ID and password, and ensure you are on the inactive server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.
- 3 Enter the number next to the Configuration option in the menu.
- 4 Enter the number next to the Cluster Configuration option in the menu.
- 5 Enter the number next to the evict_cluster option in the menu.
- 6 Exit each menu level of the command line interface to eventually return to the root level prompt by typing

```
select - x
```

and pressing the Enter key.
- 7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Stopping the SESM server application

Application

Use this procedure to stop the Succession Element and Subelement Manager (SESM) server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Verify the status of the SESM server application by typing
servman query -status -group SESMSERVICE
and pressing the Enter key.

If the response indicates	Do
running	step 3
not running	step 6

- 3 Stop the SESM server application by typing

servstop SESMSERVICE

and pressing the Enter key.

- 4 Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to stop.

- 5 Verify the SESM server application stopped as follows:

a Verify the SESM services stopped by typing

servman query -status -group SESMSERVICE

and pressing the Enter key.

Example response:

CS2K Management Tools are not running

b Verify the SESM applications stopped by typing

ptmctl status

and pressing the Enter key.

Example response:

SESM STATUS -----

COMPONENT -----	STATUS -----
Proxy Agent	NOT RUNNING
RMI Regisry	NOT RUNNING
Snmpfactory	NOT RUNNING
MI2 Server	NOT RUNNING

Current number of SESM processes running: 0 (of 4)

SESM APPLICATION STATUS: No Applications are ready

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

Stopping the SAM21 Manager server application

Application

Use this procedure to stop the SAM21 Manager server application on the SPFS-based server that is hosting the CS 2000 Management Tools.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

At your workstation

- 1 Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Verify the status of the SAM21 Manager server application by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

If SAM21EM is	Do
running	step 3
not running	step 5

- 3 Stop the SAM21EM server application by typing

```
# servstop SAM21EM
```

and pressing the Enter key.

- 4 Verify the SAM21EM server application stopped by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

Example response:

```
Executing: /opt/servman/bin/servquery -status  
-group SAM21EM
```

```
Succession SAM21 Element Manager version:  
SAM21EM_9_020_0
```

```
Current status of the Succession SAM21 Element  
Manager:
```

```
    SNMP Access Gateway is not running.
```

```
    SAM21 Element Manager Server is not running.
```

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

Configuring an SPFS-based client server to use PAM Radius

Application

Use this procedure to configure an SPFS-based client server to use PAM Radius, which uses the Integrated Element Management System (IEMS) central security server.

ATTENTION

You must perform this procedure on SPFS-based client servers after an upgrade if you were using the IEMS central security server for authentication prior to the upgrade and want to continue using the IEMS central security server for authentication.



CAUTION

System corruption

Do not execute this procedure on an SPFS-based server that is hosting the IEMS whether the IEMS is standalone or co-resident with the CS 2000 Management Tools. Executing this procedure on an SPFS-based server that is hosting the IEMS will have negative consequences.

Following is a list of SPFS-based client servers on which you can execute this procedure:

- CS 2000 Management Tools (without the IEMS)
- base and midtier servers of the Media Gateway 9000 manager
- Core and Billing Manager (CBM)

Prerequisites

The following prerequisites apply to this procedure:

- You have applied all the current patches.
- You have root user privileges.

Action

Perform the steps that follow to complete this procedure.

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the inactive server using the physical IP address of the inactive server, and ensure you are on the inactive server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Access the command line interface by typing

`# cli`

and pressing the Enter key.
- 3 Enter the number next to the “Configuration” option in the menu.
- 4 Enter the number next to the “Security Services Configuration” option in the menu.
- 5 Enter the number next to the “Security Server Location Configuration” option in the menu to configure the IEMS security server.
- 6 Enter the number next to the “security_server_ip (Configure Security Server IP)” option in the menu.
- 7 When prompted, enter the physical IP address of the SPFS-based server that is hosting the IEMS, or press the Enter key to accept the default value if one is specified. In a two-server configuration, enter the cluster IP address.
- 8 When prompted, enter the Fully Qualified Domain Name (FQDN) of the SPFS-based server that is hosting the IEMS, or press the Enter key to accept the default value if one is specified. In a two-server configuration, enter the SPFS cluster FQDN.
- 9 Accept the IP address and FQDN you just entered by typing

`ok`

and pressing the Enter key.
- 10 Return to the Security Services Configuration level of the CLI by typing

`select - x`

and pressing the Enter key.

- 11 Enter the number next to the “PAM Configuration” option in the menu.
- 12 Enter the number next to the “Central Security Client Configuration” option in the menu.
- 13 Enter the number next to the “pam_radius” option in the menu.
- 14 When prompted, enter the shared secret, or press the Enter key to accept the default value if one is specified.
The shared secret value must match what was entered for the IEMS.
- 15 When prompted, enter the Radius Client timeout (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.
- 16 When prompted, enter the SAML connection timeout, or press the Enter key to accept the default value if one is specified.
- 17 When prompted, enter the SAML request timeout, or press the Enter key to accept the default value if one is specified.
- 18 Accept the settings by typing
ok
and pressing the Enter key.
- 19 Exit each menu level of the command line interface to eventually return to the root level prompt, by typing
`select - x`
and pressing the Enter key.
- 20 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Upgrading the CS2M software

Application

Use this procedure to upgrade the CS 2000 Management (CS2M) software on the server.

Prerequisites

This procedure has the following prerequisites:

- If upgrading from CD, ensure you have the CD that contains the CS2M software for the release you are upgrading to.
- If upgrading through Electronic Software Delivery (ESD), ensure the software has been transferred and mounted onto the server.

For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

Action

Perform the steps that follow to complete this procedure.

At the server console

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

In a two-server configuration, log in to the inactive server and ensure you are on the inactive server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Verify the available disk space by typing

```
# df -k
```

and pressing the Enter key.

Ensure the file systems on the following mount points have the specified minimum of available disk space:

Note: The value under the avail column is the amount of available kilobytes.

- /opt/nortel must have a minimum of 300000 kilobytes of available disk space
- /var must have a minimum of 300000 kilobytes of available disk space
- /tmp must have a minimum of 200000 kilobytes of available disk space

- /var/run must have a minimum of 10000 kilobytes of available disk space
- / (root) must have a minimum of 500000 kilobytes of available disk space

3 Use the following table to determine your next step.

If upgrading from a	Do
directory	step 7
CD	step 4

At the server

4 Insert the CD that contains the CS2M software into the drive. In a two-server configuration, insert the CD into the inactive server.

At the server console

5 Upgrade the CS2M software from the CD by typing

```
# cd /cdrom/cdrom0/bin
```

and pressing the Enter key.

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

6 Proceed to [step 8](#).

7 Upgrade the CS2M software from the directory by typing

```
# cd /tmpmnt/bin/
```

and pressing the Enter key.

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

8 When prompted, confirm you want to upgrade by typing

```
y
```

The system begins the required checks to install the NTQCA package.

9 Use the following table to determine your next step.

If	Do
the system indicates there is enough free space in each of the directories that were checked	step 11

	If	Do
	otherwise	step 10
10	Do not enter a response to the prompt. Contact your next level of support for assistance in cleaning up the directories to ensure the required amount of disk space is available before proceeding.	
11	When prompted to install the NTQCA package, confirm you want to install it by typing y The system installs the NTQCA package, and begins the required checks to install the NTsam21em package.	
12	Use the following table to determine your next step.	
	If	Do
	the system indicates there is enough free space in each of the directories that were checked	step 14
	otherwise	step 13
13	Do not enter a response to the prompt. Contact your next level of support for assistance in cleaning up the directories to ensure the required amount of disk space is available before proceeding.	
14	When prompted to install the NTsam21em package, confirm you want to install it by typing y The system installs the NTsam21em package, and begins the required checks to install the NTsesm package.	
15	Use the following table to determine your next step.	
	If	Do
	the system indicates there is enough free space in each of the directories that were checked	step 17
	otherwise	step 16
16	Do not enter a response to the prompt. Contact your next level of support for assistance in cleaning up the directories to ensure the required amount of disk space is available before proceeding.	

- 17 When prompted to install the NTsesm package, confirm you want to install it by typing
y
The system installs the NTsesm package, and indicates the upgrade of the CS2M software package completed successfully.
- 18 You may observe the following error message at this point:

```
root: /opt/resmon/Hardware/disk_check.ksh: Disk  
or disk mirroring errors: See system alarms for  
details.
```

This is an ignorable error message.
- 19 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Unmounting and removing an ISO image from an SPFS-based server

Application

Use this procedure to perform the following tasks:

- unmount an ISO image on the SPFS-based server
- remove an ISO image from the SPFS-based server

Prerequisites

Determine the node, active or inactive, on which this procedure needs to be performed.

Action

Unmounting an ISO image on an SPFS-based server

ATTENTION

In a two-server configuration, you will unmount the ISO image on the inactive server with the exception of the APS, Media Server 2000, GWC, SAM21, MG 9000 nodes (cards) ISO images, and Patch Media ISO images, which you will unmount on the active server where you mounted the image file.

At your workstation

- 1 Change out of the /tmpmnt directory to prevent a umount failure by typing
cd /
and pressing the Enter key.
- 2 Access the command line interface to unmount the ISO image by typing
cli
and pressing the Enter key.
- 3 Enter the number next to the option `Other` in the menu.
- 4 Enter the number next to the option `umount_image` in the menu.

- 5 Exit each menu level of the command line interface to eventually return to the root level prompt, by typing
`select - x`
and pressing the Enter key.
You are now ready to remove the ISO image from the server.
- 6 Perform the steps under [Removing an ISO image from an SPFS-based server on page 451](#) to complete this procedure.

Removing an ISO image from an SPFS-based server

ATTENTION

In a two-server configuration, you will remove the ISO image from the active server.

At your workstation

- 1 Use the following table to determine your first step.

If	Do
you have a two-server configuration	step 2
otherwise	step 4

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

If	Do
you are removing the APS, Media Server 2000, GWC, SAM21, MG 9000 nodes (cards) ISO image, or Patch Media ISO image	step 4
otherwise	step 3

- 3 Establish a connection to the active server through telnet or SSH using the physical IP address of the active server, log in using the root user ID and password, and ensure you are on the active server using the `ubmstat` command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 4 Navigate to the directory where the ISO image is located by typing
 # **cd <directory_path>**
 and pressing the Enter key.
 where
 directory_path
 is /swd, /gwc, or /data/esd_iso
 List the contents of the directory:
 # **ls**
- 5 Remove the ISO image from the server by typing
 # **rm <loadname>**
 and pressing the Enter key.
- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Verifying group IDs and user IDs defined on the system

Application

Use this procedure prior to installing the IEMS on the SPFS-based server that is hosting the CS 2000 Management Tools (CMT), to determine whether any group identifiers (GID) or user identifiers (UID) defined on the system, conflict with the GIDs and UIDs required for the IEMS installation.

ATTENTION

It is necessary to perform this procedure prior to installing IEMS in an existing network as the IEMS installation expects certain GIDs and UIDs to be free. If those GIDs and UIDs are not free, the IEMS installation will fail.

Prerequisites

There are no prerequisites for this procedure.

Action

At your workstation

- 1 Log in to the SPFS-based server that is hosting CS 2000 Management Tools server.

In a two-server configuration, log in to the active server and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Display all GIDs that exist on the system by typing

```
$ cut -f1,3 -d':' /etc/group
```

and pressing the Enter key.

- 3 From the system output, record any groups that are not in the list that follows. Groups that are not in the list that follows, are user-defined groups.

admin, emsadm, emsmtc, emsro, emsrw, emssprov, lnadm, lnmtc, lnro, lnrw, lnsprov, mgadm, mgcadm, mgcmtec, mgcro, mgcrw, mgcsprov, mgmtc, mgro, mgrw, mgsprov, secadm, secmtc, secro, secrw, secsprov, succssn, trkadm, trkmtc, trkro, trkrw, trksprov, nortel, nt120-nt180, maint2, data, sshd, oinstall, dba, maint, passthru, and users

- 4 If you recorded any user-defined groups, note those that have a GID number in the 10, 100, or 1000 range.

User-defined groups that have a GID number in the 10, 100, or 1000 range need to be moved to a different GID value before starting the IEMS installation.

Note: The following Solaris default groups must not be moved: staff(10), daemon(12), and sysadmin(14).

- 5 Report any user-defined groups that have a GID number in the 10, 100, or 1000 range to Nortel Technical Support, who will assist in moving each group to a different GID, and updating the impacted file systems to reflect the new GID.

- 6 Display all UIDs that exist on the system by typing

```
# cut -f1,3 -d':' /etc/passwd
```

and pressing the Enter key.

- 7 From the system output, record any users that are not in the list that follows. Users that are not in the list that follows, are user-defined users.

root, daemon, bin, sys, adm, lp, uucp, nuucp, listen, nobody, noaccess, nobody4, sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, nortel, oracle, coadm, smmsp, bkmgrusr, Administrator, and nt120 through to nt220.

- 8** If you recorded any user-defined users, note those that have a UID number below 50000.

User-defined users that have a UID number below 50000 need to be moved to a different UID value before starting the IEMS installation.
- 9** Report any user-defined users that have a UID number below 50000 to Nortel Technical Support, who will assist in moving each user to a different UID, and updating the impacted file systems to reflect the new UID.
- 10** You have completed this procedure. If applicable, return to the higher level task or procedure that directed you to this procedure.

Returning a server to a cluster

Application

Use this procedure to return a server to a cluster. A cluster refers to a Sun Netra 240 server pair

ATTENTION

Only perform this procedure when directed to do so.

Prerequisites

You need access to the inactive server of the cluster to start this procedure.

Action

At your workstation

- 1 Establish a connection to the inactive server through telnet or SSH, log in using the root user ID and password, and ensure you are on the inactive server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Access the command line interface by typing

`# cli`

and pressing the Enter key.
- 3 Enter the number next to the Configuration option in the menu.
- 4 Enter the number next to the Cluster Configuration option in the menu.
- 5 Enter the number next to the join_cluster option in the menu.
- 6 Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

`select - x`

and pressing the Enter key.
- 7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Stopping a cluster

Application

Use this procedure to stop a cluster. A cluster refers to a Sun Netra 240 server pair.

ATTENTION

Only use this procedure when directed to do so.

Prerequisites

You must perform this procedure on the active server.

Action

Perform the steps that follow to complete this procedure.

At the server connected to the active server

- 1 Log in to the active server through the console (port A) using the root user ID and password, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Stop the cluster by typing

init 0

and pressing the Enter key.

The active server is taken down to the OK prompt and the standby (inactive) server takes over and starts providing OAM&P services as the new active server.

Note: The high-availability (HA) cluster can take up to approximately 2 hours to failover and bring up the standby server to active state.

At the console connected to the newly active server

- 3 Log in to the newly active server through the console (port A) using the root user ID and password, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 4 Verify the failover status by typing

```
# ubmstat -m
```

and pressing the Enter key.

The failover is complete once the response to this command is as follows:

```
Group      State
-----
ClusterIndicatorACT
```

```
Monitor    State
-----
ClusterIndicatorMonitorOnUnit0UNREG
ClusterIndicatorMonitorOnUnit1ACT
```

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

Starting the SESM server application

Application

Use this procedure to start the Succession Element and Subelement Manager (SESM) server application on the SPFS-based server.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

At your workstation

- 1 Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Verify the status of the SESM server application by typing
servman query -status -group SESMSERVICE
and pressing the Enter key.

If the response indicates	Do
not running	step 3
running	step 6

- 3 Start the SESM server application by typing
servstart SESMSERVICE
and pressing the Enter key.
- 4 Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.

- 5 Verify the SESM server application started as follows:
 - a Verify the SESM services started by typing

```
# servman query -status -group SESMService
```

and pressing the Enter key.

Example response:

```
CS2K Management Tools are running
```
 - b Verify the SESM applications started by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS -----
```

COMPONENT	STATUS
-----	-----
Proxy Agent	RUNNING
RMI Regisry	RUNNING
Snmpfactory	RUNNING
MI2 Server	RUNNING

Current number of SESM processes running: 4 (of 4)

SESM APPLICATION STATUS: All Applications Ready
- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Starting the SAM21 Manager server application

Application

Use this procedure to start the SAM21 Manager server application on the SPFS-based server that is hosting the CS 2000 Management Tools.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Verify the status of the SAM21 Manager server application by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

If SAM21EM is	Do
not running	step 3
running	step 5

- 3 Start the SAM21EM server application by typing

```
# servstart SAM21EM
```

and pressing the Enter key.

- 4 Verify the SAM21EM server application started by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

Example response:

```
Executing: /opt/servman/bin/servquery -status  
-group SAM21EM
```

```
Succession SAM21 Element Manager version:  
SAM21EM_9_020_0
```

```
Current status of the Succession SAM21 Element  
Manager:
```

```
    SNMP Access Gateway is running.
```

```
    SAM21 Element Manager Server is running.
```

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

Starting the IEMS server application

Application

Use this procedure to start the IEMS server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

At your workstation

- 1 Log in to the server by typing

> **telnet <server>**

and pressing the Enter key.

where

server

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

Note: In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

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

- 3 Change to the root user by typing

\$ **su - root**

and pressing the Enter key.

- 4 When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the Active server.

- 5 Verify the status of the IEMS server application by typing

```
# servman query -status -group IEMS
```

If IEMS is	Do
not running	step 6
running	you have completed this procedure

- 6 Start the IEMS server application by typing

```
# servstart IEMS
```

and pressing the Enter key.

- 7 Wait approximately 3 to 5 minutes before you proceed to the next step to allow the IEMS server application to start.

- 8 Verify that IEMS, WEBSERVER, WEBSERVICES, DATABASE, RADSVR and IS are running by typing the following command:

```
servquery -status all
```

and pressing the Enter key.

Example response

APP NAME	STATUS
=====	=====
CINOTIFIER	RUNNING
DATABASE	RUNNING
IS	RUNNING
BOOTP	RUNNING
WEBSERVER	RUNNING
CORBA	RUNNING
OMPUSH	RUNNING
WEBSERVICES	RUNNING
ORA_AUTO_BACKUP	RUNNING
DELEGATE	RUNNING
ORA_ARCHIVE_ROTATOR	RUNNING
PROP_SRV	RUNNING

IEMS	RUNNING
SNMP_POLLER	RUNNING
RADSVR	RUNNING

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

If	Do
all applications are running	step 12
otherwise	step 10

- 10** Start each application that is not running by typing
servstart <app_name>
and pressing the Enter key.

where

app_name

is the name of the application that is not in a RUNNING state, for example, IEMS

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

If	Do
all applications started	step 12
otherwise	contact your next level of support

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

Upgrading APS software

Application

Use this procedure to upgrade the APS software from release APS10 ((I)SN08) to APS11 ((I)SN09) on the same SPFS-based server as the CS 2000 Management Tools.

ATTENTION

The APS does not have a new software load for SN09U.
Therefore, no upgrade is required from release SN09 to SN09U.

If you encounter any errors during the upgrade, use the APS CLI within the CS 2000 Management Tool server to restore the system provisioning data using the backup media.

If your audio server is a Media Server 2000 Series, refer to one of the following procedures located in *MS 2000 Series Security and Administration*, NN10337-611.

- “Performing an APS-only Data Base Restore from a 4mm DAT”
- “Performing an APS-only Database restore from a CD “
- “Performing a restore of APS audio from 4mm DAT”
- “Performing a restore of APS audio files from a TAR file”

If your audio server is a Universal Audio Server, refer to procedure “Restoring audio files to a UAS node” in *UAS Fault Management*, NN10073-911.

If you use another audio server, refer to the documentation for your audio server for the procedure to restore system provisioning data.

Prerequisites

This procedure has the following prerequisites:

- Ensure you performed a backup of APS audio files and APS oracle data using the applicable procedures listed below:
 - [Performing a backup of APS audio files to tape on page 392](#), which applies to a Sun t1400 server with a DAT drive.
 - [Performing a backup of APS audio files to CD or DVD on page 394](#), which applies to a Sun Netra 240 server with a CD/DVD drive
 - [Performing a backup of APS oracle data to tape on page 396](#), which applies to a Sun t1400 server with a DAT drive.
 - [Performing a backup of APS oracle data to CD or DVD on page 398](#), which applies to a Sun Netra 240 server with a CD/DVD drive
- If upgrading from CD, ensure you have the CD that contains the APS and IPS database software required for an upgrade to release APS11. If upgrading through Electronic Software Delivery (ESD), ensure the software has been transferred and mounted onto the server. If required, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

Action

Perform the steps that follow to complete this procedure.

At the server console

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

In a two-server configuration, log in to the active server and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 List the APS software package and any patches that have been applied:

```
pkginfo | grep aps
```

Example command and system response:

```
pkginfo | grep aps
```

```
application ACaps10 APS10-22.0 Package - /opt/uas/aps.April 19, 2005  
application ACips IPS10-22.0 DB Package which goes into /usr/ntdb/aps10
```


- 3 Remove each package one at a time:
pkgrm ACaps10
Note: ACaps10 is the package identifier shown in the example system response in step [2](#)
- 4 When prompted, indicate you want to remove the aps package:
y
- 5 When prompted, indicate you want to continue with the removal of the package:
y
- 6 Remove the ips package:
pkgrm ACips
Note: ACips is the package identifier shown in the example system response in step [2](#)
- 7 When prompted, indicate you want to remove the ips package:
y
- 8 When prompted, indicate you want to continue with the removal of the package:
y
- 9 Ensure the APS software package and any patches have been removed:
pkginfo | grep aps
There should be no output for this command.
- 10 Use the following table to determine your next step.

If you are upgrading from a	Do
CD	step 11
directory	step 17
- 11 Insert the APS11 CD into the CD-ROM drive.
- 12 Wait approximately 30 seconds for the server to auto mount the CD drive.

- 13** Verify you can see the APS CD in the drive:
df
 Look for /cdrom/<APS CD (mount point)>
 where
 APS CD (mount point)
 is the label of the APS CD and its mount point
- 14** Change directory to where the software is:
cd /cdrom/cdrom0
- 15** List the contents of the directory:
ls
 You will see two loads listed.
- 16** Proceed to [step 19](#).
- 17** Change directory to the directory that contains the software:
cd /tmpmnt
- 18** List the loads:
ls
 You will see two loads listed.
- 19** Install the APS11 software package:
pkgadd -d ACaps11-<xx>.pkg
 where
 xx
 is the APS loadbuild number
- 20** When prompted, indicate you want to install all packages:
all
- 21** Use the following table to determine your next step.

If	Do
the system prompts you about installing conflicting files	step 22
otherwise	step 23

- 22** Indicate you do not want to install these conflicting files:

n

Indicate you want to continue:

y

- 23** When prompted, indicate you want to continue with the installation:

y

- 24** Install the IPS software package:

```
pkgadd -d ACips11-<xx>.pkg
```

where

xx

is the APS loadbuild number

- 25** When prompted, indicate you want to install all packages:

all

If	Do
the system prompts you about installing conflicting files	step 26
otherwise	step 27

- 26** Indicate you do not want to install these conflicting files:

n

Indicate you want to continue by typing

y

- 27** When prompted, confirm you want to continue with the installation:

y

- 28** Change directory:

```
cd /
```

- 29** Run the APS installation script:

```
/start.sh
```

Note: The installation can take approximately 30 minutes to complete.

- 30** Check the apsinst.log for application install errors:
- ```
more /var/log/aps/apsinst.log
```
- 31** Re-source your login shell:
- ```
cd /  
. /etc/profile  
. ./profile
```
- Note:** Ensure there is a space between the two first periods (.) in the last command.
- 32** Verify the database, webserver, webservices, and the APS are running:
- ```
servman query -status all
```
- 33** If the specified applications indicated in the previous step (step [32](#)) are running, proceed to step [35](#), otherwise, proceed to step [34](#)
- 34** Start each of the specified applications, indicated in step [32](#), that is not running:
- ```
servstart <app_name>
```
- where
- app_name**
is the name of an application that is not in RUNNING state, for example, WEBSERVICES
- 35** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Verifying the IEMS upgrade was successful

Application

Use this procedure to verify the upgrade of the Integrated Element Management System (IEMS) was successful.

ATTENTION

If you encounter a problem during any one of the steps in this procedure, contact your next level of support.

Prerequisites

You need the IP address or host name of the SPFS-based server that is hosting the IEMS, and a valid user name and password to launch the IEMS GUI.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2_08 and Java™ Web Start (JWS) version 1.4.2_08 installed to launch the IEMS GUI.

Note: JWS 1.4.2_08 is included as part of JRE 1.4.2_08.

Action

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

At your workstation

- 1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 7

- 2 Log in to the server using telnet by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server
is the IP address or host name of the SPFS-based server,
or the physical IP address of the active server in a
two-server configuration
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Go to [step 9](#).
- 7 Log in to the server using ssh by typing

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

and pressing the Enter key.
where
server
is the IP address or host name of the SPFS-based server,
or the physical IP address of the active server in a
two-server configuration
Note: If this is the first time you are logging in using ssh, the
system will request that you confirm to continue connecting.
Enter **yes** at the prompt.
- 8 When prompted, enter the root password.
- 9 Change directories to where the IEMS diagnostics script is
located by typing

```
# cd /opt/nortel/iems/current/bin
```

and pressing the Enter key.
- 10 Run the IEMS diagnostics script by typing

```
# ./IEMSDiagnostics.sh all
```

and pressing the Enter key.

- 11 Change directories to where the diagnostics results file is output by typing

```
# cd /opt/nortel/iems/current/logs
```

and pressing the Enter key.
- 12 View the diagnostics results file by typing

```
# cat diagnostics.txt |more
```

and pressing the Enter key.
- 13 Use the following table to determine your next step.

If	Do
any one of the tests indicate FAILED	contact your next level of support
otherwise	step 14

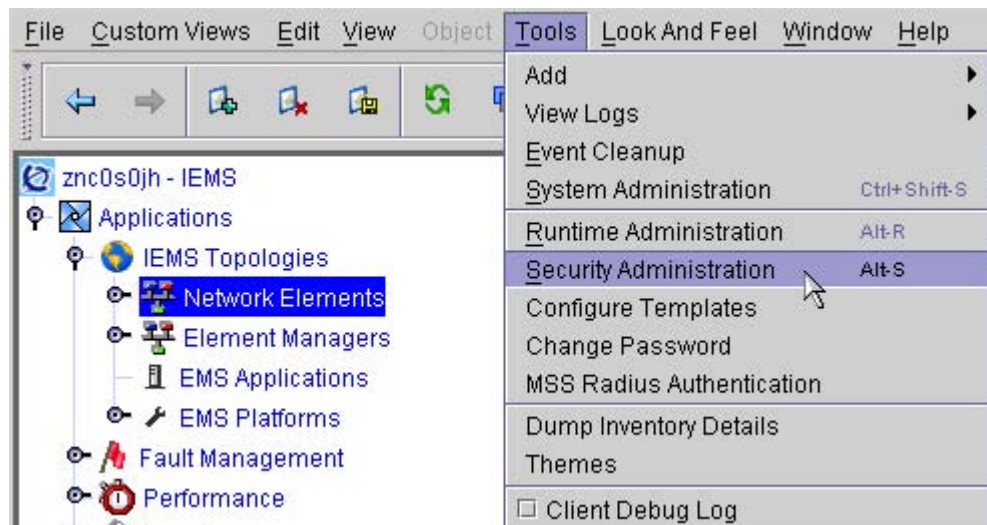
At your workstation

- 14 Clear the Java Web Start Client cache on the client workstation.
For detailed steps, refer to procedure “Clearing the JWS cache on a client workstation” in the *ATM/IP Solution-level Configuration Management document*, NN10409-500.
- 15 Launch the IEMS GUI using the Web Start Client to verify the topology information is present.
For detailed steps to launch the IEMS GUI, refer to procedure “Launching the IEMS Java Web Start Client” in *IEMS Basics*, NN10329-111.

At the IEMS GUI

- 16 Expand the IEMS Topologies tree.
- 17 Click **Network Elements** and ensure all network elements are present in the display panel.
- 18 Click **Element Manager** and ensure all element managers are present in the display panel.
- 19 Click **EMS Platforms** and ensure all EMS platforms are present in the display panel.
- 20 Click **EMS applications** and ensure all EMS applications are present in the display panel.

- 21 Under the Tools menu, select **Security Administration** as shown in the figure that follows.



The Security Administration GUI launches in a separate window.

- 22 Log in to the IEMS GUI using one of the users defined in the Security Administration GUI, and ensure the login is successful.
- 23 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Confirming the upgrade on an SPFS-based server

Application

Use this procedure to accept the upgraded environment permanently.

Note: If you want to fallback to the state prior to the upgrade, refer to procedure [Executing a fallback during an SPFS-based server upgrade on page 418](#)

ATTENTION

Only use this procedure when directed to do so.

Prerequisites

You need root user privileges.

Action

Perform the steps that follow to complete this procedure.

At the server console

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

In a two-server configuration, log in to the newly active server with the upgraded software on it using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Use the following table to determine your next step.

If you choose to	Do
accept the upgraded environment	step 3
rollback to the state prior to the upgrade	refer to procedure Executing a fallback during an SPFS-based server upgrade on page 418

- 3** Accept the upgraded environment by typing
/SSPFS_Upgrade.accept
and pressing the Enter key.
The execution of this step takes approximately 20 minutes to complete depending on system configuration.
- 4** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Cloning the image of one server in a cluster to the other server

Application

Use this procedure to clone the image of the active server in a cluster to the inactive server.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you need console access to the inactive server under the following circumstances
 - this is the first time you clone
 - you replaced the inactive server
 - you executed a reverse restore (that is, you switched unit 0 and 1)

Note: Under any of the previous circumstances, the inactive server will have a different ethernet address from the one retained in the system. Therefore, console access is required to obtain the ethernet address of the inactive server.

For information about console access, refer to [Configuring SPFS console access on page 51](#)

ATTENTION

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

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Establish a connection to the active server through telnet or SSH, and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#)

On the active server

- 2 Access the command line interface to determine the server profile by typing
`# cli`
and pressing the Enter key.
- 3 Enter the number next to the View option in the menu.
- 4 Enter the number next to the sspfs_soft option in the menu.
- 5 In the system response, note the server profile.
- 6 Exit the CLI by typing `x` until you return to the command prompt.
- 7 Use the following table to determine your next step.

If	Do
the Server Profile is cbm850	step 14
otherwise	step 8

- 8 Verify that all applications on the server are running by typing
`# servquery -status all`
and pressing the Enter key.
- 9 Use the following table to determine your next step.

If	Do
all applications are running	step 12
otherwise	step 10

- 10** Start each application that is not running by typing
servstart <app_name>
and pressing the Enter key.
where
app_name
is the name of the application that is not in a RUNNING state, for example, SAM21EM

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

If	Do
all applications started	step 12
otherwise	contact your next level of support

- 12** Verify the Patching Server Element (PSE) server application is running by typing
pse status
and pressing the Enter key.

If	Do
PSE is running	step 14
otherwise	step 13

- 13** Start the PSE server application by typing
pse start
and pressing the Enter key.

If	Do
PSE starts	step 14
otherwise	contact your next level of support

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

If	Do
this is the first time you are cloning the server, or you replaced the server, or you executed a reverse restore (that is, switched unit 0 and unit 1)	step 15
Under any of the previous circumstances, the inactive server will have a different ethernet address from the one retained in the system. Therefore, console access is required to obtain the ethernet address of the inactive server.	
otherwise	step 22

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

If	Do
you do not know the Ethernet address of the inactive server	step 16
otherwise	step 20

At the console connected to the inactive server

- 16** Log in to the inactive server through the console (port A) using the root user ID and password and ensure you are on the inactive server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#)

- 17** If the system is at the OK prompt proceed to [step 18](#), otherwise bring the system to the OK prompt by typing

init 0

and pressing the Enter key.

- 18** At the OK prompt, display the Ethernet address of the inactive server by typing

OK **banner**

and pressing the Enter key.

Example response:

Netra 240, No Keyboard | Copyright 1998-2003 Sun Microsystems, Inc. All rights reserved.
OpenBoot 4.11.4, 2048 MB memory installed,
Serial #56195961.
Ethernet address 0:3:ba:59:7b:79, Host ID:
83597b79.

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

On the active server

20

ATTENTION

If you receive timeout errors during the execution of the clone, enter the **# finishb** command, and repeat this step.

Start the cloning process on the active server by typing

startb <Ethernet address>

and press the Enter key.

where

Ethernet address

is the Ethernet address of the inactive server

If it is necessary to interrupt the **startb** process, execute the **finishb** command before proceeding.

- 21** Proceed to [step 23](#).

On the active server**22****ATTENTION**

If you receive timeout errors during the execution of the clone, enter the **# finishb** command, and repeat this step.

Start the cloning process on the active server by typing

startb

and press the Enter key.

If it is necessary to interrupt the **startb** process, execute the **finishb** command before proceeding.

23

Use the following table to determine your next step.

If	Do
the system prompts you to enter the command "boot net - image"	step 24
the system prompts you for the Ethernet address	step 16
otherwise	step 28

24

Connect to the console port of the inactive server.

If the console displays the	Do
login prompt	step 25
OK prompt	step 27

At the console connected to the inactive server**25**

Log in to the inactive server using the root user ID and password.

26

Bring the system to the OK prompt by typing

init 0

and pressing the Enter key.

- 27** At the OK prompt, boot the inactive server from the image of the active server by typing

OK **boot net - image**

and press the Enter key.

Note: There must be a space between the “-” and “image”.

Example response

```
SC Alert: Host System has Reset
Sun Fire V240, No Keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.
Rebooting with command: boot net - image
.
.
.
SC Alert: Host System has Reset
```

On the active server

- 28** Monitor the progress of the cloning from the active server. Cloning the inactive server takes approximately 40 minutes to complete, but the time can vary depending on system configuration.

Example response:

```
Waiting for network response from unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning: /export/d2
.
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become
normal.
Jun 27 16:01:38 ucary0883c unix: /data: active up
repair - standby reflected (normal)
Deleted snapshot 2.
Deleted snapshot 1.
Deleted snapshot 0.
ucary0883c-unit0(active):/>
```

- 29** Once cloning is complete, wait approximately 5 minutes before you proceed to the next step.

On the active server

- 30** Verify the status of replicated disk volumes on the active server by typing

udstat

and pressing the Enter key.

If	Do
all file systems are ACTIVE normal UP clean	step 31
otherwise	contact your next level of support

At your workstation

- 31** Establish a connection to the inactive server through telnet or SSH, and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#)

On the inactive server

- 32** Verify the status of replicated disk volumes on the inactive server by typing

udstat

and pressing the Enter key.

If	Do
all file systems are STANDBY normal UP clean	step 33
otherwise	contact your next level of support

- 33** You have completed this procedure. If applicable, return to the highlevel task or procedure that directed you to this procedure.

Stopping the PSE server application on an SPFS-based server

Application

Use this procedure to stop the Patching Server Element (PSE) server application on a Server Platform Foundation Software (SPFS)-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION In a two-server configuration, perform the steps that follow on the active server.

At your workstation

- 1 Establish a login session to the server, using one of the following methods:

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

- 2 Log in to the server using telnet (unsecure) as follows:

- a Log in to the server by typing

> telnet <server>

and pressing the Enter key.

where

server

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

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step [4](#).

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server

is the IP address or host name of the SPFS-based server, or the physical IP address of the active server

Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter `yes` at the prompt.

b When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

4 Stop the PSE server application by typing

```
# pse stop
```

and pressing the Enter key.

- 5 Verify the PSE server application stopped by typing
 # pse status
 and pressing the Enter key.
- 6 You have completed this procedure. If applicable, return to the
 high level task or procedure that directed you to this procedure.

Starting the PSE server application on an SPFS-based server

Application

Use this procedure to start the Patching Server Element (PSE) server application on a Server Platform Foundation Software (SPFS)-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

At your workstation

- 1 Establish a login session to the server, using one of the following methods:

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

- 2 Log in to the server using telnet (unsecure) as follows:

- a Log in to the server by typing

> **telnet** <server>

and pressing the Enter key.

where

server

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

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step [4](#).

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server

is the IP address or host name of the SPFS-based server, or the physical IP address of the active server

Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter `yes` at the prompt.

b When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

4 Start the PSE server application by typing

```
# pse start
```

and pressing the Enter key.

- 5 Verify the PSE server application started by typing
 # pse status
 and pressing the Enter key.
- 6 You have completed this procedure. If applicable, return to the
 high level task or procedure that directed you to this procedure.

Configuring NPM for automatic patch file delivery

Application

Use this procedure to configure the Network Patch Manager (NPM) for automatic patch file delivery, which consists of configuring the Patch File Receipt System (PFRS). You can configure PFRS using one of the following two NPM interfaces:

- [Using the NPM CLUI](#)
- [Using the NPM GUI](#)

Once the PFRS is configured, patches are automatically delivered to the NPM database and retrieved for processing on a daily basis.

An option is provided to delete patch files from the drop-off server after they have been retrieved.

Prerequisites

To configure the PFRS, you need the following information:

- the hostname or IP address of the patch file drop-off server
- the user ID and password to connect to the patch file drop-off server

Action

Perform the following steps to complete this procedure.

Using the NPM CLUI

At your workstation

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

At the NPM CLUI

- 2 Configure the PFRS by typing

```
npm> setpfrs <drop-off server> <userID> <delete patches>
```

and pressing the Enter key.

where

drop-off server

is the IP address or hostname of the drop-off server where patch files are to be delivered

userID

is the user ID that will be used to connect to the drop-off server

delete patches

is either Y or N to indicate whether you want the patch files to be deleted from the drop-off server after they have been retrieved

Note: The user ID must have read, write, and overwrite privileges in the FTP user's default directory on this server.

Example response:

Enter password for drop box:

- 3 When prompted, enter the password associated with the user ID that will be used to connect to the drop-off server.

Example response:

```
WARNING: You are about to set/reset the Patch  
File Retrieval System settings. If these values  
are incorrect they may interfere with automatic  
delivery of patches to this site.
```

```
Do you wish to continue Yes (Y) or N (N)?
```

- 4 When prompted, confirm you want to continue if acceptable by typing

y

and pressing the Enter key.

- 5 Review the PFRS settings if required by typing
`npm> viewpfrs`
and pressing the Enter key.
- 6 Enable the genreport plan by typing
`npm> enableplan genreport`
and pressing the Enter key.
Ensure that the response is:
`Plan enabled successfully.`
If you receive any other response, contact your next level of support.
- 7 Check the plan status for genreport by typing
`npm> vplan genreport`
and pressing the Enter key.
The value for **Enabled** must be set to **Y**.
Expected response

```
Name           : GENREPORT
Description    : PFRS Inform list report
generation
Status        : SCHED
Enabled       : Y
Frequency     : Daily
Execute Time  : Wed Jan 25 12:00:00 GMT-03:00
2006
Max Execut Time: No_Limit
Tasks/Reports : [TASK:PFRSGENREPORT]
System Defined : true
```


If genreport is not enabled, contact your next level of support.
- 8 Enable the getpatch plan by typing
`npm> enableplan getpatch`
and pressing the Enter key.
Ensure that the response is:
`Plan enabled successfully.`
If you receive any other response, contact your next level of support.

9 Check the plan status for getpatch by typing

npm> **vplan getpatch**

and pressing the Enter key.

The value for **Enabled** must be set to **Y**.

Expected response

```
Name           : GETPATCH
Description     : Patch file retrieval
Status         : SCHED
Enabled        : Y
Frequency      : Daily
Execute Time   : Thu Jan 26 01:00:00 GMT-03:00
                2006
Max Execut Time: No_Limit
Tasks/Reports  : [TASK:PFRSGETPATCH]
System Defined : true
```

If getpatch is not enabled, contact your next level of support.

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

Using the NPM GUI

At your workstation

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

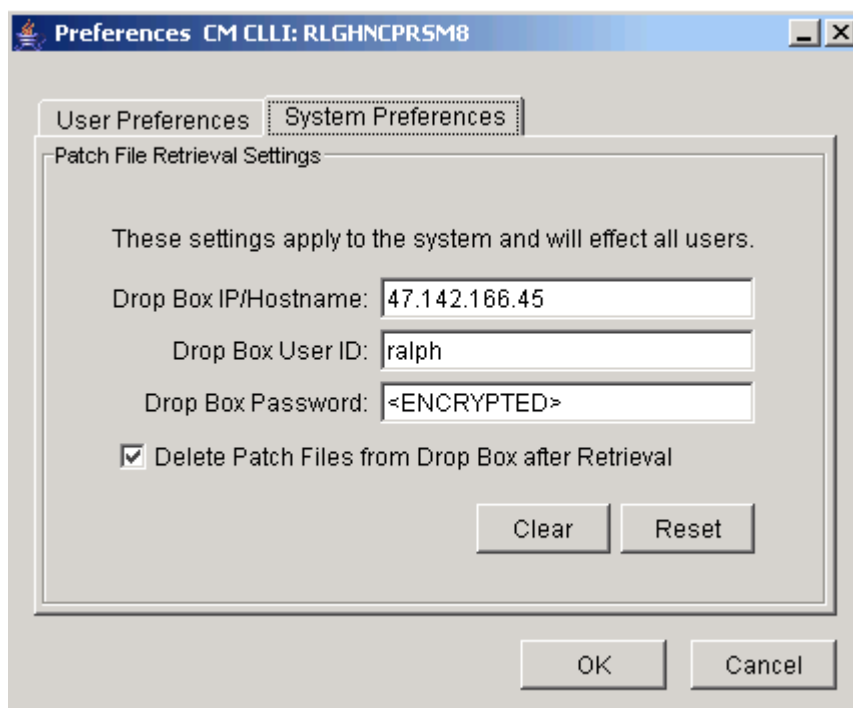
At the NPM GUI

- 2 On the Edit menu, click **Preferences....**



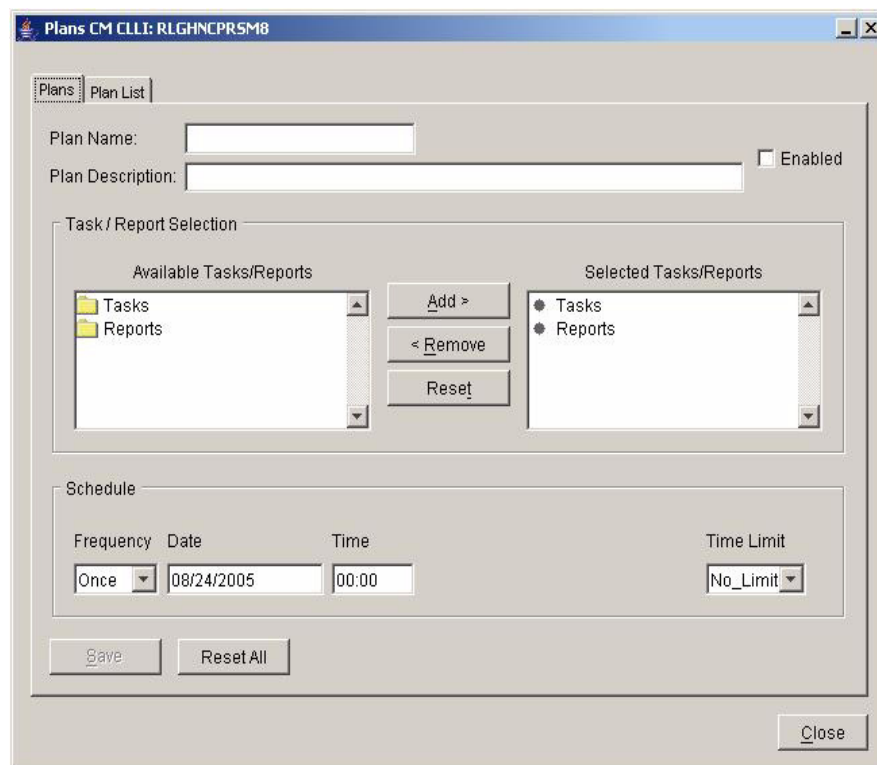
The Preferences window is displayed.

- 3 Click the **System Preferences** tab.



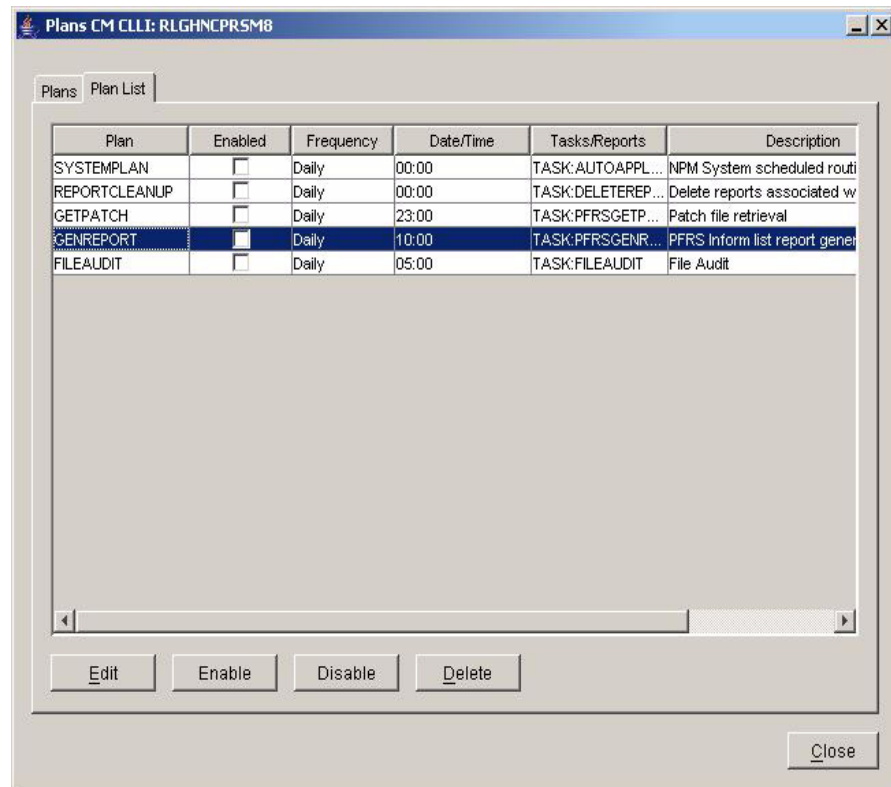
- 4 In the Drop Box IP/Hostname field, enter the host name or IP address of the drop-off server where patch files are to be delivered.

- 5 In the Drop Box User ID field, enter the user ID that will be used to connect to the drop-off server.
Note: The user ID must have read, write, and overwrite privileges in the FTP user's default directory on this server.
- 6 In the Drop Box Password field, enter the password associated with the user ID that will be used to connect to the drop-off server.
- 7 Click the Delete Patch Files from Drop Box after Retrieval box if you want the patch files to be deleted from the drop-off server after they have been retrieved, otherwise, leave it blank.
- 8 Click **OK** to complete the PFRS configuration.
- 9 On the System menu, select **Plans....**



The Plans window is displayed.

- 10 Click **Plan List** tab.



The Plan List window is displayed.

- 11 Select the GENREPORT task and click **Edit**.

The screenshot shows a window titled "Plans CM CLI: RLGHNCPRSM8" with a "Plans" tab and a "Plan List" sub-tab. The "Plan Name" field contains "GENREPORT". The "Plan Description" field contains "PFRS Inform list report generation". An "Enabled" checkbox is checked. Below this is a "Task / Report Selection" section with two lists: "Available Tasks/Reports" and "Selected Tasks/Reports". The "Available" list contains "Tasks" and "Reports". The "Selected" list contains "Tasks" and "Reports". Between the lists are buttons for "Add >", "< Remove", and "Reset". Below the selection section is a "Schedule" section with "Frequency" set to "Daily" and "Time" set to "10:00". The "Time Limit" is set to "No_Limit". At the bottom are "Save" and "Reset All" buttons. A "Close" button is in the bottom right corner.

- 12 Click the Enabled checkbox, verify the schedule for the plan, and then click **Save**.
- 13 Repeat [step 10](#) through to [step 12](#) but select the GETPATCH task this time.
- 14 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Restoring NPM patch files

Application

Use this procedure to restore NPM patch files on the server.

Note: NPM patch files saved to a location on disk are preserved over an upgrade. However, if for some reason you need to restore those patch files, contact your next level of support.

Prerequisites

This procedure has the following prerequisites:

- for a Sun Netra t1400, you need the NPM patch file archive tape
- for a Sun Netra 240, you need the NPM patch file archive CD or DVD

Action

Perform the steps using one of the following methods to complete this procedure:

- [Restoring NPM patch files from tape \(Sun Netra t1400 only\) on page 501](#)
- [Restoring NPM patch files from CD/DVD \(Sun Netra 240 only\) on page 502](#)

Restoring NPM patch files from tape (Sun Netra t1400 only)

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Stop the NPM server application if it is running. If required, refer to procedure “Stopping the NPM server application” in document *ATM/IP Security and Administration*, NN10402-600.
- 3 Re-initialize the NPM database. If required, refer to procedure “Initializing the NPM database” in document *ATM/IP Security and Administration*, NN10402-600.
- 4 Insert the NPM patch file archive tape into the drive.

- 5 Rewind the tape by typing
 # **mt rewind**
 and pressing the Enter key.
- 6 Access the NPM patch file directory by typing
 # **cd /data/npm/Au**
- 7 Restore the NPM patch files to the /data/npm/Au directory by typing
 # **tar tvf /dev/rmt/0**
 and pressing the Enter key.
- 8 Rewind and eject the tape by typing
 # **mt offline**
 and pressing the Enter key.
- 9 Remove the tape from the drive.
- 10 Start the NPM server application. If required, refer to procedure “Starting the NPM server application” in document *ATM/IP Security and Administration*, NN10402-600.
- 11 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Restoring NPM patch files from CD/DVD (Sun Netra 240 only)

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

 In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

 For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Stop the NPM server application if it is running. If required, refer to procedure “Stopping the NPM server application” in document *ATM/IP Security and Administration*, NN10402-600.
- 3 Re-initialize the NPM database. If required, refer to procedure “Initializing the NPM database” in document *ATM/IP Security and Administration*, NN10402-600.
- 4 Insert the NPM patch file archive CD/DVD into the drive.

- 5 Copy the NPM patch files to the /data/npm/Au directory by typing
cp /cdrom/patches/*.ptch* /data/npm/Au/
and pressing the Enter key.
- 6 Eject the CD or DVD from the drive as follows:
 - a Ensure you are at the root directory level by typing
cd /
and pressing the Enter key.
 - b Eject the CD by typing
eject cdrom
and pressing the Enter key.

Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:
/etc/init.d/volmgt stop
/etc/init.d/volmgt start
Then, press the eject button located on the front of the DVD drive.
 - c Remove the CD or DVD from the drive.
- 7 Start the NPM server application. If required, refer to procedure “Starting the NPM server application” in document *ATM/IP Security and Administration*, NN10402-600.
- 8 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Installing the QCA software package on a separate server

Application

Use this procedure if you want to install the QCA software package on a separate server. In doing so, you will be able to perform in-service upgrades with no loss of records.

Note: Adding another QCA instance in the network requires that the GWC be associated with that QCA. Refer to document *GWC Configuration Management*, NN10205-511, for instructions on how to associate a QoS collector to a GWC.

Prerequisites

The server on which you want to install QCA, must be running the latest release of the Server Platform Foundation Software (SPFS).

Action

Perform the following steps to complete this procedure.

At your workstation

- 1 Establish a connection to the server where the first instance of QCA is running, through telnet or SSH, and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Send the NTQCA.pkg to the other server running SPFS, through FTP.
- 3 Establish a connection to that other server running SPFS through telnet or SSH, and log in using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 4 Install the QCA software package by typing

```
# pkgadd -d NTQCA.pkg
```

and pressing the Enter key.

To configure QCA, refer to procedure “Modifying the QoS Collector Application” in document *ATM/IP Configuration Management*, NN10409-500.

- 5 If you have not started the QoS Collector Application (QCA), yet, start the QCA.

For detailed steps, refer to procedure “Starting the QoS Collector Application” in document *ATM/IP Security and Administration*, NN10402-600.
- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Verifying the CS2M upgrade was successful

Application

Use this procedure to verify the upgrade of the CS 2000 Management Tools was successful.

Prerequisites

The CS2M software has been upgraded.

Action

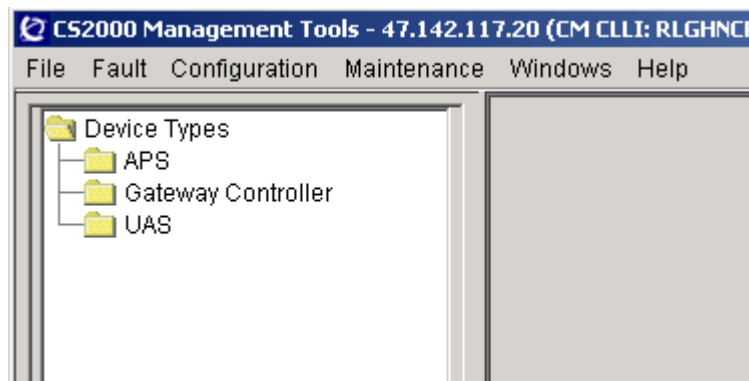
Perform the following steps to complete this procedure.

ATTENTION

If you encounter a problem during any one of the steps in this procedure, contact your next level of support. If required, refer to section “Downgrading the CS 2000 Management Tools software” in document *ATM/IP Fault Management*, NN10408-900.

At your workstation

- 1 Launch the CS2000 Management Tools application GUI.
For detailed steps, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).
Ensure the topology is displayed correctly as shown in the figure that follows.
This verifies correct restoration of the database.



- 2 Click **GatewayController**, then select a GWC from the list, and ensure correct maintenance states are displayed for the active and inactive units as shown in the figure that follows.

This verifies GWC SNMP communication.

GWC-6 Unit 0: 47.142.128.66
Unit 1: 47.142.128.67

Maintenance Provisioning

GWC-6-UNIT-0

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	providingService(3)
Activity state:	active(1)	Swact state:	manualSwActCold(2)
Isolation state:	notisolated(2)	Alarm state:	major(2) , alarmOutstanding(4)
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	PGC09AL		

Save Image Busy (Disable) RTB (Enable) Card View

GWC-6-UNIT-1

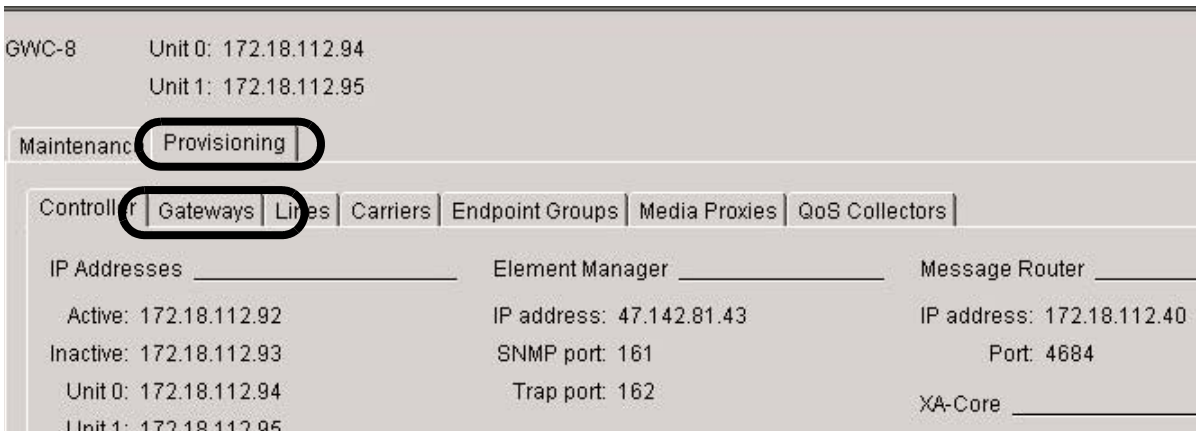
Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	hotStandby(1)
Activity state:	standby(2)	Swact state:	manualSwActWarm(1)
Isolation state:	notisolated(2)	Alarm state:	major(2) , alarmOutstanding(4)
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	PGC09AL		

Save Image Busy (Disable) RTB (Enable) Card View

☐ Force Warm Swact Cold Swact

- 3 Click the **Provisioning** tab, then the **Gateways** tab as shown in the figure that follows, and then click **Retrieve All** to retrieve all subtending gateways.

This verifies correct restoration of the database.



- 4 Under the Provisioning tab, select the **QoS Collectors** tab.
Click the **Associate** button to associate Qos on the GWC. Datafill the pop up menu fields. Select this newly added entry and click **OK**.
Verify the QoS gets associated and you can view the entry in the QoS Collector tab. Select the entry you just added and click **Disassociate** to disassociate QoS provisioning on the GWC.
- 5 Click the **Maintenance** tab, then click **Card View** to launch the CS 2000 SAM21 Manager card view.
This verifies correct operation of the CS 2000 SAM21 Manager application GUI.
- 6 From the **Fault** menu, select **Alarm Manager** as shown in the figure that follows, and verify alarms show up when a maintenance attempt is performed on a GWC unit.



- 7 Connect to OSSGate.

- For detailed steps, refer to procedure “Connecting to OSSgate” in document *ATM/IP Security and Administration*, NN10402-600.
- 8** Query a provisioned line (line solutions) or trunk (trunk solutions).
- For detailed steps, refer to the corresponding procedures in document *OSSgate User's Guide*, NE10004-512.
- This verifies the SDM OSS APS, DDMS, and core communication path.
- 9** For line solutions, launch the line maintenance manager (LMM) application GUI.
- For detailed steps, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).
- 10** Post, busy, and return a line to service.
- For detailed steps, refer to the corresponding procedures in document *ATM/IP Fault Management*, NN10408-900.
- This verifies the SDM - DMA, BMI, and core communication path.
- 11** For trunk solutions, launch the trunk maintenance manager (TMM) application GUI.
- For detailed steps, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).
- 12** Post, busy, and return a trunk to service.
- For detailed steps, refer to associated procedures in document *ATM/IP Fault Management*, NN10408-900.
- This verifies the SDM - DMA, BMI, and core communication path.
- 13** If you did not start the Network Patch Manager (NPM) GUI in any of the previous procedures, start it now to verify it is functional.
- For detailed steps, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).
- 14** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Verifying the APS upgrade was successful

Application

Use this procedure to verify the upgrade of the Audio Provisioning Server (APS) was successful.

Prerequisites

You need the IP address or host name of the SPFS-based server that is hosting the APS, and a valid user name and password to launch the APS GUI.

Action

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

At your workstation

- 1 Launch your web browser.
- 2 In the Address field enter
http://<server>:8080/aps/
where
server
is the IP address or host name of the SPFS-based server
where the APS resides
- 3 Enter a valid user ID and password.
- 4 Use the following table to determine your next step.

If	Do
the APS GUI launches	step 19
otherwise	step 5

At the CS 2000 Management Tools server

- 5 Log in to the CS 2000 Management Tools server that is hosting the APS, using the root user ID and password.

In a two-server configuration, log in to the active server and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 6 Access the APS command line interface by typing

```
# apsc1i
```

- 7 Enter the number next to the Restart APS Server Processes option in the menu.

At your workstation

- 8 Wait approximately 3 minutes, and log in to the APS GUI ([step 1](#) to [step 3](#)).

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

If	Do
the APS GUI launches	step 18
otherwise	step 10

At the CS 2000 Management Tools server

- 10 Enter the number next to the Database Queries, Reports, Status, Checks option in the menu.

- 11 Enter the number next to the Modify Passwords option in the menu.

- 12 Enter the number next to the Reset Lion Password option in the menu.

At your workstation

- 13 Wait approximately 3 minutes, and log in to the APS GUI ([step 1](#) to [step 3](#)).

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

If	Do
the APS GUI launches	step 18
otherwise	step 15

At the CS 2000 Management Tools server

- 15 Exit the APS command line interface by typing

x

- 16 Check the APS log files by typing

cd /var/log/aps

more <log file>

log file

is the name of the APS log file

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

If	Do
you can determine the nature of the problem from the information in the log files and can rectify it	rectify the problem, and return to step 1 of this procedure
otherwise	stop this procedure and contact your next level of support

At the CS 2000 Management Tools server

- 18 Exit the APS command line interface by typing

x

At the APS GUI

- 19 Click **Administration** to display the APS Administration tool.

- 20 Expand the Nodes tree, and ensure all Media Server nodes are present.

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

If	Do
all Media Server nodes are present	step 22
otherwise	Refer to procedure "Restoring the APS-specific Oracle database and application files" in <i>ATM/IP Solution-level Security and Administration</i> , NN10402-600

- 22 Click the **Back** button of the web browser to return to the GUI menu.
- 23 Click **Audio Management** to display the Audio Management Tool.
- 24 In the Physical Segments panel, click **Refresh**, and ensure the audio segments appear.
- 25 Use the following table to determine your next step.

If	Do
the audio segments are displayed	step 26
otherwise	Refer to procedure "Restoring the APS-specific Oracle database and application files" in <i>ATM/IP Solution-level Security and Administration</i> , NN10402-600

- 26 Click the **Back** button of the web browser to return to the GUI menu.
- 27 Click **Logout** to exit the APS GUI.
- 28 Repeat [step 3](#) and [step 27](#) using other user accounts including the admin user account to ensure proper login.
- 29 Use the following table to determine your next step.

If	Do
you can log in using other user accounts including the admin user account	step 30
otherwise	Refer to procedure "Restoring the APS-specific Oracle database and application files" in <i>ATM/IP Solution-level Security and Administration</i> , NN10402-600

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

Installing Using ESD

You can use a PC or Solaris to install the USP software. The following procedure is required to load the installation files onto the respective platforms.

Prerequisites

At least 500 MBytes must be available on the destination system to accommodate the USP install.

The workstation must be equipped with an FTP client application, such as WS FTP Pro or WinSCP, that supports the recursive transfer of directory structures.

Action

Perform the following tasks in the order they are presented, to prepare for a USP software installation:

- [Uncompressing the load on the ESD load repository server](#)
- [Transferring the uncompressed file to the CMT](#) or [Transferring the uncompressed file to Windows](#)

Uncompressing the load on the ESD load repository server

At the ESD load repository server

- 1 Log in to the ESD load repository server, and change directory to the drop box location.

Note: Ensure you log in with a user ID that has permission to uncompress files.

- 2 List the contents of the drop box.

```
ls *.gz
```

- 3 Locate the file you want to uncompress.

- 4 Uncompress the file.

```
gzip -d <esd_filename>.tar.gz
```

where

esd_filename

is the name of the ESD software load, for example,
USP11.1.0.NCL.NAP.VAULT.1.D

- 5 List the uncompressed file.

```
ls *.tar
```

- 6 Unpack the file.
tar -xvf <esd_filename>.tar
where
 esd_filename
 is the name of the ESD software load, for example,
 USP11.1.0.NCL.NAP.VAULT.1.D

The unpacked file is a directory that contains the USP
installation software, for example
USP11.1.0.NCL.NAP.VAULT.1.D.
- 7 Change to the directory that contains the USP installation
software.
cd <esd_filename>
where
 esd_filename
 is the name of the directory that contains the USP
 installation software, for example,
 USP11.1.0.NCL.NAP.VAULT.1.D
- 8 Remove the .tape suffix from the USP package.
**mv <usp_sys_filename>.tar.gz.tape
 <usp_sys_filename>.tar.gz**
where
 usp_sys_filename
 is the name of the USP package, for example,
 usp11.1.0_sys
- 9 Uncompress the file.
gzip -d <usp_sys_filename>.tar.gz
where
 usp_sys_filename
 is the name of the USP package, for example,
 usp11.1.0_sys
- 10 Unpack the file.
tar -xvf <usp_sys_filename>.tar
where
 usp_sys_filename
 is the name of the USP package, for example,
 usp11.1.0_sys
- 11 Log out of the ESD load repository server.

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

If you are upgrading USP on a	Do
CMT-based OAMP workstation	Transferring the uncompressed file to the CMT on page 516
non-CMT-based OAMP workstation (windows-based)	Transferring the uncompressed file to Windows on page 518

Transferring the uncompressed file to the CMT

At a PC terminal

- 1 Make a temporary directory to store the ESD software on the PC.
c:/usp/loads
- 2 Change directory to the newly created directory.
- 3 Use your FTP client application to transfer the uncompressed USP software from the ESD load repository server to the directory you created in [step 1](#).

Before the transfer, ensure your FTP client is in binary mode.

At the CMT server

- 4 Log in to the CMT server using the FIELD account and change to the root user.
For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 5 Determine the usp install directory:
cat /opt/proftpd/etc/proftpd.conf |grep usp
- 6 Use the following table to determine your next step.

If the response is	Do
/data/usp	step 7
/opt/usp	step 14

- 7 Create a temporary directory to store the ESD software:
mkdir /data/usp/iso_esd
- 8 Change directory to the newly created location:
cd /data/usp/iso_esd

- 9 Ensure that enough disk space is available for the ESD software (500 MByte is recommended):

 # **df -k /data**

 The free space on the device on which /data is mounted, is printed. The value for "avail" is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes.
- 10 Transfer the USP software installation files from the PC to the temporary directory (created in [step 7](#)) using your FTP client application at the PC terminal.

 Before the transfer, ensure your FTP client is in binary mode.
- 11 Create a temporary directory to store the ESD software:

 # **mkdir /opt/usp/iso_esd**
- 12 Move all the data from /data/usp/iso_esd/ to /opt/usp/iso_esd/:

 # **mv /data/usp/iso_esd/* /opt/usp/iso_esd/**
- 13 Proceed to [step 18](#).
- 14 Create a temporary directory to store the ESD software:

 # **mkdir /opt/usp/iso_esd**
- 15 Change directory to the newly created location:

 # **cd /opt/usp/iso_esd**
- 16 Ensure that enough disk space is available for the ESD software (500 MByte is recommended):

 # **df -k /opt**

 The free space on the device on which /opt is mounted, is printed. The value for "avail" is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes.
- 17 Transfer the USP software installation files from the PC to the temporary directory (created in [step 14](#)) using your FTP client application.
- 18 Confirm the USP installation software is present:

 # **cd /opt/usp/iso_esd/<installation_directory>**
 # **ls -l**

 installation_directory
 is the directory that contains the USP files, for example USP11.1.0.16F

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

Transferring the uncompressed file to Windows

At the Windows-based OAMP workstation

- 1 Make a temporary directory to store the ESD software on the PC.
c:/usp/loads
- 2 Change directory to the newly created directory.
- 3 Use your FTP client application to transfer the uncompressed USP software from the ESD load repository server to the directory you created in [step 1](#).
Before the transfer, ensure your FTP client is in binary mode.
- 4 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Upgrading the ABS software on the CS 2000 Management Tools server

Use this procedure to install or upgrade the alternate boot server (ABS) software on the SPFS-based server that is hosting the CS 2000 Management Tools.

Prerequisites

This procedure has the following prerequisites:

- If ABS software is currently installed on the CS 2000 Management Tools server, this procedure includes steps to backup the existing ABS software to a backup directory on the server.
 - Make sure you know the location of the backup directory. Nortel recommends a directory with unique name, such as `usp_backup`.
 - Make sure you have write access to the backup directory.
- Know the existing install path for USP software on the CS 2000 Management Tools server before you begin this procedure.
 - For offices at USP10 and lower, the default USP install path is `/data/usp`.
 - For offices at USP11 and higher, the default USP install path is `/opt/usp`.

To identify the existing install path, execute the **more bootptab** command from the `/etc` directory on the CS 2000 Management Tools server. The values for `hd` or `bf` identify the existing install path.

- If you install the USP ABS on the CS 2000 Management Tools server using the GUI mode, you must export the X-Windows display of the CS 2000 Management Tools server to a remote workstation. If you are using a Windows-based workstation, use X-Windows server software such as Hummingbird's Exceed. Refer to [Configuring Exceed for an upgrade on page 1634](#).

Action

An ABS software upgrade consists of the following tasks:

1. [Preparing to upgrade ABS software on page 520](#)
2. [Upgrading the ABS software on page 521](#)
3. [Completing the ABS software upgrade on page 531](#)

Preparing to upgrade ABS software

The steps to prepare for an upgrade of ABS software depend on the method you received ABS software. Nortel delivers ABS software through electronic software delivery (ESD) and compact disk (CD).

Use one of the following procedures:

- If you received ABS software through ESD, use procedure [Preparing to upgrade ABS software using an ESD load on page 520](#).
- If you received ABS software on CD and are accessing the server from a local workstation at the CS 2000 Management Tools server, use procedure [Preparing to upgrade ABS software from a CD at a local workstation on page 520](#).

Preparing to upgrade ABS software using an ESD load

At your workstation

- 1 Transfer the new software from the ESD load repository server.
For detailed steps, refer to procedure [Installing Using ESD on page 514](#).
- 2 From the /opt/usp/iso_esd directory, set the file permissions by typing
chmod 755 install.bin
and pressing the Enter key.
- 3 View the permissions on the install.bin file and confirm the change was successful by typing
ls -l install.bin
and pressing the Enter key.
Example of response
RWXR-XR-X 2 FIELD maint2 *date* *time*
install.bin
- 4 You have prepared ABS software for the upgrade. Go to [Upgrading the ABS software on page 521](#).

Preparing to upgrade ABS software from a CD at a local workstation

At the CS 2000 Management Tools server

- 1 Insert the USP software CD in the CD drive of the CS 2000 Management Tools server. If CS 2000 Management Tools

resides on a high-availability cluster, insert the CD in the CD drive of active server.

At your workstation

- 2 Log in to the CS 2000 Management Tools server as the root user.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#)

- 3 Change directories by typing

```
cd /cdrom/cdrom0
```

and pressing the Enter key.

- 4 Verify the install.bin file is present by typing

```
ls
```

and pressing the Enter key.

- 5 You have prepared ABS software for the upgrade. Go to [Upgrading the ABS software on page 521](#).

Upgrading the ABS software

Upgrade the ABS software. Use one of the following procedures:

- To upgrade ABS software in console mode, go to [Upgrading the ABS software in console mode on page 521](#).
- To upgrade ABS software in GUI mode, go to [Upgrading the ABS software in GUI mode on page 526](#).

Upgrading the ABS software in console mode

At the workstation

- 1 Login to the CS 2000 Management Tools server as FIELD then change to the root user.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

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

If ABS is	Do
currently installed on the server	step 3
not installed on the server	step 6

- 3 Change to the ABS directory by typing
cd /<original USP install path>/ntssgusp/abs/
and pressing the Enter key.
where
<original USP install path> is one of the following:
 - /data/usp for offices at USP10 and lower
 - /opt/usp for offices at USP11 and higher
- 4 Copy the sites folder by typing
cp -r sites <backup path>
and pressing the Enter key.
where
<backup path> is ~/usp_backup/ or the path to your backup directory for ABS software
- 5 Copy the releases folder by typing
cp -r releases <backup path>
and pressing the Enter key.
where
<backup path> is ~/usp_backup/ or the path to your backup directory for ABS software
- 6 Change directories by typing
cd /<original USP install path>/ntssgusp
and pressing the Enter key.
where
<original USP install path> is one of the following:
 - /data/usp for offices at USP10 and lower
 - /opt/usp for offices at USP11 and higher
- 7 Start the uninstall wizard by typing
./Uninstall_Universal_Signaling_Point -i console
and pressing the Enter key.
- 8 When the Introduction panel appears, click **Enter**.
- 9 Wait for the uninstall wizard to open, which can take two to three minutes.

- 10** When the uninstall wizard opens, type **1** to completely remove all USP software components, and press Enter to continue.

Note: If you want to uninstall only ABS, type **2**, select USP Software Loads and ABS Manager to uninstall, and press Enter to continue.

- 11** When the Uninstall Complete panel appears, press the Enter key to exit the uninstall process.

- 12** Change directory by typing

```
cd /<original USP install path>/ntssgusp/abs
```

and pressing the Enter key.

where

<original USP install path> is one of the following:

- /data/usp for offices at USP10 and lower
- /opt/usp for offices at USP11 and higher

- 13** Make sure the removal was successful by typing

```
ls -l |grep ABS
```

and pressing the Enter key.

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

If	Do
one or more files are listed	Return to step 7 . If you are unable to uninstall the software on a second attempt, contact your next level of support.
otherwise	step 15

- 15** Change to the directory with the new ABS software. Use the following table to determine the correct command.

If you received ABS software	Do
through ESD	type <code>cd /opt/usp/iso_esd/<installation_directory></code> where <installation_directory> is the directory where the software was extracted, for example, USP11.1.0.16F

	If you received ABS software	Do
	on CD	type <code>cd /cdrom/cdrom0</code>
- 16** Launch the install wizard. Enter **`./install.bin -i console`** and pressing the Enter key.
The application can take 2 to 3 minutes to launch.
- 17** When the Introduction panel appears, click **Enter**.
The Component Selection panel appears.
Example of Component Selection panel
- ```

1 - [] USP Software loads and ABS Manager
2 - [X] USP Graphical Interface Client
3 - [X] USP User Manuals and Documentation Suite
4 - [] USP GR-310 Mediation Application
Enter software component numbers and press
<Enter> to continue.
Components 2 and 3 are selected by default.
To view a detailed description of each software component,
enter '?<component_number>'.

```
- 18** Use the following table to determine your next step.
- | <b>If you are</b>                                          | <b>Do</b>               |
|------------------------------------------------------------|-------------------------|
| using the CS 2000 Management Tools webstart application    | <a href="#">step 19</a> |
| not using the CS 2000 ManagementTools webstart application | <a href="#">step 21</a> |
- 19** Select the USP Software loads and ABS Manager component in addition to components 2 and 3, which are selected by default, by typing
- ```
1
```
- and pressing the Enter key.
A pre-installation summary appears which displays the selected components.

Example of Pre-Installation Summary

Please review the selected software components

Product Name:

Universal Signaling Point v11.1

Software Components:

USP Software Loads and ABS Manager,

USP Graphical Interface Client ,

USP User Manuals and Documentation Suite

Press <ENTER> to continue:

- 20** Press **Enter** and go to [step 23](#).
- 21** Select the USP Software loads and ABS Manager component in addition to component 3, which is selected by default, and deselect the USP Graphical Interface Client component, by typing
- 1,2**
- and pressing the Enter key.

A pre-installation summary appears which displays the selected components.

Example of Pre-Installation Summary

Please review the selected software components

Product Name:

Universal Signaling Point v11.1

Software Components:

USP Software Loads and ABS Manager,

USP User Manuals and Documentation Suite

Press <ENTER> to continue:

- 22** Press **Enter** to continue.
- 23** If a disk space warning displays, press **Enter**.
- 24** On the Install Complete panel, press **Enter**.
- 25** Change directories by typing
- cd /opt/usp/ntssgusp/abs**
- and pressing the Enter key.

- 26 Verify the new version of ABS software. Launch the updated console-based ABS Configuration Manager application by typing
./console_abs
and pressing the Enter key.
It takes approximately 2 to 3 minutes for the application to launch and be fully populated with data.
- 27 Log in to the ABS by typing
ABSCM> **login**
and pressing the Enter key.
- 28 When prompted, enter the password for the ABS.
Note: Refer to the *ABS_Specification.pdf* document for all the command syntax of the console-based ABS Configuration manager.
- 29 Log out of the ABS by typing
ABSCM> **exit**
and pressing the Enter key.
- 30 When prompted, confirm you want to log out of the ABS by typing
Y
and pressing the Enter key.
- 31 Return to the root directory by typing
cd /
and pressing the Enter key.
- 32 You have completed this procedure. Go to [Completing the ABS software upgrade on page 531](#).

Upgrading the ABS software in GUI mode

At the workstation

- 1 Ensure that your X-Windows server software is running and that host access permissions are allowed for the CS 2000 Management Tools server. Refer to your X-Windows server software manual for details.
- 2 Login to the CS 2000 Management Tools server as FIELD.
- 3 Once logged in, change to the root user by typing:
su -

and pressing the Enter key.

- 4 Set the display variable by typing:

DISPLAY=<IP address of your PC>:0.0

and pressing the Enter key.

Note: You can find the IP address of the PC you are using by entering the command `ipconfig` from a DOS window. If you are using Contivity or similar software to connect to the network, make sure you use the IP address assigned to your PC by Contivity and not the IP address assigned to you by your LAN.

- 5 Export the display by typing:

export DISPLAY

and pressing the Enter key.

- 6 Confirm the export by typing:

echo \$DISPLAY

and pressing the Enter key.

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

If ABS is	Do
currently installed on the server	step 8
not installed on the server	step 10

- 8 Change to the ABS directory by typing

cd /<original USP install path>/ntssgusp/abs/

and pressing the Enter key.

where

<original USP install path> is one of the following:

- /data/usp for offices at USP10 and lower
- /opt/usp for offices at USP11 and higher

- 9 Copy the sites folder by typing

cp -r sites <backup path>

and pressing the Enter key.

where

<backup path> is ~/usp_backup or the path to your backup directory for ABS software

- 10 Change directories by typing
`cd /<original USP install path>/ntssgusp`
and pressing the Enter key.
where
<original USP install path> is one of the following:
 - /data/usp for offices at USP10 and lower
 - /opt/usp for offices at USP11 and higher
- 11 Start the install wizard by typing
`./Uninstall_Universal_Signaling_Point -i gui &`
and pressing the Enter key.
- 12 Wait for the install wizard to open. The application can take two to three minutes to launch and receive data.
- 13 When the uninstall wizard opens, click **Next**, then click **Completely remove all USP software components**.
Note: If you want to uninstall ABS only, you can do the following: When the uninstall wizard opens, click **Choose specific USP components to uninstall**, then select **USP Software Loads** and **ABS Manager** to uninstall.
- 14 Change directories by typing
`cd /<original USP install path>/ntssgusp/abs`
and pressing the Enter key.
where
<original USP install path> is one of the following:
 - /data/usp for offices at USP10 and lower
 - /opt/usp for offices at USP11 and higher
- 15 Try to launch the ABS Configuration Manager to ensure the removal was successful by typing
`./ABS`
and pressing the Enter key.

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

If the ABS Configuration Manager	Do
launches	Return to step 11 . If you are unable to uninstall the software on a second attempt, contact your next level of support.
fails to launch	step 17

- 17 Change to the directory with the new ABS software. Use the following table to determine the correct command.

If you receive ABS software	Do
through ESD	cd /opt/usp/iso_esd
on CD	cd /opt/usp/absCD

- 18 Launch the install wizard by typing

`./install.bin`

and pressing the Enter key.

The application can take 2 to 3 minutes to launch.

Note: If the following error appears, the DISPLAY environment variable is not set up correctly.

```
Invocation of this Java Application has caused  
an InvocationTargetException. This  
application will now exit. (LAX)
```

Stack Trace:

```
at java.lang.Class.forName0(Native Method)  
at java.lang.Class.forName (Class.java:130)
```

If any other errors occur, ensure that your X-Windows server software is running and that host access permissions are allowed for the CS 2000 Management Tools server. Refer to your X-Windows software manual for details.

If the errors persist, contact your Nortel support representative.

- 19 When the Introduction panel appears, click **Next**.

- 20 Select the **USP Software Loads and ABS Manager** package on the Package Selection panel. If using the CS 2000 Management Tools webstart application, also select the USP

- Graphical Interface Client package. Do not select other packages. Click **Install**.
- 21 If a disk space warning displays, click **OK**.
 - 22 On the Install Complete panel, click **Done**.
 - 23 Login to the CS 2000 Management Tools server as FIELD.
 - 24 Change directories by typing
cd /opt/usp/ntssgusp/abs
and pressing the Enter key.
 - 25 Ensure that your X-Windows software is running and that host access permissions are allowed for the CS 2000 Management Tools server.
 - 26 Ensure that the DISPLAY environment variable is set up correctly.
 - 27 Launch the updated graphically-based ABS Configuration Manager application by typing
./ABS &
and pressing the Enter key.
It takes approximately 2 to 3 minutes for the application to launch and be fully populated with data.
 - 28 Click **File>Login**, and as this is the first time you are launching the new release of ABS, set the password when prompted to set and confirm the password.
 - 29 When prompted, enter the password and press enter to login into ABS.
 - 30 Click **File>Exit**, then a prompt indicates
Exit Alternate Boot Server Configuration
Manager?
Click **Yes** to exit the ABS Manager.
 - 31 Exit to the root directory by typing
cd /
and pressing the Enter key.
 - 32 You have upgraded ABS software. Go to [Completing the ABS software upgrade on page 531](#)

Completing the ABS software upgrade

Perform the following procedure to complete the upgrade of ABS software.

Completing an ABS software upgrade

At your workstation

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

If you received software	Do
received software through ESD	step 2
working on a local workstation	step 4

- 2 Delete the temporary files by typing **rm -rf /opt/usp/iso_esd** and press the Enter key.
- 3 Proceed to [step 6](#).
- 4 Eject the USP Software CD-ROM disk from the drive by typing **eject cdrom** and pressing the Enter key.
- 5 Remove the CD and close the drive.
- 6 You have completed the upgrade of ABS software on the CS 2000 Management Tools server. Make sure that ABS is working correctly. Refer to [Verifying correct ABS settings for the USP \(RTC\) on page 531](#).

Verifying correct ABS settings for the USP (RTC)

From the BOOTP server

- 1 You can use the USP EM PC to perform [step 2](#) to [step 8](#) or log in to the CMT and perform the steps.
- 2 Establish a telnet connection to RTC-12 or RTC-15.
- 3 Log in with a valid user name and password.
- 4 Verify the settings on RTC-12 by typing **admin abs test rtc-12** and pressing the Enter key.
- 5 When prompted, confirm the execution of the command by typing **y**

and pressing the Enter key.

If the settings are correct and the test is successful, the prompt returns after a few seconds. Otherwise, the system displays the failure before the prompt returns. If the test is not successful, contact your next level of support.

- 6 Verify the settings on RTC-15 by typing

admin abs test rtc-15

and pressing the Enter key.

- 7 When prompted, confirm the execution of the command by typing

y

and pressing the Enter key.

If the settings are correct and the test is successful, the prompt returns after a few seconds. Otherwise, the system displays the failure before the prompt returns. If the test is not successful, contact your next level of support.

- 8 Display all ABS settings by typing

admin abs show all

and pressing the Enter key.

- 9 Verify the following information:

- the rtc-12-load-server-ipaddress is the address of the CMT ABS
- the rtc-15-load-server-ipaddress is the address of the CMT ABS
- the correct RTC loads and snapshot are selected
- all other output information is correct

Example response for a site named "Enterprise"

```
~CMD>admin abs show all
```

```
rtc-12-loadname = ss7rtc_ppc750_11_00_00_36g
```

```
rtc-15-loadname = ss7rtc_ppc750_11_00_00_36g
```

```
snapshot-version = v11.0.0
```

```
snapshot-name = v11.0.0
```

```
snapshot-description = USP11.0.0 Default  
Database
```

```
virtual-index = 1
```

```
rtc-12-load-server-ipaddress = 47.135.60.47
rtc-12-bootfile =
/data/usp/ntssgusp/abs/sites/enterprise/rtc1/r
tcboot
rtc-12-ipaddress = 47.135.60.88
rtc-12-gateway-ipaddress = 47.135.60.1
rtc-12-subnet-mask = 255.255.252.0
rtc-15-load-server-ipaddress = 47.135.60.47
rtc-15-bootfile =
/data/usp/ntssgusp/abs/sites/enterprise/rtc2/r
tcboot
rtc-15-ipaddress = 47.135.60.89
rtc-15-gateway-ipaddress = 47.135.60.1
rtc-15-subnet-mask = 255.255.252.0
rtc-12-last-test-result = alternate-boot-server
test completed successfully
rtc-15-last-test-result = alternate-boot-server
test completed successfully
~CMD>
```

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

If	Do
the information in the system response is correct	step 11
otherwise	contact your next level of support

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

Configuring the Client Session Monitor

Application

Use the following procedure to change the default settings and customize the Client Session Monitor (CSM) application.

Refer to procedure 'Launching the Client Session Monitor' in *IEMS Basics*, NN10329-111, for details on accessing the CSM.

Prerequisites

You must have the IEMS Central SS software installed.

To configure the CSMonitor Audit using command line interface (CLI), you must have root user access.

Action

Perform the the sub-procedures that follow to complete this procedure.

- [Configuring the display criteria for a CSM report on page 534](#)
- [Configuring the CSMonitor Audit using CLI on page 536](#)

Configuring the display criteria for a CSM report

At your workstation using the CSM GUI client

- 1 Decide how you want to customize the default filter criteria and then perform some or all of the following steps.

Note: The default filter criteria displays results for all currently active application sessions. It also displays historical data about the owner of each of the active application sessions. The displayed data refreshes every 60 seconds.

A window similar to the following figure is displayed on your desktop after having launched CSM. The window displays all current application sessions monitored by CSM.

Search

▼ **Predefined Filter**

☐ Currently Active Sessions ☐ Sessions Active in the last **Seconds** ▼

▼ **Custom Filter**

Attribute: User ID, Activity, Client App, Start, End

User ID: Matches ▼ Click to enter new value

FilterString: [All]

Results as of Wed Feb 23 18:54:41 EST 2005

Results

9 activity(ies)

Ses...	Use...	Activity	Client App	Start	End	Source Ip	Destination Ip	End Reason
130	dsail	authenticate		2005-02-23 17:53:17				
131	dsail	client session	MG9kEM	2005-02-23 17:53:17	2005-02-23 18:33:17	47.142.312.50	47.142.95.67	Admin Marked Done
128	gpye	authenticate		2005-02-23 18:33:17				
129	gpye	client session	MG9kEM	2005-02-23 18:33:17		47.142.312.48	47.142.95.67	
123	jksmith	authenticate		2005-02-15 18:53:17				
124	jksmith	client session	MG9kEM	2005-02-15 18:53:17	2005-02-16 02:53:17	47.142.312.60	47.142.95.67	User Exit
125	jksmith	client session	SAM21EM	2005-02-16 02:53:17	2005-02-16 10:53:17	47.142.312.60	47.142.95.67	Inactivity Timeout
126	wanjie	authenticate		2005-02-17 01:53:17				
127	wanjie	client session		2005-02-17 01:53:17	2005-02-17 08:53:17	47.142.312.43	47.142.95.67	User Exit

Mark Done

- 2 Deselect Currently Active Sessions which is the default setting.
- 3 Select the attributes you want to use as the filter criteria from the Customer Filter scroll box.

The Custom Filter scroll box allows you to build customized criteria from the list of available attributes.

For those fields that are strings, such as UserID, Activity, ClientApp, SourceIp, and DestinationIp, the criteria used to match are selected from the drop-down menu to the right of the Customer Filter scroll box. The options in this menu are Matches, Does not match, Contains, Does not contain, and Starts with. Enter the information you want to use as a criteria in the field next to the option you have selected.

For fields that are dates, such as Start Activity and End Activity, the matching criteria are Matches, Does not match, Before, Between. The date requires the format of YYYY-MM-DD HH:MM:SS. The exceptions are the term Current and Null.

- 4 Replace the default setting of 60 seconds in the Sessions Active in the last field by selecting another time period (either Seconds, Minutes, Hours, or Days) from the drop-down menu.

- 5 Click Filter to update the report once you have finished modifying the filter criteria.
A customized CSM report displays in the Results section of the window using your customized filter criteria.

Configuring the CSMonitor Audit using CLI

At your workstation

- 1 Log in to IEMS security server by typing
`> telnet <IEMS security server>`
and pressing the Enter key.
where
IEMS security server
is the IP address or host name of the IEMS security server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing
`$ su -`
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Configure the Client Session Monitor Audit (CSMonitor Audit) using CLI by following these steps.
- 6 Access the command line interface by typing
`# cli`
and pressing the Enter key.
- 7 Enter the number that corresponds to the Configuration option in the menu.
- 8 Enter the number next to the Succession Element Configuration option in the menu.
- 9 Enter the number next to the CSMCLEANUP Application Configuration option in the menu.

- 10** Enter the number next to the setCleanupTime option in the menu.

For additional information on this setting, refer to one of the following documents:

- *(I)SN09 OSS Guide Advance Feature Guide*, PLN-i09-OSS, version 01.04

Refer to section 3.8, "Configuration Walkthrough" on page 1461 of the document.

- *(I)SN09 Release Change Reference Manual*, PLN-ISN09-004, version 01.03

Refer to section 33.9, "Configuration Walkthrough" on page 1756 of the document.

All CSM sessions, even after they are closed, are recorded in the CSM database of logins and logouts. The CSMonitor Audit functionality prevents the session database from growing too large by cleaning up unwanted records of sessions. The selected time determines when polling of the database for the clean up of sessions occurs. Sessions are removed from the audit when CSMonitor Audit re-activates following the selected time period. For example, if 24 hours is the selected time, the CSMonitor Audit reactivates 24 hours after the audit begins and queries the database for sessions needing to be removed.

Note: The selection of sessions is based strictly on start time and may delete sessions that have not ended. Therefore, care must be taken to specify criteria so as not to delete any active sessions.

- 11** Enter the number next to the setCleanupCriteria option in the menu.

For additional information on this setting, refer to one of the following documents:

- *(I)SN09 OSS Guide Advance Feature Guide*, PLN-i09-OSS, version 01.04

Refer to section 3.8, "Configuration Walkthrough" on page 1461 of the document.

- *(I)SN09 Release Change Reference Manual*, PLN-ISN09-004, version 01.03

Refer to section 33.9, "Configuration Walkthrough" on page 1756 of the document.

Max sessions per user criteria keeps the sessions based on start time for each user id. Time based criteria keeps sessions based

on start time. For example, you can change the cleanup criteria from max sessions per user to deletion after 500 hours.

- 12** Exit each menu level of the command line interface to eventually exit the command line interface by typing

```
select - x
```

- 13** Restart CSMonitor_Audit in order to apply the new configuration by typing

```
servrestart CSMonitor_Audit
```

You have completed this procedure.

Starting and stopping the QoS Collector Application

Application

Use this procedure to start or stop the QoS Collector Application (QCA) on the Server Platform Foundation Software (SPFS)-based server.

Note: The QCA is installed on the same SPFS-based server as the CS 2000 Management Tools software (CS2M), but a second instance of QCA may also be installed on a separate SPFS-based server.

You need to stop and restart the QCA after you performed procedure “Configuring the QoS Collector Application” in the Configuration Management document.

Note: If QCA functionality is not desired at the site, then the QCA application need not be installed during the CS2M installation/upgrade. Starting in SN09U, CS2M installation/upgrade prompts users as to whether or not the QCA package is to be installed. For older releases, QCA has to be uninstalled manually at the sites where QCA is not desired. Refer to *ATM/IP solution-level Security and Administration*, NN10402-600.

Prerequisites

None

Action

At your workstation

- 1 Establish a login session to the server, using one of the following methods:

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

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server

is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step [4](#).

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server

is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration

Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter `yes` at the prompt.

- b** When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

- 4** Verify the status of QCA by typing

```
# servman query -status -group QCA
```

and pressing the Enter key.

Example response when QCA is running

```
A QCA instance is registered with PMFADN as Qca
and running on the portNumber=20000
```

Example response when QCA is not running

```
A QCA instance is not registered with PMFADM as
Qca
```

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

If you want to	Do
start QCA	step 6
stop QCA	step 7

- 6** Start QCA by typing

```
# /opt/nortel/qca/qca_server
```

and pressing the Enter key.

Example response

```
Registering QCA with servman.
Attempting to register QCA as Qca with PMFADM.
Have you checked the qca.properties file? Are
you sure you want to continue [ no or yes ]
```

At the prompt, enter **yes** to confirm you wish to continue.

Example response

```
Registration as Qca was ok. QCA started.
```

```
QCA has been started with the following
properties...
```

```
MaxFileSize=5
    (Supported values are 1 to 100)
MaxFileTime=15
    (Supported values are 1 to 240)
recycleToD=0
    (Supported values are 0 to 23)
portNumber=20000
    (Supported values are 20000 to 20004)
RetainFileTime=5
    (Supported values are 1 to 30)
fileExt=xml
    (Supported value is an alphanumeric
character string)
nodeName=QCA
    (Supported value is an alphanumeric
character string)
closedFileCompression=true
    (Supported values are 'true' and 'false')
oldFileCompression=true
    (Supported values are 'true' and 'false')
```

Please check /var/log/customerlog if any of the above properties does not fall within the range of supported values.

Proceed to step [8](#).

7 Stop QCA by typing

```
# /opt/nortel/qca/stop_qca
```

and pressing the Enter key.

Example response

```
Are you wure you want to stop the QCA? Have you
checked the port number in qca.properties? [no
or yes]
```

At the prompt, enter **yes** to confirm you wish to continue.

Example response

```
De-registering QCA from servman
Attempting to unregister QCA as Qca from FMFADM.
Attempting to stop local QCA on port : 20000
QCA stopped successfully.
```

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

Starting and stopping the Core Element Manager (CEM)

Application

Use this procedure to start or stop the Core Element Manager (CEM).

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

ATTENTION In a two-server configuration, perform the steps that follow on the active server.

At your workstation

- 1 Establish a login session to the server, using one of the following methods:

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

- 2 Log in to the server using telnet (unsecure) as follows:

- a Log in to the server by typing

> telnet <server>

and pressing the Enter key.

where

server

is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step [4](#).

3 Log in using ssh (secure) as follows:

a Log in to the server by typing

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

and pressing the Enter key.

where

server

is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration

Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter `yes` at the prompt.

b When prompted, enter the root password.

Note: In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

- 4 Verify the status of the CEM by typing
servman query -status -group CEM
and pressing the Enter key.
- 5 Use the following table to determine your next step.

If	Do
CEM is stopped and you need to start it	step 6
CEM is running and you need to stop it	step 7

- 6 Start the CEM by typing
servstart CEM
and pressing the Enter key.
Example response:
CEM server successfully started
Go to step [8](#)
- 7 Stop the CEM by typing
servstop CEM
and pressing the Enter key.
Example response:
CEM server successfully stopped
- 8 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.



CS 2000 Core Manager upgrade

This procedure enables you to upgrade CS 2000 Core Manager servers.

There are two methods of upgrading the CS 2000 Core Manager to a new software release:

- Out of Service (OOS) Upgrade procedure using Electronic software delivery (ESD) or tape: This procedure busies the CS 2000 Core Manager and upgrades both domains at the same time.
- Enhanced SDM upgrade procedure (ESUP), through electronic software delivery (ESD), or tape: This procedure breaks the root volume group (rootvg) mirror, applies new filesets to domain 1 rootvg, busies and reboots the system, then integrates rootvg disks.

ESUP upgrades can be performed in the following ways, using a:

- telnet connection (only for upgrades to SDM20/CS2E0070 or later)
- remote console connection (modem, terminal server, etc.) (all releases)
- local console connection (vt100 terminal/emulation) (all releases)

The following table indicates when to use the OOS Upgrade Procedure or ESUP method to upgrade your CS 2000 Core Manager to the new software release:

If you are upgrading	OOS Upgrade Procedure	ESUP
a rootvg-only system	x	
a rootvg/datavg system	x	x
the software and CPU hardware		

New in this release

Feature changes

In SN09U, there are no feature changes that affect the CS 2000 Core Manager upgrade.

Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U

Server types

The following server types are supported by this upgrade:

- Nortel Series FX platform

Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade

Time to complete an upgrade

The following table lists the tasks to upgrade CS 2000 Core Manager software and the estimated time to complete each task.

Table 1 Estimated time to complete a software upgrade

Task	Time
Preparing for the upgrade	5 hours (includes preparation procedures, backup, and 2 hours for one hardware upgrade)
Upgrading the software	ESUP - 4 hours Out-of-service (OOS) upgrade - 2 hours
Completing the upgrade	3 hours (includes backup)
Total estimated upgrade time	ESUP - 12 hours OOS - 10 hours

System Performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade.

System limitations during upgrade

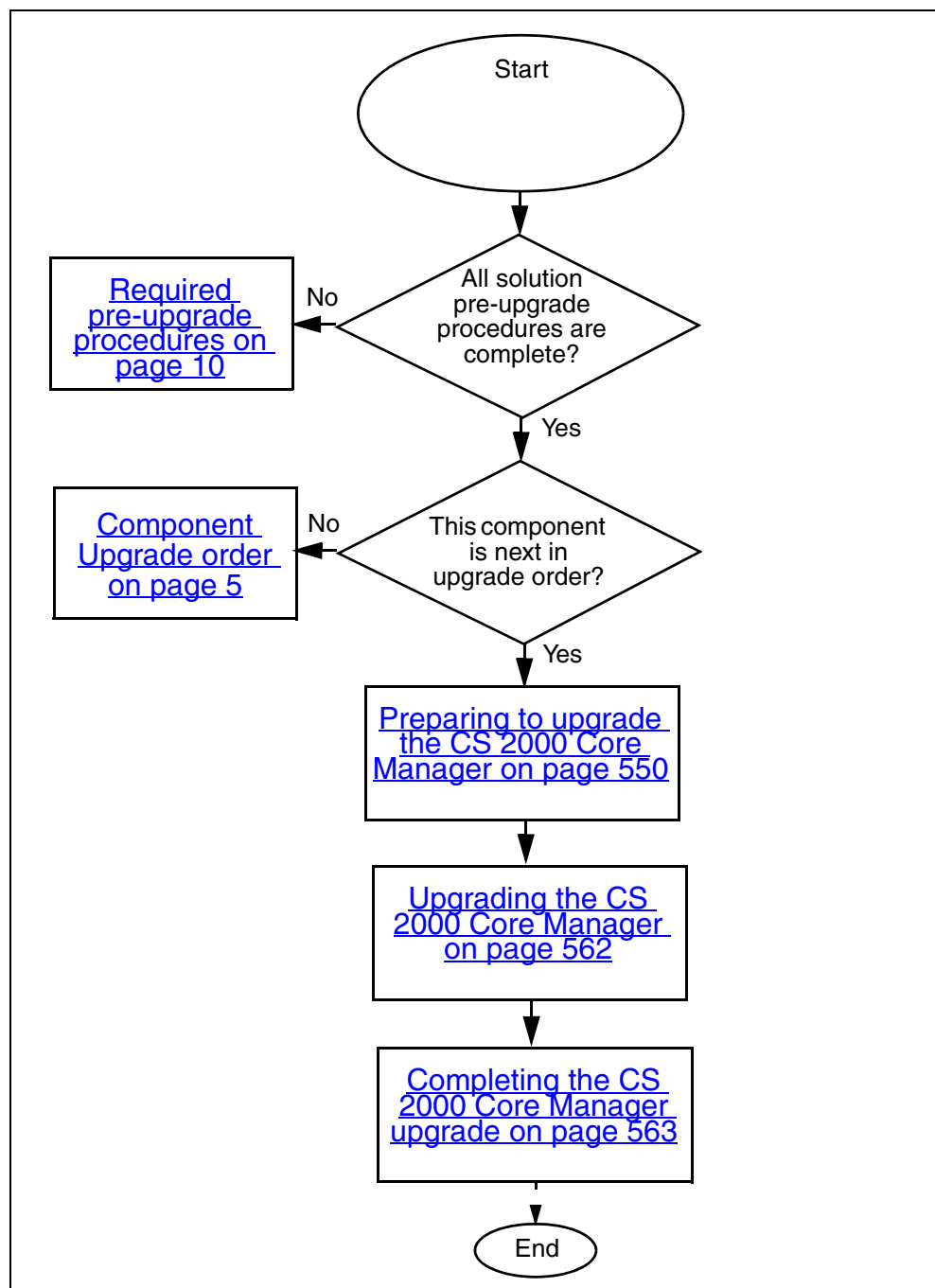
During a software upgrade, the system prohibits the following actions:

- System administration
 - adding, deleting, or modifying users
 - setting time of day
 - changing passwords
- System management
 - modifying the system name
 - adding or deleting system nodes
 - modifying the IP addresses

CS2000 Core Manager upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

CS2000 Core Manager upgrade tasks



Preparing to upgrade the CS 2000 Core Manager

The following procedures provide the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

Hardware baseline

The following table indicates the supported hardware to upgrade to the new software release.

Hardware baseline

PEC	Description
CPU	
NTRX50CG	604e - 200MHz/256MB Up to 3+1 XA-Core, SDM supports maximum billing capacity of 70KB/s with an NTRX50CG (or CH), and NTRX50GX. Higher capacity requires the NTRX50NB.
NTRX50CH	604e - 200MHz/512MB Up to 3+1 XA-Core, SDM supports maximum billing capacity of 70KB/s with an NTRX50CG (or CH), and NTRX50GX. Higher capacity requires the NTRX50NB.
NTRX50NB	Arthur 750 - 400MHz/512MB The NTRX50NB requires the NTRX50GX for total traffic in excess of 26KB/s (KB/s = billing records/hr * record size (bytes) / (3600 second * 1024).
Disk/DAT and LAN PM	
NTRX50GN	4G DAT/4G DD (rootvg) The NTRX50GN is a rootvg-only (single disk) system and does not support electronic software delivery (ESD) in SDM17 onward. Upgrade to the rootvg/datavg system with the NTRX50NM (36G rootvg) and NTRX50NL (36G+36G datavg).

Hardware baseline

PEC	Description
NTRX50ND	4G DAT/9G DD (rootvg) The NTRX50ND is the minimum hardware for GEM applications. Replacements for the NTRX50ND are filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004 the NTRX50NM is the replacement for the NTRX50ND.
NTRX50NM	12G DAT/36G DD (rootvg)
NTRX50NK	LAN personality module The NTRX50NK is used with the NTRX50NM.
NTRX50FS	LAN personality module The NTRX50FS is used with the NTRX50GN and NTRX50ND.
Disk expansion	
NTRX50GP	4G DD/4G DD (datavg)
NTRX50NC	9G DD/9G DD (datavg) The NTRX50NC is the minimum hardware for GEM applications. Replacements for the NTRX50NC are filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004 the NTRX50NL will replace the NTRX50NC.
NTRX50NL	36G DD/36G DD (datavg)
Core connectivity	
NTRX50GA	DS-512 controller module (BRISC) Note: The NTRX50CG and CH support BRISC processor and XA 1+1 processor up to 26KB/s with the NTRX50GA and up to 37KB/s with the NTRX50GX. The NTRX50GX is the minimum hardware for GEM applications.

Hardware baseline

PEC	Description
NTRX50GX	DS-512 controller module (XA-Core) The NTRX50CG and CH support BRISC processor and XA 1+1 processor up to 26KB/s with the NTRX50GA and up to 37KB/s with the NTRX50GX. The NTRX50GX is the minimum hardware for GEM applications.
NTRX50GH	DS-512 personality module
X.25 connectivity (optional)	
NTRX50FY	X.25 controller module
NTRX50FZ	X.25 personality module
NTRX50NN	X.25 personality module for UMPIO

You can have different MFIO/UMPIO datavg and rootvg combinations configured on your system. The following table lists the combinations that are supported for the new software release.

Supported MFIO and UMPIO, datavg and rootvg configurations

Configuration	Domain 0		Domain 1		Total disk storage
	Rootvg	Datavg	Rootvg	Datavg	
Most basic - not recommended	NTRX50GN 4-Gbyte	N/A	NTRX50GN 4-Gbyte	N/A	4-Gbyte (rootvg only)
Moderate	NTRX50GN 4-Gbyte	NTRX50GP 8-Gbyte	NTRX50GN 4-Gbyte	NTRX50GP 8-Gbyte	12-Gbyte
Largest with 4-Gbyte disk	NTRX50GN 4-Gbyte	NTRX50GP (8-Gbyte) + (expansion chassis) NTRX50GP (8-Gbyte) 16-Gbyte	NTRX50GN 4-Gbyte	NTRX50GP (8-Gbyte) + (expansion chassis) NTRX50GP (8-Gbyte) 16-Gbyte	20-Gbyte

Supported MFIO and UMFIIO, datavg and rootvg configurations

Configuration	Domain 0		Domain 1		Total disk storage
	Rootvg	Datavg	Rootvg	Datavg	
Basic with 9-Gbyte disk	NTRX50ND 9-Gbyte ¹	N/A	NTRX50ND 9-Gbyte ¹	N/A	9-GByte (rootvg only)
Moderate	NTRX50ND 9-Gbyte ¹	NTRX50NC 18-Gbyte ²	NTRX50ND 9-Gbyte ¹	NTRX50NC 18-Gbyte ²	27-Gbyte
Largest with 9-Gbyte disk	NTRX50ND 9-Gbyte ¹	NTRX50NC (18-Gbyte) ² + (expansion chassis) NTRX50NC (18-Gbyte) 36-Gbyte	NTRX50ND 9-Gbyte ¹	NTRX50NC (18-Gbyte) ² + (expansion chassis) NTRX50NC (18-Gbyte) 36-Gbyte	45-Gbyte
4-Gbyte/9-Gbyte mix	NTRX50GN 4-Gbyte	NTRX50NC 18-Gbyte ²	NTRX50GN 4-Gbyte	NTRX50NC 18-Gbyte ²	22-Gbyte
Basic with 36-Gbyte disk	NTRX50NM 36-Gbyte	N/A	NTRX50NM 36-Gbyte	N/A	36-Gbyte
Moderate	NTRX50NM 36-Gbyte	NTRX50NC 18-Gbyte	NTRX50NM 36-Gbyte	NTRX50NC 18-Gbyte	54-Gbyte
Largest with only 36-Gbyte disk	NTRX50NM 36-Gbyte	NTRX50NL 72-Gbyte	NTRX50NM 36-Gbyte	NTRX50NL 72-Gbyte	108-Gbyte
4-Gbyte/36-Gbyte mix	NTRX50GN 4-Gbyte	NTRX50NL 72-Gbyte	NTRX50GN 4-Gbyte	NTRX50NL 72-Gbyte	76-Gbyte

Supported MFIO and UMFI0, datavg and rootvg configurations

Configuration	Domain 0		Domain 1		Total disk storage
	Rootvg	Datavg	Rootvg	Datavg	
9-Gbyte/ 36-Gbyte mix	NTRX50ND 9-Gbyte ¹	NTRX50NL 72-Gbyte	NTRX50ND 9-Gbyte ¹	NTRX50NL 72-Gbyte	81-Gbyte
Note 1: The maximum number of NTRX50GP MFIOs allowed in a system is four. The expansion shelf is required for this configuration. Note 2: NTRX50GN and NTRX50GP are supported after November 2004. These disks must be replaced by NTRX50ND and NTRX50NM. Note 3: The maximum number of NTRX50NC MFIOs allowed in a system is four. The expansion shelf is required for this configuration. Note 4: The maximum number of NTRX50NL UMFI0s allowed in a system is two. Disk expansion shelf is not required in this configuration. Note 5: A single 4-Gbyte MFIO module cannot be mixed with a single 9-Gbyte module or a 36-Gbyte module to form a pair.					

1. Replacements for the NTRX50ND are filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004 the NTRX50NM is the replacement for the NTRX50ND.

2. Replacements for the NTRX50NC are filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004 the NTRX50NL is the replacement for the NTRX50NC.

Software baseline

You must have the latest maintenance non-CM load (MNCL) release installed on the CS 2000 Core Manager before you upgrade to the new NCL release.

When a new MNCL is released for the CS 2000 Core Manager, a technical bulletin is issued with a Notification of Availability. Check whether any technical bulletins with a Notification of availability in the title have been issued to determine if a later MNCL exists for your release. If you need to upgrade to the latest MNCL, refer to the MNCL release notes for instructions.

Fileset-to-solution mapping

The following table lists CS2E0090 filesets and provides the following information

- the solutions that use each fileset
- the DCE requirements for each fileset

Fileset-to-solution mapping (Sheet 1 of 3)

Fileset	Description	Solutions					
		IAC	IAW	PT-AAL1	PT-IP	UA-AAL1	UA-IP
SDM_Version.info	CS2E0090	Y	Y	Y	Y	Y	Y
NT_SIM.tools	Patching tools	Y	Y	Y	Y	Y	Y
SDM_ACE.dist	SDM ACE distribution	Y	Y	Y	Y	Y	Y
SDM_AFT.DMS500	SBA Automatic File Transfertime	N	N	N	N	N	N
SDM_ATA.client	ASCII Terminal Access Client	Y	Y	Y	Y	Y	Y
SDM_BASE.base	Platform base	Y	Y	Y	Y	Y	Y
SDM_BASE.client	Client Common Resources	Y	Y	Y	Y	Y	Y
SDM_BASE.dfquery	Check disks and disk drives	Y	Y	Y	Y	Y	Y
SDM_BASE.fts	File Transfer Service	Y	Y	Y	Y	Y	Y
SDM_BASE.gdd	Generic Data Delivery	Y	Y	Y	Y	Y	Y
SDM_BASE.logs.client	Log Delivery Service Client	Y	Y	Y	Y	Y	Y
SDM_BASE.logs	Log Delivery Service	Y	Y	Y	Y	Y	Y
SDM_BASE.mtce	Platform Maintenance	Y	Y	Y	Y	Y	Y
SDM_BASE.omsl	OM Access Service	Y	Y	Y	Y	Y	Y
SDM_BASE.tasl	Table Access Service	Y	Y	Y	Y	Y	Y
Note: Y= required, N=not required, O=optional							

Fileset-to-solution mapping (Sheet 2 of 3)

Fileset	Description	Solutions					
		IAC	IAW	PT-AAL1	PT-IP	UA-AAL1	UA-IP
SDM_BASE.util	Platform utilities	Y	Y	Y	Y	Y	Y
SDM_BMI.bmi	Base Maintenance Interface	Y	Y	N	Y	Y	Y
SDM_DDMS.ossaps	OSS and Application Svcs	Y	Y	N	Y	Y	Y
SDM_DDMS.osscomms	OSS Comms Svcs	Y	Y	N	Y	Y	Y
SDM_DMA.dma	DMS Maintenance Application	Y	Y	N	Y	Y	Y
SDM_DNBD.dnbd	DNBD Call Data Delivery	Y	Y	Y	Y	Y	Y
SDM_DNBD.osidp	ONE FTAM Software	Y	Y	Y	Y	Y	Y
SDM_DTS_PROVIDERS.dts	DCE DTS Time providers for global servers	Y	Y	Y	Y	Y	Y
SDM_ECR.ecr	SDM Expansion Chassis Removal tool	Y	Y	Y	Y	Y	Y
SDM_ESUP.esup	ESUP Tools	Y	Y	Y	Y	Y	Y
SDM_ETA.eta	Enhanced Terminal Access	Y	Y	Y	Y	Y	Y
SDM_ETA.client	Enhanced Terminal Access Client	Y	Y	Y	Y	Y	Y
SDM_FTP.proxy	FTP proxy	Y	Y	Y	Y	Y	Y
SDM_GR740PT.gr740pt	GR740 Pass Through	Y	Y	Y	Y	Y	Y
SDM_IMAGEDUMP.rte	Image Dump Service	Y	Y	Y	Y	Y	Y
SDM_INSTALL_inst	SDM Tools	Y	Y	Y	Y	Y	Y
SDM_LOGS.mdm	Passport Log Streamer	N	N	Y	Y	Y	N
SDM_OMDD.omdd	OM Delivery	Y	Y	Y	Y	Y	Y
Note: Y= required, N=not required, O=optional							

Fileset-to-solution mapping (Sheet 3 of 3)

Fileset	Description	Solutions					
		IAC	IAW	PT-AAL1	PT-IP	UA-AAL1	UA-IP
SDM_OpenSSH.base	Open SSH ver. 3.4p1	Y	Y	Y	Y	Y	Y
SDM_OpenScreen.base	OpenScreen	Y	Y	Y	Y	Y	Y
SDM_PRECHECK.sysaudit	System pre-check tools	Y	Y	Y	Y	Y	Y
SDM_RADIUS	PAM Radius	Y	Y	Y	Y	Y	Y
SDM_REACHTHRU.rttl1	Reach Through SPM	Y	Y	Y	Y	Y	Y
SDM_SAML.lam	LAM SAML	Y	Y	Y	Y	Y	Y
SDM_SBA.DMS500	SDM Billing Application	Y	Y	Y	Y	Y	Y
SDM_SCFT.scft	Secure Core File Transfer	Y	Y	Y	Y	Y	Y
SDM_SCM.scm	Succession SAM21 Manager	Y	Y	N	Y	Y	Y
SDM_SFT.client	Secure File Transfer Client	Y	Y	Y	Y	Y	Y
SDM_SFT.sft	Secure File Transfer	Y	Y	Y	Y	Y	Y
SDM_SWLD.swld	BOOTP Loading Service	Y	Y	N	Y	Y	Y
SDM_UPGRADE.tools	UPGRADE Tools	Y	Y	Y	Y	Y	Y
SDM_BKM-CSU-00.tape 21.3.0.0	Succession Provisioning Data Sync Manager	N	Y	N	Y	Y	Y
SDM_GEM.dmsDataSrv-<ve rsion>.tape	CEM DMS Data Server	Y	Y	Y	Y	Y	Y
SDM_TntFTPHandl.TntFTP Hndl-<version>.tape	CEM Telnet FTP Handler	Y	Y	Y	Y	Y	Y
SDM_CEM.SAF-<version>.t ape	CEM Store and Forward	Y	Y	Y	Y	Y	Y
Note: Y= required, N=not required, O=optional							

Prerequisites for a CS 2000 Core Manager upgrade

The following are prerequisites for a successful upgrade of a CS 2000 Core Manager:

- You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	<i>CS 2000 Core Manager Security and Administration</i> , NN10170-611
Displaying actions a user is authorized to perform	<i>CS 2000 Core Manager Security and Administration</i> , NN10170-611

- For the network path between the Nortel software vault and a customer's CS 2000 Core Manager, the repository server is the last file transfer point prior to the CS 2000 Core Manager. The server must have enough disk space to hold, uncompress and unarchive the CS 2000 Core Manager load. Once all of the CS 2000 Core Manager filesets are extracted, they are transferred to the CS 2000 Core Manager from the repository server by FTP.
- Before you can begin preparing the repository server for the CS 2000 Core Manager load, you will need a decompression tool on the repository server to extract the contents of the CS 2000 Core Manager load. The load transferred is a compressed tar file. If the tar file compression format used is .Z format (as seen by the filename), you will need the uncompress tool on the repository server. If the load transferred is in .gz format, you will need either a gzip or a gunzip tool. These tools and the tar command must be in your UNIX PATH environment variable.

-

ATTENTION

On the CS 2000 Core Manager, ensure that you have 3 Gbytes of free space available on datavg. To check the free space on datavg, enter the command `sdmmtc storage` at the # command prompt.

- This procedure assumes that you are using the FTP tool on the CS 2000 Core Manager to transfer the load from the external repository server to the CS 2000 Core Manager. Alternate transfer methods using secure CS 2000 Core Manager applications such as Secure File Transfer (SFT) can be available, depending on your site configuration. SFT requires that
 - both the CS 2000 Core Manager and repository server be configured as DCE clients within the same distributed computing environment (DCE) cell, and
 - the required CS 2000 Core Manager software clients be installed on the repository server.

Action

ATTENTION

Nortel strongly recommends that you perform the pre-check procedures below seven days before the start of any software upgrade, to allow time for corrective action if required.

By completing each of the pre-check tasks and submitting a list of any failed pre-check tasks to Nortel, you can minimize potential disruption to the software upgrade, minimize any risk to the call server, and assist Nortel with providing full support on the upgrade, if assistance is required. Nortel will assist in recovering a CS 2000 Core Manager if a problem arises during a software upgrade that was not preceded by this pre-check procedure, but will not provide a root cause analysis of the problem.

Preparing the CS 2000 Core Manager for an upgrade

On the client workstation

- 1 Prepare the repository server for the CS 2000 Core Manager load. For detailed steps, perform [Preparing the repository server for the CS 2000 Core Manager load on page 569](#).

- 2 If software authentication is required on the CS 2000 Core Manager, perform [Applying the SDM_CERTS.Certs package on page 573](#).
When the SDM_CERTS.Certs package is applied, all patches applied afterwards are authenticated.
- 3 Prepare the CS 2000 Core Manager for file transfer from the repository server. For detailed steps, perform [Preparing the CS 2000 Core Manager for file transfer from the repository server on page 575](#).
- 4 To prepare for completing upgrade pre-check tasks, capture the execution of the pre-check session and store the file on the CS 2000 Core Manager. For detailed steps, perform [Capturing the pre-check session file on page 578](#).
- 5 Perform the basic pre-checks. For detailed steps, perform [Performing basic pre-checks on page 580](#).
- 6 Execute a sanity check on various components of the CS 2000 Core Manager, by performing [Preparing a system audit pre-check on page 583](#).
- 7 Display the hardware PEC codes and ensure compatibility with the hardware baseline, by performing [Performing a hardware baseline pre-check on page 587](#).
- 8 Ensure that the master and checker CPU is operating as expected, by performing [Performing a CPU stability pre-check on page 589](#).
- 9 Identify potential problems with the DS512 fiber links connected from the core to the DS512 controller modules on the CS 2000 Core Manager, by performing [Performing a DS512 fiber link pre-check on page 596](#).
- 10 Verify that the applications on the CS 2000 Core Manager are in-service and configured, by performing [Performing an application and fileset status and configuration pre-check on page 601](#).
- 11 Ensure that the CS 2000 Core Manager user attributes are configured correctly, by performing [Performing a user configuration pre-check on page 604](#).
- 12 Display the status and configuration of the Ethernet interfaces, by performing [Performing an Ethernet configuration pre-check on page 606](#).
- 13 Verify that the system dump devices are not in the null state, by performing [Performing a system dump device pre-check on page 610](#).

- 14** If you are upgrading from tape, transfer the upgrade software from tape to a disk to help ensure a trouble-free upgrade by avoiding tape problems that can occur during the upgrade. For detailed steps, perform [Preparing for system software upgrades from tape on page 612](#).
- 15** You have completed this procedure. Return to [CS2000 Core Manager upgrade tasks on page 549](#).

Upgrading the CS 2000 Core Manager

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

You have completed [Preparing to upgrade the CS 2000 Core Manager on page 550](#)

Action

If you are upgrading the CS 2000 Core Manager using Enhanced SDM upgrade procedure (ESUP), perform the following procedure to upgrade the component:

- [Upgrading CS 2000 Core Manager software using ESUP on page 617](#)

If you are upgrading the CS 2000 Core Manager out-of-service, perform the following procedure to upgrade the component:

- [Upgrading CS 2000 Core Manager software out of service on page 655](#)

Completing the CS 2000 Core Manager upgrade

The following procedure provides the high-level steps to complete the component upgrade.

Prerequisites

You have completed [Upgrading the CS 2000 Core Manager on page 562](#)

Action

Perform the following procedure to complete the component upgrade.

ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Post-upgrade tasks

ATTENTION

If your system is configured with the Distributed Computing Environment (DCE) service, and you plan to remove it, make sure that you do not decommission the DCE until the CS 2000 Management Tools server is upgraded. Otherwise, communication outages between the CS 2000 Core Manager and the CS 2000 Management Tools server will occur.

Do not decommission DCE if your system is configured with any DCE-dependent application, such as ETA, ATA, SFT, or GR740 Pass Through.

At your CS 2000 Core Manager server

- 1 Verify the application state, to ensure that all applications are in-service.

- a Access the application level of the core manager maintenance interface:

sdmmtc appl

- b Determine whether all applications are in-service (as indicated by a dot for each in-service application under the State heading).

The Passport Log Streamer application is in an offline state and not configured if you had the log delivery application installed and configured with the parameter: Passport 15000 present in the network, set to No prior to this upgrade. Refer to “Installing and configuring the log delivery application” in *CS 2000 Core Manager Configuration Management*, NN10104-511, to configure it and return it to service. When complete, return to this procedure and continue where you left off.

If	Do
all applications are in service	step 2
not all applications are in service	step c

- c Manually busy (ManB) each application that is not in service:

bsy <x>

where

<x>

is the number next to one of the applications that is not in service

The system responds

Application Busied - Command complete.

- d Repeat step [c](#) for each application that is not in service.
 - e Return each application to service (RTS):

rts <x>

where

<x>

is the number next to each application you busied in the previous step.

The system responds

Application RTS - Command complete.

f Repeat step [e](#) to return each application to service.

2 To confirm that the upgrade was successful, verify the current software load.

a Exit the maintenance interface:

quit all

b Verify that the product code, located at the top left-hand corner of the screen, shows the release that you are upgrading to:

querysdm loads

If the product code	Do
is the correct release	step 3
is <i>not the correct release</i>	contact your next level of support

Note: Dashes (----) displayed next to the platform maintenance are part of a normal output.

3 Perform a backup of your new system image. Use the procedure “Creating system image backup tapes (S-tapes)” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

If you choose not to perform a backup of your new system image, the CS 2000 Core Manager will show in-service trouble (ISTb) and the status of the Backup Status alarm will show *Required* (if the alarm is enabled). You can force-clear the alarm using the procedure “Clearing a system image backup Required or Failed alarm” in *CS 2000 Core Manager Fault Management*, NN10082-911. If the backup Required alarm is disabled, the alarm will not be raised.

4 If the upgrade software was delivered using Electronic Software Delivery (ESD), you will have an ESD logical volume on your system, which must be removed to free up disk space. Remove the ESD logical volume by performing the following steps.

Attention: When you remove the ESD logical volume from the CS 2000 Core Manager, the removal is permanent.

- a Access the storage level:
`sdmmtc storage`
 - b Remove the ESD logical volume and its contents:
`esddel`
 - c When prompted, confirm the Delete command:
`y`
 - d Exit the maintenance interface:
`quit all`
- 5 If you upgraded from tape, eject the tape from the tape drive and store it in a safe place.
- 6 Remove any DDMS filesets and logical volumes which you no longer require. See the procedure [Removing DDMS filesets on page 740](#).
Attention: Carrier Voice over IP PT-AAL1 offices must perform this procedure.
- 7 Upgrade and configure any client-side application software on the workstations that are used to operate the CS 2000 Core Manager in your network. Refer to the specific application procedures in *CS 2000 Core Manager Configuration Management*, NN10104-511.
Note: You may need to contact your system administrator, as client-side upgrades require secure access to the workstations.
- 8 If the CS 2000 Core Manager has now been successfully upgraded to the new software load, but the CS 2000 Management Tools server is not yet upgraded, a communication outage between the server and the core can occur.
To re-establish the communication, stop and start the DDMS proxy on the CS 2000 Management Tools server. Refer to [Stopping and starting the DDMS proxy on page 737](#).
- 9 Stop and start the Tomcat Servlet Container component on the CS 2000 Management Tools server. Refer to [Stopping and starting the Apache Web Server and Tomcat Servlet Container on page 745](#).
- 10 Apply additional software patches that were not included on the upgrade media (tape or ESD load). Contact your Operations management office to determine if and when any patches need to be applied to your system. If you need to apply a patch, use the procedure [Upgrading the CS 2000 Core Manager with](#)

[software patches on page 683](#). For more information, contact your next level of support.

At the IEMS

11

ATTENTION

A degradation in the performance of IEMS results and duplicate logs are generated if both the CS 2000 Core Manager and Core Element Manager (CEM) have been added to the IEMS. Only the CS 2000 Core Manager or only the CEM should be used to manage devices.

Determine whether the CS 2000 Core Manager or CEM have been added to the IEMS.

- a** Launch the IEMS Java Web Start Client (refer to “Launching IEMS Java Web Start Client” in *IEMS Basics*, NN10329-111).
- b** Select the Element Managers topology panel in the IEMS Topologies tree.
- c** In the list of element managers that displays, determine whether the CS 2000 Core Manager or the CEM is present.

12 Use the following table to determine your next step.

If	Do
the CS 2000 Core Manager has been added to the IEMS	step 13
the CEM has been added to the IEMS as the element manager	step 14

13 Edit the object properties in the IEMS for the CS 2000 Core Manager you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the Device Version field.

- [Editing and viewing object properties using Web Client on page 2261](#)
- [Editing and viewing object properties using Java Web Start Client on page 2255](#)

14 Exit from the IEMS Java Web Start Client.

- 15 You have completed this procedure. Return to [CS2000 Core Manager upgrade tasks on page 549](#)

Preparing the repository server for the CS 2000 Core Manager load

Preparing the repository server for the CS 2000 Core Manager load

ATTENTION

This procedure is performed on the repository server and not on the CS 2000 Core Manager. The procedure transfers the CS 2000 Core Manager load to the repository server, through FTP. In a different procedure performed later during the upgrade, the CS 2000 Core Manager load is then transferred from the repository server to the CS 2000 Core Manager.

On the client workstation

- 1 Choose a directory location on the repository server to which the CS 2000 Core Manager load can be transferred by FTP. Ensure that this location has sufficient space for the load and its subsequent extraction. To determine space availability on the server, use the `df -k` command.

The uncompressed tar file for a major release of an CS 2000 Core Manager software load usually ranges from 1 to 1.5 gigabytes. You will need this amount of space for the uncompressed tar file, in addition to at least the same amount for the file's extracted content. It is recommended that you have a total of at least 5 gigabytes available.

- 2 Change to repository directory:

```
cd <directory_path_A>
```

where

<directory_path_A>

is the directory location on the repository server to which the CS 2000 Core Manager load is transferred, uncompressed and untarred

- 3 Create a directory for the CS 2000 Core Manager product load:

```
mkdir <load>
```

where

<load>

is the software load you are updating to

- 4 Access this new directory:
cd <load>
- 5 Display your directory:
pwd
- 6 Transfer the CS 2000 Core Manager product load by FTP to the repository server at your current location. After you have completed this step, the CS 2000 Core Manager load (a compressed tar file) appears in your current location.
- 7 List the files in the directory:
ls -al
In the list that displays, note the order name shown for the new load, for use in step [9](#)
- 8 Check the disk space availability on the server:
df -k.
The system displays the free unallocated disk space.
- 9 Depending on the tool you have available, unzip the file using one of the following commands:
gunzip <order_name>.tar.gz
or
gzip -d <order_name>.tar.gz
where
<order_name>
is the order name for the current load of this release, that was shown in the listing displayed in step [7](#)
Note: Depending on the computing capabilities of the repository server and the size of the load file, the decompression process can take from 8 to 10 minutes.
- 10 List the files in the directory:
ls -al
In the list that displays, note the order name shown for the new load, for use in step [11](#).
- 11 Unarchive (un tar) the filesets:
tar -xvf <order_name>.tar
where

<order_name>

is the order name for the current load of this release, that was shown in the listing displayed in step [10](#)

The system displays a listing of each file as it is unarchived and placed in the current directory.

Note: If errors (such as insufficient disk space) occur during the untarring process, resolve the errors and repeat this step.

- 12 Note the path to the directory created during the un-tar activity for later use (when using FTP to transfer files to the CS 2000 Core Manager).
- 13 Use the following table to determine your next step.

If you	Do
want to delete the tar file to conserve disk space	step 14
do not want to delete the tar file	step 16

14

**CAUTION**

Be sure that untarring the load file was successful (that is, that the disk did not run out of space during the extraction) or that the load is still available on the server from which you obtained the load.

To conserve disk space, remove the tar file:

```
rm <order_name>.tar
```

where

<order_name>

is the order name for the current load of this release

- 15 Go to step [17](#).
- 16 Move the tar file to a different directory:

```
mv <file_name> <directory_path>
```

where

<file name>

is the name of the tar file

<directory path>

is the location of the directory to which you are moving the tar file

- 17** You have completed this procedure. Return to step [2](#) in procedure [Preparing to upgrade the CS 2000 Core Manager](#)

Applying the SDM_CERTS.Certs package

Attention: If you are upgrading from the SN08 version of the CS 2000 Core Manager software, you must apply the corresponding SN08 version of the SDM_CERTS.Certs package. If you are upgrading from the SN09 version of the CS 2000 Core Manager software, you must apply the corresponding SN09 version of the SDM_CERTS.Certs package.

Applying the SDM_CERTS.Certs package

On the CS 2000 Core Manager

- 1 Access the SDM maintenance interface

sdmmtc

- 2 Access the SWIM level

swim

- 3 List the filesets

apply <directory path>

where <directory path> is the directory where the filesets are located

Note: <directory path> can be the /swd/sdm/esd directory.

- 4 Verify that the SDM_CERTS.Certs package listed in the available filesets on the system

If	Do
the SDM_CERTS.Certs package is listed	step 6
the SDM_CERTS.Certs package is not listed	step 5

- 5 Use either the load tape from the release you are upgrading from or the load repository server and download the SDM_CERT.Certs package for the current load on the CS 2000 Core Manager (see Attention above).

Go to step [1](#).

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

If	Do
the SDM_CERTS.Certs package is installed	step 10
the SDM_CERTS.Certs package is not installed	step 7

- 7 Select the SDM_CERTS.Certs package
select <n>
where
 <n>
 is the number next to the SDM_CERTS.Certs fileset
- 8 Apply the SDM_CERTS.Certs fileset:
apply
- 9 When prompted, confirm the apply command:
y
- 10 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Preparing the CS 2000 Core Manager for file transfer from the repository server

Preparing the CS 2000 Core Manager for file transfer from the repository server

At the client workstation

- 1 Log into the CS 2000 Core Manager as a user authorized to perform config-admin actions.
- 2 Use the following table to determine your next step:

If	Do
you want to convert an existing logical volume	step 3
you do not want to convert an existing logical volume	step 6

- 3 Access the logical volume directory that you want to convert:
cd <directory_path>
where
<directory_path>
is the logical volume directory that you want to convert

4



CAUTION

The rm command will remove all files and subdirectories from the current directory. Make sure that you are in the correct directory by typing pwd. The system displays the name of the current working directory. If it is the directory that you want to convert, proceed with the rm command. Otherwise, repeat step [3](#) to access the directory that you want to convert.

Remove all files and subdirectories within this logical volume directory:

rm -r *

- 5 Perform a backup using the procedure “Creating system image backup tapes (S-tape) manually” in *CS 2000 Core Manager*

Security and Administration, NN10170-611, so that you can restore your system at any time if necessary.

If the alarm is enabled, and you choose not to perform a backup, you can force-clear the alarm using the procedure “Clearing a system image backup Required or Failed alarm” in *CS 2000 Core Manager Fault Management*, NN10082-911.

- 6 Access the storage level:

sdmmtc storage

- 7 Add a logical volume to store the ESD loads:

esdadd

The system prompts you to enter a logical volume to be converted to the /swd/sdm/esd standard.

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

Note: When converting a logical volume to the /swd/sdm/esd standard, no contents are changed in the old logical volume.

If you	Do
want to convert an existing logical volume	enter the name of the logical volume to be converted (including the leading forward slash (/) symbol), press the Enter key, and go to step 10
do not want to convert an existing logical volume	press the Enter key and go to step 9

The CS 2000 Core Manager goes to in-service trouble (ISTb) and the status of the Backup Status alarm is Required once a logical volume is converted to the /swd/sdm/esd standard. If the backup Required alarm is disabled, the alarm is not raised

- 9 When prompted, enter the size (in MB) of the logical volume, or press the Enter key to accept the default value of 2000 MB.

Select the default size. If you do not enter a large enough size for the logical volume, you cannot put the entire load on the system. If necessary, you can increase the size of a logical volume using the procedure “Increasing the size of a logical volume” in the *CS 2000 Core Manager Security and Administration*, NN10170-611.

The logical volume /swd/sdm/esd is created.

- 10 Exit the maintenance interface:
quit all
- 11 Change to the /swd/sdm/esd upgrade directory:
cd /swd/sdm/esd
- 12 Establish an FTP session to the repository server where the ESD CS 2000 Core Manager load files are located:
ftp <repository_server>
where
<repository_server>
is the host name or IP address of the server owned by the operating company that was selected to be the destination for ESD software
- 13 Log in to the repository server.
- 14 Change directory to where the CS 2000 Core Manager load files are located on the repository server:
cd <esd_directory>
where
<esd_directory>
is the directory that contains the CS 2000 Core Manager load files.
- 15 Set the local directory:
lcd /swd/sdm/esd
- 16 Change the transfer mode to binary:
bin
- 17 Turn Interactive mode off:
prompt off
- 18 Transfer the load files to the /swd/sdm/esd directory:
mget *
- 19 Exit from the FTP session:
quit
- 20 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Capturing the pre-check session file

It is recommended that you capture the execution of the pre-check session and store the file on the CS 2000 Core Manager for ten days. Nortel support engineers can use the file to investigate any pre-check step that failed.

To capture the upgrade pre-check session, complete the following steps before starting the pre-check procedure.

Capturing the pre-check session file

At the CS 2000 Core Manager VT100 console

- 1 Start the capture of the pre-check session:

```
script -a sdmcheckcheck_YYMMDD
```

where

YYMMDD

is the current year, month, and day that the pre-check procedure is performed

The system creates a file named sdmcheckcheck_YYMMDD and places it in your current directory.

- 2 When you complete all the pre-check tasks, press Ctrl + D to terminate the capture for the sdmcheckcheck_YYMMDD session file.
- 3 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Performing basic pre-checks

Before beginning the software upgrade process, ensure that you have completed the following activities.

Performing basic pre-checks

At your CS 2000 Core Manager server

- 1 Notify the Network Operation Center before you perform this procedure and before you perform the software upgrade procedure, as both procedures can temporarily raise alarms on the core and CS 2000 Core Manager.
- 2 If DCE is configured on the CS 2000 Core Manager, obtain cell_admin password.

Note: In release SN09U, commissioning of DCE is not supported. If DCE already exists on the CS 2000 Core Manager, however, it is supported.

- 3 Obtain the IP address for the CS 2000 Core Manager, the core, and the operating company gateway and LAN (local area network).
- 4 Ensure you have the latest Maintenance Non-Computing Load (MNCL) release installed on the CS 2000 Core Manager before you upgrade to the new NCL release.
- 5 Ensure that all released DMS core-side SDM patches have been applied and that the SDM is at patch current status.
- 6 Ensure that all released DMS core-side CS 2000 Core Manager patches have been applied and that the CS 2000 Core Manager is at patch current status.
- 7 Ensure that the modem is configured and operational in the event that Nortel Field Support personnel require remote access to the CS 2000 Core Manager.
- 8 Obtain a 3-gigabyte blank DAT tape to perform a full system backup following the upgrade.

Ensure that you have selected one of the brands and lengths approved by Nortel. The approved brands are: Hewlett Packard (HP), Maxell, Verbatim, Imation. The approved lengths (from any of the listed manufacturers) are: 90-meter (90M), 120-meter (120M), or 125-meter (125M). The 125M tape is approved for UMFIOS only, provided that your system is equipped with DDS3-capable devices to read the content of the tape.

- 9 Test the SDM for CNR (call notification record) Delivery and CIPC Provisioning (applies to GEM-only applications).
- 10 Check your VT100 terminals and cables.
- 11 Clean tape drive 0 (slot 2) and tape drive 1 (slot 13) if you are upgrading from tape. Refer to the procedure "Cleaning the DAT drive" in *CS 2000 Core Manager Fault Management*, NN10082-911.
- 12 Execute a `querysdm config` command on the CS 2000 Core Manager and record the output for reference purposes.
- 13 Execute a `sdmmtc hw` command on the CS 2000 Core Manager to check if you have an X.25 device installed. Record the output for reference purposes.
- 14 Ensure that the following hardware spares are on site (check which versions of these cards you have on your system):
 - CPU controller card
 - DS512 controller card
 - spare hard drive module
 - spare DAT/hard drive module
- 15 Ensure that adequate backup space is available on the core, because the upgrade procedure stops the Billing Application for
 - over 1 hour (OOS Upgrade Procedure)
 - approximately 20 minutes (ESUP)

To determine the amount of backup space required, refer to "Preparing for SBA installation and configuration" in *CS 2000 Core Manager Accounting*, NN10126-811. To reconfigure backup volumes, refer to "Configuring SBA backup volumes" in *CS 2000 Core Manager Accounting*, NN10126-811.
- 16 Obtain the OAM and CALLP Gateway IP addresses for the Ethernet configuration pre-check from the system administrator.
- 17 List the loads installed on the CS 2000 Core Manager, by entering the following command at the command line:
`querysdm loads`

In response to this command, the system will display the loads and software fixes currently installed on the CS 2000 Core Manager, and the status of these software loads and fixes.
- 18 Display the latest configured SBA schedule by entering the following command at the command line:
`/sdm/sba/DMS500/bin/schedulelist`

- 19 You have completed this procedure. Return to step [6](#) of the procedure [Preparing to upgrade the CS 2000 Core Manager](#)

Preparing a system audit pre-check

The purpose of the system audit pre-check is to execute a sanity check on various components of the CS 2000 Core Manager. For more information on the system audit functionality, refer to the “System audit overview” in *CS 2000 Core Manager Basics*, NN10018-111.

Note: Once the core manager is upgraded to the new software load, the system audit will run automatically on a daily basis.

Installing the system audit script

At the VT100 console

- 1 Determine whether the system audit functionality exists on your CS 2000 Core Manager:

```
ls -l /sdm/mtce/smm/sysaudit
```

If sysaudit script	Do
does not exist on your system	step 2
exists on your system	Performing the system audit pre-check on page 586

- 2 Determine the fileset source.

If the fileset is	Do
on tape	insert the tape into slot 2, and continue with step 3 and wait until the tape drive stabilizes (yellow LED is off) before you proceed.
in a directory	obtain the directory path where the fileset is located, and continue with step 4

- 3 Install the system audit precheck software from tape:

```
installp -ad /dev/rmt0 SDM_PRECHECK.sysaudit
```

Example response:

installp: Please mount volume 1 on /dev/rmt0.1.

Press the Enter to key to continue.

Example response:

```
+-----+
```

```
Pre-installation Verification...
+-----+
Verifying selections...done
Verifying requisites...done
Results...

SUCSESSES
-----
Filesets listed in this section passed
pre-installation verification and will be
installed.

Selected Filesets
-----
SDM_PRECHECK.sysaudit 1.0.0.0      # System
pre-check                               tools

<< End of Success Section >>

FILESET STATISTICS
-----
1  Selected to be installed, of which:
1  Passed pre-installation verification
1  Total to be installed

+-----+
Installing Software...
+-----+

installp:      APPLYING software for:
              SDM_PRECHECK.sysaudit 1.0.0.0

Finished processing all filesets.  (Total time:
                                   1 mins 44 secs).

+-----+
Summaries:
+-----+

Installation Summary
-----
Name              Level      Part   Event    Result
-----
---SDM_PRECHECK.  1.0.0.0   USR    APPLY
SUCCESS sysaudit
```

Once you have completed this step, go to [Performing the system audit pre-check on page 586](#).

- 4 Install the system audit precheck software from a directory:

```
installp -ad <dir> SDM_PRECHECK.sysaudit
```

where:

<dir>

is the directory where the fileset is located

Example response:

```
+-----+
      Pre-installation Verification...
+-----+
Verifying selections...done
Verifying requisites...done
Results...

SUCSESSES
-----
Filesets listed in this section passed
pre-installation verification and will be
installed.

Selected Filesets
-----
SDM_PRECHECK.sysaudit 1.0.0.0      # System
pre-check                                     tools

<< End of Success Section >>

FILESET STATISTICS
-----
      1  Selected to be installed, of which:
          1  Passed pre-installation verification
          1  Total to be installed
+-----+
      Installing Software...
+-----+
installp:      APPLYING software for:
              SDM_PRECHECK.sysaudit 1.0.0.0

Finished processing all filesets. (Total time:
                                1 mins 44 secs).
```

```
+-----+
                        Summaries:
+-----+
Installation Summary
-----
Name                  Level      Part      Event      Result
-----
----SDM_PRECHECK.    1.0.0.0    USR        APPLY
SUCCESS
sysaudit
```

- 5 You have completed this procedure. Complete procedure [Performing the system audit pre-check](#).

Performing the system audit pre-check

At the VT100 console

- 1 Execute the system audit check:

sysaudit -all

Example response:

sysaudit command is in progress, please wait a few minutes for it to complete...

- 2 Display the system audit report:

sysaudit -report

Use the procedure “Viewing the system audit report and taking corrective action” in *CS 2000 Core Manager Fault Management*, NN10082-911 (start at step 2) to analyze the report and take corrective action, if necessary.

- 3 Return to the default directory:

cd

- 4 You have completed this procedure. Return to step [7](#) of the procedure [Preparing to upgrade the CS 2000 Core Manager](#)

Performing a hardware baseline pre-check

The purpose of the hardware baseline pre-check is to display the hardware PEC codes and ensure compatibility with the hardware baseline.

You must upgrade any hardware that does not meet the minimum hardware baseline before you proceed with the software upgrade.

Performing the hardware baseline pre-check

At the VT100 console

- 1 Display the information for the hardware that is installed on the CS 2000 Core Manager:
locate
- 2 Refer to [Hardware baseline on page 550](#) and verify that the product engineering codes (PECs) on the output meet the minimum hardware baseline. You need to check only the PECs for the cards located in the numbered slots in the report that is displayed in response to the locate command.
- 3 You have completed this procedure. Return to [8](#) of procedure [Preparing to upgrade the CS 2000 Core Manager](#)

Performing a CPU stability pre-check

The purpose of the CPU stability pre-check is to ensure that the master and checker CPU is operating as expected. The master CPU is taken Offline and then returned to service.



CAUTION
Executing this procedure causes a temporary loss of fault-tolerance.

Because the master CPU is Offlined, the system is in a NON-Fault tolerant mode for the duration of the pre-check.

Performing the CPU stability pre-check

At the VT100 console

- 1 Determine which CPU is currently master:

ftctl -status

Example response:

```
CPUmodule CPU-0:
  Current istate      = present
                      powered on
                      significant
                      checker
                      using backplane signals
  Current condition   = online
  Online start date   = Sun Mar 17 12:52:53 CST 2002
  Online duration     = 23 days, 06:52:36
CPUmodule CPU-1:
  Current istate      = not present
  Current condition   = offline
CPUmodule CPU-2:
  Current istate      = present
                      powered on
                      significant
                      master
                      using backplane signals
  Current condition   = online
  Master start date   = Sun Mar 17 12:44:37 CST 2002
  Master duration     = 23 days, 07:00:52
Online start date     = Sun Mar 17 12:44:37 CST 2002
Online duration       = 23 days, 07:00:52
```

Note: CPU 0 is installed in Domain 0. CPU 2 is installed in Domain 1.

- 2 Access the hardware level to determine if the CPU modules are in service:

sdmmtc hw

Example response:

```

SDM  CON  512  NET  APPL  SYS  HW  CLLI: OTWAONXBEC3
.      .      .      .      .      .      .
.      .      .      .      .      .      .
Hw
0 Quit
2      I  F  C  D  D  D  E  E  D  5
3      C  A  P  S  S  S  T  T  A  1
4 Logs  M  N  U  K  K  K  H  H  T  2
5      1  2  3  1  2
6      Domain 0 . . . . .
7 Bsy  Domain 1 . . . . .
8 RTS
9
10
11      ↕
12      ↕
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh
root
Time 11:15 >

```

3 Busy the master CPU:

bsy <domain> cpu

where

<domain>

is the domain number of the master CPU identified in step 1.

Example

bsy 1 cpu

Example response:

```

SDM  CON  512  NET  APPL  SYS  HW  CLI: OTWAONXBEC3
.      .      .      .      .      .      Host: pcary989
.      .      .      .      .      .      Fault Tolerant

Hw
0 Quit
2      I F C D D D E E D 5
3      C A P S S S T T A 1
4 Logs  M N U K K K H H T 2
5      1 2 3 1 2
6      Domain 0 . . . . .
7 Bsy   Domain 1 . . M . . . .
8 RTS
9
10
11
12
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh
root
Time 11:17 >

```

- 4 Return the busy CPU to service:

rts <domain> cpu

where

<domain>

is the domain number of the master CPU you busied in the previous step [3](#)

Example

rts 1 cpu

*The CPU status changes from M (busy) to I (re-integration).
Re-integration time will vary depending on system configuration.*

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

If the rts command	Do
succeeds	step 7
fails	step 6

- 6 The CPU reintegration can fail because the system is too busy. To determine that, examine the eeprom on the failing CPU and look for the following message: PRI: System too busy, PRI could not complete.

Example response:

```
# eeprom -vL CPU-2
.
.
```

```
Event      Time - Date      Failure Category &
Reason
=====
=====
```

```
Power on 13:59 Mar 11 2002 EST
```

```
Failure 13:59 Mar 11 2002 EST Information
report
```

```
PRI: System too busy, PRI could not complete
```

This message does not indicate a faulty CPU (no matter how many times it fails). This message means that the system is presently too busy to reintegrate the CPUs, and the reintegration must be deferred until the system load is reduced. You can attempt the reintegration as many times as necessary, until it succeeds. To reduce the system load, you may have to busy SBA or the SDM from the core using a maintenance window.

Once you have successfully reintegrated the CPUs, go to step [7](#).

- 7 Exit the hardware level:

```
quit all
```

- 8 Monitor the integration status of the CPU:

```
ftctl -status
```

Example response:

```

CPUmodule CPU-0:
  Current istate      = present
                    powered on
                    significant
                    master
                    using backplane signals
  Current condition   = online
  Master start date   = Fri Apr 26 11:37:54 EDT 2002
  Master duration     = 00:07:50
  Online start date   = Tue Apr 23 17:11:30 EDT 2002
  Online duration     = 2 days, 18:34:14
CPUmodule CPU-1:
  Current istate      = not present
  Current condition   = offline
CPUmodule CPU-2:
  Current istate      = present
                    powered on
                    not significant
                    onboard
                    not using backplane signals
  Current condition   = integrating (12% complete)
```

- 9 Wait until the CPU has been fully integrated, then re-enter the hardware level to ensure that the CPU has returned to service:

sdmmtc hw

Example response:

```

SDM   CON  512  NET  APPL SYS  HW  CLI: OTWAONXBEC3
.      .    .    .    .    .    .  Host: pcary989
.      .    .    .    .    .    .  Fault Tolerant

Hw
0 Quit
2      I F C D D D E E D 5
3      C A P S S S T T A 1
4 Logs M N U K K K H H T 2
5      1 2 3 1 2
6      Domain 0 . . . . .
7 Bsy  Domain 1 . . . . .
8 RTS
9
10
11
12
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh
root
Time 11:47 >

```

- 10 Repeat steps [3](#) to [9](#) for the second CPU. For example, if previously you have busied and returned to service CPU 1, repeat steps [3](#) to [9](#) for CPU 0.
- 11 You have completed this procedure. Return to step [9](#) in procedure [Preparing to upgrade the CS 2000 Core Manager](#)

Performing a DS512 fiber link pre-check

The purpose of the DS512 fiber link pre-check is to identify potential problems with the DS512 fiber links connected from the core to the DS512 controller modules on the CS 2000 Core Manager. It can also identify problems with DS512 modules.

**CAUTION****Possible loss of communication to the core**

The DS512 fiber link pre-check results in a temporary simplex condition on CS 2000 Core Manager links to the core. Therefore, you must perform the DS512 fiber link pre-check during a maintenance shift to ensure that the traffic on the DS512 links does not lead to message overload conditions, which can result in a loss of communication with the call server.

At the MAP terminal

- 1 Access the SDM level of the MAPCI:
mapci;mtc;appl;sdm
- 2 Identify the message switch (MS) chain cards that are configured with the DS512 controller modules and the associated DS512 fiber links that communicate from the core to the CS 2000 Core Manager:

trns1

Example response:

```

XAC  MS  IOD  Net  PM  CCS  Lns  Trks  Ext  APPL
.      .      .      .      .      .      .      .      .      .

SDM      OAMAPT ATMFW  SDM  SPMCP  SWMTC  SDMBIL  TOPSIP
0 Quit
2
3      SDM 0 InSv  Links_OOS:.
4
5 Trns1
6      Trns1
7 Bsy      SDM 0 DOMAIN 0 PORT 0 (MS 0:05:0) OK  MsgCnd:Open
8 RTS      SDM 0 DOMAIN 0 PORT 1 (MS 1:05:0) OK  MsgCnd:Open
9 OffL     SDM 0 DOMAIN 1 PORT 0 (MS 0:05:1) OK  MsgCnd:Open
10         SDM 0 DOMAIN 1 PORT 1 (MS 1:05:1) OK  MsgCnd:Open
11
12
13
14 QuerySDM
15 Locate
16
17
18 Platform
  ADMIN
Time 11:28 >

```

- 3 Post the chain card that corresponds to one of the four associated DS512 fiber links that communicate with the CS 2000 Core Manager.

mapci;mtc; ms;shelf;chain <chain_number>

where:

<chain_number>

is the number of the MS chain card

Example

mapci;mtc;ms;shelf;chain 5

Example response:

```

XAC  MS  IOD  Net  PM  CCS  Lns  Trks  Ext  APPL
.    .    .    .    .    .    .    .    .    .

CHAIN  I      Message Switch  Clock Shelf 0  Inter-MS Link 0 1
0 Quit  MS 0      .      Master      .      ..
2      MS 1      .      Slave      .      ..
3
4      Shelf0      1 1 1 1
5      Card 1 2 3 4 5 6 7 8 9 0 1 2 3
6 Tst_  Chain      < > |
7 Bsy_  MS 0      .      .      .      .      .      .
8 RTS_  MS 1      .      .      .      .      .      .
9 Offl_
10      Chain 05      Range  Link 0 1
11      MS 0      .      05-06  DS512 . .
12 Chain_ MS 1      .      05-06  DS512 . .
13 Card_
14 QueryMS 6
15 Tmsl_
16
17
18
OPERATOR
Time 11:53 >

```

- 4 Busy the DS512 fiber links that correspond to the DS512 card to be busied:

bsy 0 link <link_number>

bsy 1 link <link_number>

where:

<link_number>

is the number of the DS512 link (0 or 1)

Example

bsy 0 link 0

and

Example

bsy 1 link 0

The previous examples will busy MS 0 link 0 and MS 1 link 0 for the DS512 card on domain 0.

At the VT100 console

- 5 Access the hardware level:

```
sdmmtc hw
```

- 6 Busy the DS512 controller module:

```
bsy <domain_number> 512
```

where:

<domain_number>

is the domain number of the DS512 link

- 7 Return the DS512 controller module to service:

```
rts <domain_number> 512
```

where:

<domain_number>

is the domain number of the DS512 link

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

If the DS512 controller module	Do
returns to service	step 11
does not return to service	contact your next level of support

At the MAP terminal

- 9 Return the DS512 fiber links that correspond to the DS512 card to service:

```
rts 0 link <link_number>
```

```
rts 1 link <link_number>
```

where

<link_number>

is the number of the DS512 link (0 or 1)

Example

rts 0 link 0

and

Example

rts 1 link 0

The previous examples will return MS 0 link 0 and MS 1 link 0 for the DS512 card on domain 0 to service.

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

If the links	Do
return to service	step 11
do not return to service	contact your next level of support

- 11** Repeat the previous steps until each of the DS512 Controller Modules has been busied and returned-to-service successfully.
- 12** You have completed this procedure. Return to step [10](#) of procedure [Preparing to upgrade the CS 2000 Core Manager](#)

Performing an application and fileset status and configuration pre-check

The purpose of the application/fileset status and configuration pre-check is to verify that the applications on the CS 2000 Core Manager are in-service and configured.

At the VT100 console

- 1 Access the application level:

sdmmtc appl

Example response:

```

SDM  CON  512  NET  APPL  SYS  HW  CLLI: OTWAONXBEC3
      .      .      .      .      .      .      Host: pcary989
      .      .      .      .      .      .      Fault Tolerant
Appl
0 Quit
2      # Application                                State
3      1 SDM Billing Application                      .
4 Logs  2 Generic Data Delivery                     .
5      3 Log Delivery Service                        .
6      4 Image Dump Service                          .
7 Bsy   5 Secure File Transfer                      .
8 RTS   6 Enhanced Terminal Access                  .
9 OffL  7 Table Access Service                      .
10      8 OM Access Service                          .
11      Applications showing: 1 to 8 of 8
12 Up
13 Down
14 QuerySDM
15 Locate
16
17 Help
18 Refresh
root
Time 06:30 >

```

- 2 Verify that all applications used are in service as represented by the in-service dot [.] under the State header, as shown in the previous example. Use the up/down commands to scroll through the list of applications if necessary.

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

If	Do
all applications are in service	step 4
one or more applications are not in service	investigate and return to service if required before you proceed

- 4 Access the configuration level:

config

Example response:

```

SDM  CON  512  NET  APPL  SYS  HW  CLI: OTWAONXBEC3
      .    .    .    .    .    .    .    Host: pcary989
      .    .    .    .    .    .    .    Fault Tolerant
Config
0 Quit      Filter: OFF
2          # Fileset Description          Status
3          1 Enhanced Terminal Access    Configured
4          2 OM Delivery                   Configured
5          3 Remote Registration System    Configured
6          4 SDM Billing Application        Configured
7 Select    5 Secure File Transfer         Secure and Normal FTP Access
8 Config          Configuration programs: 1 to 5 of 5
9
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 18:55 >

```

- 5 Verify that all required in-service applications are configured as shown in the previous example graphic. Use the up/down commands to scroll through the list of applications if necessary.

- 6 You have completed this procedure. Return to step [11](#) of procedure [Performing an application and fileset status and configuration pre-check](#)

Performing a user configuration pre-check

The purpose of the user configuration pre-check is to ensure that the CS 2000 Core Manager user attributes are configured correctly.

Performing the user configuration pre-check

At the VT100 console

- 1 Display the user attributes for the root user:
`lsuser root`
- 2 Display the user attributes for the maint user:
`lsuser maint`

Example response:

```
3004-687 User "root" does not exist.
```

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

If the user	Do
does not exist	contact your next level of support
exists	step 4

- 4 You have completed this procedure. Return to step [12](#) of procedure [Preparing to upgrade the CS 2000 Core Manager](#)

Performing an Ethernet configuration pre-check

The purpose of the Ethernet configuration pre-check is to display the status and configuration of the Ethernet interfaces.

Performing the Ethernet configuration pre-check

At the VT100 console

- 1 Obtain and record the IP gateway addresses for Ethernet interface ent0 and ent1.
- 2 Display the Ethernet configuration and status:

```
lsstate -s | grep ent
```

The system will display the Ethernet configuration. The following is an example of this kind of display:

Example response:

```
pent0 c1-f2 Available online Physical Ethernet Device
pent1 c1-f4 Available online Physical Ethernet Device
pent2 c1-f13 Available online Physical Ethernet Device
pent3 c1-f15 Available online Physical Ethernet Device
ent0 Available online_both FT Logical Ethernet
ent1 Available online_both FT Logical Ethernet
```

dbgent

The system will display the Ethernet status. The following is an example of this kind of display:

Example response:

ent1:

```
member0 pent1 active (08:00:3e:26:25:21) PM: online
member1 pent3 backup (08:00:3e:26:25:25) PM: online
```

ent0:

```
member0 pent0 backup (08:00:3e:26:25:24) PM: online
member1 pent2 active (08:00:3e:26:25:20) PM: online
```

- 3 Using the information obtained in step [1](#), verify that the selected external network element can be reached.

```
ping -c 3 <ip_address>
```

The following example shows a sample ping command used to ping the Gateway router for ent0 and the format of the results that the system displays in response:

```
# ping -c 3 47.101.50.112
PING 47.101.50.112:(47.101.50.112): 56 data bytes
64 bytes from 47.101.50.112: icmp_seq=0 ttl=61 time=1 ms
64 bytes from 47.101.50.112: icmp_seq=1 ttl=61 time=1 ms
64 bytes from 47.101.50.112: icmp_seq=2 ttl=61 time=1 ms

----47.101.50.112 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=1/1/1 ms
```

- 4 Switch the active and backup Ethernet interface members:

```
dbgent -sl entn
```

where

n
is either 0 or 1

Example
dbgent -sl ent0

- 5 Verify that the switch occurred.

```
dbgent
```

The following examples show that the active and backup Ethernet interface members for ent0 have switched. Compare the display for ent0 with that for ent0 in step 2 in the example response to the dbgent command.

Example response:

ent1:

```
member0 pent1 active (08:00:3e:26:25:21) PM: online
member1 pent3 backup (08:00:3e:26:25:25) PM: online
```

ent0:

```
member0 pent0 active (08:00:3e:26:25:20) PM: online
member1 pent2 backup (08:00:3e:26:25:24) PM: online
```

- 6 Using the information obtained in step 1, verify that the selected external network element can still be reached.

ping -c 3 <ip_address>

The following example response shows a sample ping command used to ping the Gateway router for ent0 and the format of the results that the system displays in response:

```
# ping -c 3 47.101.50.112
PING 47.101.50.112:(47.101.50.112): 56 data bytes
64 bytes from 47.101.50.112: icmp_seq=0 ttl=61 time=1 ms
64 bytes from 47.101.50.112: icmp_seq=1 ttl=61 time=1 ms
64 bytes from 47.101.50.112: icmp_seq=2 ttl=61 time=1 ms

----47.101.50.112 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=1/1/1 ms
```

- 7 Switch the active and backup Ethernet interfaces.

dbgent -sl entn

where

n
is either 0 or 1

Example
dbgent -sl ent0

- 8 Verify that the switch occurred.

dbgent

The following examples show that the active and backup Ethernet interface members for ent0 have switched. Compare the display for ent0 with that for ent0 in step 5 in the example response to the dbgent command.

Example response:

ent1:

```
member0 pent1 active (08:00:3e:26:25:21) PM: online
member1 pent3 backup (08:00:3e:26:25:25) PM: online
```

ent0:

```
member0 pent0 backup (08:00:3e:26:25:24) PM: online
```

member1 pent2 active (08:00:3e:26:25:20) PM: online

- 9** Repeat steps [3](#) through [8](#) for the second Ethernet (ent0 or ent1).
- 10** You have completed this procedure. Return to step [13](#) of procedure [Preparing to upgrade the CS 2000 Core Manager](#)

Performing a system dump device pre-check

The purpose of the System dump device pre-check is to verify that the system dump devices are not in the null state. If either device is in the null state, your upgrade will fail.

Performing the system dump device pre-check

At the VT100 console

- 1 Verify the system dump (sysdump) devices by completing the following steps.

Start the verification:

```
sysdumpdev -l
```

Note: In the previous command, the “l” is a lower-case letter L.

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

If the following message is displayed	Do
primary/dev/sysdump0 secondary/dev/sysdumpnull copy directory/var/adm/ras forced copy flagFALSE always allow dumpFALSE dump compressionOFF	step 3
primary/dev/sysdump0 secondary/dev/sysdump1 copy directory/var/adm/ras forced copy flagFALSE always allow dumpFALSE dump compressionOFF	step 4

- 3 Change the sysdump devices to sysdump1:

```
sysdumpdev -P -s /dev/sysdump1
```

The following message is displayed.

```
primary/dev/sysdump0  
secondary/dev/sysdump1  
copy directory/var/adm/ras  
forced copy flagFALSE  
always allow dumpFALSE  
dump compressionOFF
```

- 4 You have completed this procedure. Return to step [14](#) of [Preparing to upgrade the CS 2000 Core Manager](#)

Preparing for system software upgrades from tape

ATTENTION

If you are planning to upgrade your system from tape, upload the software from tape to a disk, and then upgrade your system from the directory created during this procedure, in order to avoid any potential tape problems during the upgrade.

The purpose of transferring the upgrade software from tape to a disk is to help ensure a trouble-free upgrade by avoiding tape problems that can occur during the upgrade.

Installing the UPGRADE Tools fileset

At the VT100 console

- 1 Log on to the CS 2000 Core Manager using the root user ID and password.
- 2 Verify that tape drive 0 (slot 2) and tape drive 1 (slot 13) have been cleaned. If not, clean both tape drives now. Refer to the procedure "Cleaning the DAT drive" in *CS 2000 Core Manager Fault Management*, NN10082-911.
- 3 Insert the tape into the tape drive in slot 2 (DAT0) or slot 13 (DAT1).
- 4 Install the software that will be used later to copy the content of the tape to a disk, using one of the following commands.
 - If the tape is inserted in slot 2:

```
bffcreate -d /dev/rmt0.1 -t /home/swd -q  
SDM_UPGRADE
```
 - If the tape is inserted in slot 13:

```
bffcreate -d /dev/rmt1.1 -t /home/swd -q  
SDM_UPGRADE
```
- 5 Access the maintenance interface:

```
sdmmtc
```
- 6 List the filesets in directory /home/swd:

```
apply /home/swd
```

Ignore the warning messages that the system displays. Wait until the command is complete and continue with the procedure.

- 7 Select the UPGRADE Tools fileset:
select <x>
where
<x>
is the number next to the UPGRADE Tools fileset
- 8 Install the UPGRADE Tools fileset:
apply
- 9 Use the following table to determine your next step.

If	Do
the command fails, and the following message is displayed: Create the FIXES filesystem from sdmmtc; fixes and retry this, then the FIXES directory does not exist on the core manager.	create the FIXES directory using step 10
the command succeeds,	step 14

- 10 The FIXES directory does not exist on the core manager. Create the FIXES directory:
sdmmtc fixes
- 11 Exit from the maintenance interface:
quit all
- 12 Enter the maintenance interface:
sdmmtc
- 13 Return to step [6](#) and continue.
- 14 If prompted, confirm the apply command:
y
- 15 Exit the sdmmtc interface:
quit all
- 16 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Uploading the software from tape to a disk

At the VT100 console

- 1 Start the process of transferring the software load from tape to a disk:

unpacktape

- 2 When prompted, select automatic or interactive method for creating the logical volume where the tape content is transferred. Enter one of the following values:

where

- 1 creates the logical volume
- 2 creates the logical volume or allows you to select an existing logical volume

If there is not enough disk space on your system, the procedure will automatically abort. Contact your next level of support for further instructions.

- 3 When prompted, enter the location of the tape:

where

- 1 is used if the tape is inserted in slot 2
- 2 is used if the tape is inserted in slot 13

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

If in step 2 you have selected option	Do
automatic	the system provides the location of the directory where the tape load is being transferred. <i>Record the directory path for reference</i> , then go to step 9 .
interactive	continue with step 5

- 5 When prompted, specify whether you want to transfer the tape load to an existing logical volume. Enter one of the following values:

Note: If using an existing logical volume, make sure that you have at least 1400 Mbytes of free space in the volume.

where

yes

is used if you want to transfer the load to an existing logical volume

no

is used if you want to create a new logical volume

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

If you entered	Do
yes	enter the directory path where you want to transfer the load, and press the Enter key. Go to step 9 .
no	go to step 7

- 7 To continue the procedure, enter:

yes

- 8 When prompted, enter the full path to the new directory where the new logical volume is mounted.

If the system reports that there is insufficient free space on datavg and rootvg, the system aborts the procedure. Contact your next level of support for further instructions.

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

If the system	Do
completes the transfer and displays the following message: Successfully deposited all filesets to <directory name> Record the directory path for reference.	go to step 12
displays a failure message	go to step 10
Note: If this is your second attempt to complete the procedure, contact your next level of support.	

- 10 Clean the DAT drive where the tape is inserted. Refer to the procedure "Cleaning the DAT drive" in *CS 2000 Core Manager Fault Management*, NN10082-911.
- 11 Once the DAT drive is clean, repeat steps [1](#) through [9](#).

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

Upgrading CS 2000 Core Manager software using ESUP

This procedure provides information about upgrading the CS 2000 Core Manager to the new software release using an enhanced SDM upgrade procedure (ESUP).

Note: This procedure does not apply to rootvg-only systems.

This procedure references other procedures in the following NTPs:

- *CS 2000 Core Manager Fault Management*, NN10082-911
- *CS 2000 Core Manager Configuration Management*, NN10104-511
- *CS 2000 Core Manager Accounting*, NN10126-811
- *CS 2000 Core Manager Security and Administration*, NN10170-611

Ensure that you have access to those documents while performing this procedure.

You can perform this procedure from a VT100 console. You can also use this procedure if you are able to telnet to the CS 2000 Core Manager through the LAN (local area network).

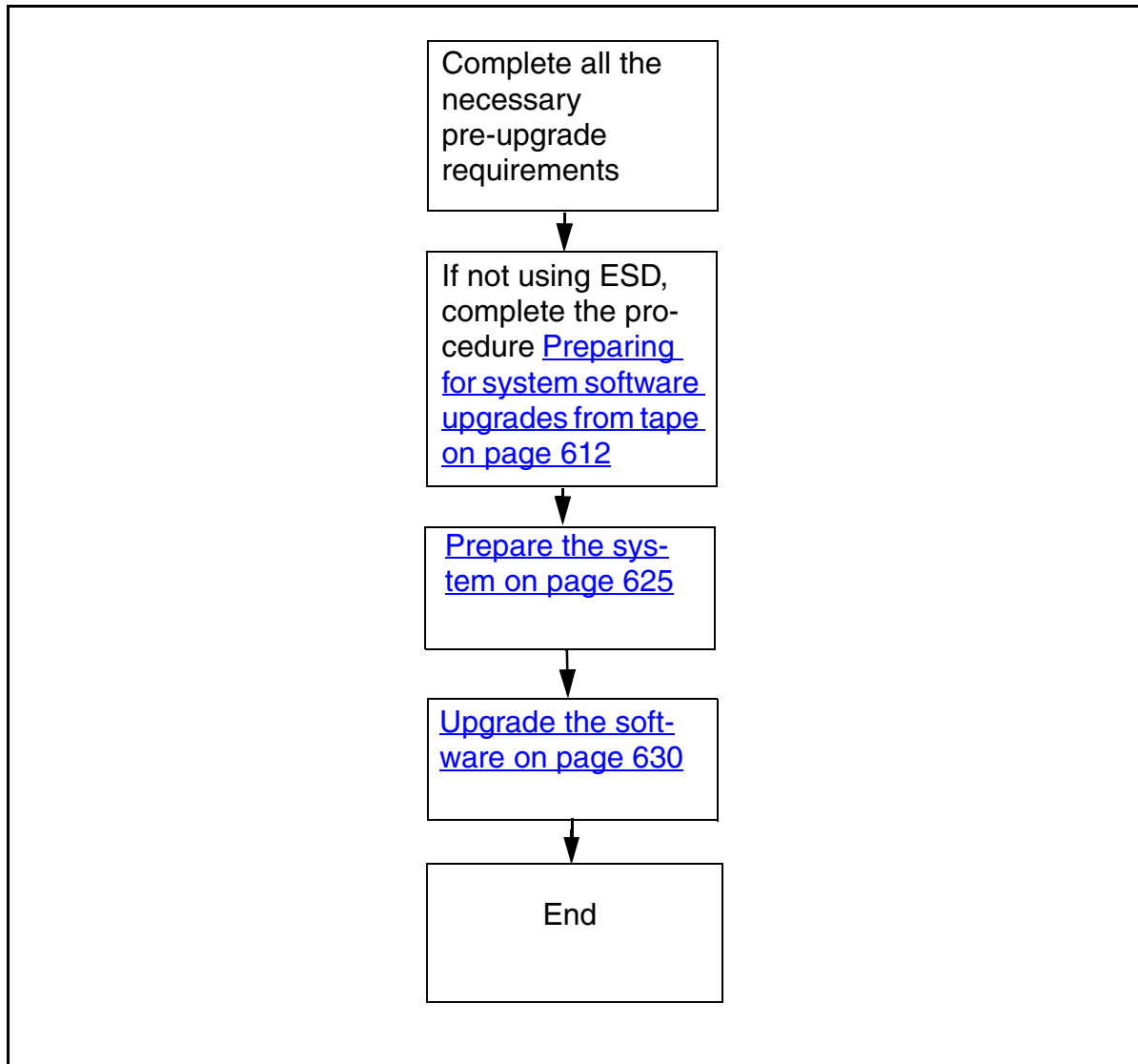
During the ESUP upgrade, the rootvg mirror is broken, the system is busied for a short time, then rootvg disks are re-integrated. The procedure takes approximately 2.5 hours. Datavg mirroring is not broken during this procedure; therefore, it does not undergo re-integration.

ATTENTION

This procedure provides on-screen information and instructions. Please read all displayed messages carefully and use them together with this high-level procedure to successfully complete the upgrade.

Task flow diagram

Use the following task flow to upgrade the CS 2000 Core Manager using the enhanced software upgrade procedure (ESUP).

Task flow for upgrading CS 2000 Core Manager software using ESUP**ATTENTION**

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

Pre-upgrade requirements

ATTENTION

Nortel recommends the usage of the system console (SP0) for the upgrade. When upgrading the software using ESUP using TELNET, ensure that the device used to connect to the console port (modem, VDU - Visual Display Unit or VT-100 terminal, terminal server, dual input VDU, etc.) is configured with flow control off. Failure to turn off flow control can cause the SDM to hang during the reboot conducted at the end of each upgrade.

Before starting this procedure, complete the following activities:

- Ensure the latest MNCL release is installed on your system.

Refer to [Fileset-to-solution mapping on page 555](#) for the software baseline.

Note: If you need to upgrade to the latest MNCL, refer to the MNCL release notes for instructions.

- Perform a system image backup.

ATTENTION

Nortel recommends that you perform a system image backup before you upgrade the base software. Use the procedure “Creating system image backup tapes (S-tapes) manually” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

Performing a system image backup does not back up billing data. Ensure that billing is operating properly before starting.

If you need to revert to a prior release during an out-of-service upgrade, refer to “Performing a full restore of the software from S-tape” in *CS 2000 Core Manager Fault Management*, NN10082-911.

- Ensure that no other users are logged on during the upgrade. Only the user at the VT100 console or the upgrade telnet session can be logged on during the upgrade.
- Obtain the IP address for the CS 2000 Core Manager.
- Execute a `querysdm config` command and record the output.

- Obtain and record the following information from your network administrator:
 - if your system has a CS 2000 SAM21 Manager installed, verify whether DNS is supported on CS 2000 SAM21 Manager client workstations
 - the host name of the CS 2000 Management Tools server that is configured to run the Login Application
 - the CommonName from the certificate on the CS 2000 Management Tools server that is configured to run the Login Application
 - the IP address of the CS 2000 Management Tools server
- If upgrading from tape, ensure that you have the tape labeled for the new software release.

Note: Nortel recommends that you upgrade your system directly from tape only if you are unable to complete the procedure [Uploading the software from tape to a disk on page 614](#).

- Install and configure the pserver application on the Preside MDM. This applies to Carrier Voice over IP offices where the CS 2000 Core Manager needs to communicate with the Preside MDM for fault data using the Passport log streamer application. Refer to the Passport 15000 and Preside MDM sections in *Solution-level Fault Management Troubleshooting*, NN10198-912, for instructions on how to configure the pserver application.
- Ensure that the system is equipped with a datavg. The CS 2000 Core Manager must be equipped with a data volume group (datavg). You can check the presence of a datavg through the maintenance interface under the storage level (sdmmtc storage).
- Check the root logical volume file system - potential disk space error. Make sure the root logical volume or file system does not exceed 70% of its total size. If the root file system exceeds the 70% mark, you must make more room on it for the upgrade to be successful. The /usr logical volume must have a minimum size of 1050Mb. Before starting the upgrade, ensure that /usr is less than 50% full. For more details, contact your next level of support.
- Ensure the CS 2000 Core Manager is alarm free. If any alarms are present, refer to the *CS 2000 Core Manager Fault Management*, NN10082-911, for alarm-clearing procedures.
- Ensure that you either
 - Have VT100 terminal emulation.Before you perform this procedure, it is recommended that you

ensure that your terminal is capable of VT100 terminal emulation and that you can establish a VT100 connection to SP0.

or

- Have a PC or UNIX workstation connected to the LAN.
Ensure that you have access to a PC or UNIX workstation from which you are able to telnet and access the CS 2000 Core Manager through the LAN. Also, verify that telnet is enabled on the CS 2000 Core Manager.
- If you have SBA on your system, query the status of RTB for each billing stream for which RTB is configured. Record all RTB streams that are InSv for reference purposes.

Note: If required, refer to the procedure “Querying the status of RTB for a billing stream” in *CS 2000 Core Manager Accounting*, NN10126-811.

- Nortel recommends that you deliver unprocessed billing files to a downstream destination. Ensure that no more than one unprocessed billing file remains on the system. The following table lists each task and the procedure in *CS 2000 Core Manager Accounting*, NN10126-811, to complete the task.

Accounting procedure for each task and file transfer mode

Task	File transfer mode	Accounting procedure
Close billing files	All	“Closing billing files”
Send billing files downstream	Outbound file transfer (OFT)	“Sending billing files from disk”
	Inbound file transfer (IFT)	“Retrieving billing files for a stream set to inbound file transfer”
	Real time billing (RTB)	“Sending billing files from disk”

Accounting procedure for each task and file transfer mode

Task	File transfer mode	Accounting procedure
	Automatic file transfer (AFT)	No manual action is required. Wait for SBA to deliver pending billing files to the downstream destination. There should be no pending files (at least, not more than one) for each AFT session. Use the following commands to query AFT sessions: billmtc, appl, aft, aftcfg, list. To verify which billing files for each session are still pending, enter the following commands: billmtc, appl, aft, query <session_name>. Note: Press the Enter key after each command.

To display the details about a stream, refer to the procedure “Listing billing streams” in *CS 2000 Core Manager Accounting*. To list all files currently stored in a stream, refer to the procedure “Listing billing files” in *CS 2000 Core Manager Accounting*, NN10126-811.

If you are unable to send billing files to a downstream destination and you want to proceed with the upgrade, Nortel recommends that you backup the billing files to a DAT tape. If required, refer to the procedure “Copying billing files to tape (backup)” in *CS 2000 Core Manager Accounting*, NN10126-811.

If you need to restore the billing files from tape and you have AFT or IFT configuration, contact your next level of support for instructions. For any other configuration, you can send the billing files from tape following the procedure “Sending billing files from tape” in *CS 2000 Core Manager Accounting*, NN10126-811.

- Remove and offline the Ineo SSH Secure File Transfer application using the procedure [Removing the Ineo SSH Secure File Transfer application on page 622](#)

Removing the Ineo SSH Secure File Transfer application

At the VT100 console or telnet session

- 1 Log on to the CS 2000 Core Manager using the root user ID and password

- 2 Access the application level of the SDMMTC interface:

sdmmtc appl

- 3 In the display, locate the Ineo SSH Secure File Transfer application.

If	Do
Ineo SSH Secure File Transfer is installed on your system	step 4
Ineo SSH Secure File Transfer is not installed on your system	step 11

- 4 If the Ineo SSH Secure File Transfer application is in service, busy it and take it offline:

bsy <number>

where

<number>

is the number displayed on the screen that is associated with the Ineo SSH Secure File Transfer application

- 5 Take the Ineo SSH Secure File Transfer application offline:

offl <number>

where

<number>

is the number displayed on the screen that is associated with the Ineo SSH Secure File Transfer application

- 6 Access the details level:

details

- 7 Select the Ineo SSH Secure File Transfer application for removal from the system:

select <number>

where

<number>

is the number displayed on the screen that is associated with the Ineo SSH Secure File Transfer application

- 8 Remove the Ineo SSH Secure File Transfer application from the system:

remove

The system will provide output similar to that in the following example:

```
WARNING: If you proceed with this action, all
versions of the following fileset will be
removed from the system.
```

```
Ineo SSH Secure File Transfer
```

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

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

- 9** Confirm the removal of this application:

```
Yes
```

- 10** Exit from the maintenance interface:

```
quit all
```

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

Post-upgrade notes

If, after an ESUP upgrade, the source command (at the sdmmtc/apply level) fails, the following message is displayed: Create the FIXES filesystem from sdmmtc;fixes and retry this. This message displays when the FIXES directory does not exist on the core manager. You should, then, create the FIXES directory as requested in this message.

Upgrade notices

**CAUTION****Possible upgrade failure**

Do not login into any of the /alt_inst file systems at any stage of the upgrade. This can cause the upgrade to fail and start an automatic recovery.

ATTENTION

Some applications that are obsolete in the new release are automatically removed.

If the Exception Reporting, Alarm Conduit, SDM Corba Framework, and Remote Registration System filesets are present, they are automatically removed when upgrading to the new software load.

ATTENTION

In cases of fallback, You can abort this procedure at every prompt. If you choose to abort before the system reboots, follow the on-screen instructions to recover the system. If you choose to abort after the system reboots, complete the procedure [Recovering the system from an ESUP failure on page 649](#)

If the CS 2000 Core Manager system initiates an automatic fallback during this procedure, contact your next level of support before attempting the recovery procedure.

Prepare the system

Use the following procedure to prepare the system for an upgrade.

Prerequisites

The following prerequisites apply to this procedure:

ATTENTION

Read the [Pre-upgrade requirements on page 619](#) and [Upgrade notices on page 625](#) sections, and complete any necessary activities before you proceed with the upgrade.

At the PC or UNIX workstation

- 1 Determine how you will connect to the CS 2000 Core Manager.

If you choose	Do
telnet session	step 2
VT100 console	step 5

- 2 Establish a telnet connection to the CS 2000 Core Manager by opening a terminal window that is VT100 compatible.
- 3 Log onto the CS 2000 Core Manager from the terminal window prompt:
telnet <ip_address>
where
<ip_address>
is the IP address of the CS2000 Core Manager
- 4 Keep window size at 80x24.

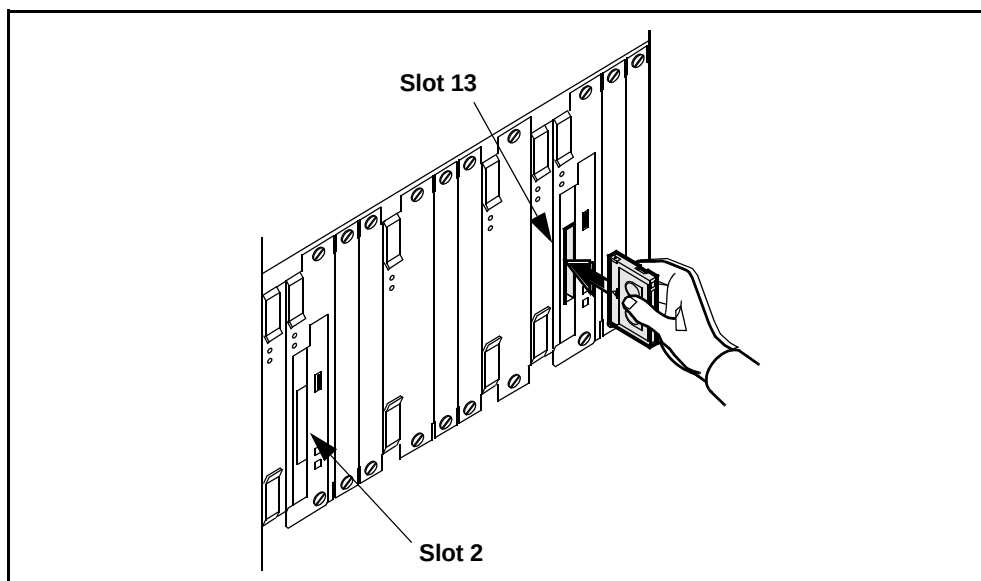
At the VT100 console or telnet session

- 5 Log on to the CS 2000 Core Manager as a user authorized to perform config-admin actions.
- 6 If you are upgrading from tape (not from ESD), verify that the procedure [Uploading the software from tape to a disk on page 614](#) has been completed. If not, perform the procedure now.

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

If you are upgrading from	Do
a directory, such as one directory created during ESD or during procedure Uploading the software from tape to a disk on page 614	step 8
directly from tape (not recommended; use this option only if you are unable to upload the software from tape to a disk)	insert the tape labeled for the new software load into the tape drive in slot 13 (DAT1) as shown in the following figure, and continue with step 8 . Note: Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

Main chassis tape drive



- 8 Remove all archived filesets from the system, which will free up disk space:
- Access the Details level:
- sdmmtc details**
- 9 Show all software:
- filter off**

- 10 Select all archived filesets:

select all

Note: If there are no archived filesets to remove, go to step [14](#).

- 11 Remove all archived filesets:

remove all

System will automatically select appropriate files to remove.

- 12 Confirm the command:

y

Once you remove the archived filesets, the state of the CS 2000 Core Manager changes to in-service trouble (ISTb), and the status of the Backup Status alarm indicates: Required. If the backup Required alarm is disabled, the alarm will not be raised. If the alarm is enabled, perform a backup of your new system image using procedure “Creating system image backup tapes (S-tape) manually” in *CS 2000 Core Manager Security and Administration*, NN10170-611. If you choose not to perform a backup, you can force-clear the alarm using procedure “Clearing a system image backup Required or Failed alarm” in *CS 2000 Core Manager Fault Management*, NN10082-911.

- 13 After removing the archived filesets, ensure that /usr logical volume is less than 50% full. To check the % full value of /usr, enter the following command:

sdmmtc storage

If /usr is more than 50% full, refer to procedure “Increasing the size of a logical volume” in *CS 2000 Core Manager Security and Administration*, NN10170-611, to increase the /usr logical volume size as required. The /usr logical volume must have minimum size of 1050Mb.

- 14 Exit the maintenance interface:

quit all

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

If you	Do
have pre-loaded the software from tape, as described in procedure Uploading the software from tape to a disk on page 614	go to step 18
are upgrading your system from an ESD directory (not after tape pre-loading)	go to step 17
are upgrading your system directly from tape inserted in slot 13	go to step 16

- 16 Install the Upgrade Tools fileset:

```
installp -ad /dev/rmt1 SDM_UPGRADE.tools
```

When prompted, press the Enter key again.

Go to step [18](#).

- 17 Install the Upgrade Tools fileset:

```
installp -ad <directory> SDM_UPGRADE.tools
```

where

<directory>

is the directory where the software is located

When prompted, press the Enter key again.

- 18 Install the ESUP software:

```
esupinstall
```

- 19 When prompted, select the location of the software load: one of the following values:

0

if you are upgrading directly from the tape in slot 2

Note: Nortel recommends that you do not use slot 2. Use slot 13 instead.

1

if you are upgrading directly from the tape in slot 13

D

if you are upgrading from a directory (ESD or pre-loaded from tape)

ABORT

if you wish to abort the procedure

If you entered	Do
D	step 20
0, 1, or ABORT	step 21

- 20** When prompted, enter the directory path where the software load is located.
- 21** Wait until the system completes the installation (up to 10 min).
When completed, the following message is displayed:
SUCCESSFULLY INSTALLED SOFTWARE FOR ESUP
- 22** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Upgrade the software

ATTENTION

All application filesets are upgraded during this procedure, except the SDM Billing Application (SBA), the SBA Automatic File Transfer (AFT) application, upgrade these application filesets after the ESUP portion of this procedure.

At the PC or UNIX workstation

- 1** Determine how you will connect to the CS 2000 Core Manager.

If you choose	Do
telnet session	step 2
VT100 console	step 5

- 2** Establish a telnet connection to the CS 2000 Core Manager by opening a terminal window that is VT100 compatible.
- 3** Log onto the CS 2000 Core Manager from the terminal window prompt:
telnet <ip_address>
where

<ip_address>

is the IP address of the CS2000 Core Manager

- 4 Keep window size at 80x24.

At the VT100 console or telnet session

- 5 When prompted, log in as a user authorized to perform config-admin actions.
- 6 Begin the upgrade:
esup
The system lists all stages of the upgrade and gives you the choice to continue the upgrade or to abort (go/abort).
- 7 To continue, type
go
- 8 When prompted to select the upgrade type, use the following table to determine your next step.

If	Do
you choose to upgrade to a higher release	type 1 and press the Enter key, then go to step 11
you choose to perform a patch-only upgrade (only patches are applied, and no other files are applied)	type 2 and press the Enter key, then go to step 9

Note: If you wish to abort, enter abort.

- 9 When prompted to enter the directory location for the patches, use the following table to determine your next step.

If the patch files	Do
are located in the default ESD directory /swd/sdm/esd	Enter go and press the Enter key.
are not located in the default directory	Enter the directory path where the patch files are located and then press the Enter key.

- 10** The system verifies the content of the directory and informs you if you entered the wrong path.

If the directory is	Do
correct, the system continues the upgrade procedure until it prompts you to busy the SDM.	step 21
not correct	1. Re-type the directory path, press the Enter key. The system continues the upgrade procedure until it prompts you to busy the SDM. Go to step 21

- 11** When prompted to select the media type, use the following table to determine your next step.

If you are upgrading from	Do
a directory (ESD or pre-loaded from tape)	type 2 and press the Enter key, then go to step 15
directly from tape	type 1 and press the Enter key, then go to step 12

Note: If you wish to abort, enter 0.

- 12** The system displays the following response:

The following device has been selected to perform the upgrade:

Media Type: TAPE /dev/rmt1

Continue (yes or no)>

Note: /dev/rmt1 is the device name for the tape drive in slot 13 (DAT1).

Verify that the displayed media type is correct and continue the upgrade:

yes

The system reports all automatic sub-processes that are taking place during this stage, as well as the start time for each

process. Also displayed is an estimated duration for each process.

Note: The estimated time may not be exact. Allow some additional time. However, if the process continues much longer than the estimate, contact your next level of support.

- 13 When prompted to insert the tape, use the following table to determine your next step.

If at this point the tape	Do
is not inserted	insert the tape labeled for the new software load into the tape drive in slot 13, enter go and press the Enter key
is inserted	make sure that the tape is in the correct drive, enter go and press the Enter key

- 14 The system verifies the content of the tape and informs you if the wrong tape is inserted.

If the inserted tape is	Do
correct, the system continues the upgrade procedure until it prompts you to busy the SDM.	step 18
not correct	1. Replace it with the tape labeled for the new software load, enter go and press the Enter key. 2. Go to step 18

- 15 The system confirms that you have selected Media Type: DISK. Continue the upgrade:

yes

Note: If you wish to abort the procedure, enter no.

The system reports all automatic sub-processes that are taking place during this stage, as well as the start time for each process. Also displayed is an estimated duration for each process.

Note: The estimated time may not be exact. Allow some additional time. However, if the process continues much longer than the estimate, contact your next level of support.

- 16 When prompted to enter the directory location for the new NCL load, use the following table to determine your next step.

If the new software load files	Do
are located in the default ESD directory /swd/sdm/esd	enter go and press the Enter key
are not located in the default directory, or are located in the directory created during the procedure Uploading the software from tape to a disk on page 614 .	enter the directory path where the files are located, then press the Enter key

- 17 The system verifies the content of the directory and informs you if you entered the wrong path.

If the directory is	Do
correct	step 18
not correct	re-type the directory path, press the Enter key, then go to step 18

- 18 When you are prompted as to whether you want to install patches, use the following table to determine your next step.

If	Do
you want to install patches	step 19
you do not want to install patches, the system continues the upgrade procedure until it prompts you to busy the SDM.	step 21

Note: If you wish to abort, enter abort.

- 19 When prompted to enter directory location for patches, use the following table to determine your next step.

If the patch files	Do
are located in the default ESD directory /swd/sdm/esd	enter go and press the Enter key
are not located in the default ESD directory	enter the directory path where the patch files are located, then press the Enter key.

- 20** The system verifies the content of the directory and informs you if you entered the wrong path.

If the directory is	Do
correct, the system continues the upgrade procedure until it prompts you to busy the SDM.	step 21
not correct	1. Re-type the directory path, press the Enter key. The system continues the upgrade procedure until it prompts you to busy the SDM. Go to step 21

- 21**

ATTENTION

Before the system prompts you to busy the SDM it automatically sets AFT and SBA applications into offline state. ESUP will automatically brings them back in service after the SDM reboots and is returned into service.

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

If	
your office is equipped with a third-party Call Agent	step 26
your office not equipped with a third-party Call Agent	step 30

At the PC or UNIX workstation

- 23** Establish a telnet connection to the CS 2000 Core Manager. Open a terminal window that is VT100 compatible.
- Log onto the CS 2000 Core Manager from the terminal window prompt:
- ```
telnet <ip_address>
```
- where



**<ip\_address>**

is the IP address of the CS 2000 Core Manager

- 24 Keep window size at 80x24.
- 25 When prompted, log in as a user authorized to perform config-admin actions.
- 26 Busy the CS 2000 Core Manager. Access the SDM maintenance level by typing  
**sdmmtc;mtc**
- 27 Busy the CS 2000 Core Manager by typing  
**bsy**
- 28 Confirm the busy request by typing  
**y**
- 29 Continue with step [33](#).

***At the MAP display***

- 30 Busy the CS 2000 Core Manager level at the MAP display accessing the SDM level of the MAP display:  
**mapci;mtc;appl;sdm**
- 31 Busy the CS 2000 Core Manager:  
**bsy**
- 32 Confirm the busy request:  
**y**

***At the MAP display***

- 33 Verify that each billing stream has entered the active backup mode by posting and querying each of your billing streams.  
**sdbmil;post<stream>;query**

**At the VT100 console or telnet session**

- 34** Continue the procedure, by typing  
**go**

**Note:** Until the CS 2000 Core Manager is fully busy, the system displays the following message: Waiting for SDM BSY.

The system automatically reboots. This process can take up to ten minutes.

**Note:** If the upgrade is being done using telnet, the system reboot will close the telnet session.

- 35** Wait until the system has finished rebooting. Use the following table to determine your next step:

| If you are using | Do                            |
|------------------|-------------------------------|
| VT100 console    | go to step <a href="#">37</a> |
| Telnet session   | go to step <a href="#">36</a> |

The upgrade automatically continues.

**At the PC or UNIX workstation**

- 36** The reboot process closed the previous telnet session. Re-establish a new telnet session:

**telnet <ip\_address>**

where

**<ip\_address>**  
is the IP address of the SDM

**Note:** Keep window size at 80x24

**At the VT100 console or telnet session**

- 37** When prompted, log in as a user authorized to perform config-admin actions.
- 38** Continue the upgrade:  
**esup**

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

| If you are                             | Do                      |
|----------------------------------------|-------------------------|
| prompted to configure DDMS clients     | step <a href="#">40</a> |
| not prompted to configure DDMS clients | step <a href="#">46</a> |

- 40 Configure the DDMS clients which are the CS 2000 Management tools servers with the SESM load.
- 41 To display a list of existing client IP addresses, from the DDMS Clients Configuration menu select option 3: List existing clients. Use the IP addresses listed to add clients as required.
- 42 Add a new client:
- 1
- 43 When prompted, enter the IP address for each of the CS 2000 Management tools servers. Press the Enter key after each entry.
- 44 Type **done** once you have entered all the IP addresses.
- 45 Exit the DDMS clients configuration screen:
- 0
- Note:** You can reconfigure the OSS Comms Svcs at any time through the sdmmtc config level.
- 46 If you have the DNBD Call Monitoring Application on your system, upgrade it by following the appropriate procedure in the International Lawful Interception NTP, and then return to step [47](#)
- 47 Use the following table to determine your next step.

| If your office                                | Do                      |
|-----------------------------------------------|-------------------------|
| is equipped with a third-party Call Agent     | step <a href="#">48</a> |
| is not equipped with a third-party Call Agent | step <a href="#">56</a> |

**At the PC or UNIX workstation**

- 48 Access the Application level of the CS 2000 Core Manager maintenance interface:
- ```
sdmmtc appl
```
- 49 Locate and busy the OSS Comms Svcs application:
- ```
bsy <x>
```
- where

<x>

is the number next to the OSS Comms Svcs fileset

- 50 Return the OSS Comms Svcs application to service:

**rts <x>**

where

<x>

is the number next to the OSS Comms Svcs fileset

- 51 Continue with step [52](#) (the system automatically returns to service).

***At the VT100 console or telnet session***

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

| If your office                                | Do                                                                                  |
|-----------------------------------------------|-------------------------------------------------------------------------------------|
| is equipped with a third-party Call Agent     | continue with step <a href="#">53</a> (the system automatically returns to service) |
| is not equipped with a third-party Call Agent | when prompted to return the SDM to service, go to step <a href="#">56</a>           |

***At the PC or UNIX workstation***

- 53 The reboot process closed the previous telnet session. Re-establish a new telnet session:

**telnet <ip\_address>**

where

<ip\_address>

is the IP address of the SDM

**Note:** Keep window size at 80x24

***At the VT100 console or telnet session***

- 54 When prompted, log in as a user authorized to perform config-admin actions.

- 55 Continue the procedure:

**esup**

*The upgrade continues until you are prompted to return the SDM to service.*

**At the MAP display**

- 56 When prompted, return the CS 2000 Core Manager to service by accessing the SDM level of the MAP display:

**mapci;mtc;appl;sdm**

- 57 Return the CS 2000 Core Manager to service:

**rts**

**Note:** Ensure that the CS 2000 Core Manager has returned to service completely before performing step [58](#).

**At the VT100 console or telnet session**

- 58 Continue by typing

**go**

*The following response: Waiting for SDM RTS, will appear until the system is fully in service. It will take 2 to 10 minutes for the CS 2000 Core Manager to return to service.*

**At the MAP display**

- 59 Verify that all billing streams are either in-service or in recovery on the CS 2000 Core Manager side:

**sdbmil;post<stream>;query**

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

| If your system                                                                         | Do                      |
|----------------------------------------------------------------------------------------|-------------------------|
| has CS 2000 SAM21 Manager application, and you are upgrading from CS2E0070 or CS2E0080 | step <a href="#">61</a> |
| does not have CS 2000 SAM21 Manager application                                        | step <a href="#">68</a> |

**At the PC or UNIX workstation**

- 61 Configure CS 2000 SAM21 Manager application. Locate and have available your records from the [Pre-upgrade requirements](#) section.

- 62 Access the Config level:

**sdbmtc config**

- 63 Start the configuration process:

**config <x>**

where

&lt;x&gt;

is the number next to the SAM21 Manager application

- 64 When prompted whether DNS is supported on CS 2000 SAM21 Manager workstations, enter Y (yes) or N (no), and press the Enter key.

| If you enter | Do                      |
|--------------|-------------------------|
| Y (yes)      | step <a href="#">65</a> |
| N (no)       | step <a href="#">66</a> |

- 65 When prompted, enter the CommonName from the certificate on the CS 2000 Management Tools server that is configured to run the Login Application, and press the Enter key.
- 66 When prompted, enter the host name of the CS 2000 Management Tools server that is configured to run the Login Application, and press the Enter key.
- 67 Exit the maintenance interface:  
**quit all**

***At the VT100 console or telnet session***

- 68 The system displays a message confirming that the CS 2000 Core Manager has been upgraded successfully. Read the message and follow the on-screen instructions. Use the following table to determine your next step.

| If you wish to       | Do                                                                                                                                       |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| continue the upgrade | step <a href="#">69</a>                                                                                                                  |
| abort the upgrade    | type abort and press the Enter key, then complete the procedure <a href="#">Recovering the system from an ESUP failure on page 649</a> . |

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

| If you                         | Do                      |
|--------------------------------|-------------------------|
| have SBA on your system        | step <a href="#">70</a> |
| do not have SBA on your system | step <a href="#">75</a> |

***At the PC or UNIX workstation***

- 70 Establish a telnet connection to the SDM. Open a terminal window that is VT100 compatible.

- 71 Log onto the SDM from the terminal window prompt:  
`telnet <ip_address>`  
where  
`<ip_address>`  
is the IP address of the SDM  
**Note:** Keep window size at 80x24.
- 72 When prompted, log in as a user authorized to perform config-admin actions.
- 73 Query the status of each RTB stream that was InSv before the upgrade (refer to your records from the [Pre-upgrade requirements](#) section). If none were recorded, continue with step [75](#).  
**Note:** If required, refer to the procedure “Querying the status of RTB for a billing stream” in *CS 2000 Core Manager Accounting*, NN10126-811.
- 74 If the status of RTB for any stream changed from InSv to ManB, manually return each of these RTB stream instances to service. Refer to the procedure “Returning RTB stream instance to service” in *CS 2000 Core Manager Accounting*, NN10126-811.

**At the VT100 console or telnet session****75****CAUTION****Possible loss of service**

Once you begin the re-integration process, you cannot use the abort command to return to the previous version of the CS 2000 Core Manager software. If you decide to return to the previous version of the CS 2000 Core Manager software after the reintegration process, you must take the CS 2000 Core Manager off-line and restore the previous version of the CS 2000 Core Manager software from an S-tape. There is a loss of service for several hours when you restore the previous software.

Begin the integration process:

**go**

When the system confirms that the upgrade is complete, go to step [76](#).

**76** Complete any post-upgrade commissioning:

**sdmconfig auto**

**77** If you have the SDM Billing Application (with or without the SBA Automatic File Transfer application), proceed to the section [Upgrade the SBA and AFT applications on page 645](#), and then return to step [78](#).

**78** Determine whether you need to install new applications and services. For information about any new applications and features introduced for the new software release, refer to [New in this release on page 547](#). For a list of applications required for each Succession solution, refer to [Preparing to upgrade the CS 2000 Core Manager on page 550](#). Use the following table to determine your next step.

| If you                                               | Do                      |
|------------------------------------------------------|-------------------------|
| need to install new applications and services        | step <a href="#">79</a> |
| do not need to install new applications and services | step <a href="#">80</a> |



- 79** Install new applications and services. Use either the procedures shown in the table below or the procedures in the CS 2000 Core Manager suite of NTPs that correspond to the applications or services you want to install. Only install the required applications. When you have completed the installations, return to this procedure and proceed to step [80](#).

**Note:** Install new applications and services from the VT100 console.

| Application or service | Installation procedure to use                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| DDMS                   | <a href="#">Installing or upgrading DDMS on page 691</a>                                                                  |
| DCE                    | <a href="#">Upgrading DCE on page 703</a>                                                                                 |
| OMD                    | <a href="#">Installing and configuring the OM Data Delivery application on page 705</a>                                   |
| OpenSSH                | <a href="#">Installing or upgrading OpenSSH on page 713</a>                                                               |
| SPM reach through      | <a href="#">Installing or upgrading Reach Through SPM on page 715</a>                                                     |
| GR740                  | <a href="#">Installing or upgrading the GR740PT application server on page 717</a>                                        |
| Backup restore manager | <a href="#">Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager on page 722</a> |
| CEM filesets           | <a href="#">Installing CEM filesets on page 729</a>                                                                       |
| X.25 connectivity      | <a href="#">Commissioning X.25 connectivity on page 732</a>                                                               |

- 80** You have completed this procedure. Return to [CS2000 Core Manager upgrade tasks on page 549](#).

## Upgrade the SBA and AFT applications

### ATTENTION

During the time period between the end of the ESUP and prior to the completion of the upgrade of the SBA application package, SBA maintenance commands related to stream configuration are not available. Therefore, do not attempt to enter SBA maintenance commands for adding, changing, deleting, or listing a billing stream during that time period.

Complete this procedure only if you have the SDM Billing Application (with or without the SBA Automatic File Transfer application) on your system.

**Note:** If you do not have the SBA Automatic File Transfer (AFT) application, disregard any references to AFT.

### ATTENTION

The following steps stop the SBA for approximately 20 minutes. Ensure that adequate backup space is available on the core before continuing with these steps. To determine the amount of backup space required, refer to the “Disk space requirements” section in “Preparing for SBA installation and configuration” in *CS 2000 Core Manager Accounting*, NN10126-811. To set up the backup space, refer to procedure “Configuring the SBA on the Communication Server 2000 core” in *CS 2000 Core Manager Accounting*, NN10126-811.

### At the VT100 console or telnet session

- 1 Access the maintenance interface:  
**sdmmtc**
- 2 Use the following table to determine your next step.

| If upgrading from                         | Do                     |
|-------------------------------------------|------------------------|
| a directory (ESD or pre-loaded from tape) | step <a href="#">3</a> |
| directly from tape                        | step <a href="#">9</a> |

- 3 List the filesets:

**apply <directory path>**

where

**<directory\_path>**

is the directory where the filesets are located

**Note:** <directory path> can be the /swd/sdm/esd directory.

- 4 If, after an ESUP upgrade, the apply command fails and the following message is displayed: Create the FIXES filesystem from sdmmtc;fixes and retry this, then the FIXES directory does not exist on the CS 2000 Core Manager. Use the following table to determine your next step.

| If upgrading from                                                                                            | Do                                                                |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| If the apply command failed and you received the error message requesting you to create the FIXES filesystem | You must create the FIXES directory. Go to step <a href="#">5</a> |
| If the apply command was successful                                                                          | step <a href="#">10</a>                                           |

- 5 Create the fixes directory:

**sdmmtc fixes**

- 6 Exit from the maintenance interface:

**quit all**

- 7 Restart the maintenance interface:

**sdmmtc**

- 8 Return to step [3](#).

- 9 List the filesets:

**apply <domain\_number>**

where

**<domain\_number>**

indicates the domain where you inserted the tape. Type 0 or 1.

- 10 Select all versions of the SDM Billing Application filesets and, if required, the SBA Automatic File Transfer filesets:

**select <x> <y>**

where

**<x> <y>**

are the numbers next to the SDM Billing Application filesets and the SBA Automatic File Transfer filesets. Specify as many numbers after the command as necessary.

**Note:** If you do not have the SBA Automatic File Transfer application on your system, do not select the AFT filesets.

- 11 Apply the SDM Billing Application fileset and, if required, the SBA Automatic File Transfer fileset:

**apply**

*The system automatically selects the SDM\_ACE fileset, which is required by the SBA and AFT applications. When you confirm the apply command, the system will, if necessary, automatically install the ACE fileset first.*

*Example response*

You have selected to install the following new filesets or fileset updates.

```
SBA Automatic File Transfer xx.xx.xx.x
SDM Billing Application xx.xx.xx.x
```

You did not select the following filesets that are required by some of the selected filesets. If you proceed, they will be applied automatically before the selected filesets.

```
SDM ACE distribution x.x.x.x
```

Do you wish to proceed?  
Please confirm ("YES", "Y", "NO", or "N")

- 12 When prompted, confirm the apply command:

**y**

- 13 Exit the maintenance interface:

**quit all**

- 14 If applicable, access the billing maintenance interface to restart the AFT application:

**billmtc**

- 15 Access the APPL (application) level:

**appl**

- 16 Access the AFT level:  
**aft**
- 17 Restart the AFT application:  
**start <session\_name>**  
*where*  
**<session\_name>**  
is the name of the AFT session
- 18 Exit the billing maintenance interface:  
**quit all**
- 19 You have completed this procedure. Return to step [77](#) in the procedure, [Upgrade the software](#).

---

## Recovering the system from an ESUP failure

---

### Purpose

If an upgrade fails, you must recover the CS 2000 Core Manager from the failure. Follow this procedure to recover the CS 2000 Core Manager from a software failure during an enhanced SDM upgrade procedure (ESUP).

During ESUP, you can choose to abort the procedure at different stages of the upgrade, or the system can initiate an automatic fallback.

Use this procedure only under the following conditions:

- You have chosen to abort the upgrade after the system rebooted.
- After an automatic fallback occurred, your next level of support instructed you to complete this procedure.

### Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Other activities related to using this procedure

| Procedure                                          | Document                                                              |
|----------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager             | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying actions a user is authorized to perform | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

## Procedure

### ATTENTION

This recovery procedure applies only to ESUP upgrades. This procedure is only applicable if you aborted the upgrade after the upgrade system reboot, or if you were instructed to complete this procedure by your next level of support.

### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Recovering the system from an ESUP failure

### *At the PC or UNIX workstation*

- 1 Determine how you will connect to the CS 2000 Core Manager.

| If you choose  | Do                     |
|----------------|------------------------|
| telnet session | step <a href="#">2</a> |
| VT100 console  | step <a href="#">7</a> |

- 2 Establish a telnet connection to the CS 2000 Core Manager by opening a terminal window that is VT100 compatible.
- 3 Log onto the CS 2000 Core Manager from the terminal window prompt:  

```
telnet <ip_address>
```

where  

```
<ip_address>
```

is the IP address of the CS2000 Core Manager
- 4 Keep window size at 80x24.

### *At the VT100 console or telnet session*

- 5 If you are not already logged in and have ESUP activated, when prompted, log in as a user authorized to perform config-admin actions.

- 6 Enter the following command at the shell prompt:

**ESUP**

*The system displays the following message:*

Please BUSY the SDM now!

Enter 'go' once the SDM BSY command has been executed (go):

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

| If you choose                                                | Do                      |
|--------------------------------------------------------------|-------------------------|
| If your office is equipped with a third-party Call Agent     | step <a href="#">8</a>  |
| If your office is not equipped with a third-party Call Agent | step <a href="#">15</a> |

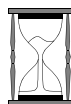
**ATTENTION**

Before the system prompts you to busy the SDM it automatically puts the AFT and SBA applications into an offline state. ESUP automatically brings them back into service after the SDM reboots and is returned into service.

**At the PC or UNIX workstation**

- 8 Establish a telnet connection to the CS 2000 Core Manager. Open a terminal window that is VT100 compatible.
- 9 Log onto the CS 2000 Core Manager from the terminal window prompt:
- ```
telnet <ip_address>
```
- where:
- ```
<ip_address>
```
- is the IP address of the CS 2000 Core Manager
- 10 When prompted, log in as a user authorized to perform config-admin actions.
- 11 Busy the CS 2000 Core Manager. Access the SDM maintenance level:
- ```
sdmmtc;mtc
```
- 12 Busy the CS 2000 Core Manager:
- ```
bsy
```





3 min.

- 13 Confirm the busy request:

y

- 14 Continue with step [18](#).

**At the MAP display**

- 15 Busy the CS 2000 Core Manager. Access the SDM level of the MAP display:

**mapci;mtc;appl;sdm**

- 16 Busy the CS 2000 Core Manager:

**bsy**

- 17 Confirm the busy request:

y

**At the MAP display**

- 18 Verify that each billing stream has entered the active backup mode by posting and querying each of your billing streams:

**sdbil;post<stream>;query**

**At the VT100 console or telnet session**

- 19 When the CS 2000 Core Manager is fully busy, continue the procedure:

**go**

**Note:** Until the CS 2000 Core Manager is fully busied, the system displays the following message: Waiting for SDM BSY.

The system automatically reboots. This process can take up to 10 minutes. If the abort is being done using telnet, the system reboot closes the telnet session.

- 20 Wait until the system has finished rebooting. Use the following table to determine your next step:

| If using a     | Do                      |
|----------------|-------------------------|
| telnet session | step <a href="#">21</a> |
| VT100 console  | step <a href="#">23</a> |

***At the PC or UNIX workstation***

- 21** The reboot process closed the previous telnet session. Re-establish a new telnet connection. Log onto the CS 2000 Core Manager from the terminal window prompt:

```
telnet <ip_address>
```

where

**<ip\_address>**

is the IP address of the CS 2000 Core Manager

- 22** Keep the window size at 80x24.

***At the VT100 console or telnet session***

- 23** When prompted, log in as a user authorized to perform config-admin actions.

- 24** Enter the following command at the shell prompt:

```
esup
```

*The system displays the following message:*

```
Please RTS the SDM now!
```

```
Enter 'go' once the SDM RTS command has been
executed (go):
```

If your office is not equipped with a third-party Call Agent, go to step (the CS 2000 Core Manager automatically returns to service). Otherwise, continue with step.

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

| If you choose                                                                                                            | Do                      |
|--------------------------------------------------------------------------------------------------------------------------|-------------------------|
| If your office is not equipped with a third-party Call Agent (the CS 2000 Core Manager automatically returns to service) | step <a href="#">28</a> |
| Otherwise                                                                                                                | step <a href="#">26</a> |

***At the MAP display***

- 26** Access the SDM level of the MAP display:

```
mapci;mtc;appl;sdm
```

- 27** Return the CS 2000 Core Manager to service:

```
rts
```

***At the VT100 console or telnet session***

- 28** When the system is back in service, type go and press the Enter key.

**go**

*The system responds:*

The message: Waiting for SDM RTS, is displayed until the system is fully in service. It will take 2 to 10 minutes for the CS 2000 Core Manager to return to service on the core side.

***At the MAP display***

- 29** Verify that all billing streams are either in-service or in recovery on the CS 2000 Core Manager side:

**sdbil;post<stream>;query**

***At the PC or UNIX workstation***

- 30** The reboot process closed the previous telnet session. Establish a new telnet connection by logging onto the CS 2000 Core Manager from the terminal window prompt:

**telnet <ip\_address>**

where

**<ip\_address>**

is the IP address of the CS 2000 Core Manager

- 31** When prompted, log in as a user authorized to perform config-admin actions.
- 32** If SBA is configured on your system, query the status of any real time billing (RTB) stream that exists on your system. If the status changed from InSv to ManB after busying the CS 2000 Core Manager, manually return each affected RTB stream to service.

If required, refer to the following procedures in *CS 2000 Core Manager Accounting*, NN10126-811:

- “Querying the status of RTB for a billing stream”
- “Returning RTB stream instance to service”

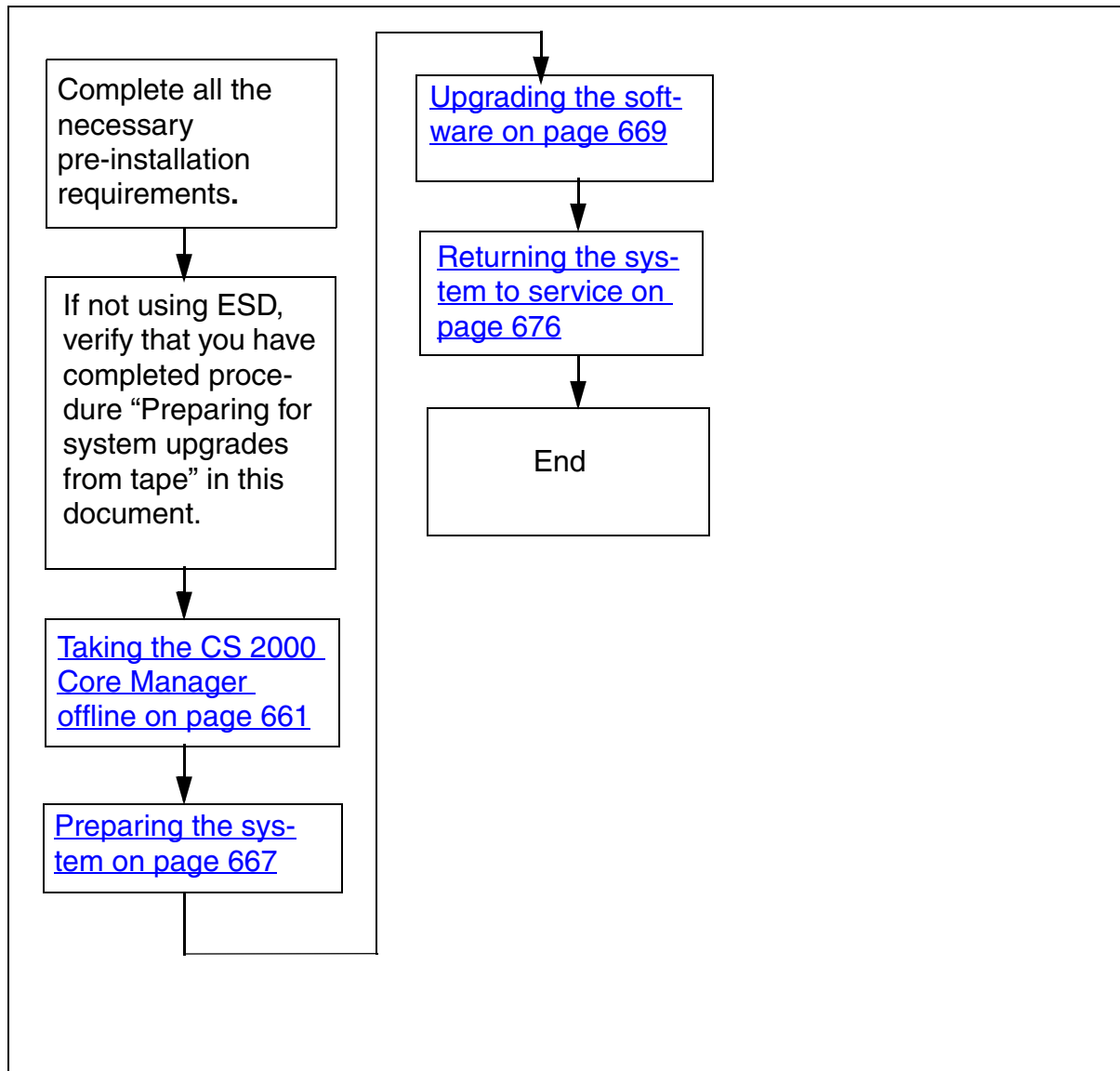
***At the VT100 console or telnet session***

- 33** The recovery process continues until the Abort complete prompt is displayed. This process can take approximately 30 minutes.
- 34** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Upgrading CS 2000 Core Manager software out of service

Use the following task flow to upgrade CS 2000 Core Manager software while the Core Manager is out of service.

### Task flow for upgrading CS 2000 Core Manager software out of service



## Purpose

This procedure describes the process to upgrade the CS 2000 Core Manager to the new software release using the out-of-service (OOS) Upgrade Procedure. During the OOS upgrade, the system is busied and both domains are upgraded at the same time.

This procedure references other procedures in the following NTPs:

- *CS 2000 Core Manager Basics*, NN10018-111
- *CS 2000 Core Manager Fault Management*, NN10082-911
- *CS 2000 Core Manager Configuration Management*, NN10104-511
- *CS 2000 Core Manager Accounting*, NN10126-811
- *CS 2000 Core Manager Security and Administration*, NN10170-611

Ensure that you have access to those documents while performing this procedure.

## Pre-upgrade requirements

Before starting this procedure, complete the following activities:

- Ensure that the latest MNCL release is installed on your system.

Refer to [Fileset-to-solution mapping on page 555](#) for the software baseline.

**Note:** If you need to upgrade to the latest MNCL, refer to the MNCL release notes for instructions.

- Perform a system image backup.

### ATTENTION

Nortel recommends that you perform a system image backup before you upgrade the base software. Use the procedure “Creating system image backup tapes (S-tapes) manually” in *CS 2000 Core Manager Administration and Security*, NN10170-611.

Performing a system image backup does not back up billing data. Ensure that billing is operating properly before starting.

If you need to revert to a prior release during an out-of-service upgrade, refer to “Performing a full restore of the software from S-tape” in *CS 2000 Core Manager Fault Management*, NN10082-911.

- Obtain the password for the user authorized to perform config-admin actions.

You must log on to the CS 2000 Core Manager as a user authorized to perform config-admin actions, to perform the upgrade. Failure to log on as the user authorized to perform config-admin actions can cause your upgrade to fail. Furthermore, ensure that no other users are logged on during the upgrade. Only the user at the VT100 console can be logged on. For a procedure used to determine who is logged on, refer to the section, "Accessing the CS 2000 Core Manager" in *CS 2000 Core Manager Basics*, NN10018-111.

- Obtain and record the following information from your network administrator:
  - if your system has a CS 2000 SAM21 Manager installed, verify whether DNS is configured on the CS 2000 SAM21 Manager client workstations
  - the host name of the CS 2000 Management Tools server that is configured to run the Login Application
  - the CommonName from the certificate on the CS 2000 Management Tools server that is configured to run the Login Application
  - the IP address of the CS 2000 Management Tools server
- Obtain the right tape if upgrading from tape. Ensure that you have the tape labeled for the new software load.
- Ensure the pserver application is installed and configured on the Preside MDM server prior to upgrading the CS 2000 Core Manager. This applies to Succession offices where the CS 2000 Core Manager needs to communicate with the Preside MDM for fault data, using the Passport log streamer application. Refer to the Passport 15000 and Preside MDM in *Succession Networks Fault Management Troubleshooting*, NN10198-912, for instructions on how to configure the pserver application.
- Check the root logical volume file - potential disk space error. Make sure the root logical volume (/) file system does not exceed 70% of its total size. If the root file system exceeds the 70% mark, you must make more room on the root file system for the upgrade to be successful. The /usr logical volume must have a minimum size of 1050Mb. Before starting the upgrade, ensure that /usr is less than 50% full. For more details, contact your next level of support.
- Check for the presence of a datavg if required.  
If upgrading a rootvg-datavg, ensure datavg is present. You can check the presence of a datavg through the maintenance interface under the storage level (sdmmtc storage).

- Make sure the CS 2000 Core Manager is alarm free. If any alarms are present, refer to *CS 2000 Core Manager Fault Management*, NN10082-911 for alarm-clearing procedures.
- Have VT100 terminal emulation. Before you perform this procedure, make sure that your terminal is configured for VT100 terminal emulation and that you can establish a connection to SP0 either locally or remotely through modem or terminal server.
- Offline and remove the Ineo SSH Secure File Transfer application using the procedure [Removing the Ineo SSH Secure File Transfer application on page 658](#)

## Removing the Ineo SSH Secure File Transfer application

### At the VT100 console or telnet session

- 1 Log on to the CS 2000 Core Manager using the root user ID and password.
- 2 Access the application level of the SDMMTC interface:  
**sdmmtc appl**
- 3 In the display, locate the Ineo SSH Secure File Transfer application.

| If                                                            | Do                     |
|---------------------------------------------------------------|------------------------|
| Ineo SSH Secure File Transfer is installed on your system     | step <a href="#">4</a> |
| Ineo SSH Secure File Transfer is not installed on your system | step <a href="#">9</a> |

- 4 If the Ineo SSH Secure File Transfer application is in service, busy it and take it offline:  
**bsy <number>**  
where  
**<number>**  
is the number displayed on the screen that is associated with the Ineo SSH Secure File Transfer application
- 5 Take the Ineo SSH Secure File Transfer application offline:  
**offl <number>**  
where  
**<number>**  
is the number displayed on the screen that is associated with the Ineo SSH Secure File Transfer application

- 6 Access the details level:  
**details**
- 7 Select the Ineo SSH Secure File Transfer application for removal from the system:  
**select <number>**  
where  
**<number>**  
is the number displayed on the screen that is associated with the Ineo SSH Secure File Transfer application
- 8 Remove the Ineo SSH Secure File Transfer application from the system:  
**remove**  
*The system will provide output similar to that in the following example:*  
  
WARNING: If you proceed with this action, all versions of the following fileset will be removed from the system.  
  
Ineo SSH Secure File Transfer  
  
Do you wish to proceed?  
Please confirm ("YES", "Y", "NO", or "N")
- 9 Confirm the removal of this application:  
**Yes**
- 10 Exit from the maintenance interface:  
**quit all**
- 11 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Post-upgrade notes

If, after this upgrade, the source command (at the sdmmtc/apply level) fails, the following message is displayed: Create the FIXES filesystem from sdmmtc;fixes and retry this. This message displays when the FIXES directory does not exist on the core manager. You should, then, create the FIXES directory as requested in this message.



## Upgrade notices

### ATTENTION

Some applications are automatically removed.

If the Exception Reporting, Alarm Conduit, SDM Corba Framework, and Remote Registration System filesets are present, they are automatically removed when upgrading to the new software load.

## Procedures

### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### ATTENTION

Read the instructions in [Pre-upgrade requirements on page 656](#) and [Upgrade notices on page 660](#), and complete any necessary activities before you proceed with the upgrade.

### ATTENTION

Nortel recommends that you deliver unprocessed billing files downstream. Ensure that no unprocessed billing file remains on the system.

### ATTENTION

Nortel recommends that you complete the entire upgrade procedure in one session, without interruption, to avoid any unnecessary disruption in billing file processing.

## Preparing for a software upgrade from tape

### *At the VT100 console*

- 1 If you are upgrading from tape, verify that the procedure [Preparing for system software upgrades from tape on page 612](#) has been completed.

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

### Taking the CS 2000 Core Manager offline

#### ***At the console connected to SP0 (local VT100 terminal or remote access)***

- 1 Log on to the CS 2000 Core Manager as a user authorized to perform config-admin actions.
- 2 If the SDM Billing Application (SBA) is installed on your system, determine the operational status of the SBA application and record this status for future reference. You will be asked to return the SBA application to this operational state later on in this procedure. Use the following table to determine your first step.

| If the SBA application                                 | Do                      |
|--------------------------------------------------------|-------------------------|
| is installed on your system and is not busy or offline | step <a href="#">3</a>  |
| is installed on your system, but is busy or offline    | step <a href="#">27</a> |
| is not installed on your system                        | step <a href="#">28</a> |

#### ***At the MAP display***

- 3 Busy all billing streams on the core. Post the required billing stream:  
  
**mapci;mtc;appl;sdmbil;post<stream>**  
where  
  
**<stream>**  
is the name of the billing stream
- 4 If necessary, to display the details about a stream, refer to the procedure “Listing billing streams” in *CS 2000 Core Manager Accounting*, NN10126-811. To list all files currently stored in a stream, refer to the procedure “Listing billing files” in *CS 2000 Core Manager Accounting*, NN10126-811.
- 5 Busy the posted stream:  
  
**bsy**
- 6 Confirm the request to **bsy**:  
  
**y**

- 7 Verify that the status of the posted stream changed to ManB (manual busy):

**status**

- 8 Repeat steps [3](#) through [7](#) for each billing stream.

- 9 Examine the SDMB 621 logs to determine the volume names and backup file names for each billing stream:

**logutil;open sdmb 621;back 10**

*In response to the command, the system displays the sdmb 621 log.*

```
BRW_CENTREX SDMB621 AUG03 14:19:05 4500 INFO SDM
BILLING BACKUP
```

```
 STREAM= AMA: Backup started to
record to file.
```

```
 VOLUME= S00DAMA FILE= BACK01AMA_01
```

- 10 For each configured billing stream, verify that at least one backup file exists on at least one of the configured backup volumes.

Display the names of the backup volumes configured for the specified billing stream:

**mapci;mtc;appl;sdmbil;conf view <stream>**

where

**<stream>**

is the name of the billing stream

- 11 Verify that SBA backup file exists on at least one of the displayed backup volumes:

| If the backup disk type is | Enter command                            |
|----------------------------|------------------------------------------|
| DDU                        | <b>dskut;liv &lt;volume name&gt; all</b> |
| IOP                        | <b>diskut;if &lt;volume name&gt;</b>     |
| SLM                        | <b>diskut;if &lt;volume name&gt;</b>     |

**Note:** The name of each backup file begins with BK.

- 12 Repeat steps [10](#) and [11](#) for each billing stream, then go to step [13](#).

**At the console connected to SP0 (local VT100 terminal or remote access)**

- 13 Close all unprocessed billing files by performing the procedure “Closing billing files”, located in *CS 2000 Core Manager Accounting*, NN10126-811.
- 14 Send all unprocessed billing files downstream using the following table to determine which procedure to perform.

| File transfer mode            | Procedure to use in Accounting, NN10126-811                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Outbound file transfer (OFT)  | “Sending billing files from disk”                                                                                                                                                                                                                                                                                                                                                                                          |
| Inbound file transfer (IFT)   | “Retrieving billing files for a stream set to inbound file transfer”                                                                                                                                                                                                                                                                                                                                                       |
| Real-time billing (RTB)       | “Sending billing files from disk”                                                                                                                                                                                                                                                                                                                                                                                          |
| Automatic file transfer (AFT) | <p>No manual action is required. Wait for SBA to deliver pending billing files to the downstream destination. There should be no pending files for each AFT session.</p> <p>Use the following commands to query AFT sessions: billmtc, appl, aft, aftcfg, list.</p> <p>To verify which billing files for each session are still pending, enter the following commands: billmtc, appl, aft, query &lt;session_name&gt;.</p> |
| For any other configuration   | <p>Send the billing files from tape using the procedure “Sending billing files from tape”</p> <p><b>Note:</b> If you need to restore the billing files from tape and you have AFT or IFT configuration, contact your next level of support for instructions.</p>                                                                                                                                                           |

- 15 If you are unable to send billing files to a downstream destination and you want to proceed with the upgrade, Nortel recommends that you backup the billing files to a DAT tape. If required, refer to the procedure “Copying billing files to tape (backup)” in *CS 2000 Core Manager Accounting*, NN10126-811. Otherwise, continue with the next step.

- 16** If applicable, you can display the details about a stream, refer to the procedure “Listing billing streams” in *CS 2000 Core Manager Accounting*, NN10126-811. To list all files currently stored in a stream, refer to the procedure “Listing billing files” in *CS 2000 Core Manager Accounting*, NN10126-811.

**17**



**CAUTION**

Before continuing with the upgrade, verify that there are no files in the /sba/ama/closedNotSent directory. Otherwise, the billing center may receive duplicate billing records.

Determine whether files exist in the /sba/ama/closedNotSent directory. If they do, perform a manual backup. If files still exist in the /sba/ama/closedNotSent directory after manual backup, contact your next level of support.

- 18** Access the APPL level of the maintenance interface:

**sdmmtc appl**

| If the AFT application          | Do                      |
|---------------------------------|-------------------------|
| is installed on your system     | step <a href="#">19</a> |
| is not installed on your system | step <a href="#">23</a> |

- 19** Determine the current operational status of the AFT application and record this status for future reference. You will be asked to return the AFT application to this operational state later on in this procedure. Use the following table to determine your next step.

| If the AFT application | Do                      |
|------------------------|-------------------------|
| is in service          | step <a href="#">20</a> |
| is busy                | step <a href="#">22</a> |
| is offline             | step <a href="#">23</a> |

- 20** Busy the AFT application:

**bsy <application\_number>**

where

- <application\_number>**  
is the number next to the Automatic File Transfer application
- 21 Confirm the command:  
**y**
- 22 Offline the AFT application:  
**offl <application\_number>**  
where  
**<application\_number>**  
is the number next to the Automatic File Transfer application
- 23 Busy the SDM Billing Application (SBA):  
**bsy <application\_number>**  
where  
**<application\_number>**  
is the number next to the SDM Billing Application
- 24 Confirm the command:  
**y**
- 25 Take the SBA offline:  
**offl <application\_number>**  
where  
**<application\_number>**  
is the number next to the SDM Billing Application
- 26 Exit from the maintenance interface:  
**quit all**  
Go to step [28](#)

***At the console connected to SP0 (local VT100 terminal or remote access)***

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

| If the SBA application | Do                      |
|------------------------|-------------------------|
| is busy                | step <a href="#">25</a> |
| is offline             | step <a href="#">28</a> |

***At the console connected to SP0 (local VT100 terminal or remote access)***

**28** Use the following table to determine your next step.

| <b>If your core manager</b>             | <b>Do</b>               |
|-----------------------------------------|-------------------------|
| is connected to a CS 2000 - Compact     | step <a href="#">29</a> |
| is not connected to a CS 2000 - Compact | step <a href="#">36</a> |

**29** Busy the CS 2000 Core Manager. Access the MTC level of the maintenance interface:

**sdmmtc mtc**

**30** Check that the CS 2000 Core Manager is in a fault-free state. If the CS 2000 Core Manager is not in a fault-free state, correct all faults and alarms before continuing this procedure. Refer to the *CS 2000 Core Manager Fault Management*, NN10082-911, for alarm-clearing procedures. If you have alarms or faults that you cannot clear, stop and contact your next level of support.

**31** Busy the CS 2000 Core Manager:

**bsy**

**32** Offline the CS 2000 Core Manager:

**offl**

**33** Confirm the busy request:

**y**

**34** Exit from maintenance interface:

**quit all**

**35** Go to step [41](#).

***At the MAP display***

**36** Access the SDM level of the MAP display:

**mapci;mtc;appl;sdm**

**37** Check that the CS 2000 Core Manager is in a fault-free state. If the CS 2000 Core Manager is not in a fault-free state, correct all faults and alarms before continuing this procedure. Refer to the *CS 2000 Core Manager Fault Management*, NN10082-911, for alarm-clearing procedures. If you have alarms or faults that you cannot clear, stop and contact your next level of support.

- 38 Busy the CS 2000 Core Manager:  
**bsy**
- 39 Confirm the busy request:  
**y**
- 40 Take the CS 2000 Core Manager offline:  
**off1**
- 41 You have completed this procedure.

### Preparing the system

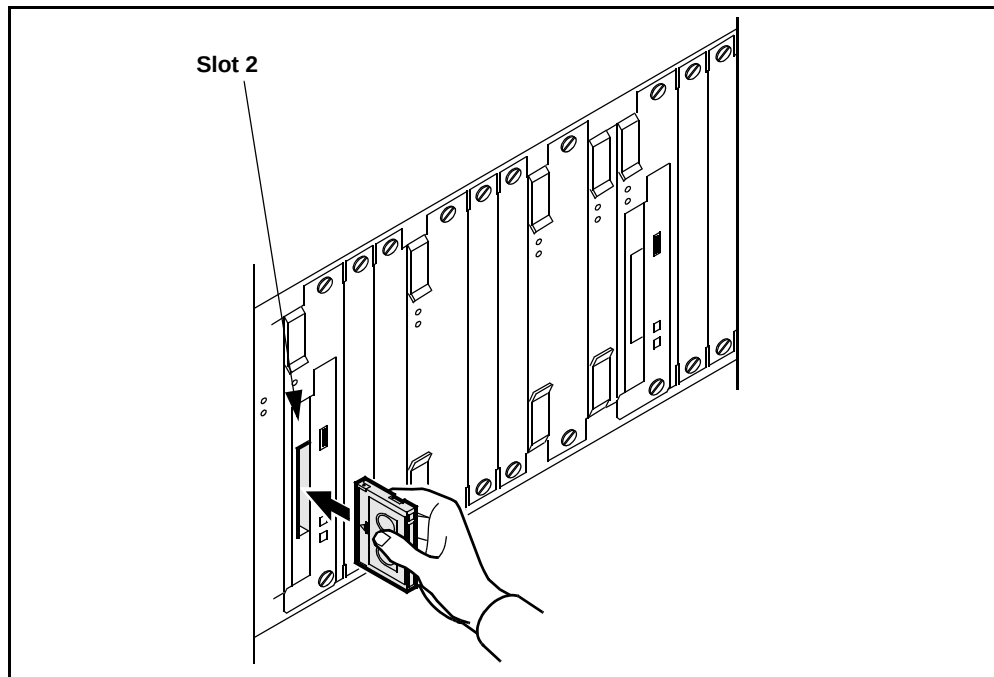
#### *At the local VT100 console*

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

| If you are upgrading                                                                                                                                     | Do                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| from a directory created during ESD or during the procedure <a href="#">Preparing for system software upgrades from tape on page 612</a>                 | step <a href="#">3</a>                                                                                                                                                                                                          |
| directly from tape<br><b>Caution:</b> This method is not recommended. Use this method only if you are unable to upload the software from tape to a disk. | insert the tape labeled for the new software load into the tape drive in slot 2, as shown in the following figure.<br>Wait until the tape drive stabilizes (yellow LED is off) before you proceed with step <a href="#">2</a> . |



## Inserting a tape into the tape drive slot 2



- 2 If you are upgrading from the CS2E0006, or later, release, verify the version of the tape. Otherwise, continue with step [3](#).

Verify the version of the tape:

**querytape dat0**

*Example response*

SDM\_VERSION.info: CS2E0080.0 : 21.60.8.0

The displayed product name (in this example, CS2E0080.0) must match the label on the tape that you inserted in step [1](#).

- 3 Remove all archived filesets from the system, to free up disk space. Access the Details level:

**sdmmtc details**

- 4 Show all software:

**filter off**

- 5 Select all archived filesets:

**select all**

- 6 Remove all archived filesets:

**remove all**

**Note:** The system will automatically select appropriate files to remove.

- 7 Confirm the removal:  
**y**
- 8 After removing the archived filesets, ensure that /usr logical volume is less than 50% full. To check the percent full value for /usr, enter the following command:  
**sdmmtc storage**  
If /usr is more than 50% full, refer to procedure “Increasing the size of a logical volume” in *CS 2000 Core Manager Security and Administration*, NN10170-611, to increase the /usr logical volume size as required. The /usr logical volume must have minimum size of 1050Mb. Otherwise continue to the next step.
- 9 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Upgrading the software

#### ***At the console connected to SP0 (local VT100 terminal or remote access)***

- 1 From the “sdmmtc details” level, use the following table to determine your next step.

| If you are upgrading                                                                                                                                     | Do                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| from a directory created during ESD or during the procedure <a href="#">Preparing for system software upgrades from tape on page 612</a>                 | list the filesets: apply <directory path><br><b>Note:</b> <directory path> is the directory where your filesets are located. The directory depends on whether you are upgrading after ESD or after tape pre-loading. |
| directly from tape<br><b>Caution:</b> This method is not recommended. Use this method only if you are unable to upload the software from tape to a disk. | list the filesets: apply 0 and go to step <a href="#">2</a>                                                                                                                                                          |

- 2 Select all the new application filesets:  
**select new**
- 3 Apply all the new software:  
**apply**

#### 4 Confirm the apply command:

**y**

Wait until the upgrade is complete before you proceed. The upgrade can take up to 2.5 hours, depending on which release you are upgrading from, and how many filesets require upgrading.

| If the command response      | Do                                                                        |
|------------------------------|---------------------------------------------------------------------------|
| indicates any errors         | contact your next level of support before you proceed with this procedure |
| does not indicate any errors | step <a href="#">5</a>                                                    |

#### 5 Use the following table to determine your next step.

| If you are                                                                                                              | Do                      |
|-------------------------------------------------------------------------------------------------------------------------|-------------------------|
| prompted to configure OSS Comms Svcs<br>In the sdmmtc maintenance interface window:<br>OSS Comms Svcs<br>MORE... (100%) | step <a href="#">6</a>  |
| not prompted to configure OSS Comms Svcs                                                                                | step <a href="#">10</a> |

#### 6 Press the space bar to display the DDMS Clients Configuration menu.

*The system responds:*

```
#####
Configuring 'SDM_DDMS.osscomms'.
#####

#####
Configuring DDMS clients
#####

 DDMS Clients Configuration

0. Quit
1. Add new clients
2. Remove existing client
3. List existing clients

Enter choice:
```

- 7 Configure the DDMS clients which are typically the CS 2000 Management tools servers with the SESM load. Add a new DDMS client:
  - 1
- 8 When prompted, enter the IP address for each of the CS 2000 Management tools servers. Press the Enter key after each entry and type **done** once you have entered all the IP addresses.
- 9 Exit the DDMS clients configuration screen:
  - 0

**Note:** You can reconfigure the OSS Comms Svcs at any time through the sdmmtc config level.

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

| If you are                                  | Do                      |
|---------------------------------------------|-------------------------|
| prompted to configure the SAM21 Manager     | step <a href="#">11</a> |
| not prompted to configure the SAM21 Manager | step <a href="#">15</a> |

- 11 Ensure that you records obtained from the [Pre-upgrade requirements on page 656](#) section ready for reference.
- 12 To configure SAM21 Manager application, when prompted whether DNS is supported on SAM21 EM workstations, enter Y (yes) or N (no), and press the Enter key.

| If you enter | Do                      |
|--------------|-------------------------|
| Y (yes)      | step <a href="#">13</a> |
| N (no)       | step <a href="#">14</a> |

- 13 When prompted, enter the CommonName from the certificate on the CS 2000 Management Tools server that is configured to run the Login Application, and press the Enter key.
- 14 When prompted, enter the host name of the CS 2000 Management Tools server that is configured to run the Login Application, and press the Enter key.

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

| If the system                 | Do                                                     |
|-------------------------------|--------------------------------------------------------|
| prompts you to reboot         | step <a href="#">16</a>                                |
| does not prompt you to reboot | press Enter, and continue with step <a href="#">21</a> |

- 16 When prompted, confirm the system reboot:

**y**

- 17 Once the system has finished rebooting, log into the CS 2000 Core Manager as a user authorized to perform config-admin actions.

- 18 Wait until all cards at the hardware level are in service before you proceed. Monitor the status of the cards as described in steps [19](#) and [20](#).

- 19 Access the hardware level of the maintenance interface:

**sdmmtc hw**

- 20 Check that no faults exist on the CS 2000 Core Manager:

**querysdm flt**

| If                    | Do                                                                                                                                              |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| faults are present    | correct the faults using the procedures in <i>CS 2000 Core Manager Fault Management</i> , NN10082-911, and return to this step in the procedure |
| no faults are present | step <a href="#">21</a>                                                                                                                         |

- 21 Use the following table to determine your next step for installing the sdm bundle.

| If you are upgrading                                                                                                                     | Do                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| from a directory created during ESD or during the procedure <a href="#">Preparing for system software upgrades from tape on page 612</a> | list the filesets: apply <directory path><br><b>Note:</b> <directory path> can be the /swd/sdm/esd directory. |
| directly from tape                                                                                                                       | list the filesets: apply 0                                                                                    |
| <b>Caution:</b> This method is not recommended. Use this method only if you are unable to upload the software from tape to a disk.       |                                                                                                               |

- 22 Install the sdm software:

**apply bundle sdm**

If you are upgrading directly from tape, the system prompts you to confirm the apply command.

| If you are                                | Do                      |
|-------------------------------------------|-------------------------|
| prompted to confirm the apply command     | step <a href="#">23</a> |
| not prompted to confirm the apply command | step <a href="#">29</a> |

- 23 Confirm the apply command:

**y**

*The system responds*

Command completed with no errors

| If you are                        | Do                                                    |
|-----------------------------------|-------------------------------------------------------|
| prompted to reboot the system     | step <a href="#">24</a>                               |
| not prompted to reboot the system | press Enter and continue with step <a href="#">29</a> |

- 24 Confirm the system reboot:

**y**

- 25 Once the system has finished rebooting, log into the CS 2000 Core Manager as a user authorized to perform config-admin actions.
- 26 Wait until all cards at the hardware level are in service before you proceed. Monitor the status of the cards as described in steps [27](#) and [28](#).

- 27 Access the hardware level of the maintenance interface:

**sdmmtc hw**

- 28 Check that no faults exist on the CS 2000 Core Manager:

**querysdm flt**

| If                    | Do                                                                                                                                              |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| faults are present    | correct the faults using the procedures in <i>CS 2000 Core Manager Fault Management</i> , NN10082-911, and return to this step in the procedure |
| no faults are present | step <a href="#">29</a>                                                                                                                         |

- 29 Verify if you have X.25, using your notes obtained from the “Basic pre-checks” list in [Preparing to upgrade the CS 2000 Core Manager on page 550](#). Use the following table to determine your next step.

| If you           | Do                      |
|------------------|-------------------------|
| have X.25        | step <a href="#">30</a> |
| do not have X.25 | step <a href="#">35</a> |

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

| If you are upgrading                                                                                                                     | Do                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| from a directory created during ESD or during the procedure <a href="#">Preparing for system software upgrades from tape on page 612</a> | list the filesets: apply <directory path><br><br><b>Note:</b> <directory path> can be the /swd/sdm/esd directory. |
| directly from tape                                                                                                                       | list the filesets: apply 0                                                                                        |
| <b>Caution:</b> This method is not recommended. Use this method only if you are unable to upload the software from tape to a disk.       |                                                                                                                   |

- 31 Install the X.25 software:

**apply bundle x25**

If you are upgrading directly from tape, the system prompts you to confirm the apply command.

| If you are                                | Do                      |
|-------------------------------------------|-------------------------|
| prompted to confirm the apply command     | step <a href="#">32</a> |
| not prompted to confirm the apply command | step <a href="#">35</a> |

- 32 Confirm the apply command:

**y**

*The system responds*

Command completed with no errors

| If you are                        | Do                                                    |
|-----------------------------------|-------------------------------------------------------|
| prompted to reboot the system     | step <a href="#">33</a>                               |
| not prompted to reboot the system | press Enter and continue with step <a href="#">35</a> |

- 33 Confirm the system reboot:

**y**



- 34** Once the system has finished rebooting, log into the CS 2000 Core Manager as a user authorized to perform config-admin actions.
- 35** Wait until all cards at the hardware level are in service before you proceed. Monitor the status of the cards as described in steps [36](#) and [37](#).
- 36** Access the hardware level of the maintenance interface:  
**sdmmtc hw**
- 37** Check that no faults exist on the CS 2000 Core Manager:  
**querysdm flt**

| If                    | Do                                                                                                                                              |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| faults are present    | correct the faults using the procedures in <i>CS 2000 Core Manager Fault Management</i> , NN10082-911, and return to this step in the procedure |
| no faults are present | step <a href="#">38</a>                                                                                                                         |

- 38** If you have the DNBD Call Monitoring Application on your system, upgrade it by following the appropriate procedure in the International Lawful Interception NTP, and then return to step [39](#)
- 39** You have completed this procedure.

### Returning the system to service

- 40** After returning your CS 2000 Core Manager to service, consult the notes you recorded about the pre-upgrade operational status of the SBA application in step [2](#) and about the pre-upgrade operational status of the AFT application in step [19](#) of the procedure, [Taking the CS 2000 Core Manager offline on page 661](#).

***At the console connected to SP0 (VT100 or remote access)***

**41** Use the following table to determine your next step.

| <b>If your core manager</b>               | <b>Do</b>               |
|-------------------------------------------|-------------------------|
| is connected to the CS 2000 - Compact     | step <a href="#">42</a> |
| is not connected to the CS 2000 - Compact | step <a href="#">47</a> |

**42** Return the CS 2000 Core Manager to service. Access the MTC level of the maintenance interface:

**sdmmtc mtc**

**43** Busy the CS 2000 Core Manager:

**bsy**

**44** Return the CS 2000 Core Manager:

**rts**

**45** Exit from SDMMTC:

**quit all**

**46** Go to step [50](#)

***At the MAP display***

**47** Access the SDM level of the MAP display:

**mapci;mtc;appl;sdm**

**48** Change the state of the CS 2000 Core Manager from offline to busy:

**bsy**

**49** Return the CS 2000 Core Manager to service:

**rts**

**Note:** It will take at least 5 minutes for the CS 2000 Core Manager to return to service on the core side.

***At the console connected to SP0 (local VT100 terminal or remote access)***

**50** Use the following table to determine your next step.

| If the SBA application               | Do                      |
|--------------------------------------|-------------------------|
| was not offline prior to the upgrade | step <a href="#">51</a> |
| was offline prior to the upgrade     | step <a href="#">67</a> |
| is not installed on your system      | step <a href="#">67</a> |

**51** Access the APPL level of the maintenance interface:

**sdmmtc appl**

**52** Wait until the Table Access Service application is in service (InSv), then continue with the procedure. If the application does not return to service after 15 minutes, contact your next level of support.

**53** Busy the SBA:

**bsy <application\_number>**

where

**<application\_number>**

is the number for the SDM Billing Application

**54** Confirm the command:

**y**

| If the SBA application              | Do                      |
|-------------------------------------|-------------------------|
| was in service prior to the upgrade | step <a href="#">55</a> |
| was busy prior to the upgrade       | step <a href="#">67</a> |

**55** Return the SBA to service:

**rts <application\_number>**

where

**<application\_number>**

is the number next to the SDM Billing Application

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

| If the AFT application          | Do                      |
|---------------------------------|-------------------------|
| is installed on your system     | step <a href="#">57</a> |
| is not installed on your system | step <a href="#">61</a> |

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

| If the AFT application               | Do                      |
|--------------------------------------|-------------------------|
| was not offline prior to the upgrade | step <a href="#">58</a> |
| was offline prior to the upgrade     | step <a href="#">61</a> |

- 58 Busy the AFT application:

**bsy <application\_number>**

where

**<application\_number>**

is the number next to the Automatic File Transfer application

- 59 Confirm the command:

**y**

| If the AFT application                  | Do                      |
|-----------------------------------------|-------------------------|
| was in service prior to the upgrade     | step <a href="#">60</a> |
| was not in service prior to the upgrade | step <a href="#">61</a> |

- 60 Return the AFT application to service:

**rts <application\_number>**

where

**<application\_number>**

is the number next to the Automatic File Transfer application

***At the MAP display***

- 61 Return all billing streams to service. For each stream, post the required billing stream:

```
mapci;mtc;appl;sdbil;post<stream>
```

where

**<stream>**

is the name of the billing stream

- 62 Return the posted stream to service:

```
rts
```

- 63 Repeat steps [61](#) and [62](#) for each billing stream.

- 64 Check to ensure that all billing streams are either in-service or in recovery on the core side before continuing.

***At the console connected to SP0 (local VT100 terminal or remote access)***

- 65 Verify that billing is collecting records. Query the steam:

```
query <stream_name>
```

where

**<stream\_name>**

is the name of the billing stream, for example, ama.

- 66 Note the number of records, wait approximately 10 seconds, and repeat the query command for each billing stream.

| If the number of records                                                       | Do                                 |
|--------------------------------------------------------------------------------|------------------------------------|
| increased from the first query command (meaning billing is working)            | step <a href="#">67</a>            |
| did not increase from the first query command (meaning billing is not working) | contact your next level of support |

- 67 Determine whether you need to install new applications and services. For information about any new applications and features introduced for the new software release, refer to [New in this release on page 547](#). For a list of applications required for each Succession solution, refer to [Preparing to upgrade the CS](#).

[2000 Core Manager on page 550](#). Use the following table to determine your next step.

| If you                                               | Do                      |
|------------------------------------------------------|-------------------------|
| need to install new applications and services        | step <a href="#">68</a> |
| do not need to install new applications and services | step <a href="#">69</a> |

- 68** Install new applications and services from the console connected to SP0 (local VT100 terminal or remote access). Use either the procedures shown in the table below or the procedures in the CS 2000 Core Manager suite of NTPs that correspond to the applications or services you want to install. Only install the required applications. When you have completed the installations, proceed to step [69](#).

| Application or service | Installation procedure to use                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| DDMS                   | <a href="#">Installing or upgrading DDMS on page 691</a>                                                                  |
| DCE                    | <a href="#">Upgrading DCE on page 703</a>                                                                                 |
| OMD                    | <a href="#">Installing and configuring the OM Data Delivery application on page 705</a>                                   |
| OpenSSH                | <a href="#">Installing or upgrading OpenSSH on page 713</a>                                                               |
| SPM reach through      | <a href="#">Installing or upgrading Reach Through SPM on page 715</a>                                                     |
| GR740                  | <a href="#">Installing or upgrading the GR740PT application server on page 717</a>                                        |
| Backup restore manager | <a href="#">Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager on page 722</a> |
| CEM filesets           | <a href="#">Installing CEM filesets on page 729</a>                                                                       |
| X.25 connectivity      | <a href="#">Commissioning X.25 connectivity on page 732</a>                                                               |

- 69** You have completed this procedure. Return to [CS2000 Core Manager upgrade tasks on page 549](#).

---

## Upgrading the CS 2000 Core Manager with software patches

---

### Purpose

Use this procedure to upgrade your CS 2000 Core Manager with software patches, also called fix filesets.

### Prerequisites

The following prerequisites apply to this procedure:

#### **ATTENTION**

Before continuing with patch application, verify that there are no files in the /sba/ama/closedNotSent directory. Otherwise, the billing center can receive duplicate billing records. If files exist in the /sba/ama/closedNotSent directory, perform a manual backup. If files still exist in the /sba/ama/closedNotSent directory after manual backup, contact your next level of support.

### Application

The information that follows indicates how to upgrade your CS 2000 Core Manager with software patches, and includes the following procedures:

- [Applying the SDM\\_CERTS.Certs package on page 573](#)
- [Setting the schedule to apply fixes automatically on page 688](#)
- [Applying fix filesets manually on page 687](#)
- [Changing the default fixes directory on page 690](#)

#### **ATTENTION**

Before applying the fixes fileset, capture the session file. See [Capturing the pre-check session file on page 578](#).

Upgrading your CS 2000 Core Manager with software fixes (referred to in this procedure as fix filesets) involves replacing entire filesets. Fix filesets are delivered to you electronically from the Regional Patch Selector (RPS).

If software authentication has been enabled on your system, monitor the maintenance interface for any logs or alarms respecting software authentication failures. To utilize the software authentication feature in this procedure, the SDM\_CERTS.Certs package must be applied.



The Regional Patch Selector (RPS) is an automated patch management and delivery system. RPS maintains information about patches and offices, calculates which patches are required in each office, and uploads the patches to the required sites.

Once your office information is entered in RPS, you will receive any fix filesets that apply to the CS 2000 Core Manager configuration for that office. The fix filesets you receive replace installed versions of the same filesets on your CS 2000 Core Manager.

If you have multiple CS 2000 Core Manager locations, you can choose to have each location set up in RPS, or have only one location set up in RPS. When you choose to have a single location set up in RPS, you are responsible for propagating any fix filesets to the other CS 2000 Core Manager locations if and when required.

Fix filesets are sent to the location specified in RPS, which can be the CS 2000 Core Manager itself or an intermediate server that has a connection to the CS 2000 Core Manager:

- when the fix filesets are sent directly to the CS 2000 Core Manager, they are placed in a configured directory (refer to [Location of fix filesets on page 687](#) for more details on the configured directory)
- when the fix filesets are sent to an intermediate server, they are placed in a dropbox

A release notes file is sent with each fix fileset. This file is in ASCII format and contains information about the fix.

RPS collects the <cli>.informfile from the CS 2000 Core Manager itself or from the dropbox on the server at configured intervals, and delivers any fix filesets to your office as soon as they are available in RPS.

If your office is set up with an intermediate server connected to the CS 2000 Core Manager, you need to move or copy the fix filesets from the dropbox on the server to the configured directory on the CS 2000 Core Manager. You also need to ensure that your latest <cli>.informfile, located in /swd/sdm, is available in the dropbox on the server when RPS is scheduled to collect it.

You can transfer the fix filesets from the dropbox to the CS 2000 Core Manager, and the <cli>.informfile (ASCII file) from the CS 2000 Core Manager to the dropbox using file transfer protocol (FTP), Secure file transfer (SFT), or SFT2. To use SFT, refer to the procedure “Transferring and retrieving files using SFT” in *CS 2000 Core Manager Security and Administration*, NN10170-611.

You are notified through e-mail when fix filesets have been successfully delivered to your site.

Once the fix filesets are accessible in the configured directory on the CS 2000 Core Manager, they must be applied. Fix filesets that do not require user intervention can be applied automatically according to a set schedule. Refer to [Automatic installation of fix filesets on page 685](#). Fix filesets that require user intervention need to be applied manually. Refer to [Manual installation of fix filesets on page 687](#).

Once the fix filesets have been successfully applied, they are deleted from the configured directory. The associated release notes, if present, are also deleted.

At any time, you can remove a fix fileset and restore a previous version of the fileset using the remove command at the Details level of the maintenance interface.

## Automatic installation of fix filesets

You can set the scheduled time for when you want fix filesets to be automatically applied from the Fixes level. As shown in the following figure, the fix filesets that can be auto-applied have Y under header AA (auto apply), and the fix filesets that are scheduled to be auto-applied have a status of SCHED under Status header.

**Fixes level screen**

```

SDM CON 512 NET APPL SYS HW CLI: MSH10
* * * * * * * * Host: nsh10sdn
 Fault Tolerant

Fixes
0 Quit
2 Source
3 Reload
4 Sched
5
6
7 Select
8 Apply
9
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 16:54 >

```

Source: the directory /swd/sdn/fixes.  
Filter: OFF

| # | Fileset                      | Description | Version   | Status | AA |
|---|------------------------------|-------------|-----------|--------|----|
| 1 | Generic Data Delivery        |             | 18.17.1.1 | SCHED  | Y  |
| 2 | Platform Maintenance         |             | 18.17.1.1 | SCHED  | Y  |
| 3 | Passport Log Streamer        |             | 18.14.0.0 | SCHED  | Y  |
| 4 | umfioFX Run Time Environment |             | 1.3.0.6   | SCHED  | Y  |

Available Fixes: 1 to 4 of 4

**ATTENTION**

If any fix filesets have a status of INCOMP (incomplete), the fix fileset has dependencies that have not been installed and are not available. Contact your Nortel representative.

Fix filesets that are scheduled to be applied automatically can only be applied from the configured directory on the CS 2000 Core Manager. Refer to [Location of fix filesets on page 687](#) for more details on the configured directory.

You can apply fix filesets manually outside of the specified schedule. Refer to [Manual installation of fix filesets on page 687](#).

**ATTENTION**

The system generates log SDM610 when a fix fileset is scheduled to be applied automatically and either applies successfully or fails to apply. If you receive this log because a fix fileset failed to apply, contact your Nortel representative.

Previous versions of patch files of a fix fileset are removed when the patch files are applied.

## Manual installation of fix filesets

You need to manually apply fix filesets that require a reboot or have prerequisite filesets that need to be installed and require a reboot. The fix filesets that you need to apply manually have N under the AA header (auto apply), and AVAIL under the Status header.

### Location of fix filesets

The directory path to the fixes default directory on your CS 2000 Core Manager, is /swd/sdm/fixes. You can change the default fixes directory using the procedure that follows.

**Note 1:** The directory must have a minimum of 200 MB of available space. The recommended amount of available space is 400 MB, which is the default.

**Note 2:** Beginning with release SDM20, the SDM maintenance interface (sdmmtc) expects a filesystem, rather than a directory, that contains patches. Prior to the SDM20 release, sdmmtc could list patches from any directory, whether or not the directory was a filesystem.

### Procedures

#### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Applying fix filesets manually

#### ATTENTION

Before continuing with patch application, verify that there are no files in the /sba/ama/closedNotSent directory. Otherwise, the billing center can receive duplicate billing records. If files exist in the /sba/ama/closedNotSent directory, perform a manual backup. If files still exist in the /sba/ama/closedNotSent directory after manual backup, contact your next level of support.

#### *At the CS 2000 Core Manager*

- 1 Log into the CS 2000 Core Manager as the root user.
- 2 Access the SWIM level:

```
sdmmtc swim
```

- 3 Access the Fixes level:

**fixes**

**Note:** Ensure the fix filesets are accessible in the configured directory on the CS 2000 Core Manager (refer to [Location of fix filesets on page 687](#) for more details on the configured directory).

- 4 Select the fix fileset you want to apply:

**select <n>**

where

**<n>**

is the number next to the fix fileset you want to apply

- 5 Apply the fix fileset:

**apply**

- 6 You have completed this procedure. Return to step [15](#) of procedure [Completing the CS 2000 Core Manager upgrade](#)

### Setting the schedule to apply fixes automatically

#### ATTENTION

Before continuing with patch application, verify that there are no files in the /sba/ama/closedNotSent directory. Otherwise, the billing center can receive duplicate billing records. If files exist in the /sba/ama/closedNotSent directory, perform a manual backup. If files still exist in the /sba/ama/closedNotSent directory after manual backup, contact your next level of support.

### At the CS 2000 Core Manager

- 1 Log into the CS 2000 Core Manager as the root user.

- 2 Access the SWIM level:

**sdmmtc swim**

- 3 Access the Fixes level:

**fixes**

If you are accessing the Fixes level for the first time, you are prompted to enter the size of the fixes source directory, and the path of a new logical volume to be created for fixes. The minimum size is 200 MB and the maximum size is 1000 MB. The recommended size is 400 MB, which is the default.

*Example response:*

The /swd/sdm/fixes directory has been successfully created.  
Press ENTER to continue.

- 4 Press the Enter key to continue.
- 5 Use the following table to determine your next step.

| If                                                                                                  | Do                                                              |
|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| the system responds with the message: The directory /swd/sdm/fixes does not exist or cannot be read | step stop the procedure and contact your next level of support. |
| Otherwise                                                                                           | step <a href="#">7</a>                                          |

- 6 To set the time interval, enter the schedule level:

**sched**

*Example response:*

Choose the interval desired:

1. Monthly
2. Weekly
3. Daily
4. None

Enter a number from 1 to 4 to make your choice or type abort:

- 7 Enter the number that is next to the interval you want, and complete the prompts for the specified interval.
- 8 When prompted, confirm your entry:

**y**

*Example response:*

Auto fix schedule has been updated.

Press Enter...

- 9 Press Enter to return to the Fixes level.
- 10 You have completed this procedure. Return to step [15](#) of procedure [Completing the CS 2000 Core Manager upgrade](#)

## Changing the default fixes directory

### *At the CS 2000 Core Manager*

- 1 Log into the CS 2000 Core Manager as the root user.
- 2 Access the swim level:  
**sdmmtc swim**
- 3 Access the Options level:  
**options**
- 4 Change the value of the default fixes directory:  
**change 2**
- 5 Enter the new value for the default fixes directory.  
**Note:** Enter the full directory path when specifying a directory.  
*Example response:*  
Change 2 - Command complete
- 6 Access the Fixes level:  
**fixes**
- 7 Press Enter to confirm the changed default fixes directory.
- 8 You have completed this procedure. Return to step [15](#) of procedure [Completing the CS 2000 Core Manager upgrade](#)

---

## Installing or upgrading DDMS

---

Use this procedure to install and configure DDMS for the first time, which consists of using two processes, [Creating user IDs on the CM](#) and [Installing or upgrading DDMS filesets](#).

The following mandatory user IDs created on the CM must also be added when you configure DDMS: SDM01, SDM02, SDM03, SDM04. These user IDs are mandatory on the CM and DDMS.

If Enhanced Password Control is in effect on the CM, the DDMS software will manage automatic password changing on the CM before the passwords expire. You therefore do not have to manually change the passwords for users SDM01-SDM04 on the CM.

When DDMS software is returned to service (rts), it reads the OFPCOPT and OFCENG tables on the CM to determine whether Enhanced Password Control is in effect. If Enhanced Password Control is in effect, the software will read the password lifetime value and automatically change passwords one day before expiry. If you make manual changes to the password lifetime value or turn on/off Enhanced Password control, then these changes must be synchronized with the DDMS software by busying/returning to service (bsy/rts) the DDMS. However, if any of the SDM01-SDM04 passwords are changed on the CM manually, you need to apply the same password changes in the DDMS configuration file. Refer to [Changing passwords in the DDMS configuration file](#).

Also use this procedure to upgrade DDMS prior to a CM one night process (ONP), which consists of [Installing or upgrading DDMS filesets](#). However, The DDMS application must be stopped before the CM Swact. Refer to procedure "Controlling SDM applications" in the *CS 2000 Core Manager Security and Administration*, NN10170-611 to stop DDMS. When the CM ONP is complete, restart DDMS using the same procedure.



## Prerequisites for DDMS installation

Following are the prerequisites for a successful DDMS installation:

- Hardware requirements
  - CS 2000 Core Manager Fault Tolerant (FT) Platform
  - VT100 terminal
- Software requirements
  - Installed CS 2000 Core Manager base software including the OM access and table access applications, and the filesets associated with the log delivery application. Refer to procedure “Installing and configuring the log delivery application” in *CS 2000 Core Manager Configuration Management*, NN10104-511.
  - The Log Delivery Service application must be in service.

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

### Other activities related to using this procedure

| Procedure                                          | Document                                                              |
|----------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager             | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying actions a user is authorized to perform | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

## Creating user IDs on the CM

### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Creating user IDs on the CM

### ATTENTION

If Enhanced Password Control is in effect on the CM, the password created must be at least six characters in length.

If any of the SDM01-SDM04 passwords are changed on the CM, you must apply the same password changes in the DDMS configuration file. Refer to [Changing passwords in the DDMS configuration file](#).

### *At the CLI prompt on the switch*

- 1 The CS 2000 Core Manager requires you to create at least four user IDs with passwords on the CM.

Use the following command create the first user id and password, then press Enter.

```
permit sdm01 <sdm01_pswd> 4 10000 english all
```

where

**<sdm01\_pswd>**

is the CM password for user sdm01

**Note:** If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

- 2 Use the following command create the second user id and password, then press Enter.

```
permit sdm02 <sdm02_pswd> 4 10000 english all
```

where

**<sdm02\_pswd>**

is the CM password for user sdm02

- 3 Use the following command create the third user id and password, then press Enter.

```
permit sdm03 <sdm03_pswd> 4 10000 english all
```

where

**<sdm03\_pswd>**

is the CM password for user sdm03

- 4 Use the following command create the forth user id and password, then press Enter.

**permit sdm04 <sdm04\_pswd> 4 10000 english all**

where

**<sdm04\_pswd>**

is the CM password for user sdm04

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

### Changing passwords in the DDMS configuration file

#### *At the CS 2000 Core Manager*

- 1 Log on the client workstation as a user authorized to perform config-admin actions.

- 2 Access the maintenance interface:

**sdmmtc**

- 3 Access the application level:

**appl**

- 4 Locate and busy the OSS Comms Svcs application:

**bsy <n>**

**<n>**

is the number next to the OSS Comms Svcs fileset

- 5 Change the passwords in the DDMS configuration file as follows:

- a Access the configuration level:

**config <n>**

**<n>**

is the number next to the OSS Comms Svcs fileset

- b Perform steps 8 through 29 in [Installing or upgrading DDMS filesets](#), which follows.

- c Once you have completed the configuration, return the OSS Comms Svcs application to service:

**rts <n>**

<n>

is the number next to the OSS Comms Svcs fileset

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

## Installing DDMS filesets

The DDMS software is located in filesets on the CS 2000 Core Manager non-CM load (NCL) digital audio tape (DAT). The following table shows the names, descriptions and contents of the DDMS filesets. These filesets are automatically installed when the schema fileset appropriate for your switch is installed.

### DDMS contents of CS 2000 Core Manager NCL DAT tape

| Fileset name      | Fileset description               | Contents                                                                                                                                                                                                             |
|-------------------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SDM_DDMS.ossaps   | OSS and Application Svcs (OSSAPS) | OSS and Application Svcs<br>Transaction Manager (ddmstxmgr)<br>View Server (ddmsschema)<br>Data Input Handler (ddmsdih)<br>Data Change Notification Handler (ddmsdcnh)<br>Synchronizing Interface Module (ddmssimif) |
| SDM_DDMS.osscomms | OSS Comms Svcs (OSSCOMMS)         | OSS Communications Services<br>Communications Manager (ddmscomms)<br>Passthru Interface Manager (ddmspim)<br>User Administration (ddmsuAdmin)<br>System Administration (ddmssysadm)                                  |

### Installing or upgrading DDMS filesets

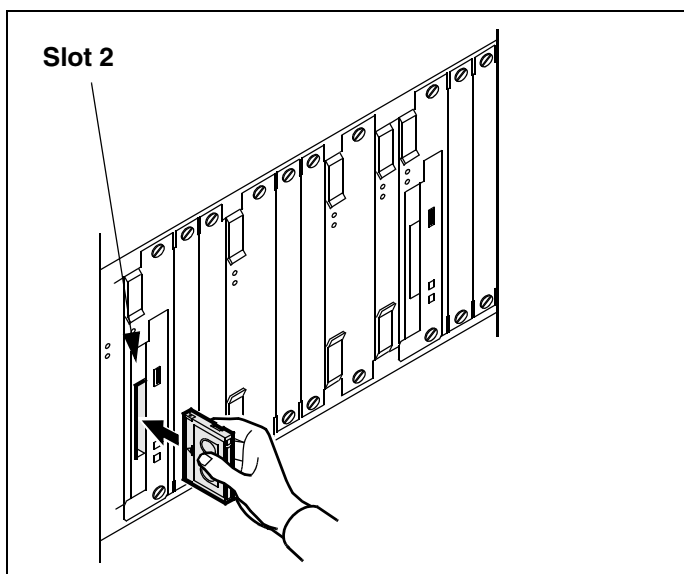
#### *At the CS 2000 Core Manager*

- 1 Log on the client workstation as a user authorized to perform config-admin actions.

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

| If the software is | Do                                                                                                                                                                                                                   |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| on tape            | insert the tape labeled for the new software load into the tape drive in slot 2 as shown in the following figure, wait until the tape drive stabilizes (yellow LED is off), then proceed with step <a href="#">3</a> |
| in a directory     | step <a href="#">3</a>                                                                                                                                                                                               |

### Main chassis tape drive



- 3 Access the maintenance interface:

**sdmmtc**

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

| If the software is | Do                                                                             |
|--------------------|--------------------------------------------------------------------------------|
| on tape            | list the filesets by typing apply 0 and pressing the Enter key                 |
| in a directory     | list the filesets by typing apply <directory path> and pressing the Enter key. |

- 5 Select the filesets to install or upgrade:

**select <x>**

where

<x>

is the number next to the following filesets

- OSS Comms Svcs
- OSS and Application Svcs

*The system highlights the filesets as they are selected.*

- 6 Apply the selected filesets:

**apply**

*The system displays the list of required filesets.*

**y**

- 7 Confirm the Apply command:

**y**

*The system responds:*

```
Command in progress, 2 filesets to process.
Processing fileset 1
Applying OSS Comms Svcs 17.x.x.x
```

**Note:** Applying the filesets can take up to 10 minutes to complete.

- 8 When prompted, press Enter to begin configuration of the OSS and Application Svcs, and the OSS Comms Svc filesets.

- 9 When prompted, press Enter to start the logroute tool.

*The Logroute Main Menu appears, as shown in figure the following figure.*

#### DDMS logroute tool banner

```
#####
Adding DDMS logroute configuration
#####
Please add DDMS log routing:
 Device type = file
 File = /data/logs/ossaps/ossapslog
 Routing = addrep
 log_type = DDMS
Press <RETURN> when ready
```

## Logroute tool main menu

```
Logroute Main Menu

1 - Device List
2 - Global Parameters
3 - CM Configuration File
4 - GDD Configuration
5 - Help
6 - Quit Logroute

Enter Option ==>
```

- 10** Set up a path and file to store DDMS customer logs. Select the Device List menu:

**1**

*The Device List Menu screen is displayed.*

| If the list                                            | Do                          |
|--------------------------------------------------------|-----------------------------|
| includes device<br>/data/logs/ossaps/ossapslog         | sub-step <a href="#">22</a> |
| does not include device<br>/data/logs/ossaps/ossapslog | sub-step <a href="#">11</a> |

- 11** Begin to add a new device:

**2**

- 12** Select a file device:

**3**

*The system responds:*

Enter file name ==> /data/logs/

- 13** Complete the path name:

**ossaps/ossapslog**

You have set up the log routing for the DDMS.



- 14** When prompted, enter the log format (from the range displayed). Use STD (the default format) or SCC2 if you want the following information to be displayed in all log reports:
- user-defined office ID, same for all logs and streams
  - the name of the node (ECORE) from which the log is generated
  - the sequence number in dual (global and device) format
- Other formats that can be used include: STD\_OLD or SCC2\_OLD
- 15** When prompted, set the Ecore option. Enter ON, if you want the log-generating node name to be displayed in all reports (requires the STD or SCC2 format). Otherwise, enter OFF.
- 16** Select addrep:
- a**
- 17** Enter the log identifier (in uppercase):
- DDMS**
- 18** Save the new device:
- y**
- The system responds:*
- Save completed -- press return to continue
- 19** Press the Enter key to return to the Add Device screen.
- 20** Return to the Device List Menu screen:
- 5**
- 21** Return to the Device List Menu screen:
- 6**
- 22** Exit logroute:
- 6**
- 23** The CM User Setup screen is displayed as shown in the following example.
- The required CM users, SDM01-SDM04, for DDMS are added to the DDMS configuration file. The passwords for these users must be the same as those entered in [Creating user IDs on the CM](#) in this procedure, during the NCL installation. The userIDs and passwords are not case sensitive

**DDMS CM user setup screen**

```
 CM User Setup

0. QUIT
1. Add user
2. Delete user (by ID)
3. Update passwd (by ID)
4. Display users (ID)

Enter choice:
```

**24** Add a new user:

**1**

**25** When prompted, enter the user name (that is, sdm01).

**26** When prompted enter the user password.

Your first entry of a user name and password will cause a file not valid error message. Ignore this message and continue to add the other user names and passwords.

**27** Return to step [24](#) and repeat to add other new users.

**28** Exit the CM User Setup screen:

**0**

*The DDMS Clients Configuration screen is displayed as shown in the following figure.*

**DDMS Clients Configuration screen**

```
 DDMS Clients Configuration

0. Quit
1. Add new clients
2. Remove existing clients
3. List existing clients

Enter choice:
```

**29** Configure the DDMS clients. Add a new client:

**1**

**Note:** The DDMS clients are the CS 2000 Management tools servers with the SESM load.

- 30 When prompted, enter the IP address for each of the CS 2000 Management tools servers. Press the Enter key after each entry and type **done** once you have entered all the IP addresses.
- 31 Exit the DDMS clients configuration screen:  
0
- 32 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure

---

## Upgrading DCE

---

### Purpose

Use this procedure to upgrade your Distributed Computing Environment (DCE).

### Application

**ATTENTION**

This procedure will upgrade the DCE system files and provide the cell\_admin user with sdm\_admin sub administrator account access permissions.

Access permissions allow the cell\_admin to default to the sdm\_admin user id when prompted elsewhere in SDM upgrade and administration actions. If the cell\_admin declines to enter the user id and password in this procedure, the cell\_admin user id and password must be specified when performing subsequent CS 2000 Core Manager DCE administration and upgrade tasks.

For more information about DCE, refer to the following procedures:

- “Creating a DCE user” in *CS 2000 Core Manager Security and Administration*, NN10170-611
- “Configuring an SDM in a DCE cell” in *CS 2000 Core Manager Configuration Management*, NN10104-511
- “Removing an SDM from a DCE cell” in *CS 2000 Core Manager Configuration Management*, NN10104-511
- “Deleting a DCE user” in *CS 2000 Core Manager Security and Administration*, NN10170-611
- “Updating DCE principal names” in *CS 2000 Core Manager Security and Administration*, NN10170-611

### Procedure

#### Upgrading DCE

**ATTENTION**

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

**At the CS 2000 Core Manager**

- 1 Begin the DCE upgrade:

**dceupgrade**

The system displays the status of each step during the DCE upgrade.

*Example response:*

```
Update mkdce file now...
Stop dce daemons now...
Update rc.dce file and restart the dce daemons
now...
It may take about 3 minutes, please wait...
You are required to login as cell_admin for the
following operations
```

```
DCE administrator user ID [cell_admin]:
```

- 2 At the prompt, enter the DCE cell\_admin user ID.

If you do not have a DCE cell\_admin user ID, press the Enter key to accept the default user ID (cell\_admin).

*Example response:*

```
DCE administrator password:
```

- 3 At the prompt, enter the password for the DCE cell\_admin user ID.

*Example response:*

```
Update access permission for sdm_admin now...
Dceupgrade command complete
The DCE upgrade is complete.
```

- 4 If you did not have a DCE cell\_admin user ID and you pressed Enter in step 2 to accept the default DCE user ID, press Enter at the password prompt.

*The response indicates that the DCE login failed; however, the DCE upgrade completed correctly and you can continue.*

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

## Installing and configuring the OM Data Delivery application

### Purpose

Use this procedure to install and configure the Operational Measurements (OM) Data Delivery application.

### Application

The OM Data Delivery application collects and stores operational measurement (OM) data from the call server core. The application stores the data in comma separated value (CSV) files which are sent to the client operations support system (OSS).

The application's Tuple Number option allows you to activate or disable a tuple number so that it can be included in or exclude from a CSV file with other OM information. You must activate or disable the Tuple Number option at the Config menu level on the CS 2000 Core Manager.

#### ATTENTION

You must busy (BSY) and return to service (RTS) the OM Data Delivery application for the Tuple Number option to be either activated or disabled.

### Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Other activities related to using this procedure

| Procedure                                          | Document                                                              |
|----------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager             | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying actions a user is authorized to perform | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

If you are installing the OM Data Delivery application for the first time, ensure that the OM Access Service and Table Access Service

application filesets are installed and in service on your CS 2000 Core Manager before executing this procedure.

For the wireless market, the Nortel support group must increase the buffer size within the OM Access Service to 2.5 MB. This is done to accommodate the amount of data being transferred by the front end for a transfer period of every 30 minutes.

## Procedures

### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

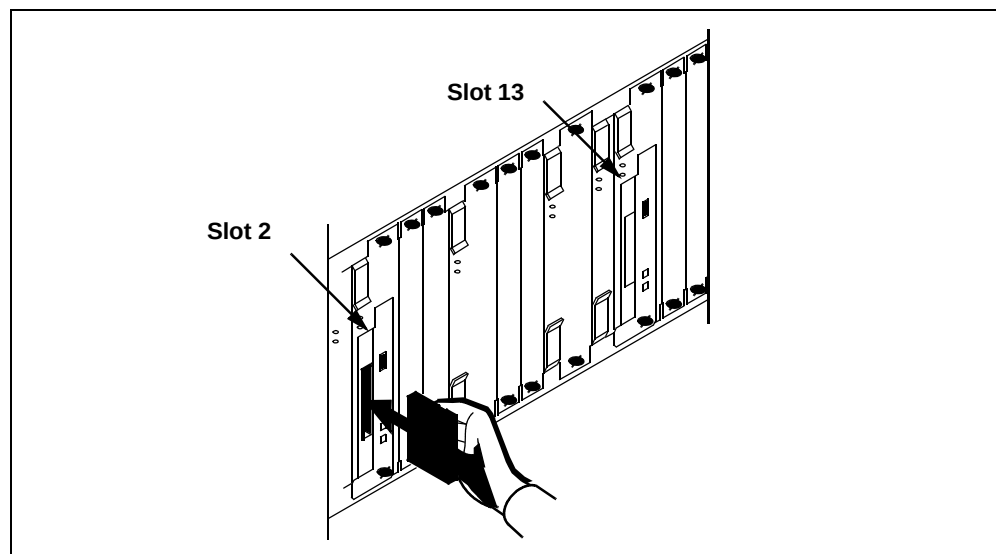
## Installing the OM Data Delivery application

### *At the CS 2000 Core Manager*

- 1 Insert the tape for the software load into one of the tape drives (slot 2 or slot 13) of the main chassis, as shown in the following figure.

Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

### Inserting a tape into the slot 2 tape drive of the main chassis



**At the maintenance interface**

- 2 Determine the installation method.

| <b>If you choose to install OM Data Delivery by</b>                                | <b>Do</b>                                                                                                                                        |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| logging onto a local VT100 terminal connected directly to the CS 2000 Core Manager | log on to the CS 2000 Core Manager as a user authorized to perform config-admin actions at the VT-100 terminal, and go to step <a href="#">6</a> |
| using telnet from a remote UNIX workstation to the CS 2000 Core Manager            | step <a href="#">3</a>                                                                                                                           |

- 3 Open a VT-100 compatible terminal window at the remote UNIX workstation.

**Note:** To install the OM Data Delivery application using a remote UNIX workstation, verify that telnet is enabled on the CS 2000 Core Manager.

- 4 Log into the CS 2000 Core Manager from the terminal window prompt:

```
telnet <ip_address>
```

where

**<ip\_address>**

is the IP address of the CS 2000 Core Manager you want to install the OM Data Delivery application on.

- 5 When prompted, enter the login ID and password for a user authorized to perform config-admin actions.

- 6 Access the maintenance interface level:

```
sdmmtc
```

- 7 Access the software inventory manager (SWIM) level:

```
swim
```

*The CS 2000 Core Manager lists the software applications currently installed.*

- 8 List the contents of the tape you previously inserted:

```
apply <n>
```

where



**<n>**

is either 0 (slot 2) or 1 (slot 13).

- 9 Locate the OM Data Delivery application fileset.

If necessary, use the up (enter 12, u, or up) and down (enter 13, d, or down) commands to locate the OM Data Delivery application fileset.

**Note:** If you have a previous release of the OM Data Delivery application installed, its release number appears in the *Current* column, while the new version you are installing appears in the *Available* column.

- 10 Select and install the new OM Data Delivery application fileset:

**apply <n>**

where

**<n>**

is the number next to the OM Data Delivery application fileset.

*Example response:*

```
You have selected to install the following new
filesets or fileset updates.OM Delivery
Application 19.0.xx.0. Do you wish to proceed?
Please confirm ("YES", "Y", "NO", or "N"):
```

- 11 Confirm the apply command:

**y**

*Example response:*

```
Command in progress.
```

```
APPLYING fileset: 9
SDM_OMDD.OMD 19.0.XX.0
```

## Configuring the OM Data Delivery application

### *At the CS 2000 Core Manager console*

- 1 Access the Config menu:

**sdmmtc config**

- 2 Configure OM Data Delivery:

**config <n>**

where

&lt;n&gt;

is the number next to OM Data Delivery under fileset description

| If OM Data Delivery                                               | Do                     |
|-------------------------------------------------------------------|------------------------|
| is being initially installed or upgraded to the new software load | step <a href="#">3</a> |
| has already been installed and is currently active                | step <a href="#">4</a> |
| has already been installed and is currently disabled              | step <a href="#">5</a> |

- 3 Determine if the Tuple Number option is undefined.

*Example response:*

The Tuple number inclusion option is currently undefined.

Do you want the Tuple number to be provided with the OM Group information (Y/N) [N]?

**Note:** For fresh installations or upgrades from releases prior to CS2E0070, the default value is *disabled (N)*.

| If you                                          | Do                                                                     |
|-------------------------------------------------|------------------------------------------------------------------------|
| activate the Tuple Number option                | enter <b>y</b> , press the Enter key, and go to step <a href="#">6</a> |
| do not want to activate the Tuple Number option | press the Enter key, and go to step <a href="#">6</a>                  |

- 4 The system indicates that the Tuple Number option is active.

*Example response:*

The Tuple number inclusion option is currently active.

Do you want the Tuple number to be provided with the OM Group information (Y/N) [Y]?

| If you                                         | Do                                                                     |
|------------------------------------------------|------------------------------------------------------------------------|
| want to disable the Tuple Number option        | enter <b>n</b> , press the Enter key, and go to step <a href="#">6</a> |
| do not want to disable the Tuple Number option | press the Enter key, and go to step <a href="#">6</a>                  |

- 5 Determine if the Tuple Number option is disabled.

*Example response:*

The Tuple number inclusion option is currently disabled.  
Do you want the Tuple number to be provided with the OM Group information (Y/N) [N]?

| If you                                          | Do                                                                     |
|-------------------------------------------------|------------------------------------------------------------------------|
| want to activate the Tuple Number option        | enter <b>y</b> , press the Enter key, and go to step <a href="#">6</a> |
| do not want to activate the Tuple Number option | press the Enter key, and go to step <a href="#">6</a>                  |

*The system prompts you to confirm if the MDM and SDM are integrated.*

Are the MDM and SDM integrated [Y|N]?

- 6 Confirm the MDM and SDM are integrated:

**y**

- 7 Configure the CS 2000 Core Manager to communicate with the Preside MDM. When prompted, enter the IP address of the first MDM:
- 8 When prompted, enter the hostname of the first MDM
- 9 When prompted, enter the IP address of the second MDM
- 10 When prompted, enter the hostname of the second MDM
- 11 When prompted, enter the port for 5-minute PM data
- 12 When prompted, enter the port for 30-minute PM data
- 13 When prompted, indicate whether you want to use custom retry settings.

| If you                                   | Do                                                                             |
|------------------------------------------|--------------------------------------------------------------------------------|
| do not want to use custom retry settings | type <b>n</b> , press the Enter key, and go to step <a href="#">15</a>         |
| want to use custom retry settings        | type <b>y</b> , press the Enter key, and continue with step <a href="#">14</a> |

- 14 Respond to the prompts with your custom retry settings and press the Enter key after each entry:

**Note:** The retry setting values shown here are examples. Retry setting values are in seconds (values higher than 300 seconds are not recommended as they can adversely affect recovery time).

**Enter the first connection retry interval: 2**

**Enter the number of retry attempts at that interval: 10**

**Enter the second connection retry interval: 10**

**Enter the number of retry attempts at that interval: 40**

**Enter the third connection retry interval: 60**

- 15 When prompted, confirm the data:

**y**

- 16 Determine the state of the OM Data Delivery application.

| If the OM Data Delivery application            | Do                      |
|------------------------------------------------|-------------------------|
| is ManB or Offl                                | step <a href="#">17</a> |
| is in any state <i>other</i> than ManB or Offl | step <a href="#">18</a> |

- 17 The system indicates that the configuration is complete.

*Example response:*

Configuration complete. Please press Enter . . .

Press the Enter key, and go to step [19](#).

- 18 The system indicates that the changes will take place after the OM Data Delivery application is restarted.

*Response:*

Changes will take effect after OM Delivery is restarted.  
Configuration complete. Please press Enter . . .

Press the Enter key, and go to step [19](#).

- 19 Exit the CS 2000 Core Manager maintenance interface:

**quit all**

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

## Installing or upgrading OpenSSH

### Purpose

Use this procedure to install the OpenSSH files.

For more information on OpenSSH, refer to section “OpenSSH overview” in *CS 2000 Core Manager Basics*, NN10018-111.

### Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Other activities related to using this procedure

| Procedure                                          | Document                                                              |
|----------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager             | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying actions a user is authorized to perform | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

### Procedure

#### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

#### At the CS 2000 Core Manager

- 1 Log on to the CS 2000 Core Manager as a user authorized to perform config-admin actions.

| If the software is | Do                     |
|--------------------|------------------------|
| on tape            | step <a href="#">2</a> |
| in a directory     | step <a href="#">3</a> |

- 2 Insert the tape labeled for the new software load into the tape drive in slot 2. Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

- 3 Access the maintenance interface:

**sdmmtc**

| If the software is | Do                                           |
|--------------------|----------------------------------------------|
| on tape            | list the filesets: apply 0                   |
| in a directory     | list the filesets: apply<br><directory_path> |

- 4 Select the latest version of the OpenSSH fileset:

**select <x>**

where

<x>

is the number next to the OpenSSH fileset.

- 5 Apply the selected fileset:

**apply**

- 6 Confirm the apply command:

**y**

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

## Installing or upgrading Reach Through SPM

### Purpose

This procedure provides instructions on how to install or upgrade the Reach Through SPM application on the CS 2000 Core Manager.

### Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Other activities related to using this procedure

| Procedure                                          | Document                                                              |
|----------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager             | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying actions a user is authorized to perform | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

### Procedure

#### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

#### Installing Reach Through SPM

##### *At the CS 2000 Core Manager*

- 1 Log on to the CS 2000 Core Manager as a user authorized to perform config-admin actions.

| If the software is | Do                     |
|--------------------|------------------------|
| on tape            | step <a href="#">2</a> |
| in a directory     | step <a href="#">3</a> |



- 2 Insert the new software tape into slot 2 of the tape drive. Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

- 3 Access the maintenance interface:

**sdmmtc**

| If the software is | Do                                           |
|--------------------|----------------------------------------------|
| on tape            | list the filesets: apply 0                   |
| in a directory     | list the filesets: apply<br><directory path> |

- 4 Select the Reach Through SPM fileset:

**select <n>**

where

<n>

is the number next to the Remote Registration System fileset.

- 5 Apply the selected fileset:

**apply**

- 6 Confirm the apply command:

**y**

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

## Installing or upgrading the GR740PT application server

### Purpose

Use this procedure to install or upgrade the GR740 Pass Through (PT) application server on the core manager.

### Prerequisites

To ensure a successful GR740PT application server operation, the following must first be configured:

- the settings for office parameters `eadas_dc_interface` and `eadas_nm_interface` in table OFCVAR, and the settings for EADAS SOC OAM00005 and OAM00006 are correct for your configuration.
- OAM00004 for EADAS/DC is ON and that office parameters `eadas_mpc_and_link` and `netminder_mpc_and_link` are appropriately datafilled in table OFCVAR, when BX25 connectivity is required.

The following table lists the supported configurations for EADAS GR740PT application server.

### CM EADAS TCP/IP configurations

| Supported configurations               | Setting for <code>eadas_dc_interface</code> | Setting for <code>eadas_nm_interface</code> | SOC OAM00005 | SOC OAM00006 |
|----------------------------------------|---------------------------------------------|---------------------------------------------|--------------|--------------|
| DC and NM over BX25                    | X25                                         | N/A                                         | ON           | IDLE         |
| DC and NM over TCP/IP                  | TCP_IP                                      | N/A                                         | ON           | IDLE         |
| DC and Netminder over BX25             | X25                                         | X25                                         | IDLE         | ON           |
| DC over BX25 and Netminder over TCP/IP | X25                                         | TCP_IP                                      | IDLE         | ON           |
| DC over TCP/IP and Netminder over BX25 | TCP_IP                                      | X25                                         | IDLE         | ON           |
| DC and Netminder over TCP/IP           | TCP_IP                                      | TCP_IP                                      | IDLE         | ON           |

The following table lists the channel assignments for EADAS. Note that DC EADAS channels 1, 2 and 3 support TR-740/746 compliant header

and message. NM EADAS channels 1, 2 and 3 support SR3942 and TR746 to Netminder.

### EADAS channel assignments

| Description   | Service name       | TCP port | MTS offset |
|---------------|--------------------|----------|------------|
| DC EADAS lc 1 | DC_EADAS_LOG_CHAN1 | 9550     | 234        |
| DC EADAS lc 2 | DC_EADAS_LOG_CHAN2 | 9551     | 235        |
| DC EADAS lc 3 | DC_EADAS_LOG_CHAN3 | 9552     | 236        |
| NM EADAS lc 1 | NM_EADAS_LOG_CHAN1 | 9553     | 237        |
| NM EADAS lc 2 | NM_EADAS_LOG_CHAN2 | 9554     | 238        |
| NM EADAS lc 3 | NM_EADAS_LOG_CHAN3 | 9555     | 239        |

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

### Other activities related to using this procedure

| Procedure                                          | Document                                                              |
|----------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager             | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying actions a user is authorized to perform | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

## Procedure

### Installing the GR740PT application server

#### *At the core manager*

- 1 Log in to the core manager as a user authorized to perform config-admin actions.

| If the NCL filesets are | Do                     |
|-------------------------|------------------------|
| on tape                 | step <a href="#">2</a> |

| If the NCL filesets are | Do                     |
|-------------------------|------------------------|
| in a directory          | step <a href="#">3</a> |

- 2 Insert the new software tape in slot 2 of the tape drive. Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

- 3 Access the maintenance interface:

**sdmmtc**

*The maintenance menu appears, with menu selections highlighted in the left column.*

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

| If the NCL filesets are | Do                                             |
|-------------------------|------------------------------------------------|
| on tape                 | list the filesets: > apply 0                   |
| in a directory          | list the filesets: > apply<br><directory path> |

- 5 Select the GR740 fileset:

**select <x>**

where

**<x>**

is the number next to the GR740 TCP/IP Pass Through fileset

- 6 Apply the GR740 fileset:

**apply**

- 7 Confirm the apply command:

**y**

*The system responds:*

```
GR740PT application server Installation
```

```
Command in Progress, x filesets to process.
Processing fileset x.
```

```
APPLYING GR740PT xx.xx.xx.xx
```

```
Since the following filesets were applied to the system
for the first time, their configuration programs will
now be executed.
```

- 8** Press Enter to begin the configuration. Use the following table to determine your next step.

| If                                               | Do                            |
|--------------------------------------------------|-------------------------------|
| you are configuring GR740PT in non-secure mode   | Go to step <a href="#">9</a>  |
| you are configuring GR740PT in local secure mode | Go to step <a href="#">13</a> |
| you are configuring GR740PT in DCE secure mode   | Go step <a href="#">17</a>    |

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

| If                                    | Do                      |
|---------------------------------------|-------------------------|
| your system is configured for DCE     | Step <a href="#">10</a> |
| your system is not configured for DCE | Step <a href="#">11</a> |

- 10** In response to the prompt that asks whether you want to configure the GR740PT fileset using DCE, respond by typing N or No.
- 11** In response to the prompt: Enter mode of security, select 1 (Non-secure mode).  
*After the configuration is complete, the system displays a response indicating successful installation.*
- 12** Go to step [19](#)
- 13** Use the following table to determine your next step.

| If                                    | Do                      |
|---------------------------------------|-------------------------|
| your system is configured for DCE     | Step <a href="#">14</a> |
| your system is not configured for DCE | Step <a href="#">15</a> |

- 14** In response to the prompt that asks whether you want to configure the GR740PT fileset using DCE, respond by typing N or No.
- 15** In response to the prompt: Enter mode of security, select 2 (Local [SSH] secure mode).  
*After the configuration is complete, the system displays a response indicating successful installation.*

- 16** Go to step [19](#)
- 17** In response to the prompt that asks whether you want to configure the GR740PT fileset using DCE, respond by typing Y or Yes.

*You are prompted for the DCE administrator's ID (sdm\_admin) and password.*

**18**

**ATTENTION**

If you decide not to configure GR740PT in DCE secure mode (selection 3), then to complete the configuration, choose either 1 (and go to step [9](#)) for non-secure mode or 2 (and go to step [13](#)) for local secure mode.

Select 3 (DCE security Secure mode) in response to the prompt to enter the mode of security.

*After the configuration is complete, the system displays a response indicating successful installation.*

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

## Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager

### Purpose

Use this procedure to install and configure the Backup Restore Manager application on the CS 2000 Core Manager

### Application

The Backup Restore Manager application functionality requires the appropriate software resident and configured on platforms that require synchronized imaging. Although no CS 2000 Core Manager data is backed up through the Backup Restore Manager, the Backup Restore Manager software must be installed on the CS 2000 Core Manager to allow control of the XA-core and 3PC (Compact) backup.

### Prerequisites

You must be a user authorized to perform config-admin actions.

Before executing this procedure, ensure that a user name and password used for logging into the core to initiate an image dump is created and enabled. For assistance refer to procedure, "Creating the backup user ID on the core for SBRM" in *CS 2000 Core Manager Configuration Management*, NN10104-511, or in *ATM/IP Solution-level Security and Administration*, NN10402-600.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Other activities related to using this procedure

| Procedure                                          | Document                                                              |
|----------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager             | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying actions a user is authorized to perform | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

## Procedures

### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

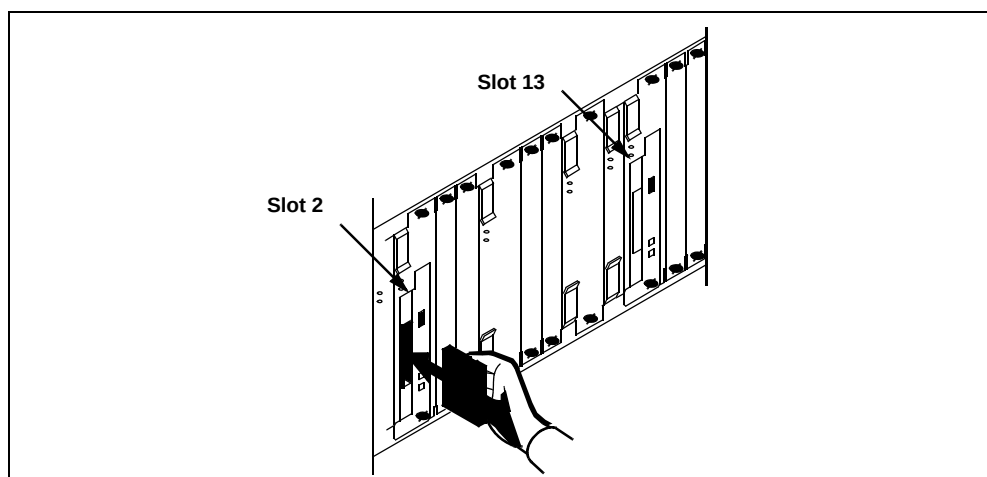
Use the following table to determine the correct procedure to use.

| If                                                                                                                           | Do                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| you are installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager for the first time     | procedure <a href="#">Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager</a> |
| you are only reconfiguring the user name and password for an existing Backup Restore Manager application on the Core Manager | procedure <a href="#">Reconfiguring the Backup Restore Manager application on the CS 2000 Core Manager on page 727</a>  |

### Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager

#### *At the CS 2000 Core Manager*

- 1 Insert the tape for the software load into one of the tape drives (slot 2 or slot 13) of the main chassis, as shown in the following figure. Wait until the tape drive stabilizes (yellow LED is off) before you proceed.





**At the maintenance interface**

- 2 Determine the installation method.

| <b>If you choose to install OM Data Delivery by</b>                       | <b>Do</b>                                                                                                                                        |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| logging onto a local VT100 terminal connected to the CS 2000 Core Manager | log on to the CS 2000 Core Manager as a user authorized to perform config-admin actions at the VT-100 terminal, and go to step <a href="#">6</a> |
| using telnet from a remote UNIX workstation to the CS 2000 Core Manager   | step <a href="#">3</a>                                                                                                                           |

- 3 Open a VT-100 compatible terminal window at the remote UNIX workstation.
- 4 Log onto the CS 2000 Core Manager from the terminal window prompt:

**telnet <ip\_address>**

where

**<ip\_address>**

is the IP address of the CS 2000 Core Manager you want to install the Backup Restore Manager application on.

- 5 When prompted, enter the login ID and password for a user authorized to perform config-admin actions.

- 6 Access the maintenance interface level:

**sdmmtc**

- 7 Access the software inventory manager (SWIM) level:

**swim**

*The CS 2000 Core Manager lists the software applications currently installed.*

- 8 List the contents of the tape you previously inserted:

**apply <n>**

where

**<n>**

is either 0 (slot 2) or 1 (slot 13).

- 9 Locate the Java Runtime Environment (JRE) 1.3 packages.  
**Note:** If necessary, use the up (enter 12, u, or up) and down (enter 13, d, or down) commands to locate the JRE 1.3 packages.
- 10 Select and install the Java Runtime Environment Executables 1.3.0.0 package:  
**apply <n>**  
where  
**<n>**  
is the number next to the Java Runtime Environment Executables 1.3.0.0 package.
- 11 Confirm the apply command:  
**y**
- 12 Select and install the Java Runtime Environment Libraries 1.3.0.0 package:  
**apply <n>**  
where  
**<n>**  
is the number next to the Java Runtime Environment Libraries 1.3.0.0 package.
- 13 Confirm the apply command:  
**y**
- 14 Select and install the Java Runtime Environment Executables 1.3.0.15 package:  
**apply <n>**  
where  
**<n>**  
is the number next to the Java Runtime Environment Executables 1.3.0.15 package.
- 15 Confirm the apply command:  
**y**
- 16 Select and install the Java Runtime Environment Libraries 1.3.0.15 package:  
**apply <n>**  
where

- <n>**  
is the number next to the Java Runtime Environment Libraries 1.3.0.15 package.
- 17** Confirm the apply command:
- y**
- 18** Select and install Succession Provisioning Data Sync Manager (or Backup Restore Manager fileset, SDM\_BKM.bkm).
- apply <n>**  
where  
**<n>**  
is the number next to the Backup Restore Manager fileset, SDM\_BKM.bkm (or Succession Prov Data Sync Manager)
- 19** Confirm the apply command:
- y**  
*The application installation script runs.*
- 20** As part of the Backup Restore Manager application installation, a script runs that enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). As the script runs, you are prompted for the user name. The script restricts the name to a maximum of 16 characters.

**ATTENTION**

The user name must be one that exists and is used to log in to the core to initiate an image dump. The user name you enter must also be enabled on the core. For assistance, refer to procedure, "Creating the backup user ID on the core for SBRM" in *CS 2000 Core Manager Configuration Management*, NN10104-511, or in *ATM/IP Solution-level Security and Administration*, NN10402-600.

- 21 You are prompted for the password of the user you entered in the previous step. The script restricts the password to a maximum of 16 characters.

**ATTENTION**

This password is set up when the user name in the previous step is created. For assistance refer to procedure, "Creating the backup user ID on the core for SBRM" in *CS 2000 Core Manager Configuration Management*, NN10104-511, or in *ATM/IP Solution-level Security and Administration*, NN10402-600.

- 22 You are prompted for the logical volume where the backup is stored. This is the device on which the core image dump is stored. Ensure that this device has enough space to store the backup.
- 23 You are prompted for the core type: either XA-core or Compact.  
**Note:** This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 24 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Reconfiguring the Backup Restore Manager application on the CS 2000 Core Manager

At any time after the configuring the Backup Restore Manager is complete, you wish to reconfigure user access to the core for the SBRM

### ***At the maintenance interface***

- 1 Access the config level of the SDM maintenance interface:  
**sdmmtc config**
- 2 From the list of filesets that display, locate the application number of the Succession Provisioning Data Sync Manager fileset or Backup Restore Manager fileset, SDM\_BKM.bkm, then type:  
**config <n>**  
where  
**<n>**  
is the application number for the Succession Provisioning Data Sync Manager fileset or Backup Restore Manager fileset, SDM\_BKM.bkm

- 3 If applicable, confirm the config command:  
**y**  
*The Backup Restore Manager application script runs that enables you to reconfigure access to the core for the Synchronous Backup Restore Manager (SBRM).*
- 4 You are prompted for the user name. The script restricts the name to a maximum of 16 characters.

**ATTENTION**

The user name must be one that exists and is used to log in to the core to initiate an image dump. The user name you enter must also be enabled on the core. For assistance, refer to procedure, "Creating the backup user ID on the core for SBRM" in *CS 2000 Core Manager Configuration Management*, NN10104-511, or in *ATM/IP Solution-level Security and Administration*, NN10402-600.

- 5 You are prompted for the password of the user you entered in the previous step. The script restricts the password to a maximum of 16 characters.

**ATTENTION**

This password is set up when the user name in the previous step is created. For assistance refer to procedure, "Creating the backup user ID on the core for SBRM" in *CS 2000 Core Manager Configuration Management*, NN10104-511, or in *ATM/IP Solution-level Security and Administration*, NN10402-600.

- 6 You are prompted for the logical volume where the backup is stored. This is the device on which the core image dump is stored. Use the same logical volume used previously, unless otherwise specified.
- 7 You are prompted for the core type: either XA-core or Compact. Enter the same core type previously used, unless otherwise specified.  
**Note:** This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 8 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Installing CEM filesets

---

### Purpose

Use this procedure to install the following Core Element Manager (CEM) filesets in the order listed:

- AX4<release>-dmsDataSrv-CSU-000.tape
- AX4-<release>-TntFTPHandl-CSU-000.tape
- AX4-<release>-SAF-CSU-000.tape

For more information about the CEM filesets, refer to *CS 2000 Core Manager Basics*, NN10018-111.

### Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Other activities related to using this procedure

| Procedure                                          | Document                                                              |
|----------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager             | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying actions a user is authorized to perform | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

## Procedure

### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

#### *At the CS 2000 Core Manager*

- 1 Log on to the CS 2000 Core Manager as a user authorized to perform config-admin actions.

| If the software is | Do                     |
|--------------------|------------------------|
| on tape            | step <a href="#">2</a> |
| in a directory     | step <a href="#">3</a> |

- 2 Insert the tape labeled for the new software load into the tape drive in slot 2. Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

- 3 Access the maintenance interface:

**sdmmtc**

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

| If the software is | Do                                           |
|--------------------|----------------------------------------------|
| on tape            | list the filesets: apply 0                   |
| in a directory     | list the filesets: apply<br><directory_path> |

- 5 Select the latest version of AX4<release>-dmsDataSrv-CSU-000.tape fileset:

**select AX4<release>-dmsDataSrv-CSU-000.tape**

- 6 Apply the selected fileset:

**apply**

- 7 Confirm the apply command:

**y**

- 8 Select the latest version of one of the AX4-<release>-TntFTPHandl-CSU-000.tape fileset:

**select AX4-<release>-TntFTPHandl-CSU-000.tape**

- 9 Apply the selected fileset:  
**apply**
- 10 Confirm the apply command:  
**y**
- 11 Select the latest version of one of the AX4-<release>-SAF-CSU-000.tape fileset:  
**select AX4-<release>-SAF-CSU-000.tape**
- 12 Apply the selected fileset:  
**apply**
- 13 Confirm the apply command:  
**y**
- 14 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Commissioning X.25 connectivity

### Purpose

Use this procedure to commission or recommission X.25 connectivity on the CS 2000 Core Manager from the configuration level (sdmconfig). You can also commission or recommission X.25 from the X25 level of the maintenance interface (sdmmtc x25). The same commands are used at both levels to set the X.25 base and controller licenses, and the Data Terminal Equipment (DTE) addresses for both X.25 ports.

### Prerequisites

You must be a user authorized to perform config-admin actions.

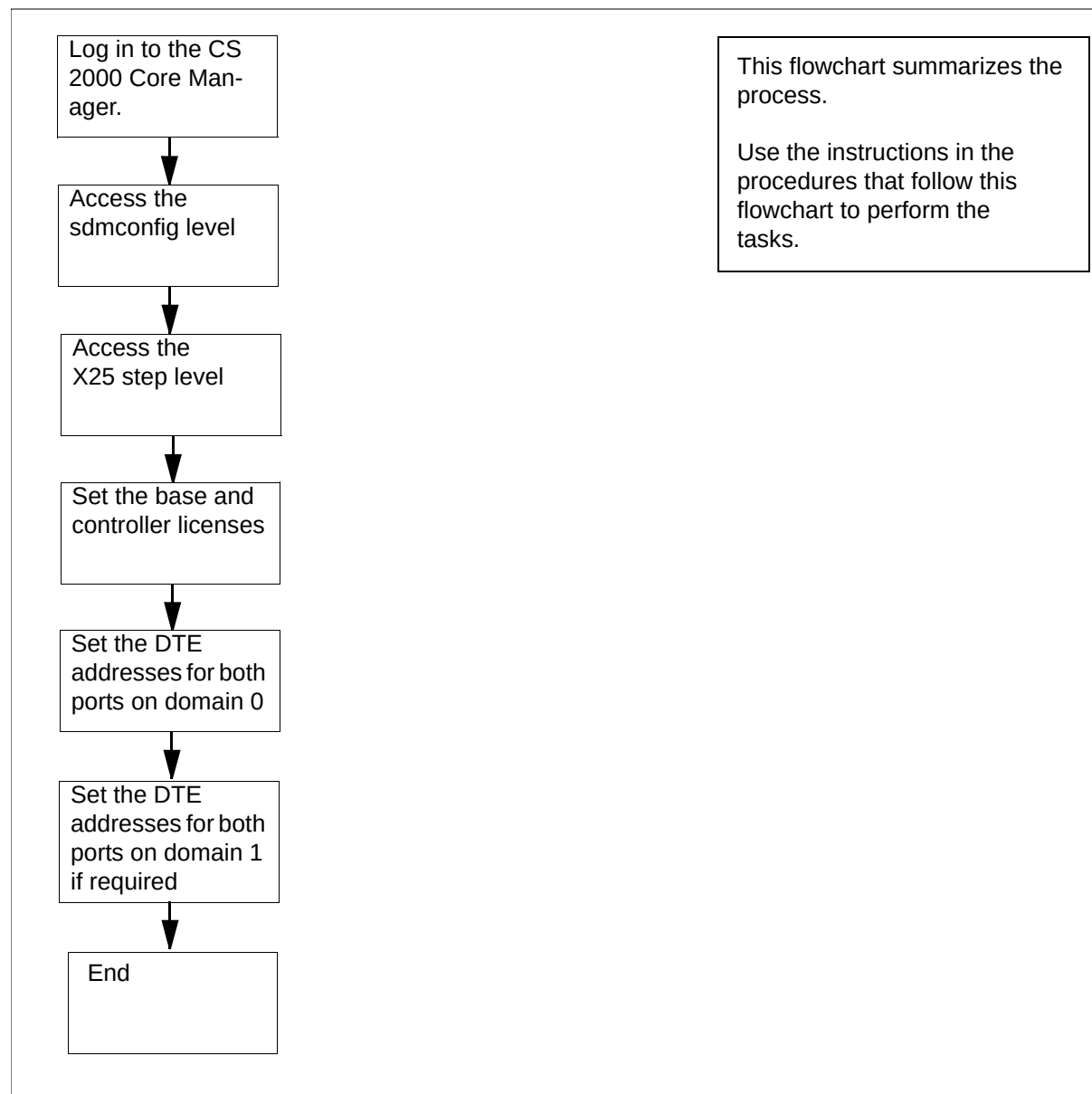
For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Other activities related to using this procedure

| Procedure                                          | Document                                                              |
|----------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager             | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying actions a user is authorized to perform | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

### Procedure

The following task flow diagram provides an overview of the process for commissioning X.25 connectivity. Use the instructions in the procedure that follows the flowchart to complete the tasks.

**Task flow for commissioning X25 connectivity**

If you are commissioning X.25 connectivity for the first time, follow the instructions in the following procedure [Configuring X.25 licences](#). If you are recommissioning X.25 on domain 0 or domain 1, follow the instructions in [Configuring DTE addresses on page 735](#).

## Configuring X.25 licences

### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### *At the CS 2000 Core Manager*

- 1 Log in to the CS 2000 Core Manager as a user authorized to perform config-admin actions.
- 2 Access the configuration level:  
**sdmconfig**
- 3 Access the X.25 commissioning step level:  
**step <#>**  
*where*  
**<#>**  
is the number next to the X.25 commissioning step.
- 4 Initiate the configuration process:  
**change**
- 5 When prompted, enter the new Base license key. The Base license key is the 28 alphanumeric character string for the X.25 hardware that you are commissioning.
- 6 When prompted, enter the new Controller license key. The Controller license key is the 28 alphanumeric character string for the X.25 hardware that you are commissioning.

#### *Example response:*

X25 Connectivity values to be changed:

Base license key: 3xcmwj6p4wmnxhyknmnbwvqzr2aa  
Controller license key:  
5me5q7itsuba5hyknmnbwvqzr2aa

Proceed with these values?

Enter Y to confirm, N to reject, or E to edit:

- 7 When prompted, confirm the values:

**y**

*Example response:*

Change - Command submitted.

- 8 You have completed this procedure. Continue commissioning X.25 connectivity, by following the instructions in the procedure [Configuring DTE addresses](#).

**Configuring DTE addresses*****At the CS 2000 Core Manager***

- 1 If you are not already at the commissioning step level, complete steps 1 through 3 of procedure [Configuring X.25 licences](#), then go the next step of this procedure. Otherwise, go to the next step.

- 2 Configure the DTE addresses of the X25 ports on domain 0:

**change 0 <port>**

where

**<port>**

is 0 or 1

- 3 Enter the DTE address (5 to 15 digits) that corresponds to the port.

*Example response*

X25 Connectivity values to be changed:

DTE address for domain 0 port 0: 123456

This action will affect service on the specified port.

Proceed with these values?

Enter Y to confirm, N to reject, or E to edit:

- 4 Confirm the values:

**y**

*Example response:*

Change 00 - Command submitted.

- 5 Repeat steps [2](#) to [4](#) for the other port in domain 0.

| If the system                         | Do                      |
|---------------------------------------|-------------------------|
| has an X25 card in domain 1           | step <a href="#">6</a>  |
| does not have an X25 card in domain 1 | step <a href="#">10</a> |

- 6 Configure the DTE addresses of the X25 ports on domain 1:  
**change 1 <port>**  
*where*  
**port**  
is 0 or 1
- 7 Enter the DTE address (5 to 15 digits) that corresponds to the port, and press the Enter key.  
*Example response:*  
X25 Connectivity values to be changes:  
  
DTE address for domain 1 port 0: 123456  
  
This action will affect service on the specified port.  
  
Proceed with these values?  
Enter Y to confirm, N to reject, or E to edit:
- 8 Confirm the values:  
**y**  
*Example response:*  
Change 10 - Command submitted.
- 9 Repeat steps [6](#) through [8](#) for the other port in domain 1.
- 10 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Stopping and starting the DDMS proxy

### Application

#### ATTENTION

Use this procedure only if you have been directed to do so such as after a software upgrade.

Use this procedure to stop and start the DDMS proxy on the CS 2000 Management Tools server. The DDMS proxy enables communication between the CS 2000 Management Tools server and the core.

### Prerequisites

There are no prerequisites for this procedure.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Establish a login session to the inactive server, using one of the following methods:

| If using          | Do                     |
|-------------------|------------------------|
| telnet (unsecure) | step <a href="#">2</a> |
| ssh (secure)      | step <a href="#">3</a> |

- 2 Log in to the server using telnet (unsecure) as follows:

- a Log in to the server by typing

> **telnet** <**server**>

and pressing the Enter key.

where

**server**

is the physical IP address of the inactive server

- b When prompted, enter your user ID and password.
  - c Change to the root user by typing  
`$ su -`  
and pressing the Enter key.
  - d When prompted, enter the root password.  
Proceed to step [4](#).
- 3 Log in using ssh (secure) as follows:
  - a Log in to the server by typing  
`> ssh -l root <server>`  
and pressing the Enter key.  
where  
**server**  
is the physical IP address of the inactive server  
**Note:** If this is the first time you are logging in using ssh,  
the system will request that you confirm to continue  
connecting. Enter `yes` at the prompt.
  - b When prompted, enter the root password.
- 4 Access the command line interface by typing  
`# cli`  
and pressing the Enter key.
- 5 Enter the number next to the “Configuration” option in the menu.

- 6 Enter the number next to the "Succession Element Configuration" option in the menu.
- 7 Enter the number next to the "DDMSProxy Application Configuration" option in the menu.
- 8 Enter the number next to the "ddmsproxy\_stop" option in the menu.

*Example response*

```
===Executing "ddmsproxy_stop"
```

```
ddmsproxy service stopping
```

```
=== "ddmsproxy_stop" completed successfully
```

- 9 Enter the number next to the "ddmsproxy\_start" option in the menu.

*Example response*

```
===Executing "ddmsproxy_start"
```

```
ddmsproxy service starting
```

```
=== "ddmsproxy_start" completed successfully
```

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



## Removing DDMS filesets

### Purpose

Use this procedure to remove the DDMS filesets, as well as the DDMS logical volumes.



#### CAUTION

This procedure completely removes all information used by DDMS. Use this procedure only if DDMS is no longer required on your system.

### Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Other activities related to using this procedure

| Procedure                                          | Document                                                              |
|----------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CS 2000 Core Manager             | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |
| Displaying actions a user is authorized to perform | <i>CS 2000 Core Manager Security and Administration</i> , NN10170-611 |

## Procedure

### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Removing DDMS filesets

#### *At the local VT100 console*

- 1 Log into the CS 2000 Core Manager as a user authorized to perform config-admin actions.
- 2 Access the SWIM level of the maintenance interface:  
**sdmmtc swim**
- 3 Access the Details level:  
**details**
- 4 Remove the DDMS filesets:  
**remove <n>**  
where  
    <n>  
        is the number next to each of the following DDMS filesets:  
        OSS and Application Svcs and OSS Comms Svcs
- 5 When prompted, confirm the remove command:  
**y**
- 6 Delete the file log device for DDMS. Start the log delivery commissioning tool if it does not automatically appear:  
**logroute**  
*The Logroute Main Menu screen appears.*

#### Logroute Main Menu

- 1 - Device List
- 2 - Global Parameters
- 3 - CM Configuration File
- 4 - Gdd Configuration
- 5 - Help
- 6 - Quit Logroute

Enter Option ==>

**7** Access the Device List Menu:**1***The Device List Menu screen appears.*

```
Device List Menu

1 - View Device
2 - Add Device
3 - Delete Device
4 - Modify Device
5 - Help
6 - Return to Main Menu

Enter Option ==>
```

**8** Access the Delete Device menu screen:**3***The system displays the list of configured devices and prompts you to enter the number of the device that you want to delete.**Example response:*

```
Delete Device Menu

Enter ABORT to return to Device List Menu

Devices:
1 - HOST: any PORT: 8551 Type: TCPIN
2 - HOST: 10.102.4.4 PORT: 14450 TCP
3 - /data/logs/faults FILE

Enter device number to delete ==>
```

**9** Delete the file log device for DDMS:**<x>**

where

**<x>**

is the number next to the file log device for DDMS  
(/data/logs/ossaps/ossapslog)

*The system responds:*

Device will be deleted permanently. Continue...  
(Y/N) [N] :

- 10** Confirm that you want to delete the selected device:

**y**

*The system responds:*

Save data completed -- press return to continue

- 11** Return to the Device List menu screen:

**abort**

- 12** Return to the Logroute Main menu screen:

**6**

- 13** Quit the logroute tool:

**6**

- 14** List the DDMS logical volumes:

**df -k**

The logical volumes you need to remove are

- /osscomms
- /ossapslog
- /ossaps

- 15** Proceed with the removal. Change directory to the root level:

**cd /**

- 16** Unmount the /ossaps directory:

**umount /ossaps**

- 17** Unmount the /ossapslog directory:

**umount /ossapslog**

- 18** Unmount the /osscomms directory:

**umount /osscomms**

- 19** Remove the /ossaps file system:

**rmfs /ossaps**

- 20** Remove the /ossapslog file system:

**rmfs /ossapslog**

- 21 Remove the /osscomms file system:  
**rmfs /osscomms**
- 22 Remove the /ossaps directory:  
**rmdir /ossaps**
- 23 Remove the /ossapslog directory:  
**rmdir /ossapslog**
- 24 Remove the /osscomms directory:  
**rmdir /osscomms**
- 25 Remove the /ossaps file in the /data/logs directory:  
**rm /data/logs/ossaps**
- 26 Remove the /ossaps file in the /data directory:  
**rm /data/ossaps**
- 27 Remove the /ossapslogs file in the /data directory:  
**rm /data/ossapslog**
- 28 Remove the /osscomms file in the /data directory:  
**rm /data/osscomms**
- 29 Change directory to the /sdm directory:  
**cd /sdm**
- 30 Remove the osscomms directory along with all files and directories inside osscomms, without verification:  
**rm -rf osscomms**
- 31 Remove the ossaps directory along with all files and directories inside ossaps without verification:  
**rm -rf ossaps**
- 32 You have completed this procedure. Return to step [6](#) of procedure [Completing the CS 2000 Core Manager upgrade](#)

## Stopping and starting the Apache Web Server and Tomcat Servlet Container

---

### Application

#### ATTENTION

Use this procedure only if you have been directed here from [Completing the CS 2000 Core Manager upgrade on page 563](#).

Use this procedure to stop and start the Apache Web Server and Tomcat Servlet Container components on the CS 2000 Management Tools server.

### 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 Use the following table to determine your next step.

| If you want to                                           | Do                     |
|----------------------------------------------------------|------------------------|
| stop the Apache web server and Tomcat servlet container  | step <a href="#">6</a> |
| start the Apache web server and Tomcat servlet container | step <a href="#">7</a> |

- 6 Stop the Apache Tomcat component by typing  
**# servstop WEBSERVER**  
and pressing the Enter key.
- 7 Start the Apache Tomcat component by typing  
**# servstart WEBSERVER**  
and pressing the Enter key.
- 8 You have completed this procedure.



# Core and Billing Manager 850 Upgrades

This procedure enables you to upgrade Core and Billing Manager (CBM) servers.

## New in this release

### Feature changes

In SN09U, the CBM media is delivered on a single media. Prior to release SN09U, each CBM flavor used a unique media (disk or ESD file) and upgrade procedure. Starting with release SN09U, all of the CBM flavors share a single, converged media (disk or ESD file) and use a unified upgrade procedure. In the CBM upgrade procedure, the `cbm_setup` program maps the flavor of CBM and its previous release profile to a new UCBM profile.

In addition, the `queryloads` tool has been updated to correctly show CBM product, profile, and version information, the packages installed for a profile, and any applied patches. The installation date is shown for each package and patch.

## Upgrade paths

Nortel supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U

The CBM is provided in several flavors for the following Wireline markets:

- Time Division Multiplexed (TDM)
- Succession



## Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade

### Time to complete an upgrade

The following table lists the tasks to upgrade CBM 850 software and the estimated time to complete each task.

**Table 1 Estimated time to complete a software upgrade**

| Task                      | Time    |
|---------------------------|---------|
| Preparing for the upgrade | 3 hours |
| Upgrading the software    | 1 hour  |
| Completing the upgrade    | 2 hours |
| Total upgrade time        | 6 hours |
| Performing a fallback     | 1 hour  |

**Note 1:** A full system backup is performed at the end of the “Preparing for the upgrade” task and at the end of the “Completing the upgrade” task. The estimated time for each backup is 1.5 hours.

**Note 2:** Execution of the “Preparing for the upgrade” task should be planned for one maintenance shift. The “Upgrading the software” and “Completing the upgrade” tasks should be planned for execution together during another, separate maintenance shift.

**Note 3:** The Total upgrade time shown above does not include time required for backups.

## System Performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade.

## System limitations during upgrade

During a software upgrade, performing the following actions is not recommended:

- System administration
  - adding, deleting, or modifying users
  - setting time of day
  - changing passwords
- System management
  - modifying the system name
  - adding or deleting system nodes
  - modifying the IP addresses

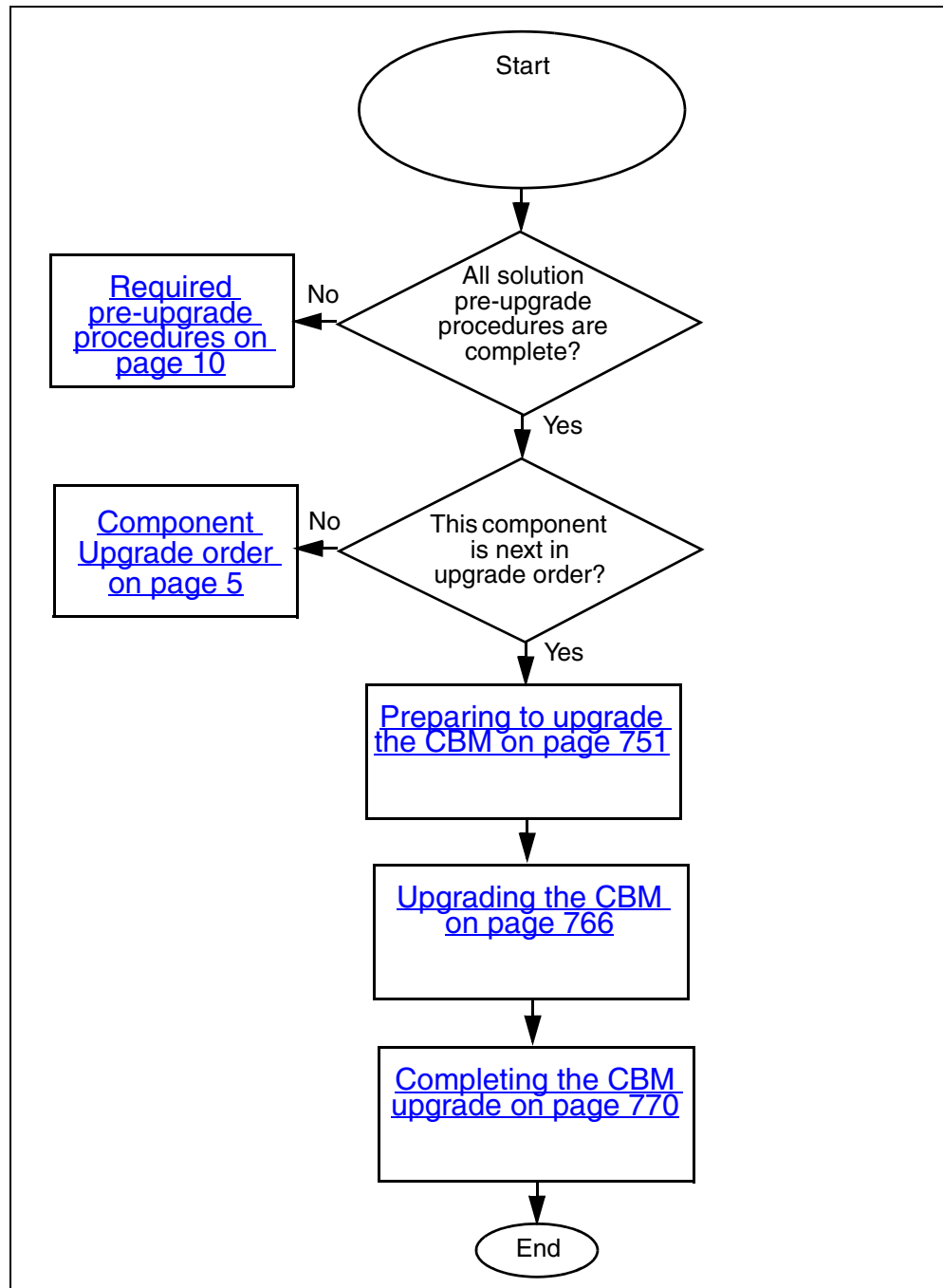
### ATTENTION

During the upgrade, after the upgraded node has become active, you are advised to not configure or re-configure SBA or RTB file transfer schedules, or OMDD file transfer destinations. Performing a fallback will not preserve these changes, and these applications will fail.

## CBM upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

**Figure 1 CBM upgrade tasks**



## Preparing to upgrade the CBM

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

The following table contains information that you need prior to starting an upgrade. Use the checklist to confirm that a prerequisite has been met and to record any information that you will need for the upgrade.

#### Prereq items

| Item | Description                                                                                                                    | Checklist |
|------|--------------------------------------------------------------------------------------------------------------------------------|-----------|
| A    | Identify the load that you are upgrading from:                                                                                 |           |
|      | CBM00080/SN08                                                                                                                  |           |
|      | CBM00090/SN09                                                                                                                  |           |
|      |                                                                                                                                |           |
| B    | SPFS media for SN09U (3 disks or ESD-delivered ISO files, and additional disk if there is an MNCL)                             |           |
| C    | CBM media for UCBM0010 (1 disk or ESD file)                                                                                    |           |
| D    | Media for CBM backup prior to and after upgrade (box of 10 DVD-RW disks)                                                       |           |
| E    | SPFS patch media (1 disk or ESD file)                                                                                          |           |
| F    | Shipped or created date and version on the SPFS media (item <a href="#">B</a> ). For ESD, use date in ESD confirmation e-mail. |           |
| G    | CBM patch media (1 disk or ESD file)                                                                                           |           |
| H    | Shipped or created date and version on the CBM media (item <a href="#">C</a> ). For ESD, use date in ESD confirmation e-mail.  |           |
| I    | CBM Cluster IP address                                                                                                         |           |
| J    | CBM root password (obtain and memorize, do not write down)                                                                     |           |

**Prereq items**

| Item | Description                                                                                                                                                                                                                          | Checklist |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| K    | CLLI code of Core (on CBM, type 'cli')                                                                                                                                                                                               |           |
| L    | NPM functionality to be on this CBM (yes/no) Refer to the table <a href="#">Network Patch Manager (NPM) decision matrix for CBM on page 754</a> and copy in the appropriate indication, YES or NO.                                   |           |
| M    | Network Patch Manager (NPM) cluster IP; if item <a href="#">L</a> = YES, use item <a href="#">I</a> ; if item <a href="#">L</a> = NO, use the IP address to the SPFS-based machine the NPM resides on                                |           |
| N    | NPM server root password (obtain and memorize, do not write down); if item <a href="#">L</a> = yes, use item <a href="#">J</a> ; if item <a href="#">L</a> = no, use the root password of the SPFS-based machine the NPM resides on. |           |
| O    | Pick and record a password for the soon-to-be-created cbmpat user ID (memorize, do not write down)                                                                                                                                   |           |
| P    | PFRS patch file drop-off server IP address<br><b>Note:</b> This may not exist yet, if item <a href="#">L</a> = NO                                                                                                                    |           |
| Q    | PFRS patch file drop-off server user ID/password<br><b>Note:</b> This may not exist yet, if item <a href="#">L</a> = NO                                                                                                              |           |
| R    | PFRS patch file drop-off keep patches (yes/no)<br><b>Note:</b> This may not exist yet, if item <a href="#">L</a> = NO                                                                                                                |           |
| S    | IP address of, and user ID/password for, the ESD server if using ISO files items <a href="#">B</a> , <a href="#">C</a> , <a href="#">E</a> , or <a href="#">G</a>                                                                    |           |
| T    | Directory path for software loads on ESD server if using ISO files items <a href="#">B</a> , <a href="#">C</a> , <a href="#">E</a> , or <a href="#">G</a>                                                                            |           |
| U    | Internet web browser access to www.nortel.com                                                                                                                                                                                        |           |
| V    | Nortel global ID/password or customer registration on www.nortel.com in Support/Training.                                                                                                                                            |           |
| W    | ftp / sftp file transfer access to CBM and PFRS drop-off server from Windows-based PC                                                                                                                                                |           |
| X    | console or telnet/ssh access to CBM from Windows-based PC                                                                                                                                                                            |           |

**Prereq items**

| Item | Description                                                                                                                                                                                                                                                                                                                                                                          | Checklist |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Y    | email account, Internet reachable from www.nortel.com for access to Patch Audit tool results in Windows-based PC                                                                                                                                                                                                                                                                     |           |
| Z    | CBM 850 consoles for access to the CBM 850 servers during the upgrade. One console is required for each CBM 850 server. Terminals may either be located at the CBM 850 site or they can be connected to terminal servers or modems for remote access. For information about console access, refer to <a href="#">Configuring SPFS console access on page 51</a>                      |           |
| AA   | If item <a href="#">L</a> = NO (NPM server does not reside on the CBM) ssh / ftp / sftp file transfer access from CBM to NPM server                                                                                                                                                                                                                                                  |           |
| AB   | ftp / sftp file transfer access from CBM to ESD server if using ISO files items <a href="#">B</a> , <a href="#">C</a> , <a href="#">E</a> , or <a href="#">G</a>                                                                                                                                                                                                                     |           |
| AC   | <p>NN10363-811, <i>Core and Billing Manager 850 Accounting</i></p> <p>NN10351-911, <i>Core and Billing Manager 850 Fault Management</i></p> <p>NN10353-511, <i>Core and Billing Manager 850 Configuration Management</i></p> <p>NN10408-900, <i>ATM/IP Fault Management</i></p> <p>NN10402-600, <i>ATM/IP Security and Administration</i></p> <p>NN10329-111, <i>IEMS Basics</i></p> |           |
| AD   | When requested in the upgrade, record the PC directory path.                                                                                                                                                                                                                                                                                                                         |           |
| AE   | When requested in the upgrade, record the CBM applications that are in the offline (OFFL) state.                                                                                                                                                                                                                                                                                     |           |

**Prereq items**

| Item  | Description | Checklist |
|-------|-------------|-----------|
| Name: |             |           |
| Date: |             |           |

The following table contains information about the NPM location with relation to the CBM load you are upgrading from.

**Network Patch Manager (NPM) decision matrix for CBM**

| Upgrading to UCBM0010, coming from load: |                             |                             |
|------------------------------------------|-----------------------------|-----------------------------|
| Solution                                 | SN08                        | SN09                        |
| TDM                                      | YES - NPM to reside on CBM  | YES - NPM to reside on CBM  |
| Succession                               | NO - NPM exists, not on CBM | NO - NPM exists, not on CBM |

## Action

### Preparing to upgrade the CBM

#### *On the active CBM 850 node*

- 1 Print out and fill in table [Prereq items on page 751](#) prior to the upgrade. Ensure that you have this filled-in table available for quick reference during the upgrade procedure.

#### *On the inactive CBM 850 node*

- 2 Verify the state of the cluster. For detailed steps, refer to [Verifying the state of a cluster on page 400](#)

#### *On the active CBM 850 node*

- 3 At the command line, enter the following command:

```
appctrl -q all
```

In the display, note which applications are not inservice (INSV) or offline (OFFL). For these applications, either offline or return the application to service using the cbmmtc appl maintenance interface.

- 4 Ensure that no SBA alarms are currently raised.

Check for alarms using procedure “Strategy for clearing a CBM 850 fault condition” in *Core and Billing Manager 850 Fault Management*, NN10351-911.

- 5 Display all CBM software applications that are off-line:

```
appctrl -q all | grep -i offl
```

Record any applications that are offline (OFFL) for use later in the upgrade in procedure in item [AE](#) of the [Prereq items](#) table.

- 6 During the CBM 850 upgrade, the billing application will briefly go into backup. Ensure that adequate backup space per billing stream is available on the core for the duration of the scheduled maintenance window.

To determine the amount of backup disk space required, refer to Disk Space Requirements, in section “Preparing for SBA installation and configuration” in *Core and Billing Manager 850 Accounting*, NN10363-811. To reconfigure backup volumes, refer to the procedure “Configuring SBA backup volumes on the core” in *Core and Billing Manager 850 Accounting*, NN10363-811.

- 7 If you are using ESD for the CBM media (see item [C](#) in the [Prereq items](#) table), ensure that the UCBM iso.gz.tape image is



located in the /swd/sdm directory, on the ACTIVE node of the CBM 850 cluster.

If the file has not been placed in that directory (see items [S](#), [I](#), and [AB](#) in the [Prereq items](#) table), perform the procedure [Uncompressing and transferring an ISO image to a CBM server on page 781](#)

- 8 Ensure that SPFS is at the latest maintenance release (MNCL) level for the release you are currently running. Contact your system administrator if necessary. For detailed steps to view the SPFS release on the server, refer to the procedure [Determining the SPFS software MNCL level on page 424](#)
- 9 Use the following table to determine your next step:

| If                                                                                                                       | Perform                 |
|--------------------------------------------------------------------------------------------------------------------------|-------------------------|
| the load you are upgrading from is CBM00090 (see item <a href="#">A</a> in the <a href="#">Prereq items</a> table)       | step <a href="#">43</a> |
| the load you are upgrading from is any other load (see item <a href="#">A</a> in the <a href="#">Prereq items</a> table) | step <a href="#">10</a> |

- 10 Ensure that the running CBM load is patch-current. Perform [Ensuring the SN08 CBM load is patch-current for upgrades on page 796](#)

**Attention:** You must perform this step. If the CBM is not patch-current, your upgrade will fail.

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

| If                                                                                                                            | Do                      |
|-------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| NPM functionality is, or is to be, on this CBM (item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table)       | step <a href="#">12</a> |
| NPM functionality is not, or is not to be on this CBM (item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table) | step <a href="#">16</a> |

- 12 There are two sets of patches to obtain and copy to the CBM/NPM in advance of the upgrade. These patches are supplied on disk or in an ESD file (see item [E](#) of the [Prereq items](#) table). One set of patches is for the SPFS platform and the other set is for the CBM. The two sets consist of released patches from

the interval between the SPFS and CBM NCL media being frozen and the date your upgrade media was ordered and created.

The following steps enable you to obtain SPFS patches for the new load in advance of the upgrade. Use the following table to determine your next step

| If you                                                                                                   | Do                      |
|----------------------------------------------------------------------------------------------------------|-------------------------|
| received patches in an ISO image file (item <a href="#">E</a> in the <a href="#">Prereq items</a> table) | step <a href="#">13</a> |
| received patches on a disk (item <a href="#">E</a> in the <a href="#">Prereq items</a> table)            | step <a href="#">15</a> |
| did not receive any SPFS patches                                                                         | step <a href="#">37</a> |

- 13** Obtain SPFS patches prior to the upgrade.  
For detailed steps, refer to procedure [Obtaining patch files from ISO before a CBM upgrade on page 816](#)
- 14** Go to [step 37](#).
- 15** Transfer patches from the disk to the CBM.  
For detailed steps, refer to procedure [Obtaining patch files from CD before a CBM upgrade on page 814](#)  
Go to step [37](#)

- 16** There are two sets of patches to obtain and copy to the CBM/NPM in advance of the upgrade. These patches are supplied on disk or in an ESD file (see item [E](#) of the [Prereq items](#) table). One set of patches is for the SPFS platform and the other set is for the CBM. The two sets consist of released patches from the interval between the SPFS and CBM NCL media being frozen and the date your upgrade media was ordered and created.

The following steps enable you to obtain SPFS patches for the new load in advance of the upgrade. Use the following table to determine your next step.

| If you                                                                                                                                                                               | Do                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| received patches in an ISO image file (item <a href="#">E</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table | step <a href="#">17</a> |
| received patches in an ISO image file (item <a href="#">E</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table  | step <a href="#">19</a> |
| received patches on a disk (item <a href="#">E</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table            | step <a href="#">23</a> |
| received patches on a disk (item <a href="#">E</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table             | step <a href="#">25</a> |
| you did not receive any SPFS patches                                                                                                                                                 | step <a href="#">26</a> |

- 17** On the CBM on which the NPM resides, transfer and mount the patch ISO image on the server.  
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 18** Go to step [20](#)

- 19 On the SPFS server on which the NPM resides (see item [M](#) in the [Prereq items](#) table), transfer and mount the patch ISO image on the server.  
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 20 Transfer the patches from the ISO image file to the NPM database.  
For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).
- 21 Unmount and remove the patch ISO image from the server.  
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 22 Go to [step 26](#).
- 23 On the CBM on which the NPM resides, transfer the patches from the disk to the NPM database.  
For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).
- 24 Go to [step 26](#).
- 25 On the SPFS server on which the NPM resides (see item [M](#) in the [Prereq items](#) table), transfer the patches from the disk to the NPM database.  
For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).
- 26 The following steps enable you to obtain CBM patches for the new load in advance of the upgrade. Use the following table to determine your next step.

| If you                                                                                                                                                                               | Do                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| received patches in an ISO image file (item <a href="#">G</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table | step <a href="#">27</a> |
| received patches in an ISO image file (item <a href="#">G</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table  | step <a href="#">29</a> |

| If you                                                                                                                                                                    | Do                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| received patches on a disk (item <a href="#">G</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table | step <a href="#">33</a> |
| received patches on a disk (item <a href="#">G</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table  | step <a href="#">35</a> |
| did not receive any CBM patches                                                                                                                                           | step <a href="#">41</a> |

- 27 On the CBM on which the NPM resides, transfer and mount the patch ISO image on the server.  
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 28 Go to step [30](#)
- 29 On the SPFS server on which the NPM resides, transfer and mount the patch ISO image on the server.  
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 30 Transfer the patches from the ISO image file to the NPM database.  
For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).
- 31 Unmount and remove the patch ISO image from the server.  
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 32 Go to [step 41](#).
- 33 On the CBM on which the NPM resides, transfer the patches from the disk to the NPM database.  
For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).
- 34 Go to step [41](#)
- 35 On the SPFS server on which the NPM resides (see item [M](#) in the [Prereq items](#) table), transfer the patches from the disk to the NPM database.

For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).

- 36** Go to step [41](#)
- 37** The following steps enable you to obtain CBM patches for the new load in advance of the upgrade. Use the following table to determine your next step

| If you                                                                                                   | Do                      |
|----------------------------------------------------------------------------------------------------------|-------------------------|
| received patches in an ISO image file (item <a href="#">G</a> in the <a href="#">Prereq items</a> table) | step <a href="#">38</a> |
| received patches on a disk (item <a href="#">G</a> in the <a href="#">Prereq items</a> table)            | step <a href="#">40</a> |
| did not receive any CBM patches                                                                          | step <a href="#">41</a> |

- 38** Obtain patches for the CBM prior to the upgrade.  
For detailed steps, refer to procedure [Obtaining patch files from ISO before a CBM upgrade on page 816](#)
- 39** Go to [step 41](#).
- 40** Transfer patches from the disk to the CBM.  
For detailed steps, refer to procedure [Obtaining patch files from CD before a CBM upgrade on page 814](#)
- 41** CBM and SPFS patches for the new load may have been released since your upgrade media was created. You must obtain the patches for this interval prior to the upgrade. Refer to [Obtaining pre-upgrade patches released after upgrade media shipped on page 818](#)
- 42** Perform a full system backup on the current load.  
For detailed steps, refer to [Performing a backup of file systems on an SPFS-based server on page 379](#)  
Go to step [66](#)
- 43** Ensure that the running CBM load is patch-current. Perform [Using Patch Audit to ensure CBM SN09 and higher loads are patch-current on page 804](#)  
**Attention:** You must perform this step. If the CBM is not patch-current, your upgrade will fail.

- 44** There are two sets of patches to obtain and copy to the CBM/NPM in advance of the upgrade. These patches are supplied on disk or in an ESD file (see item [E](#) of the [Prereq items](#) table). One set of patches is for the SPFS platform and the other set is for the CBM. The two sets consist of released patches from the interval between the SPFS and CBM NCL media being frozen and the date your upgrade media was ordered and created.

The following steps enable you to obtain SPFS patches for the new load in advance of the upgrade. Use the following table to determine your next step.

| If you                                                                                                                                                                               | Do                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| received patches in an ISO image file (item <a href="#">E</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table | step <a href="#">45</a> |
| received patches in an ISO image file (item <a href="#">E</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table  | step <a href="#">47</a> |
| received patches on a disk (item <a href="#">E</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table            | step <a href="#">51</a> |
| received patches on a disk (item <a href="#">E</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table             | step <a href="#">53</a> |
| you did not receive any SPFS patches                                                                                                                                                 | step <a href="#">54</a> |

- 45** On the CBM on which the NPM resides, transfer and mount the SPFS patch ISO image on the server.  
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 46** Go to step [48](#)

- 47** On the SPFS server on which the NPM resides (see item [M](#) in the [Prereq items](#) table), transfer and mount the SPFS patch ISO image on the server.
- For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 48** Transfer the patches from the ISO image file to the NPM database.
- For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).
- 49** Unmount and remove the patch ISO image from the server.
- For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 50** Go to [step 54](#).
- 51** On the CBM on which the NPM resides, transfer the patches from the disk to the NPM database.
- For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).
- 52** Go to [step 54](#).
- 53** On the SPFS server on which the NPM resides (see item [M](#) in the [Prereq items](#) table), transfer the patches from the disk to the NPM database.
- For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).
- 54** The following steps enable you to obtain CBM patches for the new load in advance of the upgrade. Use the following table to determine your next step.

| If you                                                                                                                                                                               | Do                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| received patches in an ISO image file (item <a href="#">G</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table | step <a href="#">55</a> |
| received patches in an ISO image file (item <a href="#">G</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table  | step <a href="#">57</a> |



| If you                                                                                                                                                                    | Do                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| received patches on a disk (item <a href="#">G</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table | step <a href="#">61</a> |
| received patches on a disk (item <a href="#">G</a> in the <a href="#">Prereq items</a> table), and item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table  | step <a href="#">63</a> |
| did not receive any CBM patches                                                                                                                                           | step <a href="#">64</a> |

- 55** On the CBM on which the NPM resides, transfer and mount the CBM patch ISO image on the server.  
For detailed steps, refer to procedure [Transferring an ISO image to an SPFS-based server on page 430](#).
- 56** Go to step [58](#)
- 57** On the SPFS server on which the NPM resides, transfer and mount the CBM patch ISO image on the server.  
For detailed steps, refer to procedure [Transferring an ISO image to an SPFS-based server on page 430](#).
- 58** Transfer the patches from the ISO image file to the NPM database.  
For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).
- 59** Unmount and remove the patch ISO image from the server.  
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 60** Go to [step 64](#).
- 61** On the CBM on which the NPM resides, transfer the patches from the disk to the NPM database.  
For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).
- 62** Go to step [64](#)
- 63** On the SPFS server on which the NPM resides, transfer the patches from the disk to the NPM database.  
For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).

- 64** CBM and SPFS patches for the new load may have been released since your upgrade media was created. You must obtain the patches for this interval prior to the upgrade. Refer to [Obtaining pre-upgrade patches released after upgrade media shipped on page 818](#)
- 65** Perform a full system backup on the current load.  
For detailed steps, refer to [Performing a backup of file systems on an SPFS-based server on page 379](#)
- 66** Use the following table to determine your next step.

| If                                                                                                                                                                                                                               | Perform                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| the load you are upgrading from is CBM00090 (see item <a href="#">A</a> in the <a href="#">Prereq items</a> table) and NPM functionality is on this CBM (item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table) | step <a href="#">67</a> |
| otherwise                                                                                                                                                                                                                        | step <a href="#">69</a> |

- 67** Save the NPM user-defined data.  
For detailed steps, refer to procedure [Archiving the NPM database into a file on page 383](#)
- 68** Save the NPM patch files.  
For detailed steps, refer to procedure [Saving the NPM patch and database files on page 385](#)
- 69** This procedure is complete. Return to [CBM upgrade tasks on page 750](#)

---

## Upgrading the CBM

---

Upgrading the CBM 850 involves upgrading both the SPFS platform and software and upgrading the CBM 850 software. The SPFS upgrade consists of two stages:

- upgrading the Solaris operating system
- upgrading the SPFS software

The CBM upgrade consists of three stages:

- preparing the CBM upgrade media
- CBM profile and optional package selection
- applying and patching the new CBM software

The CBM upgrade is automatically initiated during the SPFS upgrade. The inactive CBM 850 node is first upgraded with the new load. Then a manual swact occurs that makes the upgraded CBM 850 node active. Finally, a manual clone occurs that synchronizes the new software for both CBM 850 nodes. The out-of-service time for the CBM 850 cluster is limited to the duration of the CBM 850 manual swact.

If errors are encountered during the CBM 850 upgrade, you have the choice of accessing a maintenance shell command line prompt or performing a fallback to the previous release. The maintenance shell provides the ability to correct the issue causing the error. Upon exiting the maintenance shell, the operation that failed will be re-executed. A fallback causes the unit being upgraded to be at the ok prompt, either automatically or manually (as indicated in the various fallback scenarios). A clone is required to return both nodes to the previous SPFS and CBM 850 release.

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

**Important:** During the upgrade prior to the reboot of the node being upgraded, both CBM 850 nodes are running the current (old) software load. Thus, if a problem occurs on the active node running the previous release, CBM application functionality will be maintained when the inactive node becomes active. If this occurs, you will need to defer the upgrade until that unit has recovered, or an outage will occur when the node being upgraded reboots.

## Prerequisites

You have completed [Preparing to upgrade the CBM on page 751](#)

## Action

### Upgrading the CBM

#### *At the inactive node*

- 1 Start the SPFS platform and software upgrade. For detailed steps, refer to procedure [Upgrading SPFS software on page 403](#)
- 2 Select the CBM 850 upgrade media. For detailed steps, refer to procedure [Selecting the CBM upgrade media on page 786](#)
- 3 Confirm the CBM media upgrade selection. For detailed steps, refer to procedure [Confirming the CBM upgrade media selection on page 788](#)
- 4 Press the Enter key to acknowledge the attention message that displays about the /opt/cbm\_post\_upgrade script that must be run. This script executes additional post-upgrade scripts and installs new optional software packages.
- 5 Observe a series of checks to ensure that the image is a valid CBM ISO and that adequate disk space exists. For an ESD upgrade, an additional message about Media Preparation will display.

The cbm\_setup program checks:

- to verify SPFS boot environment
- to verify remote node communication
- for any Major or Critical alarms on either node and notifies you with information about any alarms that have been found
- to verify disk space

**Note:** It is recommended that you enter a maintenance shell if problems are encountered during these checks. When you enter a maintenance shell, a maintenance shell prompt displays. You can then enter commands to perform a maintenance action. To exit from the maintenance shell after you have completed the maintenance action, you then enter exit. The system will then repeat the last action it performed before you opened the maintenance shell.

- 6 The CBM program examines the upgrade environment and prepares the system for the CBM upgrade. You may be prompted to select the appropriate UCBM profile for your CBM.

For instruction on how to respond to this prompt, refer to procedure [Selecting the CBM upgrade profile on page 790](#)

- 7 The upgrade program automatically selects required and non-required (optional) CBM packages to apply, based on the CBM profile you have selected. You may be prompted to select for application any optional CBM packages that are not currently applied. For instruction on how to respond to this prompt, refer to procedure [Selecting the CBM packages on page 793](#)

**Note:** Required packages for your CBM profile that are not on the previous load, and any optional packages selected above, will be applied automatically in the `cbm_post_upgrade` script.

- 8 Observe the following actions performed by the upgrade program:
- application of any optional CBM packages and application of any patches that were present on the CBM media
  - tasks such as preserving logs, preparing data formatting, removing the old release from the upgrade environment, creating load base line information, and checking the system for alarms

When the CBM upgrade is complete, the final phase of the SPFS program resumes. The final phase prepares and performs the first of two system-initiated reboots on the inactive node, while the active node continues to provide service on the previous software load.

**Note:** If you are using SPFS and CBM media disks for the upgrade, you are prompted to reinsert SPFS upgrade disk 3 into the DVD drive. After inserting the disk, enter:

**ok**

The disk will not start until the `ok` command is entered.

During the final phase, the following sequence of activities are observed at the inactive console:

- An activation of the new boot environment occurs.
- A message may display about how to manually reset the boot device in the event the pending reboot fails.
- Two reboots occur automatically.

**Note 1:** Following the CCPU package installation but prior to the reboots that occur automatically, `ubmgr_init` logs may appear on the inactive console. These can be ignored.

**Note 2:** The first reboot takes considerably longer than a normal node reboot.

- 9 Verify that the upgrade of the CBM 850 inactive node has been successful up to this point. Perform [Performing an inactive CBM 850 upgrade post-reboot sanity check on page 828](#)
- 10 Use the following table to determine your next step:

| If                                      | Do                      |
|-----------------------------------------|-------------------------|
| you want to complete the upgrade        | step <a href="#">12</a> |
| you do not want to complete the upgrade | step <a href="#">11</a> |

- 11 To fallback to the state prior to the upgrade, refer to procedure [Executing a fallback during an SPFS-based server upgrade on page 418](#).
- 12 This procedure is complete. Return to [CBM upgrade tasks on page 750](#).

## Completing the CBM upgrade

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

You have completed [Upgrading the CBM on page 766](#)

You have completed [Preparing to upgrade the CBM on page 751](#)

### Action

#### Completing the CBM upgrade

##### *At the inactive node*

- 1 Install any SPFS MNCLs for the new load (see item [B](#) in the [Prereq items](#) table). An MNCL can be either a CD or an ISO file.

Refer to the instructions provided with the MNCL to install any SPFS MNCL. Perform this activity only if you received a notification bulletin that an SPFS MNCL is available for the new software release.

- 2 Determine whether the Patching Server Element (PSE) is configured on the CBM:

```
/opt/NTpse/pse status
```

Use the following table to determine your next step:

| If                          | Do                      |
|-----------------------------|-------------------------|
| PSE has not been configured | step <a href="#">3</a>  |
| PSE is not running          | step <a href="#">11</a> |
| PSE is running              | step <a href="#">12</a> |

- 3 Access the command line interface:  

```
cli
```
- 4 Enter the number next to the Configuration option in the menu.
- 5 Enter the number next to the Succession Element Configuration option in the menu.

- 6 Enter the number next to the PSE Application Configuration option in the menu.
- 7 Enter the number next to the Configure\_PSE (Configure the Patching Server Element) option in the menu.
- 8 Enter the NPM IP address (see item [M](#) in the [Prereq items](#) table).
- 9 If the IP address is acceptable, enter y.
- 10 When prompted, enter x to exit each level until you exit the command line interface.
- 11 Start the PSE:  
**pse start**
- 12 Use the following table to determine your next step.

| If                                                                                                     | Do                      |
|--------------------------------------------------------------------------------------------------------|-------------------------|
| item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table (NPM to reside on the CBM)      | step <a href="#">13</a> |
| item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table (NPM will not reside on the CBM) | step <a href="#">15</a> |

- 13 Patch the inactive node by typing  
**patchUpToDate -directory /data/npm\_patches**  
In response to the system prompt, confirm the list of devices that can be patched.  
If you are prompted for a system reboot, answer YES and perform the reboot now.
- 14 Go to step [24](#)
- 15 Log in as root to the NPM cluster IP address:  
**ssh -l root <NPM cluster IP address>**  
where  
**<NPM cluster IP address>**  
is the NPM cluster IP address in item [M](#) in the [Prereq items](#) table.
- 16 Connect to the NPM CLUI. Enter the following command:  
**npm**  
Log in to the NPM CLUI using the user ID and password (see item [O](#) in the [Prereq items](#) table).



- 17** The NPM device list will not be valid until a device audit completes.

Enter the following command to determine whether the device audit has completed:

**rr devicelist**

Examine the list of devices that is displayed and use the following table to determine your next step.

| If                                                                       | Do                      |
|--------------------------------------------------------------------------|-------------------------|
| no devices are shown, or any devices are shown with an UNKNOWN label     | step <a href="#">18</a> |
| For example,<br><br>CBM_ACE_had3-unit1,UNKNOWN,FALSE,TRUE,PSE_had3-unit1 |                         |
| no devices are shown with an UNKNOWN label                               | step <a href="#">20</a> |

- 18** Enter the following command to start the audit now:

**rt audit**

- 19** Enter the following command to determine whether the device audit has completed:

**rr devicelist**

If after re-running the command several times any devices are shown with an UNKNOWN label, contact your next level of support.

- 20** Apply the patches, using NPM. The amount of time required to apply the patches is dependent upon the number of patches to be applied.

**apply set emg\_not\_app set gen\_not\_app**

Read and follow special application instructions for any patches that require special handling.

- 21** Determine whether a restart of any devices is required in order to enable any of the patches. Enter the following command:

**q restartlist**

**Example system response:**

NPM\_wcarsx0h-unit0,NPf80O91,A,FALSE,2006-03-20  
22:37:04.000

PSE\_wcarsx0h-unit1,PF610O91,A,FALSE,2006-03-20  
23:16:20.000

SSPFS\_wcarsx0h-unit0,LAX77121,A,FALSE,2006-03-21  
01:30:11.000

Devices listed in the system response must be restarted.

**Note:** A restart is not required on the SSPFS device.

Enter the following command for each device, except the SSPFS device:

**restart set devicestorestart**

- 22 Exit from the NPM CLUI:

**quit**

- 23 Log off of the NPM server.

**At the Active node**

- 24 Refer to item [AE](#) in the [Prereq items](#) table. Use the following table to determine your next step.

| If                  | Do                      |
|---------------------|-------------------------|
| SBA is not off-line | step <a href="#">25</a> |
| SBA is off-line     | step <a href="#">26</a> |

- 25 Deliver any unprocessed billing files to the downstream destination. No more than one unprocessed billing file should remain on the system.

On the active node of the CBM 850 cluster, close any billing files that are to be sent downstream using procedure “Closing billing files” in *Core and Billing Manager 850 Accounting*, NN10363-811. Send the billing files downstream by performing procedure “Sending billing files from disk” in *Core and Billing Manager 850 Accounting*, NN10363-811.

**Important:** If you are unable to send billing files to a downstream destination, Nortel recommends that you back up the billing files to a writable DVD, using procedure “Copying billing files to DVD using SBADVWRITE” in *Core and Billing Manager 850 Accounting*, NN10363-811.

- 26** Enter the following command to determine whether all filesystems are in a ACTIVE normal UP clean (active) state:

**udstat**

If the response to this command indicates that the filesystems do not appear to be in normal UP clean (active) state, contact your next level of support.

- 27** Ensure that no system alarms are currently raised:

**querycbm flt**

Check for alarms using procedure “Strategy for clearing a CBM 850 fault condition” in *Core and Billing Manager 850 Fault Management*, NN10351-911

Troubleshoot any alarms that are raised before continuing with this procedure.

- 28** Force a cluster activity change to bring up services on the upgraded node. This will make the upgraded node the active node. Enter the following command on the active node:

**init 6**

When the cluster activity change completes, continue with the next step.

- 29** Determine whether both the SPFS and CBM upgrades are successful up to this point. For detailed steps, refer to procedure [Performing an active CBM 850 upgrade sanity check on page 830](#)

#### ***At the new Active node***

- 30** Ensure that no SBA alarms are currently raised.

Check for alarms using procedure “Strategy for clearing a CBM 850 fault condition” in *Core and Billing Manager 850 Fault Management*, NN10351-911

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

| if                                                                                                | Do                      |
|---------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">L</a> = NO (NPM will not reside on the CBM) in the <a href="#">Prereq items</a> table | step <a href="#">49</a> |

| if                                                                                                                                                                      | Do                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">L</a> = YES (NPM to reside on the CBM) in the <a href="#">Prereq items</a> table and <a href="#">A</a> = CBM00080 in the <a href="#">Prereq items</a> table | step <a href="#">32</a> |
| <a href="#">L</a> = YES (NPM to reside on the CBM) and <a href="#">A</a> = CBM00090 in the <a href="#">Prereq items</a> table                                           | step <a href="#">41</a> |

- 32 Configure the NPM. Access the command line interface:  
**cli**
- 33 Enter the number next to the Configuration option in the menu.
- 34 Enter the number next to the Succession Element Configuration option in the menu.
- 35 Enter the number next to the NPM Application Configuration option in the menu.
- 36 Enter the number next to the ConfigureNpm (Configure the Network Patch Manager) option in the menu.
- 37 If you are ready to proceed with NPM application configuration, enter y.
- 38 When prompted, enter x to exit each level until you exit the command line interface.
- 39 Start the NPM:  
**servstart NPM**
- 40 Create a patchlist file using the following command. The command is entered on a single line; there is a space between \*.\* and > and between > and /data.  
**ls /data/npm\_patches/\*. \* > /data/npm\_patches/current.patchlist**
- 41 Connect to the NPM CLUI. Enter the following command:  
**npm**  
Log in to the NPM CLUI using the user ID and password (see item [Q](#) in the [Prereq items](#) table).
- 42 Retrieve the patch files for the NPM to process using the following command.  
**getpatch /data/npm\_patches/current.patchlist**

- 43** The NPM device list will not be valid until a device audit completes.

Enter the following command to determine whether the device audit has completed:

**rr devicelist**

Examine the list of devices that is displayed and use the following table to determine your next step.

| If                                                                       | Do                      |
|--------------------------------------------------------------------------|-------------------------|
| no devices are shown, or any devices are shown with an UNKNOWN label     | step <a href="#">44</a> |
| For example,<br><br>CBM_ACE_had3-unit1,UNKNOWN,FALSE,TRUE,PSE_had3-unit1 |                         |
| no devices are shown with an UNKNOWN label                               | step <a href="#">46</a> |

- 44** Enter the following command to start the audit now:

**rt audit**

- 45** Enter the following command to determine whether the device audit has completed:

**rr devicelist**

If after re-running the command several times any devices are shown with an UNKNOWN label, contact your next level of support.

- 46** Apply the patches, using NPM.

**apply set emg\_not\_app set gen\_not\_app**

Read and follow special application instructions for any patches that require special handling.

- 47** Determine whether a restart of any devices is required in order to enable any of the patches. Enter the following command:

**q restartlist**

**Example system response:**

NPM\_wcarsx0h-unit0,NPf80O91,A,FALSE,2006-03-20  
22:37:04.000

PSE\_wcarsx0h-unit1,PF610O91,A,FALSE,2006-03-20  
23:16:20.000

SSPFS\_wcarsx0h-unit0,LAX77121,A,FALSE,2006-03-21  
01:30:11.000

Devices listed in the system response must be restarted.

**Note:** A restart is not required on the SSPFS device.

Enter the following command for each device, except the SSPFS device:

**restart set devicestorestart**

**48** Exit from the NPM CLUI:

**quit**

**49** Use the following table to determine your next step.

| If                                                                               | Do                      |
|----------------------------------------------------------------------------------|-------------------------|
| you want to accept the new environment permanently                               | step <a href="#">52</a> |
| you want to fallback to the state prior to the upgrade and lose all upgrade work | step <a href="#">50</a> |

**50** To fallback to the state prior to the upgrade, refer to procedure [Executing a fallback during an SPFS-based server upgrade on page 418](#).

**51** Go to step [68](#).

#### ***At the previously-active node***

**52** Enter the following command at the console of the inactive node (running the previous load):

**init 0**

#### ***At the newly-active node***

**53** When the ok prompt appears on the inactive node, enter the following command on the active node:

**/SSPFS\_Upgrade.accept**

**Note:** It may take several minutes before the prompt appears. Wait until the prompt appears before continuing.

**54** For a successful upgrade after you have accepted the SPFS upgrade in step [53](#), you must manually execute the /opt/cbm\_post\_upgrade script. This script executes additional post-upgrade sub-scripts and installs new optional packages

selected earlier during the upgrade. Enter the following command to execute this script:

**/opt/cbm\_post\_upgrade**

- 55 To ensure that any new packages that were applied are patch-current, perform [Using Patch Audit to ensure CBM SN09 and higher loads are patch-current on page 804](#)
- 56 Use the following table to determine your next step.

| If                                                                                                     | Do                      |
|--------------------------------------------------------------------------------------------------------|-------------------------|
| item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table (NPM to reside on the CBM)      | step <a href="#">57</a> |
| item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table (NPM will not reside on the CBM) | step <a href="#">58</a> |

- 57 Perform [Configuring NPM for automatic patch file delivery on page 493](#)
- 58 Use the following table to determine your next step.

| If                                 | Do                      |
|------------------------------------|-------------------------|
| you have an IEMS provisioned       | step <a href="#">59</a> |
| you don't have an IEMS provisioned | step <a href="#">64</a> |

### ***At the IEMS***

- 59 The NPM should reside on the IEMS. Log in as root to the IEMS using the NPM cluster IP address:

**ssh -l root <NPM cluster IP address>**

where

**<NPM cluster IP address>**

is the NPM cluster IP address in item [M](#) in the [Prereq items](#) table.

**60****ATTENTION**

A degradation in the performance of IEMS results and duplicate logs are generated if both the CBM 850 and Core Element Manager (CEM) have been added to the IEMS. Only the CBM 850 or only the CEM should be used to manage devices.

Determine whether the CBM 850 or CEM have been added to the IEMS.

- a Launch the IEMS Java Web Start Client (refer to “Launching IEMS Java Web Start Client” in *IEMS Basics*, NN10329-111).
- b Select the Element Managers topology panel in the IEMS Topologies tree.
- c In the list of element managers that displays, determine whether the CBM 850 or the CEM is present.

**61** Use the following table to determine your next step.

| If                                                        | Do                      |
|-----------------------------------------------------------|-------------------------|
| the CBM 850 has been added to the IEMS                    | step <a href="#">62</a> |
| the CEM has been added to the IEMS as the element manager | step <a href="#">63</a> |

**62** Edit the object properties in the IEMS for the CBM 850 you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version to be “SN09FF” in the Device Version field.

- [Editing and viewing object properties using Web Client on page 2261](#)
- [Editing and viewing object properties using Java Web Start Client on page 2255](#)

**63** Exit from the IEMS Java Web Start Client.

**At the newly-active node**

**64** To remove fix and patch files that are no longer needed, perform the following steps:

```
cd /swd/fixes/incoming
```



```
pwd
rm -rf *
cd /export/home/cbmpat
pwd
ls
```

From the listing shown in response to the preceding ls command, determine any patch-related files from the upgrade to be removed. Then, use the following command to remove each of these upgrade patch-related files:

```
rm <patch-related file from upgrade>
ls
```

From the listing shown in response to the preceding ls command, confirm that all patch-related files from the upgrade have been removed.

```
cd
```

- 65 Synchronize the new software for both CBM 850 nodes. Perform the procedure [Cloning the image of one server in a cluster to the other server on page 478](#).
- 66 Perform a full system backup on the new load.  
For detailed steps, refer to procedure [Performing a backup of file systems on an SPFS-based server on page 379](#)
- 67 If this is a geographically-redundant configuration, upgrade the standby CBM 850 server. Refer to procedures “Installing the remote backup server” and “Scheduling automatic backups on the remote server”, in *Carrier Voice over IP, Disaster Recovery Procedures*, NN10450-900.
- 68 You have completed this procedure. Return to [CBM upgrade tasks on page 750](#)

---

## Uncompressing and transferring an ISO image to a CBM server

---

### Application

Use this procedure to uncompress and transfer an ISO image file from the Electronic Software Delivery (ESD) load repository server to a Core and Billing Manager (CBM) server.

The CBM is a boot server for some products. Use this procedure only for CBM loads. Do not use this procedure for non-CBM loads that may reside on the CBM server.

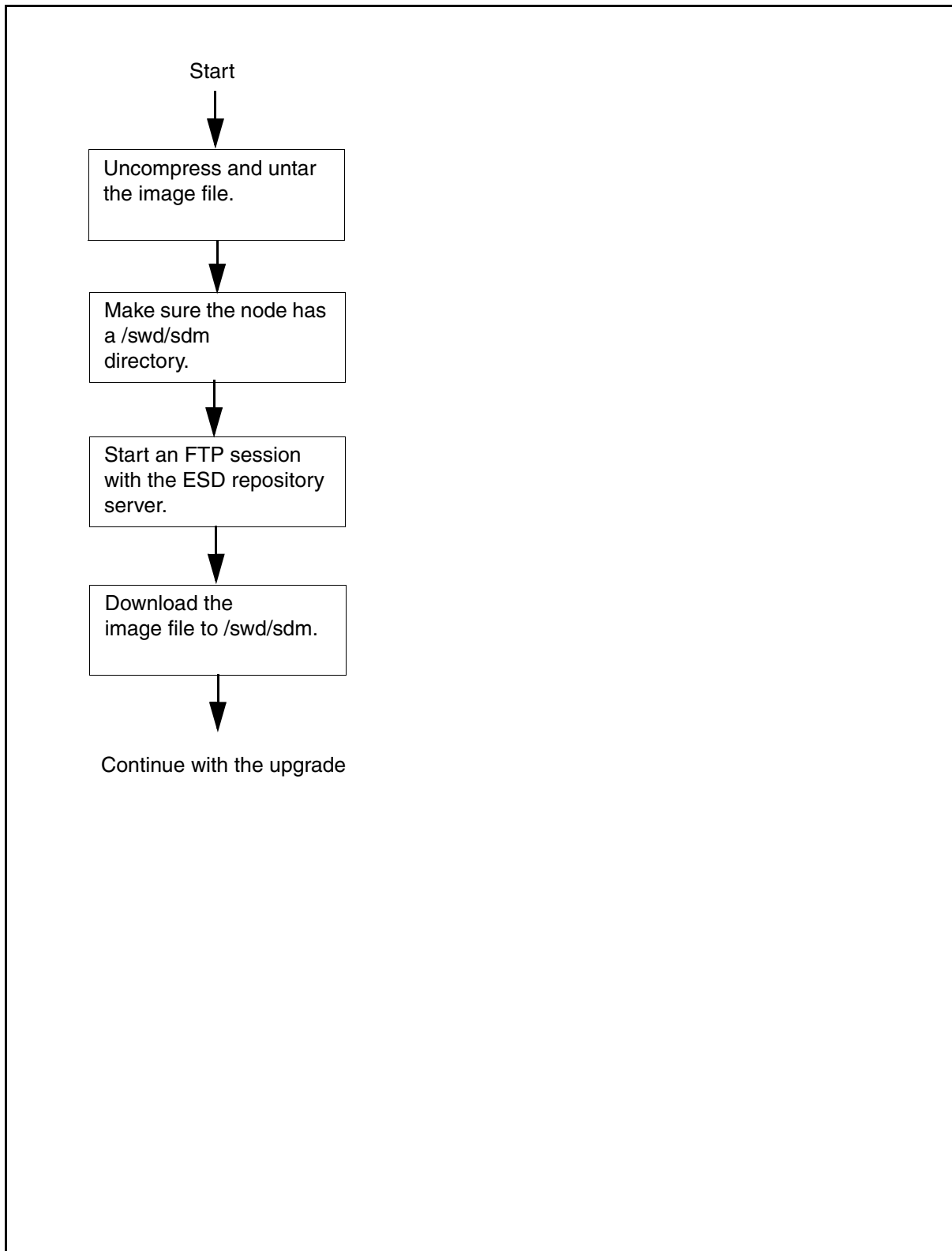
### Prerequisites

This procedure has the following prerequisites:

- You must know the name or IP address of the load repository server and the location of the dropbox directory on the server.
- You must know the user ID and password for the load repository server
- You must know the name or IP address of the CBM server.
- You must know the root password for the CBM server.

### Action

Use the flowchart as an overview of the tasks required to complete this procedure. Use the step-by-step instructions to complete the procedure.

**Overview of steps to uncompress and transfer an ISO image to a CBM server**

## Uncompressing and transferring an ISO image to a CBM server

### *At the ESD load repository server*

- 1 Log in to the ESD load repository server, and change directory to the drop box location.

**Note:** Ensure you log in with a user ID that has permission to uncompress files.

- 2 List the contents of the drop box:

```
ls *.gz
```

- 3 Locate the file you want to uncompress.

- 4 Uncompress the file:

```
gzip -d <esd_filename>.tar.gz
```

where

**esd\_filename**

is the name of the ESD software load, for example:

UCBM0010.10.LAB.NCL.NAP.VAULT.2.D

- 5 List the uncompressed file:

```
ls *.tar
```

- 6 Unpack the file:

```
tar -xvf <esd_filename>.tar
```

where

**esd\_filename**

is the name of the ESD software load, for example:

UCBM0010.10.LAB.NCL.NAP.VAULT.2.D

The unpacked file is a directory that contains the UCBM installation software.

- 7 Log out of the ESD load repository server.

### *At your workstation*

- 8 Log in as root to the active CBM server.

**Note:** The CBM server supports a variety of secure and non-secure login options. Follow office policy or check the user documentation for your release.

- 9 Change to the software delivery directory:

```
cd /swd
```

- 10 Determine whether the sdm directory exists:

```
ls -d sdm
```

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

| If the response is        | Do                      |
|---------------------------|-------------------------|
| No such file or directory | <a href="#">step 12</a> |
| sdm                       | <a href="#">step 13</a> |

- 12 Create the directory:

```
mkdir sdm
```

- 13 Change to the sdm directory:

```
cd sdm
```

- 14 Start an FTP session with the ESD repository server:

```
ftp <ESD_repository_server_ip>
```

where

**<ESD\_repository\_server\_ip>**

is the machine owned by the operating company that was selected to be the destination for ESD software.

When prompted, enter the user ID and the password.

- 15 List the directories on the ESD repository server:

```
ls
```

- 16 Change directory to the drop box directory:

```
cd <dropbox_directory>
```

where

**<dropbox\_directory>**

is the name of the your dropbox directory.

- 17 List the contents of the drop box:

```
ls -l
```

- 18 Change the transfer mode to binary:

```
bin
```

- 19 Transfer the ESD software load to the CBM server:

```
get <iso_image>
```

where

**<iso\_image>**

is the full name of the image file

- 20 End the FTP session:  
**bye**
- 21 Make sure the files successfully transferred to the CBM server.  
List the files in /swd/sdm:  
**ls -l /swd/sdm**
- 22 You have completed this procedure. Return to the step in [Preparing to upgrade the CBM](#) that sent you to this procedure.

## Selecting the CBM upgrade media

### Selecting the CBM upgrade media

#### *At your workstation*

- 1 The CBM 850 upgrade process is automatically initiated during the SPFS upgrade process. When the program running the CBM 850 upgrade starts you are presented with a list of software delivery options. Review the available options and use the following table to determine your next step.

In response to the prompt you may:

- enter **esd** to start the upgrade if electronic software delivery is being used for this upgrade
- enter **disc** to start the upgrade if cdrom is being used for this upgrade
- enter **shell** to suspend the upgrade and enter a Maintenance shell before continuing the upgrade
- enter **fallback** to cancel the entire upgrade procedure

| If in response to the system prompt | Action                                                                                                   |
|-------------------------------------|----------------------------------------------------------------------------------------------------------|
| you entered esd                     | Return to step <a href="#">3</a> in <a href="#">Upgrading the CBM</a> .                                  |
| you entered disc                    | Return to step <a href="#">3</a> in <a href="#">Upgrading the CBM</a> .                                  |
| you entered shell                   | See step <a href="#">2</a> for a description of the system response and the next action you can perform. |
| you entered fallback                | See step <a href="#">3</a> for a description of the system response and the next action you can perform. |

- 2 The following table shows the system responses and possible actions you can perform when you enter a maintenance shell.

| If in response to the system prompt to proceed with the shell, System response |                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you entered yes                                                                | A maintenance shell prompt displays. You can now enter commands to perform a maintenance action.<br><br>When you are done, enter exit. After entering the exit command, the system will repeat the last action it performed before you opened the maintenance shell. |
| you entered no                                                                 | When you enter no, the system will repeat the last action it performed before you opened the maintenance shell.                                                                                                                                                      |

- 3 The following table shows the system responses and possible actions you can perform when you enter fallback.

| If in response to the system prompt to proceed with the fallback, System response |                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you entered yes                                                                   | The CBM 850 upgrade is cancelled and the node is brought to an ok prompt. Perform procedure <a href="#">Executing a fallback during an SPFS-based server upgrade on page 418</a> |
| you entered no                                                                    | When you enter no, the system will repeat the last action it performed before you selected to fallback.                                                                          |

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



## Confirming the CBM upgrade media selection

### Confirming the upgrade media selection

#### *At your workstation*

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

| If                                       | Do                     |
|------------------------------------------|------------------------|
| you are using DISC media for the upgrade | step <a href="#">2</a> |
| you are using ESD for the upgrade        | step <a href="#">3</a> |

- 2 If you are using DISC media as the software delivery method for the upgrade, the system prompts you to insert the UCBM disk into the DVD drive. After you have inserted the disk into the drive, the system prompts you to enter one of the commands shown in the following table:

| If in response to the system prompt | System response                                                                                                                                               |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you entered continue                | The upgrade begins. Return to step <a href="#">4</a> in <a href="#">Upgrading the CBM on page 766</a>                                                         |
| you entered shell                   | Perform <a href="#">Selecting the CBM upgrade media on page 786</a> starting at step <a href="#">2</a>                                                        |
| you entered fallback                | Perform <a href="#">Selecting the CBM upgrade media on page 786</a> starting at step <a href="#">3</a>                                                        |
| you entered media                   | The system prompts you to select the software delivery method to be used for the upgrade. Perform <a href="#">Selecting the CBM upgrade media on page 786</a> |

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

| If                                                         | Do                     |
|------------------------------------------------------------|------------------------|
| more than one ESD image is found in the /swd/sdm directory | step <a href="#">4</a> |
| only one ESD image is found in the /swd/sdm directory      | step <a href="#">5</a> |

- 4 The following table shows the system responses and possible actions you can perform.

| If in response to the system prompt            | System response                                                                                                                                                                                                                                                                |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you entered the number of the ESD image to use | The system retrieves the ESD image you have selected. Go to step <a href="#">5</a>                                                                                                                                                                                             |
| you entered shell                              | The system suspends the upgrade and you enter a maintenance Shell to retrieve the ESD image if the correct image appears to not be available. Refer to <a href="#">Selecting the CBM upgrade media on page 786</a> starting at step <a href="#">2</a> for the system response. |
| you entered fallback                           | The system cancels the entire upgrade procedure. Refer to <a href="#">Selecting the CBM upgrade media on page 786</a> starting at step <a href="#">3</a> for the system response.                                                                                              |
| you entered media                              | <p>The system prompts you to select the software delivery method.</p> <p>If you select the disk delivery method in response, see step <a href="#">2</a> for a description of the system response and the action you can perform.</p>                                           |

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

## Selecting the CBM upgrade profile

The CBM is provided in several flavors for the following markets:

- Wireline (Time Division Multiplexing, Succession)
- Wireless (CDMA, GSM)

Prior to release SN09U, each CBM flavor used a unique medium (CD or ESD file) and upgrade procedure. Starting with release SN09U, all of the CBM flavors share a single, converged medium (DVD or ESD file) and use a unified upgrade procedure.

In the CBM upgrade procedure, the `cbm_setup` program maps the flavor of CBM and its previous release profile to a new UCBM profile. The following table shows the CBM profile mapping.

| Type                   | From CBM0070 | From CBM0080 | From CBM0090 | UCBM010 CBM Profile |
|------------------------|--------------|--------------|--------------|---------------------|
| Wireline CS2K          | NA           | CBM850       | CBM850       | SCBM                |
| Wireline CCA           | NA           | CBM850       | CBM850       | SCBM                |
| Wireless CDMA          | CCBM0130     | NA           | NA           | CCBM                |
| Wireless CDMA (Packet) | PCBM0130     | NA           | NA           | CCBM                |
| GSM                    | GCBM0180     | NA           | NA           | GCBM                |

The `cbm_setup` program prompts you to select the appropriate profile for your CBM. This procedure shows how you may respond to this prompt.

## Selecting the CBM upgrade profile

### *At your workstation*

- 1 When the CBM 850 cbm\_setup program presents you with a list of software profile options, use the following table to determine your next step.

In response to the prompt you may:

- enter the number next to profile in the list, to select the profile
- enter **up** or **down** to migrate to a profile selection in the list
- enter **help** to display help information about the profile selection procedure
- enter **shell** to suspend the upgrade and enter a Maintenance shell before continuing the upgrade
- enter **fallback** to cancel the entire upgrade procedure

| If in response to the system prompt | Action                                                                                                                                                                             |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you entered a profile selection     | Confirm or reject the selection. If you reject the selection, perform step <a href="#">1</a> again.<br><br>Return to step <a href="#">7</a> in <a href="#">Upgrading the CBM</a> . |
| you entered up or down              | Return to step <a href="#">7</a> in <a href="#">Upgrading the CBM</a> .                                                                                                            |
| you entered help                    | Return to step <a href="#">1</a>                                                                                                                                                   |
| you entered shell                   | See step <a href="#">2</a> for a description of the system response and the next action you can perform.                                                                           |
| you entered fallback                | See step <a href="#">3</a> for a description of the system response and the next action you can perform.                                                                           |

- 2 The following table shows the system responses and possible actions you can perform when you enter a maintenance shell.

| If in response to the system prompt to proceed with the shell, | System response                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you entered yes                                                | A maintenance shell prompt displays. You can now enter commands to perform a maintenance action.<br><br>When you are done, enter exit. After entering the exit command, the system will repeat the last action it performed before you opened the maintenance shell. |
| you entered no                                                 | When you enter no, the system will repeat the last action it performed before you opened the maintenance shell.                                                                                                                                                      |

- 3 The following table shows the system responses and possible actions you can perform when you enter fallback.

| If in response to the system prompt to proceed with the fallback, | System response                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you entered yes                                                   | The CBM 850 upgrade is cancelled and the node automatically undergoes Mtce reboots. Wait for the Mtce reboots to complete (about 10 minutes). Then, after the node is brought to the login prompt, perform procedure <a href="#">Executing a fallback during an SPFS-based server upgrade on page 418</a> |
| you entered no                                                    | When you enter no, the system will repeat the last action it performed before you selected to fallback.                                                                                                                                                                                                   |

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

---

## Selecting the CBM packages

---

The CBM upgrade program uses the CBM profile you selected during the upgrade to automatically apply or display the appropriate CBM packages for that profile. There are two classifications of packages:

- Required packages, which are either
  - upgraded automatically if they existed on the previous software load in your CBM
  - or
  - installed automatically through the `cbm_post_upgrade` script
- Optional packages, which are either
  - upgraded automatically if they existed on the previous software load in your CBM
  - or
  - prompted for selection during the upgrade, to be installed through the `cbm_post_upgrade` script
  - or
  - added manually after the upgrade is finished, using the procedure *Installing optional software on a CBM 850*

**Note:** To minimize the quantity of optional packages presented for selection during the upgrade, the list excludes prerequisite (lower-level) packages required by the optional packages.

## Selecting the CBM packages

### *At your workstation*

- 1 When the CBM 850 cbm\_setup program presents you with a list of optional CBM packages appropriate for your CBM profile to be installed automatically, use the following table to determine your next step.

In response to the prompt you may:

- enter the number next to one or more of the packages in the list, to select the package for automatic installation
- enter **up** or **down** to migrate to a package selection in the list
- enter **continue** to enter a package selection
- enter **help** to display help information about the package selection procedure
- enter **shell** to suspend the upgrade and enter a Maintenance shell before continuing the upgrade
- enter **fallback** to cancel the entire upgrade procedure

| If in response to the system prompt   | Action                                                                                                                                                                                                                 |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you have finished a package selection | Enter Continue. You will then be prompted to confirm your selection. If you reject the selection, perform step <a href="#">1</a> again.<br><br>Return to step <a href="#">8</a> in <a href="#">Upgrading the CBM</a> . |
| you entered up or down                | Return to step <a href="#">8</a> in <a href="#">Upgrading the CBM</a> .                                                                                                                                                |
| you entered help                      | Return to step <a href="#">1</a>                                                                                                                                                                                       |
| you entered shell                     | See step <a href="#">2</a> for a description of the system response and the next action you can perform.                                                                                                               |
| you entered fallback                  | See step <a href="#">3</a> for a description of the system response and the next action you can perform.                                                                                                               |

- 2 The following table shows the system responses and possible actions you can perform when you enter a maintenance shell.

| If in response to the system prompt to proceed with the shell, | System response                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you entered yes                                                | A maintenance shell prompt displays. You can now enter commands to perform a maintenance action.<br><br>When you are done, enter exit. After entering the exit command, the system will repeat the last action it performed before you opened the maintenance shell. |
| you entered no                                                 | When you enter no, the system will repeat the last action it performed before you opened the maintenance shell.                                                                                                                                                      |

- 3 The following table shows the system responses and possible actions you can perform when you enter fallback.

| If in response to the system prompt to proceed with the fallback, | System response                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you entered yes                                                   | The CBM 850 upgrade is cancelled and the node automatically undergoes Mtce reboots. Wait for the Mtce reboots to complete (about 10 minutes). Then, after the node is brought to the login prompt, perform procedure <a href="#">Executing a fallback during an SPFS-based server upgrade on page 418</a> |
| you entered no                                                    | When you enter no, the system will repeat the last action it performed before you selected to fallback.                                                                                                                                                                                                   |

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



---

## Ensuring the SN08 CBM load is patch-current for upgrades

---

To ensure a successful CBM upgrade, it is mandatory that the load you are upgrading from is patch-current prior to the upgrade.

Nortel maintains a web-based Patch Audit Tool that is used for obtaining patches for several of its products through e-mail notification. These patches are bundled in a single tar.Z file for easier transfer from the web site through your PC and to the CBM.

The Patch Audit Tool can be used in two ways during an upgrade:

- When an “inform” file is generated for the CBM, it contains a list of all patches currently applied to the CBM. Sending this file to the Patch Audit Tool before an upgrade generates a delta file of released patches required to make the load running in the CBM patch-current.
- All released patches from a specific date for the new CBM release and loads indicated in the pre-upgrade file are returned. This requires a pre-upgrade text file to be manually created with a text editor on your PC.

The following procedure provides the steps you need to perform to ensure that the CBM 850 SN08 load is patch-current. The procedure consists of the following basic tasks:

- Create a new user ID for upgrade patching and ftp file transfer
- Generate an inform file
- Transfer the inform file to the PC
- Submit the inform file to the Patch Audit Tool
- Download the delta patch tar.Z bundle file received from the Patch Audit Tool to the PC
- Transfer the delta patch tar.Z bundle file to the CBM
- Apply the delta patch tar.Z bundle to the active CBM, on the load the CBM is being upgraded from.

### Prerequisites

Table [Prereq items on page 751](#) contains information that you need for performing this procedure. Ensure that you have this filled-in table available for quick reference during this procedure.

**Attention:** This procedure can be used only for a CBM running at release level SN08.

## Action

### Ensuring the SN08 CBM load is patch-current for upgrades

#### *On the active CBM 850 node*

- 1 Create a new user ID (cbmpat) and password for upgrade patching and ftp file transfer (item [Q](#) in the [Prereq items](#) table you filled out prior to the upgrade):

```
useradd -g emsadm -G succssn -m -d
/export/home/cbmpat -s /bin/ksh cbmpat
```

```
passwd -r files cbmpat
```

- 2 Create an Inform file on the CBM by performing the following steps:

```
cd
```

```
queryloads -m inform >
/export/home/cbmpat/<clli>.cbm.inform.txt
```

where

**<clli>**

is the clli in item [K](#) of the [Prereq items](#) table.

- 3 Transfer the inform file onto your PC from the CBM, by performing the following steps.
  - a On your PC, click the Windows Start button and select Run. In the Open text entry window, enter the following command:

```
ftp <IP address>
```

where

**<IP address>**

is the cluster IP address you wrote down in item [I](#) in the [Prereq items](#) table.

**Note:** If FTP is turned off on the CBM, you will need to identify a separate FTP server to relay the file through. In this event, you will use FTP on this other server to transfer the file from the CBM to the server and then from the server to the PC.

- b Log in using the cbmpat user ID and password that you wrote down in item [Q](#) in the [Prereq items](#) table.
  - c Enter the following command:

```
binary
```

- d Transfer the inform file to your PC:

```
cd /export/home/cbmpat
```

```
get <cli>.cbm.inform.txt
```

where

<cli>

is the cli from item [K](#) in the [Prereq items](#) table.

- e To determine the location of the inform file on your PC, enter the following command:

```
lcd
```

- f Disconnect from the CBM:

```
quit
```

- 4 Submit the inform file on your PC to [www.nortel.com](http://www.nortel.com) Patch Audit Tool, by performing the following steps.

- a Launch your web browser from the PC on which the inform file resides.
- b Go to [www.nortel.com](http://www.nortel.com).
- c In the Support and Training/Technical Support tab pull-down, click Software Downloads.
- d If you see the message, “Welcome Guest. You are not logged in” in the top left corner of the screen, click on Log In and enter your Nortel user ID and password that you wrote down in item [V](#) in the [Prereq items](#) table.
- e In the Find Products window, click Products A-Z, and then click C.
- f Scroll down to Core and Billing Manager (CBM) on the screen and then click Tools under Core and Billing Manager (CBM).
- g Click Patch Audit for Inform Lists.
- h Next to Tool Access, click Patch Audit Application[appl]
- i Enter your full external email address that you wrote down in item [Y](#) in the [Prereq items](#) table.
- j Click the Choose/Browse file button, navigate to the location of the inform file on your PC, and then select the inform file.
- k Click the process INFORM button.

In response, a note displays indicating the patch audit report is being processed and that you will receive the patch audit results.

**Note:** The patch audit report processing can take up to one hour to perform.

- 5 When the patch audit results email arrives at your PC, view the patch audit results file. Before the expiry date of your patch audit information, download the delta patch tar.Z bundle to the PC, by performing the following steps.
  - a Open the patch audit results email and click on the link that appears in the email.
  - b When the PC web browser link opens, scan the summary to see if any ACT/OBE/OBS exist that will require special processing.
  - c Click the Download All Recommended Patches link.

**Note:** If there are no recommended patches for download, quit the PC web browser and go to step [13](#).

In response, a delta patch tar.Z file will be downloaded to your PC. Note the name and location of this file on your PC.

**Attention:** Do not uncompress the file on the PC.
  - d Quit the PC web browser.
- 6 Transfer the delta patch tar.Z file from your PC to the CBM, by performing the following steps.
  - a On your PC, click the Windows Start button and select Run. In the Open text entry window, enter the following command:  
**ftp <IP address>**  
where  
**<IP address>**  
is the cluster IP address you wrote down in item [I](#) in the [Prereq items](#) table.

**Note:** If FTP is turned off on the CBM, you will need to identify a separate FTP server to relay the file through. In this event, you will use FTP on this other server to transfer the file from the CBM to the server and then from the server to the PC.
  - b Log in using the cbmpat user ID and password from item [O](#) in the [Prereq items](#) table.
  - c Enter the following commands:  
**cd /export/home/cbmpat**  
**binary**
  - d Enter the following command to determine your current directory location on the PC:  
**lcd**

Change your directory location, as necessary, to the location of the patch file you are going to transfer that you noted in step [5c](#):

```
lcd <directory location>
```

- e Transfer the patch file to the CBM:

```
mput *tar.Z
```

**Note:** If there are multiple patch files, only type Y for the patch file just downloaded to your PC.

- f Disconnect from the CBM:

```
quit
```

- 7 Reconnect to the CBM and log in as cbmpat. Uncompress the delta patch tar.Z bundle file and copy the patches to the appropriate directory:

```
cd /export/home/cbmpat
```

```
ls *.Z
```

```
uncompress <patchfile>.tar.Z
```

where

**<patchfile>**

is the name of the delta patch tar.Z bundle file

```
ls *.tar
```

```
tar -xvf <patchfile>.tar
```

```
ls
```

```
cp <patchfile dir>/*.patch /swd/fixes/incoming
```

where

**<patchfile dir>**

is the new directory created by the tar command you entered above.

```
cd
```

- 8 Enter the following command:

```
ls /swd/fixes/incoming/NTSIM*
```

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

| If                                                      | Do                      |
|---------------------------------------------------------|-------------------------|
| the system response indicates that there are patches    | step <a href="#">10</a> |
| the system response indicates that there are no patches | step <a href="#">11</a> |

- 10 Enter the following command:

```
patchctrl -f /swd/fixes/incoming/<NTSIM full patch name>
```

where

**<NTSIM full patch name>**

is the name of the patch displayed in step [8](#).

- 11 Enter the following command:

```
patchctrl -d /swd/fixes/incoming
```

If you receive a prompt recommending that you apply the patches on the inactive node first, enter the following command:

```
patchctrl -i <-f or -d> <full path>/<patch file>
```

where

**<-f or -d>, <full path>, and <patch file>**

are from the original command entries you made above.

**Note:** For more information about the patchctrl tool and commands, see [Information about the patchctrl tool on page 802](#)

- 12 Check that the patches were applied:

```
queryloads -m patches | egrep -i 'nt|cbm'
```

- 13 This procedure is complete. Return to step [11](#) in [Preparing to upgrade the CBM](#)

### Information about the patchctrl tool

Apply the delta patches to the CBM. You apply the patches using the patchctrl tool. The patchctrl tool applies a single patch or multiple patches located in the source directory that you specify. The patchctrl tool automatically ensures that patches are applied in the correct order when the patches require additional patches from the source directory or patches that are already applied on the node.

You may apply three types of patches: active apply patches, inactive apply patches, or manual apply patches. Active apply patches are applied on the active node of a CBM 850 cluster first and then on the inactive node of the cluster. Inactive apply patches are normally applied on the inactive node of a CBM 850 cluster first and then on the active node of the cluster. Manual apply patches can be applied on either node of a CBM 850 cluster first and are then applied on the other node of the cluster.

**Note:** Interactive patches are not applied on the system but are, instead, moved by the patchctrl tool to a special directory for possible manual application at a later time. When the patches have been moved to this directory, the release notes that accompany the patches can, however, be displayed using the patchctrl tool.

If the patch requires a reboot of a CBM node, the tool will detect this and will prompt you to authorize the reboot before it continues with the application of the patches. The system also prompts you to authorize the SwAct of the nodes if the patches are applied on the inactive node first.

**Note 1:** If any patches have been applied on only one node of the cluster and a SwAct to the other node in the cluster is aborted by the customer, it is the responsibility of the customer to remove any patches that have been applied on the one node in the cluster.

**Note 2:** Ensure that you do not enter the patchctrl command from within a replicated file system.

**Note 3:** If inactive-apply patches are found, the system prompts you to indicate the node on which to apply the patch, or patches, first. You should always enter Inactive. You should contact your next level of support if you want to apply the patch, or patches, on the Active node first.

**Note 4:** If any of the patches you are applying require a system reboot, the system will notify and prompt you to authorize the reboot before beginning the patch application. If multiple patches are being applied, the system will reboot the node only one time, after all of the patches have been applied on that node. If you do not authorize the

reboot, the patching transaction is stopped, without applying any patches to either node of the system, and you are returned to the command line.

**Note 5:** When any of the patches you are applying require a system reboot (which only occurs when they are being applied on the inactive node first), after the reboot you will be prompted to authorize a SwAct (software activation) to the other node of the cluster. The patch, or patches, are then applied on the node made inactive by the SwAct (originally active node of the cluster). Finally, the system prompts you to authorize a reboot of this newly-inactive node. You must enter Yes and authorize the reboot; if you do not authorize the reboot, the system will be left in an unsupported state.

**Note 6:** You may receive a prompt from the patchctrl tool warning you that the patches you are about to apply require a reboot on the active node, which will result in a swact, a loss of connection, and the software on the nodes being out of sync. The prompt recommends that you apply the patches on the inactive node first by including the *i* option in the patchctrl command. In this event, it is recommended that you abort the current patching operation by entering Abort, and then enter the following command to perform the patching operation:

**patchctrl -i <-f or -d> <full\_path>/<patch\_file>**

*where:*

**-i**

is the *i* option, that indicates the patchctrl command is to be performed on the inactive node.

If you wish, instead, to continue the patching operation without first aborting and entering the patch command with the *i* option, you should contact your next level of support.



## Using Patch Audit to ensure CBM SN09 and higher loads are patch-current

The following procedure provides the steps you need to perform to ensure that the CBM 850 SN09 or higher load is patch-current prior to the upgrade. This is a mandatory requirement for the upgrade.

**Attention:** This procedure can be used only for a CBM running at release level SN09 and up. The Patch Audit utility is part of Network Patch Management (NPM).

### Prerequisites

Table [Prereq items on page 751](#) contains information that you need for performing this procedure. Ensure that you have this filled-in table available for quick reference during this procedure.

### Action

#### Using Patch Audit to ensure CBM SN09 and higher loads are patch-current

##### *On the active CBM 850 node*

- 1 Verify that the Patch Server Element (PSE) is operational.  
Check PSE status:

**/opt/NTpse/pse status**

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

| If                    | Do                      |
|-----------------------|-------------------------|
| PSE is running        | step <a href="#">13</a> |
| PSE is not running    | step <a href="#">11</a> |
| PSE is not configured | step <a href="#">3</a>  |

- 3 Enter the command line interface (cli) tool:  
**cli**
- 4 Enter the number next to the Configuration option in the menu.
- 5 Enter the number next to the Succession Element Configuration option in the menu.
- 6 Enter the number next to the PSE Application Configuration option in the menu.
- 7 Enter the number next to the Configure PSE option in the menu.

- 8 In response to the prompt, enter the primary/cluster IP address of the NPM server (item M in the Prereq items table).
- 9 In response to the prompt, enter y to confirm the IP address.
- 10 Enter x to exit each level until you have exited from the cli tool.
- 11 Start the PSE server:  
**/opt/NTpse/pse start**
- 12 Verify that the server has started. If the server does not start, contact your next level of support.  
**/opt/NTpse/pse status**
- 13 Use the following table to determine your next step.

| If                                                                                 | Do                      |
|------------------------------------------------------------------------------------|-------------------------|
| item L = YES in the Prereq items table (the NPM functionality is to be on the CBM) | step <a href="#">14</a> |
| item L = NO in the Prereq items table (the NPM is not to be on the CBM)            | step <a href="#">25</a> |

- 14 Verify NPM is running:  
**servquery -status -group NPM**
- 15 Use the following table to determine your next step.

| If                                                          | Do                      |
|-------------------------------------------------------------|-------------------------|
| the system display indicates that the NPM is not configured | step <a href="#">16</a> |
| the system display indicates that the NPM is not running    | step <a href="#">23</a> |
| the system display indicates that the NPM is running        | step <a href="#">26</a> |

- 16 Configure the NPM on the CBM. Access the command line interface:  
**cli**
- 17 Enter the number next to the Configuration option in the menu.
- 18 Enter the number next to the Succession Element Configuration option in the menu.

- 19 Enter the number next to the NPM Application Configuration option in the menu.
- 20 Enter the number next to the ConfigureNpm (Configure the Network Patch Manager) option in the menu.
- 21 If you are ready to proceed with NPM application configuration, enter y.
- 22 When prompted, enter x to exit each level until you exit the command line interface.
- 23 Start the NPM server:  
**servstart NPM**
- 24 Verify NPM is running:  
**servquery -status -group NPM**  
Go to step [26](#)
- 25 Log in as root to the NPM cluster IP address:  
**ssh -l root <NPM cluster IP address>**  
where  
**<NPM cluster IP address>**  
is the NPM cluster IP address in item M in the Prereq items table.
- 26 Determine whether a cbmpat user ID on NPM already exists:  
**groups cbmpat**

| If                                                                 | Do                      |
|--------------------------------------------------------------------|-------------------------|
| the response indicates that a cbmpat user ID on NPM already exists | step <a href="#">27</a> |
| the response indicates that a cbmpat user ID on NPM does not exist | step <a href="#">28</a> |

- 27 Delete the existing cbmpat user ID on NPM:  
**userdel cbmpat**
- 28 Create a new cbmpat user ID on NPM to avoid any user ID conflict:  
**useradd -g emsadm -G succssn -m -d /export/home/cbmpat -s /bin/ksh cbmpat**

- 29** Set the password for the new account (item O in the Prereq items table):
- ```
passwd -r files cbmpat
```
- 30** Connect to the NPM CLUI. Enter the following command:
- ```
npm
```
- Log in to the NPM CLUI using the new user ID and password that you created in step [28](#) (see item O in the Prereq items table).
- 31** Determine if the PFRS drop box is already configured:
- ```
viewpfrs
```
- 32** Compare the information that is displayed to you with the information that you wrote down in items P, Q, and R of the Prereq items table.

If	Do
the PFRS drop box is already configured, and the information you see displayed matches items P, Q, and R of the Prereq items table	step 35
the PFRS drop box is already configured, but the information you see displayed differs from the items P, Q, and R of the Prereq items table	step 33
the PFRS drop box is not configured	step 34

- 33** Resolve the difference between the display and the Prereq items table entries P, Q, and R before continuing. Contact your company's NPM patch administrator and obtain the user ID and password for the displayed PFRS drop-off server. Record this in item P, Q, and R of the Prereq items table.
- 34** Set up the Patch File Receipt System (PFRS) drop-off server. Use the information for the PFRS drop-off server that you wrote down in items P, Q, and R of the Prereq items table.

Note: You must use the IP address, rather than the hostname, as this procedure requests.

Perform the procedure [Configuring NPM for automatic patch file delivery on page 493](#) and then return to this step.

- 35** If you have just finished configuring NPM for the first time, the inform file will not be valid until a device audit completes. Enter the following command to determine whether the device audit has completed:

rr devicelist

Examine the list of devices that is displayed and use the following table to determine your next step.

If	Do
no devices are shown, or any devices are shown with an UNKNOWN label	step 36
For example, CBM_ACE_had3-unit1,UNKNOWN,FALSE,TRUE,PSE_had3-unit1	
no devices are shown with an UNKNOWN label	step 38

- 36** Enter the following command to start the audit now:
- rt audit**
- 37** Enter the following command to determine whether the device audit has completed:
- rr devicelist**
- If the audit has not yet completed, and qrunning shows no audits in the queue, re-run the command. If after re-running the command several times any devices are shown with an UNKNOWN label, contact your next level of support.
- 38** While still logged into the NPM CLUI, create the inform file that will include CBM and other components' patches. Enter the following command:
- runtask pfrsgenreport**
- 39** Transfer the inform file onto your PC from the PFRS drop-off server, by performing the following steps (refer to item W in the Prereq items table).
- a** On your PC, click the Windows Start button and select Run. In the Open text entry window, enter the following command:
- ftp <IP address>**
- where

<IP address>

is the PFRS drop-off server IP address you wrote down in item P of the Prereq items table

- b** Log in using the PFRS drop-off server user ID and password that you wrote down in item Q of the Prereq items table.
- c** Enter the following command:

binary

- d** Determine whether the inform file arrived:

ls *.inform

If the inform file is present, it will look similar to the following example.

Example

<cli>.npm.inform.

where

<cli> is the value you wrote down in item K of the Prereq items table.

- e** Transfer the correct inform file to your PC:

get <cli>.npm.inform

- f** To determine the location of the inform file on your PC, enter the following command:

lcd

Record this location in item AD of the Prereq items table.

- g** Disconnect from the PFRS drop-off server:

quit

- 40** The inform file name must conform to the following naming convention: **<cli>.<product>.inform.txt**. Refer to item K in the Prereq items table for the **<cli>**. Rename the inform file on your PC in the following format: **<cli>.npm.inform.txt**
- 41** Submit the inform file on your PC to www.nortel.com Patch Audit Tool, by performing the following steps.
 - a** Launch your web browser from the PC on which the inform file resides. (See item U in the Prereq items table.)
 - b** Go to www.nortel.com.
 - c** In the Support and Training/Technical Support tab pull-down, move the mouse to Technical Support and click Software Downloads.

- d If you see the message, "Welcome Guest. You are not logged in" in the top left corner of the screen, click on Log In and enter your Nortel user ID and password that you wrote down in item V of the Prereq items table.
- e In the Find Products window, click Products A-Z, and then click C.
- f Scroll down to Core and Billing Manager (CBM) on the screen and then click Tools under Core and Billing Manager (CBM).
- g Click Patch Audit for Inform Lists.
- h Next to Tool Access, click Patch Audit Application[appl]
- i Enter your full external email address that you wrote down in item Y of the Prereq items table.
- j Click the Browse/Choose file button, navigate to the location of the inform file on your PC, and then select the inform file.
- k Click the process INFORM button.

In response, a note displays indicating the patch audit report is being processed and that you will receive the patch audit results.

Note: If the CLLI of the core (item K in the Prereq items table) is not registered at Nortel, the Patch Audit Tool will reject the request. Contact your Nortel service representative for assistance.

- 42 When the patch audit results email arrives, download the delta patch tar.Z bundle to the PC by performing the following steps.
- a Open the patch audit results email and click on the link that appears in the email.
 - b When the PC web browser link opens, scan the summary to see if any ACT/OBE/OBS exist that will require special processing.
 - c Click the Download All Recommended Patches link.

Note 1: Using the same path as recorded in item AD of the Prereq items table may make subsequent file transfer steps easier.

Note 2: If there are no recommended patches for download, quit the PC web browser and go to step [47](#).

In response, a delta patch tar.Z file will be downloaded to your PC. Note the name and location of this file on your PC (item AD of the Prereq items table).

- d** Quit the PC web browser.

e Uncompress the delta patch tar.Z file on your PC.

43 Transfer the delta patch files from your PC to the PFRS drop-off server, by performing the following steps:

a On your PC, click the Windows Start button and select Run. In the Open text entry window, enter the following command:
ftp <PFRS drop-off server IP address>
where
<PFRS drop-off server IP address>
is the IP address you wrote down in item P of the Prereq items table.

b Log in using the PFRS drop-off server user ID and password that you wrote down in item Q of the Prereq items table.

c Enter the following command:
binary

d Enter the following command to determine your current location on the PC:
lcd
Change your directory location, as necessary, to the location of the patch file you are going to transfer (see item AD of the Prereq items table):
lcd <new directory location>

e Enter the following command:
prompt off

f Transfer the patch files to the PFRS drop-off server:
mput *

g Disconnect from the PFRS drop-off server:
quit

44 Connect to the NPM to transfer patches from the PFRS drop-off server, by performing the following steps.

a Connect to the server that NPM resides on using the NPM cluster IP address that you wrote down in item M of the Prereq items table.

Note: If item L = NO in the Prereq items table, connect to the NPM through SSH; otherwise the NPM is located on the CBM)

- b** Log in to the NPM CLUI using the new user ID and password that you created in step [28](#) (see item O in the Prereq items table)
- c** Retrieve the patches:

runtask pfrsgetpatch

- 45** Apply the patches, using NPM, by performing the following steps.

- a** Enter the following command:

```
apply set emg_not_app set gen_not_app
```

- b** Read and follow special application instructions for any patches that required special handling.
- c** Determine whether a restart of any devices is required in order to enable any of the patches. Enter the following command:

q restartlist

Example system response:

NPM_wcarsx0h-unit0,NPf80O91,A,FALSE,2006-03-20
22:37:04.000

PSE_wcarsx0h-unit1,PF610O91,A,FALSE,2006-03-20
23:16:20.000

SSPFS_wcarsx0h-unit0,LAX77121,A,FALSE,2006-03-21
01:30:11.000

Devices listed in the system response must be restarted.

Note: A restart is not required on the SSPFS device.

Enter the following command for each device, except the SSPFS device:

```
restart set devicestorestart
```

- d** Quit from NPM.

- 46** If an SSPFS device is shown in the list that the system displayed in step [45](#), display the patch associated with it and follow the special instructions to determine how to enable the patch.

Log in to the NPM CLUI and enter the following command:

vp <patchid>

Follow the instructions in the test and warning sections of the patch information that displays. To avoid rebooting a unit

multiple times, ensure that you have read the instructions for all of the patches before performing a reboot of a unit.

Attention: If you are using a VT100 terminal without a scroll bar, do not log in to the NPM CLUI. Instead, enter the following command from the command line, making sure that you enter the single quotation marks shown in the command description below:

```
npm 'vp <patchid> output <filename>'
```

When prompted, enter the user ID and password (see item O in the Prereq items table).

Read and follow the instructions from the patch file stored in the specified <filename>.

- 47** This procedure is complete. Return to the high level task or procedure that directed you to this procedure.

Obtaining patch files from CD before a CBM upgrade

Use this procedure to manually transfer new release patches obtained from CD to a CBM prior to the upgrade of the CBM.

Obtaining patch files from CD before a CBM upgrade

ATTENTION

Perform the steps that follow on the active node.

At your workstation

- 1 Establish a login session to the server, using one of the following methods:

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

- 2 Log in to the server using telnet (unsecure) as follows:

- a Log in to the server by typing

```
telnet <server>
```

where

server

is the physical IP address of the active server

- b When prompted, enter your user ID and password.
- c Change to the root user by typing

```
su -
```

- d When prompted, enter the root password.

Note: Ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step [4](#).

- 3 Log in using ssh (secure) as follows:

- a Log in to the server by typing
ssh -l root <server>
where
server
is the physical IP address of the active server
Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter *yes* at the prompt.
 - b When prompted, enter the root password.
- 4 Make a directory to hold the patch files you want to install:
mkdir /data/npm_patches
- 5 Access the newly-created directory:
cd /data/npm_patches
- 6 Copy the patches from /cdrom:
cp /cdrom/cdrom0/*.patch /data/npm_patches
- 7 Verify that the patches are in the /data/npm_patches directory on the CBM:
ls
- 8 Change permissions for the patch directory and for the files in the directory:
chmod -R 777 /data/npm_patches
- 9 Eject the CD:
eject cdrom
- 10 You have completed this procedure. Return to [Preparing to upgrade the CBM](#).

Obtaining patch files from ISO before a CBM upgrade

Use this procedure to manually transfer new release patches in an ISO image to the CBM prior to the upgrade of the CBM.

Obtaining patch files from ISO before a CBM upgrade

ATTENTION

Perform the steps that follow on the active node.

At your workstation

- 1 Establish a login session to the server, using one of the following methods:

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

- 2 Log in to the server using telnet (unsecure) as follows:

- a Log in to the server by typing

```
telnet <server>
```

where

server

is the physical IP address of the active server

- b When prompted, enter your user ID and password.
- c Change to the root user by typing

```
su -
```

- d When prompted, enter the root password.

Note: Ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step [4](#).

- 3 Log in using ssh (secure) as follows:

- a Log in to the server by typing
ssh -l root <server>
where
server
is the physical IP address of the active server
Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter *yes* at the prompt.
 - b When prompted, enter the root password.
- 4 Make a directory to hold the patch files you want to install:
mkdir /data/npm_patches
- 5 Mount the ISO image file.
For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)
- 6 Copy the patches from /tmpmnt:
cp /tmpmnt/*.patch /data/npm_patches
- 7 Verify that the patches are in the /data/npm_patches directory on the CBM:
ls /data/npm_patches
- 8 Change permissions for the patch directory and for the files in the directory:
chmod -R 777 /data/npm_patches
- 9 Unmount and remove the ISO image file from the server.
For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#)
- 10 You have completed this procedure. Return to [Preparing to upgrade the CBM](#)

Obtaining pre-upgrade patches released after upgrade media shipped

The following procedure provides the steps you need to obtain all released patches onward from a specified date. Typically, the date used is the shipped or created date on the SPFS and CBM media (see items [E](#) and [H](#) in the [Prereq items](#) table). The procedure requires that two pre-upgrade files be manually created with a text editor (for example, Notepad) on your PC. Each of these files must be submitted separately to the Patch Audit Tool.

Attention: This procedure is mandatory for the upgrade.

Prerequisites

The [Prereq items](#) table contains information that you need for performing this procedure. Ensure that you have this filled-in table available for quick reference during this procedure.

Action

Obtaining pre-upgrade patches released after upgrade media shipped

On your PC:

- 1 Using a text editor tool on your PC (such as Notepad), create an SPFS pre-upgrade file. In this file, add the following three lines of content:

```
PRODUCT:SPFS0091  
MTG_DATE:yyyymmdd  
Version:<number>
```

where

MTG_DATE and **Version**

are found in item [E](#) of the [Prereq items](#) table

Note: If the SPFS or CBM patch CD were not received or if they are damaged, set MTG_DATE to 20060101. This will ensure that all patches are obtained, including the contents of the two patch CDs.

Example of file content:

PRODUCT:SPFS0091
MTG_DATE:20060101
Version:1

Note: The contents of the file must be exactly as indicated, with regard to case, underscores, and colons.

Save the file as:

<cli>.npm.patreq.txt

where

<cli> is item [K](#) in the [Prereq items](#) table

Example of file name:

RALEIGHDS02.npm.patreq.txt

- 2 Submit the file on your PC to www.nortel.com Patch Audit Tool, by performing the following steps.
 - a Launch your web browser from the PC on which the inform file resides (see item [U](#) in the [Prereq items](#) table).
 - b Go to www.nortel.com.
 - c In the Support and Training/Technical Support tab pull-down, click Software Downloads.
 - d If you see the message, "Welcome Guest. You are not logged in" in the top left corner of the screen, click on Log In and enter your Nortel user ID and password that you wrote down in item [V](#) in the [Prereq items](#) table.
 - e In the Find Products window, click Products A-Z, and then click C.
 - f Scroll down to Core and Billing Manager (CBM) on the screen and then click Tools under Core and Billing Manager (CBM).
 - g Click Patch Audit for Inform Lists.
 - h Next to Tool Access, click Patch Audit Application[appl]
 - i Enter your full external email address that you wrote down in item [Y](#) in the [Prereq items](#) table.
 - j Click the Browse file button, navigate to the location of the inform file on your PC, and then select the inform file.
 - k Click the process INFORM button.

In response, a note displays indicating the patch audit report is being processed and that you will receive the patch audit results.

Note: The patch audit report processing can take up to one hour to perform.

- 3 Modify the file you created in step [1](#) to create a CBM pre-upgrade file. For the PRODUCT field only, change SPFS0091 to UCBM0010. Use the date and version from item [H](#) in the [Prereq items](#) table.

Save the file with the same name that you used in step [1](#)

- 4 Submit the file on your PC to the www.nortel.com Patch Audit Tool, by performing the following steps.
 - a Launch your web browser from the PC on which the inform file resides (see item [U](#) in the [Prereq items](#) table).
 - b Go to www.nortel.com.
 - c In the Support and Training/Technical Support tab pull-down, click Software Downloads.
 - d If you see the message, “Welcome Guest. You are not logged in” in the top left corner of the screen, click on Log In and enter your Nortel user ID and password that you wrote down in item [V](#) in the [Prereq items](#) table.
 - e In the Find Products window, click Products A-Z, and then click C.
 - f Scroll down to Core and Billing Manager (CBM) on the screen and then click Tools under Core and Billing Manager (CBM).
 - g Click Patch Audit for Inform Lists.
 - h Next to Tool Access, click Patch Audit Application[appl]
 - i Enter your full external email address that you wrote down in item [Y](#) in the [Prereq items](#) table.
 - j Click the Browse file button, navigate to the location of the inform file on your PC, and then select the inform file.
 - k Click the process INFORM button.

In response, a note displays indicating the patch audit report is being processed and that you will receive the patch audit results.

Note: The patch audit report processing can take up to one hour to perform.

- 5 Perform this step for each product, SPFS and CBM. When both patch audit results emails arrive at your PC, view the patch audit results files through the link to Nortel.com shown in the e-mail (see item [Y](#) in the [Prereq items](#) table).
- Open the patch audit results email and click on the link that appears in the email.
 - When the PC web browser link opens, scan the summary to see if any ACT/OBE/OBS exist that will require special processing.
- Note:** If the quantity of patches requiring action is NONE for the SPFS product, view the quantity of patches requiring action for the CBM product. If the quantity of patches requiring action is NONE for both the SPFS and CBM, go to step [37](#).
- Click the Download All Recommended Patches link.
- In response, a delta patch tar.Z file will be downloaded to your PC. Record the name and location of this file on your PC in item [AD](#) of the [Prereq items](#) table.
- Attention:** Do not uncompress the file on the PC.
- Quit the PC web browser.
- 6 Use the following table to determine your next step.

If	Do
the load you are upgrading from is CBM00090 (see item A in the Prereq items table) and NPM functionality is on this CBM (item L = YES in the Prereq items table)	step 12
the load you are upgrading from is any other load (see item A in the Prereq items table) and NPM functionality is not on this CBM (item L = NO in the Prereq items table)	step 7

- 7 Log in as root to the NPM cluster IP address:
- ```
ssh -l root <NPM cluster IP address>
```
- where

**<NPM cluster IP address>**

is the NPM cluster IP address in item [M](#) in the [Prereq items](#) table.

- 8** Determine whether a cbmpat user ID on NPM already exists:

**groups cbmpat**

| If                                                                 | Do                      |
|--------------------------------------------------------------------|-------------------------|
| the response indicates that a cbmpat user ID on NPM already exists | step <a href="#">9</a>  |
| the response indicates that a cbmpat user ID on NPM does not exist | step <a href="#">10</a> |

- 9** Delete the existing cbmpat user ID on NPM:

**userdel cbmpat**

- 10** Create a new cbmpat user ID on NPM to avoid any user ID conflict:

**useradd -g emsadm -G succssn -m -d  
/export/home/cbmpat -s /bin/ksh cbmpat**

- 11** Set the password for the new account (item [Q](#) in the [Prereq items](#) table):

**passwd -r files cbmpat**

- 12** Transfer both delta patch tar.Z files from your PC to the SPFS server on which the NPM resides or will reside (see item [L](#) in the [Prereq items](#) table), by performing the following steps.

- a** On your PC, click the Windows Start button and select Run. In the Open text entry window, enter the following command:

**ftp <IP address>**

where

**<IP address>**

is the cluster IP address in item [M](#) in the [Prereq items](#) table.

**Note:** If the FTP server has been disabled on the CBM/NPM to satisfy local security policy requirements, you will need to identify a separate FTP server to relay the file through. In this event, you will transfer the files from your PC to this FTP server. You will then use the

CBM/NPM FTP client to initiate file transfer from the FTP server to the CBM/NPM.

- b Log in using the cbmpat user ID and password from item [O](#) in the [Prereq items](#) table.

- c Enter the following commands:

```
cd /export/home/cbmpat
binary
```

- d Enter the following command to determine your current directory location on the PC:

```
lcd
```

Change your directory location, as necessary, to the location of the patch file you are going to transfer (see item [AD](#) in the [Prereq items](#) table).

```
lcd <directory location>
```

- e Transfer both patch files to the CBM/NPM:

```
mput *tar.Z
```

**Note:** If there are multiple patch files, only type Y for the patch file just downloaded to your PC.

- f Disconnect from the CBM/NPM:

```
quit
```

- 13 Reconnect to the CBM/NPM (see item [M](#) in the [Prereq items](#) table) and log in as cbmpat. Uncompress both delta patch tar.Z bundle files and copy the patches to the appropriate directory.

```
cd /export/home/cbmpat
```

```
ls *.Z
```

```
uncompress <patchfile>.tar.Z
```

where

**<patchfile>**

is the name of one of the two delta patch tar.Z bundle files

```
ls *.tar
```

```
tar -xvf <patchfile>.tar
```

```
ls
```

Log out of the CBM/NPM as cbmpat.

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

| If                                                                                                                       | Perform                 |
|--------------------------------------------------------------------------------------------------------------------------|-------------------------|
| the load you are upgrading from is CBM00090 (see item <a href="#">A</a> in the <a href="#">Prereq items</a> table)       | step <a href="#">15</a> |
| the load you are upgrading from is any other load (see item <a href="#">A</a> in the <a href="#">Prereq items</a> table) | step <a href="#">34</a> |

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

| If                                                                                             | Do                      |
|------------------------------------------------------------------------------------------------|-------------------------|
| Item <a href="#">L</a> = NO in the <a href="#">Prereq items</a> table (NPM is not on this CBM) | step <a href="#">16</a> |
| Item <a href="#">L</a> = YES in the <a href="#">Prereq items</a> table (NPM is on this CBM)    | step <a href="#">17</a> |
| you didn't receive any patches for either product                                              | step <a href="#">37</a> |

- 16** Log in as root to the NPM cluster IP address:

```
ssh -l root <NPM cluster IP address>
```

where

**<NPM cluster IP address>**

is the NPM cluster IP address in item [M](#) in the [Prereq items](#) table.

- 17** Check to see if the /data/npm\_patches directory exists:

```
ls -d /data/npm_patches
```

| If                          | Do                      |
|-----------------------------|-------------------------|
| the directory doesn't exist | step <a href="#">18</a> |
| the directory exists        | step <a href="#">19</a> |

- 18** Make a directory to hold the patch files you want to install:

```
mkdir /data/npm_patches
```

- 19** For each uncompressed and untarred patchfile directory in /export/home/cbmpat, copy the patches to the /data/npm\_patches directory:

```
cp /export/home/cbmpat/<patchfile dir>/*.patch /data/npm_patches
```

where

**<patchfile dir>**

is the one of the two new directories created by the tar command you entered in step [13](#).

**Note:** There is a space between patch and /data in the command shown above.

- 20** Change permissions for the patch directory and for the files in the directory:

```
chmod -R 777 /data/npm_patches
```

- 21** Determine if a tmp directory exists in the npm directory by typing

```
ls -d /data/npm/tmp
```

and pressing the Enter key.

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

| <b>If</b>                      | <b>Do</b>               |
|--------------------------------|-------------------------|
| a tmp directory does not exist | step <a href="#">23</a> |
| otherwise                      | step <a href="#">24</a> |

- 23** Make a temporary directory for the patchlist file:

```
mkdir /data/npm/tmp
```

- 24** Change the permissions for the temporary directory:

```
chmod 777 /data/npm/tmp
```

- 25** Create the .patchlist file for all the patches that are on the CD in the temporary directory by typing

```
find /data/npm_patches -name '*.patch' > /data/npm/tmp/current.patchlist
```

- 26 Verify the NPM server application is running by typing  
**servquery -status -group NPM**

**If the NPM server application is**

|             |                         |
|-------------|-------------------------|
| running     | step <a href="#">28</a> |
| not running | step <a href="#">27</a> |

- 27 Start the NPM server application:  
**servstart NPM**
- 28 Access the directory:  
**cd /data/npm/tmp**
- 29 Access the NPM command line user interface (CLUI):  
**npm**
- 30 When prompted, enter your user ID and password.  
**Note:** Do not change directories.
- 31 Retrieve the patch files copied from the CD:  
**getpatch current.patchlist**  
**Note:** Ignore the following error message which may appear if an older load cannot verify a patch for a newer load:
- ```
Error: Patch file
/data/npm/patch_upgrade/lex83o9s.ptchoamp
cannot be verified. Copying to golden
directory.
```
- 32 Exit the NPM CLUI:
quit
- 33 Go to step [37](#)
- 34 Use the following table to determine your next step.

If	Do
Item L = NO in the Prereq items table (NPM is not going to reside on the CBM)	step 16

If	Do
Item L = YES in the Prereq items table (NPM is going to reside on the CBM)	step 35
you didn't receive any patches for either product	step 37

- 35** For each patchfile directory, copy the patches to the /data/npm_patches directory:
- ```
cp <patchfile dir>/*.patch /data/npm_patches
```
- where
- <patchfile dir>**  
is the one of the two new directories created by the tar command you entered in step [13](#).
- 36** Change permissions for the patch directory and for files in the directory:
- ```
chmod -R 777 /data/npm_patches
```
- 37** This procedure is complete. Return to the step that directed you to this step.

Performing an inactive CBM 850 upgrade post-reboot sanity check

Performing an inactive CBM 850 upgrade post-reboot sanity check

At your workstation

- 1 Wait until the upgraded server fully comes up from the boot before you proceed.
- 2 Log back in to the server through the console, using the root user ID and password.
- 3 Verify that your system is running the SN09U version of the SPFS as follows:

Note: You must be the root user to execute the steps that follow.

- a Access the command line interface by typing
`cli`
and pressing the Enter key.
- b Enter the number next to the View option in the menu.
- c Enter the number next to the sspfs_soft option in the menu.
- d Note the SPFS version that displays.

If the SPFS version is	Do
09.x	step 4
anything else	contact your next level of support

- 4 When prompted, enter x to exit each level until you exit the command line interface.
- 5 Enter the following command:

ubmstat

In the system output, determine whether the inactive node is in a ClusterIndicatorSTBY (standby) state. Re-run this command until the inactive node is shown to be in the standby state. If after re-running the command several times the node doesn't appear to be in standby state, contact your next level of support.

Note: For this command, and for the remaining commands shown in this procedure, you may need to re-run the command because the system requires time to become

stable. If after re-running the command several times the desired result is not achieved, contact your next level of support.

- 6 Enter the following command to determine whether all filesystems are in a STANDBY normal UP clean (standby) state:

udstat

Re-run this command until all filesystems are shown to be in the standby state. If after re-running the command several times the filesystems do not appear to be in standby state, contact your next level of support.

- 7 Enter the following command to determine whether SAM is running:

appctrl -p

In response the system should display Command Complete. Re-run this command until this response is displayed, indicating that SAM is running. If after re-running the command several times Command Complete does not display, contact your next level of support.

- 8 You have completed this procedure. Return to step [10](#) of [Upgrading the CBM](#)

Performing an active CBM 850 upgrade sanity check

Performing an active CBM 850 upgrade sanity check

At your workstation

- 1 Wait until the upgraded server fully comes up from the boot before you proceed.
- 2 Log back in to the server using the root user ID and password.
- 3 Verify that your system is running the SN09U version of the SPFS as follows:

Note: You must be the root user to execute the steps that follow.

- a Access the command line interface by typing
cli
and pressing the Enter key.
- b Enter the number next to the View option in the menu.
- c Enter the number next to the sspfs_soft option in the menu.
- d Note the SPFS version that displays.

If the SPFS version is	Do
09.x	step 4
anything else	contact your next level of support

- 4 When prompted, enter x to exit each level until you exit the command line interface.
- 5 Enter the following command:

ubmstat

From the system results that display, determine whether the active node is in a ClusterIndicatorACT state. Re-run this command until the active node is shown to be in the active state. If after re-running the command several times the node doesn't appear to be in active state, contact your next level of support.

Note: For this command, and for the remaining commands shown in this procedure, you may need to re-run the command because the system requires time to become stable. If after re-running the command several times the

desired result is not achieved, contact your next level of support.

- 6 Enter the following command to determine whether all filesystems are in a ACTIVE normal UP clean state:

udstat

Re-run this command until all filesystems are shown to be in the active state. If after re-running the command several times the filesystems do not appear to be in active state, contact your next level of support.

- 7 Enter the following command to determine whether SAM is running:

appctrl -p

In response the system should display Command Complete. Re-run this command until this response is displayed, indicating that SAM is running. If after re-running the command several times Command Complete does not display, contact your next level of support.

- 8 Display all CBM software applications that are currently off-line:

appctrl -q all | grep -i offl

Compare any applications that are offline (OFFL) with the list of offline applications that you recorded earlier in item AE of the Prereq items table. For any that were previously in the OFFL state, offline these applications now using the cbmmtc appl maintenance interface.

- 9 Enter the following command to ensure that all applications on the CBM are in service or are offline:

appctrl -q all

Re-run this command until all applications are shown to be either in the INSV (in service) or in the OFFL (offline) state.

- 10 Enter the following command to determine whether any CBM faults exist:

querycbm flt

Re-run this command until any faults are cleared.

Note: The following logs may display:

** SPFS310 Disk or disk mirroring errors ...

** SPFS310 Abnormal Cluster State ...

Both of these logs should be ignored.

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



Multiservice Data Manager upgrade

This procedure enables you to upgrade Multiservice Data Manager (MDM) servers.

New in this release

Feature changes

In SN09U, both Solaris-based and SPFS-based servers can host the MDM software application. Solaris is supported on a SunFire V480 or Sun Netra t1400 server. SPFS is supported only on a Sun Netra 240 server.

Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U

Server types

The following server types are supported by this upgrade:

- Sun Fire V480 (NOC-based MDM deployment model)
- Sun Netra t1400 (NOC-based MDM deployment model)
- Sun Netra 240 (CO-based MDM and NOC-based MDM deployment models)

Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade

Time to complete an upgrade

The following table lists the tasks to upgrade MDM software and the estimated time to complete each task.

Table 1 Estimated time to complete a software upgrade

Task	Time
Preparing for the upgrade	60 minutes
Upgrading the software	40 minutes
Completing the upgrade	60 minutes
Total estimated upgrade time	2 hours 40 minutes
Performing a rollback	60 minutes

System Performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade.

System limitations during upgrade

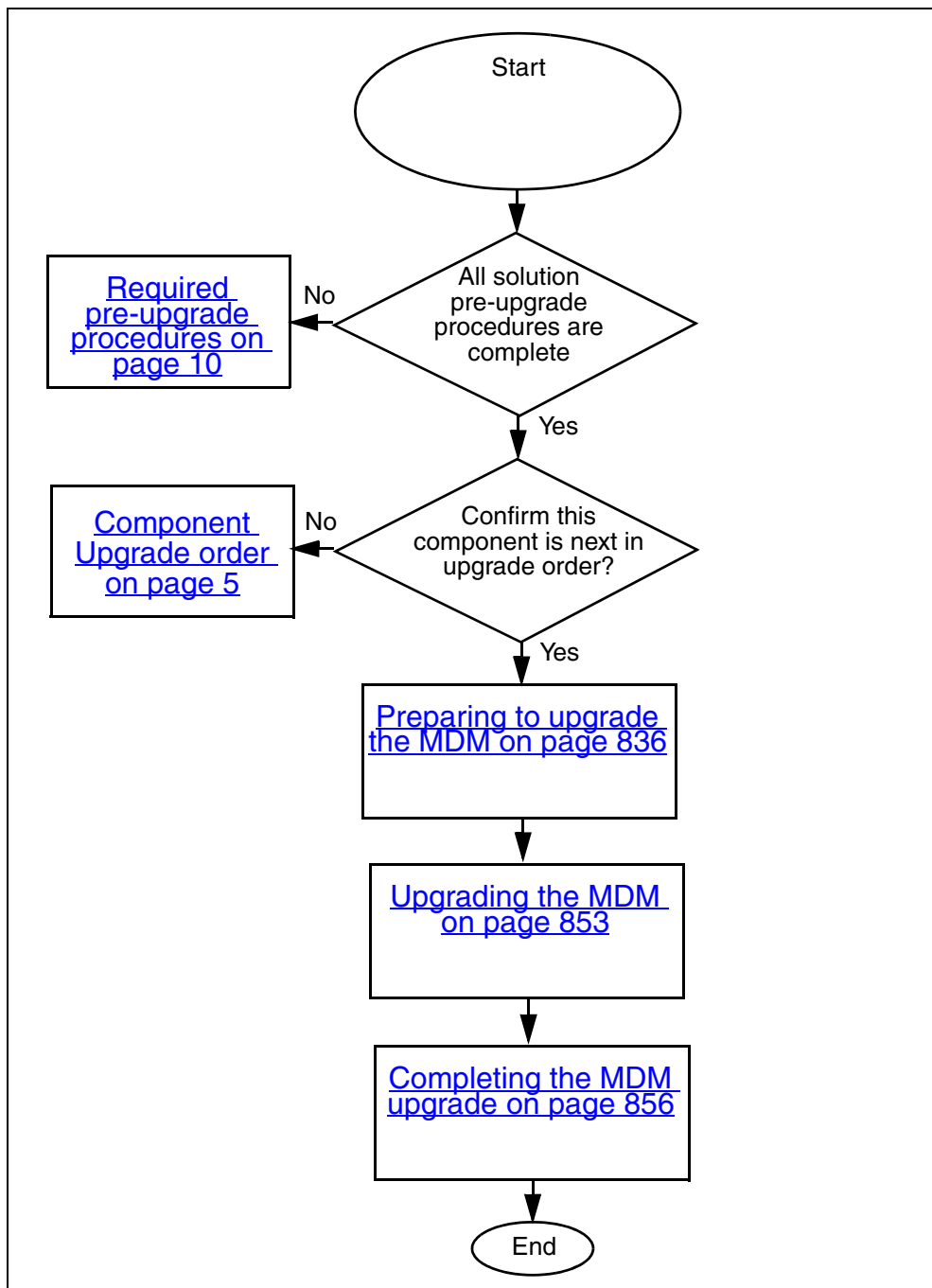
During a software upgrade, the system prohibits the following actions:

- System administration
 - adding, deleting, or modifying users
 - setting time of day
 - changing passwords
- System management
 - modifying the system name
 - adding or deleting system nodes
 - modifying the IP addresses

MDM upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

MDM upgrade tasks



Preparing to upgrade the MDM

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

Before starting the upgrade, confirm that you have met the following prerequisites.

- GUI-based applications launched through a remote session must be launched on a trusted workstation. To start a trusted session, or to learn more about the MDM toolset, operator client interfaces, and processes that are common to all MDM tools, refer to NTP 214-6001-122, *Using Toolset and Operator Client Interfaces*.
- Upgrade MDM servers before upgrading the MSS 15000/MG 15000 nodes they manage. MDM software is backwards compatible and can manage the current and previous releases of MSS/MG, but is not necessarily forward compatible.
- To ensure that one MDM server remains in contact with the CS 2000 Core Manager, CBM, Integrated EMS, or the OSS at all times and continues to provide OAM&P information, isolate and completely upgrade one server while the other server remains fully operational. Following the successful upgrade of the first server, isolate and upgrade the second server using the same procedure.
- Ensure both MDM servers are sane and operating without any errors by doing the following:
 - Ensure both servers are in service, operating in a redundant capacity, and capable of supporting traffic and network management functions with no major or critical alarms.
 - Check the Alarm Display and the System Log Display tools and ensure there are no serious or unexplained logs or alarms.
 - Ensure that the second server (the one not being upgraded) is sane before proceeding with the upgrade.
 - If using disk mirroring, ensure it is enabled on both servers and operating without any errors.
- The baseline configuration must be achieved before performing an upgrade.

See [MDM deployment considerations on page 837](#) and [Solution level migration logistics on page 840](#) for more information regarding standalone/server and client-sets baseline configuration.

The [MDM feature baseline on page 841](#) lists the features that must be activated before you upgrade.

- If you have deployed client-sets and are not re-deploying them as MDM Admin servers, upgrade them before completing the upgrade.
- If you have not deployed MDM servers according to the standard deployment, refer to the Multiservice Data Manager (MDM) base documentation and release notes for additional information when performing the upgrade.
- If you are upgrading Solaris-based MDM servers from CD-ROM, you must have an X11 terminal with IP connectivity to the Sun Fire V480 or Sun Netra t1400 server that you are upgrading. If using a CD to perform the upgrade, you must have access to the CD-ROM drive. If upgrading from software that you download from Nortel Electronic Software Distribution (ESD) page, you only need access to the downloaded file. You must also have access to a text editor, such as UNIX vi, so that you can edit various files during the upgrade.
- Review the *Multiservice Data Manager Release 15.4 Supplement*. The release supplement describes the features that are new to the software release and includes information on differences in functionality and capability from the old release to the new release. It is essential that you understand the potential impacts before beginning the upgrade.
- If you have deployed firewalls in your network, you need to understand which sockets the firewalls have been deployed on. For more information, see NN10225-512 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-AAL2*.
- You must have MG 15000 patch distribution schedule information that includes:
 - the time at which MG 15000 patch updates are put on the SDSs
 - the time intervals, which include the time of week, time of day, start, and end times, scheduled for MG 15000 patch applications to the switches
- You must have IP addresses for the CS 2000 Core Manager, CBM, or Integrated EMS.

MDM deployment considerations

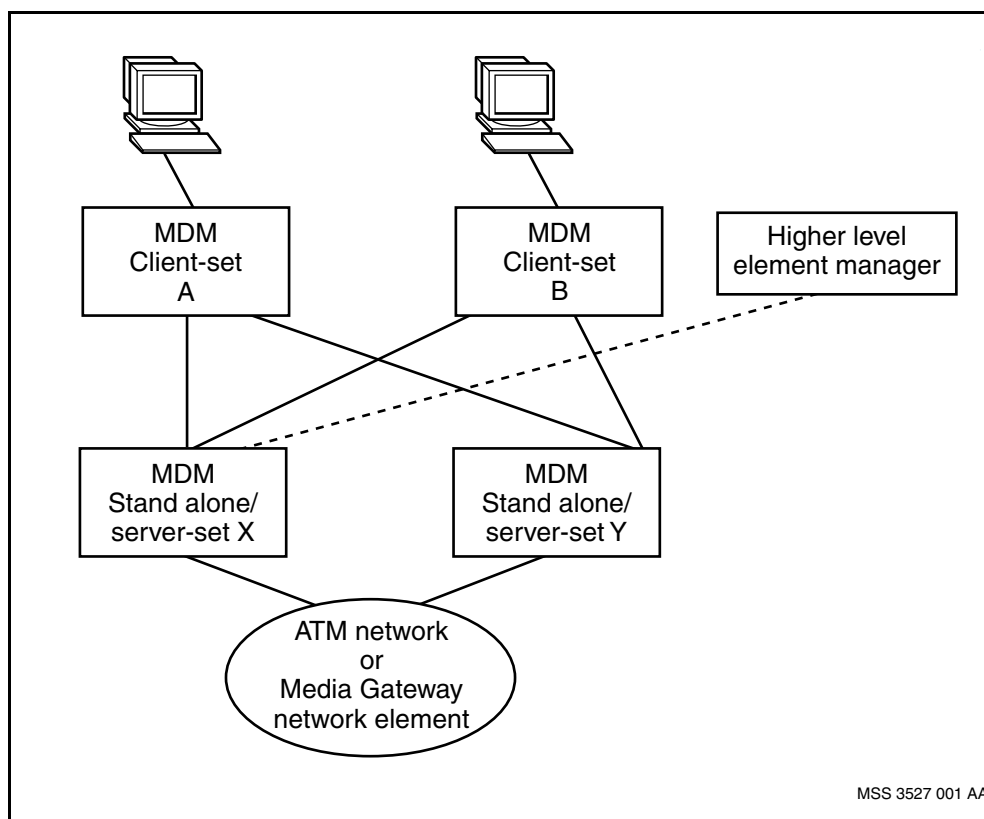
Since Nortel MDM can be deployed in many ways, upgrading cannot be viewed simply from the perspective of upgrading a single server but must be viewed from the perspective of upgrading MDM in a Carrier

Voice over IP deployment. Some common Carrier Voice over IP deployment options are:

- stand-alone/server-set (combined server and client-sets)
- separate client-sets
- distributed server and client-sets
- MDM Admin Server (VOA only)
- MDM Server (VoIP only)

[Typical client-set/standalone/server-set deployment on page 838](#) illustrates the common deployments. Note that the server and client-sets are deployed as a redundant pair.

Typical client-set/standalone/server-set deployment



Standalone/server-sets

Standalone/server-sets support the main server processes that allow MDM to perform surveillance and gather network data (fault and/or performance). They are usually run without a monitor and keyboard.

Client-sets

Client-sets host the servers that allow operators to view the surveillance information and network data, and perform provisioning. They are dependent on the standalone/server-sets for the acquisition of surveillance, network data, and communication to MDM nodes. Client-sets can host operator desk tops (remote users) as indicated in [Typical client-set/standalone/server-set deployment on page 838](#).

Separate standalone/server and client-sets

While separate server and client-sets are not mandatory to Nortel MDM deployment, they do optimize performance in a large network.

Note: A single MDM supporting a VoA and VoIP (a tri-modal) configuration is not a Carrier Voice over IP supported configuration.

MDM Servers in VoIP

MDM Servers in a VoIP solution provide web access to Operator Client environment from remote operator desktops and X11 access to MDM Toolset environment. They support the main server processes for performing surveillance, gathering network data (fault, security, and/or performance), and provide network data to higher level management systems. They also provide an interface to the IEMS central AAA service and host the Java Web Start (JWS) server for the Operator Client user environment.

MDM Admin Servers in VoA

MDM Admin Servers in a VoA solution provide web access to Operator Client environment from remote operator desktops and X11 access to MDM Toolset environment. They support the main server processes for performing surveillance, gathering network data (fault, security, and/or performance). They also host the central AAA service and the Java Web Start (JWS) server for the optional Operator Client user environment.

If you have decided to deploy Operator Client (OC) in your VoA network, client-sets can be re-deployed as MDM Administration Servers (MDM Admin Servers). The MDM Admin Servers host the full set of MDM servers found on the MDM server-set and provide a base for the security and GUI servers of the OC feature. The MDM Admin Servers host the following new servers that support OC with centralized user administration: the Sun ONE Identity Server (IS), the Sun ONE Directory Server (DS), and the RADIUS server. These Operator Client servers are installed with the traditional MDM servers.

Updating MDM license files

Before you can run MDM server software, you need a license password and a customer identifier. This comes with your MDM server upgrade

CD. For information on how to upgrade and configure your new server license, see “Software licenses for MDM (mandatory)” in *Nortel Multiservice Data Manager Software Installation and Initial Configuration*, 241-6001-100. If you do not have the license, you will need to order one. Contact your Nortel Sales Representative for additional information.

MDM15.4 is available as an Entry or Comprehensive package. Other MDM optional features such as MDP are offered as well.

The MDM Operator Client and centralized user management is an optional feature. The number of Operator Client sessions and active Sun ONE Identity Server (IS) users dictates sizing requirements. You can order a 10 Client/100 user package, a 50 Client/500 user package, or a 100 Client/1000 user package. A license is required for Operator Client User Administration.

In previous releases, the MDM Entry and Comprehensive packages included the software CD-ROMs and the Electronic Software Download (ESD) entitlement in addition to the license component. In this release, the Entry and Comprehensive packages now only include the License RTU component. A separate order code for the MDM Software CD-ROM set is provided and must be ordered separately if required. Electronic Software Distribution will only be available to users with valid support agreements

Software license keys are provided based on the features ordered, and on an individual site basis. Users migrating from MDM 14.3 or earlier must obtain a new key for MDM R15.x installations. Keys for previous releases will not work. The Carrier VoIP SN09U Security Software packages contains security software and functionality and must be ordered separately. See the *Multiservice Data Manager Release 15.4 Supplement* for more information on packaging and licensing.

Solution level migration logistics

Before performing an upgrade, you must consider:

- redundancy (stand-alone/server-set, client-sets)
- impact on the OSS and the higher level element manager (this can be the CS2000 Core Manager (VoA) or Integrated EMS (VoIP))
- order of migration of the server vs.client-sets

Note: If an MDM server pair is managing multiple offices, you are not required to migrate all offices prior to the upgrade of the MDM server pair.

Redundancy ensures that the network can be observed and network data collected. Redundancy is unavoidably lost during an upgrade when the server is rebooted (applies to either the server or client-set). At that point the system is running in simplex mode. To minimize the risk of losing the ability to observe the network and collect data, upgrade only one of the redundant servers (both server and client-sets) at any given time.

A Nortel MDM feature can possibly impact the OSS and the higher level element manager. Software changes may need to be addressed at the OSS level to ensure that incompatibilities do not exist and prevent the OSS and the higher level element manager from losing network visibility.

The general rule when performing migrations is to migrate the most north-bound system first. Migrate systems in the following order:

- OSS applications
- CS 2000 Core Manager or CBM
- Integrated EMS
- client-set A
- client-set B
- Standalone/server-set A
- Standalone/server-set B
- Multiservice Switch and/or Media Gateway nodes

Migrate the client-sets before the standalone/server-sets because MDM is backwards compatible but not forwards compatible. Home the operator desktops to the client that is not being migrated to prevent any loss of visibility to the desktops. Migrate one client-set at a time.

When migrating a standalone/server-set, ensure that the client-sets are not homed into that server-set, otherwise you will see an outage because clients do not dynamically switch from one client-set to another. This way, you can service select a client-set that is not actively being migrated. Migrate one standalone/server-set at a time.

MDM feature baseline

MDM features can be Carrier VoIP-specific, or not specific to Carrier Voice over IP. This section lists the features relevant to Carrier Voice over IP.

For Media Gateway customers outside these deployments, you must activate the features listed in table [MDM feature baseline on page 841](#). This table:

- lists the features that must be activated (appropriate to individual deployments)
- identifies the applicability of the feature to the server vs. client-sets
- identifies where the feature originated from: MDM base or Carrier Voice over IP

Activate these features on MDMs in all Media Gateway installations to ensure compatibility with the MDMs managing the MG 15000. You must establish this baseline before you can upgrade the MDM.

MDM baseline feature list

Feature Name	Required for Solution?		Server or Client-set feature	Originator
VoA VoIP				
Core functionality:				
MDM Patched to current level	Y	Y	server, client-set	MDM base
client-set servers	N	N	client-set	MDM base
Redundancy (server-set)	Y	Y	server, client-set	MDM base
Redundancy (client-sets- if deployed)	N	N	server, client-set	MDM base
Software Distribution Site	Y	Y	server (simplex)	MDM base
Data Collection (MDP)	Y	Y	server (simplex)	MDM base
Generating and setting secure passwords for MDM servers (FMDR, PMSP) password encryption	Y	Y	server	MDM base
Secure FTP	Y	Y	server	MDM base

MDM baseline feature list

Feature Name	Required for Solution?		Server or Client-set feature	Originator
	VoA	VoIP		
Multiservice Switch backup and Restore	Y	Y	server	MDM base
Network Model & Viewer configuration	Y	Y	server	MDM base
MDP Administration enhancement	Y	Y	server	MDM base
Shelf View enhancement	Y	Y	client-set	MDM base
Server Administration enhancements	Y	Y	server	MDM base
Operator client (OC)	N		MDM Admin server, Operator Client	MDM base
Centralized user management	Y if OC is used			MDM base
Security Audit logging	Y	Y	server	MDM base
SCC2 SALs	Y	Y	server	Carrier VoIP
Nodal Provisioning Template Audit	Y	Y	server	Carrier VoIP
OS hardening	N			MDM base
SSH	N			MDM base
IPSec	N			MDM base
HSM Migration (UA-IP MG)	n/a	Y	server	Carrier VoIP
MDM auto-patch of MSS/MG nodes	Y	Y	server	MDM base
Additional features:				
XNTP Support	Y	Y	server, client-set	MDM base

MDM baseline feature list

Feature Name	Required for Solution?		Server or Client-set feature	Originator
	VoA	VoIP		
Network Time Protocol Support	Y	Y	server, client-set	MDM base
FDTM Succession configuration	Y	Y	server	Carrier VoIP
Support for Seasonal time change	N	N	server	Carrier VoIP
pserver process	Y	Y	server	MDM base
NP template installation	Y	Y	server	MDM base
Multiservice Switch 15000 Configuration Model Server	Y	Y	server	MDM base
MDP to make BDF files accessible	Y	Y	server	MDM base
MDP file prober collection times	Y	Y	server	MDM base
Succession Enabling	Y	Y	client-set	Carrier VoIP
Note: Enabling Succession also ensures that the SASM and SISM tools appear in the MDM toolset.				
PMs (pmsp & supporting directory structures)	Y	Y	server	Carrier VoIP
real-time alarm collection (rtac)	Y	Y	server	MDM base
File mover for BDF files	Y	Y	server	MDM base
Shared memory and semaphore setting	Y	Y	server	MDM base
Support for 5 min. PMs	Y	Y	server	Carrier VoIP
SASM	Y	N	server	Carrier VoIP

MDM baseline feature list

Feature Name	Required for Solution?		Server or Client-set feature	Originator
	VoA	VoIP		
Succession Release Name GUI	Y	Y	server	Carrier VoIP
Solaris 9 Upgrade	Y	Y	server, client-set, MDM Admin server, Operator client (UNIX)	Carrier VoIP
Note: Perform the Solaris 9 upgrade after upgrading MDM.				

Action

Follow the link associated with the appropriate release for your upgrade.

- [Preparing to upgrade an MDM server from SN08 to SN09U on page 845](#)
- [Preparing to upgrade an MDM server from SN09 to SN09U on page 848](#)

Preparing to upgrade an MDM server from SN08 to SN09U**At your PC**

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

If	Do
you are using Exceed for remote access to the MDM	step 2
you are not using Exceed for remote access to the MDM	step 12

- 2 Start the Exceed Xconfig application. Reference [Configuring Exceed for an upgrade on page 1634](#)
- 3 Launch Exceed in passive mode to run in the background on your PC
- 4 Telnet or SSH to the MDM and ensure that the DISPLAY environment variable is set. When X11Forwarding is being used

with SSH, the DISPLAY variable is set automatically. Otherwise set the DISPLAY variable back to your PC

DISPLAY=<your PC's IP address>:0.0

- 5 The user is now able to launch any X11 applications and have it displayed on the PC desktop.

From the MDM server

- 6 For deployments using central user authentication and authorization for the MDM server with IEMS, restore the configuration files to the pre-secure version created during the initial installation by performing the following steps. For additional detail, refer to Disabling central user authentication and authorization for an MDM server, in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*.
 - a Create a copy of the current secure configuration:

```
cp /etc/pam.conf /etc/pam.conf_postsecurity
cp /etc/nsswitch.conf /etc/nsswitch.conf_postsecurity
```
 - b Disable the PAM interface:

```
cp /etc/pam.conf_presecurity /etc/pam.conf
cp /etc/nsswitch.conf_presecurity /etc/nsswitch.conf
```
- 7 Perform an MDM backup. For detailed steps, refer to [Performing an MDM backup on page 860](#)
- 8 Unharden the OS if required. This step is not mandatory, but if you wish to perform this step, it should be performed at this point in the procedure. For detailed steps, refer to Disabling MDM platform hardening, in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*.
- 9 Verify the state of disk space available on the server. For detailed steps, refer to [Ensuring that there is enough disk space on the servers on page 864](#)
- 10 Ensure the SPFS or non-SPFS OS software is at the latest maintenance release level for the release you are currently

running and is patch current. For detail steps, refer to [Verifying Solaris and its patch level on page 866](#)

If	Do
For detailed steps on viewing the SPFS release on the server	refer to the procedure Determining the SPFS software MNCL level on page 424
To view the Solaris release level on non-SPFS based platforms	refer to the procedure Verifying Solaris and its patch level on page 866

11 Verify the status of the currently-installed MDM software and its patches.

- a** Check the currently-active software version by entering the following on the command line:

`/opt/MagellanNMS/system/inst/nmsLinks`

- b** Verify that the MDM patches are up to date for the current release. Install any MDM patches required for the current release at this time. For detailed steps, refer to [Installing MDM patches on page 895](#)

Note: If it is determined that patches need to be downloaded for installation, refer to [Downloading MDM patches on page 871](#)

- c** Verify that MDM servers and processes are running. For detailed steps, refer to [Verifying that MDM servers and processes are running on page 882](#)
- d** Verify that the MDM toolset is functioning. For detailed steps, refer to [Verifying that the MDM toolset is functioning on page 884](#)

12 Use the following table to determine your next step.

If	Do
you are installing the software using CDs	step 14
you are installing software downloaded from the Nortel web site	step 13

13 Retrieve the MDM software for the release to which you are upgrading. For detailed steps, refer to [Retrieving MDM software on page 868](#)

- 14 Download any MDM patches required for the release to which you are upgrading. For detailed steps, refer to [Downloading MDM patches on page 871](#)
- 15 Set the shared memory size. For detailed steps, refer to [Setting the shared memory size on page 873](#)
- 16 This procedure is complete. Return to [MDM upgrade tasks on page 835](#)

Preparing to upgrade an MDM server from SN09 to SN09U

At your PC

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

If	Do
you are using Exceed for remote access to the MDM	step 2
you are not using Exceed for remote access to the MDM	step 12

- 2 Start the Exceed Xconfig application. Reference [Configuring Exceed for an upgrade on page 1634](#)
- 3 Launch Exceed in passive mode to run in the background on your PC
- 4 Telnet or SSH to the MDM and ensure that the DISPLAY environment variable is set. When X11Forwarding is being used with SSH, the DISPLAY variable is set automatically. Otherwise set the DISPLAY variable back to your PC
DISPLAY=<your PC's IP address>:0.0
- 5 The user is now able to launch any X11 applications and have it displayed on the PC desktop.

From the MDM server

- 6 For deployments using central user authentication and authorization for the MDM server with IEMS, restore the configuration files to the pre-secure version created during the initial installation by performing the following steps. For additional detail, refer to Disabling central user authentication and authorization for an MDM server, in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and*

Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements.

- a Create a copy of the current secure configuration:

```
cp /etc/pam.conf /etc/pam.conf_postsecurity
cp /etc/nsswitch.conf
/etc/nsswitch.conf_postsecurity
```

- b Disable the PAM interface:

```
cp /etc/pam.conf_presecurity /etc/pam.conf
cp /etc/nsswitch.conf_presecurity
/etc/nsswitch.conf
```

- 7 For an SPFS-based server, It is recommended that you perform a complete SPFS filesystem backup now. This backup will include a backup of the MDM data and configuration files.

If	Do
you wish to backup your SPFS-based server	Performing a backup of file systems on an SPFS-based server on page 379 When the backup is complete, go to step 9
you do not wish to backup your SPFS-based server	step 8

- 8 For non-SPFS based platforms, or if you previously opted not to perform the complete SPFS filesystem backup, perform an MDM backup. For detailed steps, refer to [Performing an MDM backup on page 860](#)
- 9 Unharden the OS if required. This step is not mandatory, but if you wish to perform this step, it should be performed at this point in the procedure. For detailed steps, refer to Disabling MDM platform hardening, in NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*.

10 Use the following table to determine your next step.

If	Do
you are upgrading the MDM on an SPFS-based platform	step 11
you are upgrading the MDM on a non-SPFS-based platform	step 25

11 For SPFS-based platforms only, upgrade the Server Platform Foundation Software (SPFS). For detailed steps, refer to [Upgrading SPFS software on page 403](#).

12 Verify that the Patch Server Element (PSE) is operational. Check PSE status:

```
/opt/NTpse/pse status
```

13 Use the following table to determine your next step.

If	Do
PSE is running	step 24
PSE is not running	step 22
PSE is not configured	step 14

14 Enter the command line interface (cli) tool:

```
cli
```

15 Enter the number next to the Configuration option in the menu.

16 Enter the number next to the Succession Element Configuration option in the menu.

17 Enter the number next to the PSE Application Configuration option in the menu.

18 Enter the number next to the Configure PSE option in the menu.

19 In response to the prompt, enter the primary/cluster IP address of the NPM server.

20 In response to the prompt, enter y to confirm the IP address.

21 Enter x to exit each level until you have exited from the cli tool.

22 Start the PSE server:

```
/opt/NTpse/pse start
```

- 23 Verify that the server has started. If the server does not start, contact your next level of support.
- /opt/NTpse/pse status**
- 24 Ensure that the SPFS is patch-current. For detailed steps, refer to [Applying patches using the NPM on page 2319](#)
- 25 Verify the state of disk space available on the server. For detailed steps, refer to [Ensuring that there is enough disk space on the servers on page 864](#)
- 26 Verify the status of the currently-installed MDM software and its patches.
- a Check the currently-active software version by entering the following on the command line:
- /opt/MagellanNMS/system/inst/nmsLinks**
- b Verify that the MDM patches are up to date for the current release. Install any MDM patches required for the current release at this time. For detailed steps, refer to [Installing MDM patches on page 895](#)
- Note:** If it is determined that patches need to be downloaded for installation, refer to [Downloading MDM patches on page 871](#)
- c Verify that MDM servers and processes are running. For detailed steps, refer to [Verifying that MDM servers and processes are running on page 882](#)
- d Verify that the MDM toolset is functioning. For detailed steps, refer to [Verifying that the MDM toolset is functioning on page 884](#)
- 27 Use the following table to determine your next step.

If	Do
you are installing the software using CDs	step 29
you are installing software downloaded from the Nortel web site	step 28

- 28 Retrieve the MDM software for the release to which you are upgrading. For detailed steps, refer to [Retrieving MDM software on page 868](#)

- 29** Download any MDM patches required for the release to which you are upgrading. For detailed steps, refer to [Downloading MDM patches on page 871](#)
- 30** Set the shared memory size. For detailed steps, refer to [Setting the shared memory size on page 873](#)
- 31** This procedure is complete. Return to [MDM upgrade tasks on page 835](#)

Upgrading the MDM

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

You have completed [Preparing to upgrade the MDM on page 836](#)

ATTENTION

Install Nortel Multiservice Data Manager (MDM) and MDP software packages using the MDM Installer tool. Do not use Solaris software package tools.

The InstallAnywhere program removes files that need to be removed before loading the new software. The system retains the previous version of MDM software on the server as a back up while installing the new version.

MDM configuration data is persistent. As a result, you will not lose your configuration data when MDM packages are deleted. For more information about installing MDM software, see *Nortel Multiservice Data Manager Software Installation and Initial Configuration*, 241-6001-100.

Action

Follow the link associated with the appropriate release for your upgrade.

- [Upgrading an MDM server from SN08 to SN09U on page 853](#)
- [Upgrading an MDM server from SN09 to SN09U on page 855](#)

Upgrading an MDM server from SN08 to SN09U

From the MDM server

- 1 Install the MDM software. For detailed steps, refer to procedure [Installing MDM software on page 887](#)
- 2 Install any MDM patches for the new release. For detailed steps, refer to procedure [Installing MDM patches on page 895](#)

3 Use the following table to determine your next step.

If	Do
the Solaris OS is already at release level Solaris 9	step 4
the Solaris OS is not already at release level Solaris 9	step 5

- 4** Activate new features for MDM for SN09U. For detailed steps, refer to procedure [Activating new features for MDM when upgrading from SN08 to SN09U on page 900](#)
- 5** Set the solution release name. Refer to [Setting the solution release name identification on page 905](#)
- 6** This procedure is complete. Return to [MDM upgrade tasks on page 835](#)

Upgrading an MDM server from SN09 to SN09U

From the MDM server

- 1 Install the MDM software. For detailed steps, refer to procedure [Installing MDM software on page 887](#)
- 2 Install any MDM patches for the new release. For detailed steps, refer to procedure [Installing MDM patches on page 895](#)
- 3 Activate new features for MDM for SN09U. For detailed steps, refer to procedure [Activating new features for MDM when updating from SN09 to SN09U on page 899](#)
- 4 Set the solution release name. Refer to [Setting the solution release name identification on page 905](#)
- 5 This procedure is complete. Return to [MDM upgrade tasks on page 835](#)

Completing the MDM upgrade

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

You have completed [Upgrading the MDM on page 853](#)

You must have access to a text editor, such as Unix vi, on the terminal connected to the servers so that you can open various files.

Action

Follow the link associated with the appropriate release for your upgrade.

- [Completing the upgrade of an MDM server from SN08 to SN09U on page 856](#)
- [Completing the upgrade of an MDM server from SN09 to SN09U on page 858](#)

Completing the upgrade of an MDM server from SN08 to SN09U

From the MDM server

- 1 Verify the status of the currently-installed MDM software.
 - a Verify that MDM servers and processes are running. For detailed steps, perform [Verifying that MDM servers and processes are running post-migration on page 897](#)
 - b Verify that the MDM toolset is functioning. For detailed steps, refer to [Verifying that the MDM toolset is functioning on page 884](#)

Note: If you discover an error and need to fall back to the previous release, refer to [Uninstalling MDM software on page 911](#)

- 2 Ensure that there is enough disk space on the servers for MDM to function properly. For detailed steps, perform [Ensuring that there is enough disk space on the servers on page 864](#)
- 3 Perform an MDM backup. For detailed steps, perform [Performing an MDM backup on page 860](#)
- 4 Restart the syslog daemon.
/etc/init.d/syslog stop

/etc/init.d/syslog start

- 5 If you are upgrading from Solaris 8 to Solaris 9, upgrade to Solaris 9 now. For detailed steps, perform [Upgrading the Solaris operating system on page 875](#)

Note: Upgrading from Solaris 8 to an SPFS-based platform is classified as a greenfield installation rather than an upgrade. In this event, you can move the files backed up in step 3 to a safe location on a separate workstation and replace them following the OS installation.

- 6 Verify the status of the currently-installed MDM software following the OS upgrade.
- a Verify that the MDM servers and processes are running. For detailed steps, perform [Verifying that MDM servers and processes are running post-migration on page 897](#)
 - b Verify that the MDM toolset is functioning. For detailed steps, refer to [Verifying that the MDM toolset is functioning on page 884](#)
- 7 If the OS was upgraded from Solaris 8 to Solaris 9, then the new security features have not yet been activated. Activate new security features now. Refer to *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*, NN10180-612.
- 8 Using the IEMS GUI, update the Device version field of the managed objects hosted on the CMT server to reflect the new software version. The hosted managed objects are as follows:
- under EMS platforms: SPFS platform
 - under Element Managers: MDM
 - under EMS Applications: LMM, TMM, OSSGate, QoS Collector and NPM
- For detailed steps on how to update the software version in the Device Version field, refer to one of the following procedures:
- [Editing and viewing object properties using Java Web Start Client on page 2255](#)
 - [Editing and viewing object properties using Web Client on page 2261](#)
- 9 Accept the upgraded environment by typing
- # /SSPFS_Upgrade.accept**

and pressing the enter key. The execution of this step takes approximately 20 minutes to complete depending on system configuration.

- 10 If you choose to fallback, refer to procedure [Executing a fallback during an SPFS-based server upgrade on page 418](#)
- 11 This procedure is complete. Return to [MDM upgrade tasks on page 835](#)

Completing the upgrade of an MDM server from SN09 to SN09U

From the MDM server

- 1 Verify the status of the currently-installed MDM software.
 - a Verify that MDM servers and processes are running. For detailed steps, perform [Verifying that MDM servers and processes are running post-migration on page 897](#)
 - b Verify that the MDM toolset is functioning. For detailed steps, refer to [Verifying that the MDM toolset is functioning on page 884](#)

Note: If you discover an error and need to fall back to the previous release, refer to [Uninstalling MDM software on page 911](#)
- 2 Ensure that there is enough disk space on the servers for MDM to function properly. For detailed steps, perform [Ensuring that there is enough disk space on the servers on page 864](#)
- 3 For an SPFS-based server, it is recommended that you perform a complete SPFS filesystem backup now. This backup will include a backup of the MDM data and configuration files.

If	Do
you wish to backup your SPFS-based server	Performing a backup of file systems on an SPFS-based server on page 379 When the backup is complete, go to step 5
you do not wish to backup your SPFS-based server	step 4

- 4 Perform an MDM backup. For detailed steps, refer to [Performing an MDM backup on page 860](#)

- 5 Deployments using central user authentication were instructed in the MDM pre-upgrade procedure to disable the PAM interfaces prior to the upgrade. For instructions on how to re-enable the PAM interfaces, refer to Securing user access for the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager network elements, in *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*, NN10180-612.
- 6 Using the IEMS GUI, update the Device version field of the managed objects hosted on the CMT server to reflect the new software version. The hosted managed objects are as follows:
 - under EMS platforms: SPFS platform
 - under Element Managers: MDM
 - under EMS Applications: LMM, TMM, OSSGate, QoS Collector and NPMFor detailed steps on how to update the software version in the Device Version field, refer to one of the following procedures:
 - [Editing and viewing object properties using Java Web Start Client on page 2255](#)
 - [Editing and viewing object properties using Web Client on page 2261](#)
- 7 Accept the upgraded environment by typing
/SSPFS_Upgrade.accept
and pressing the enter key. The execution of this step takes approximately 20 minutes to complete depending on system configuration.
- 8 If you choose to fallback, refer to procedure “Executing a fallback during an SPFS-based server upgrade” in document *ATM/IP Fault Management*, NN10408-900.
- 9 This procedure is complete. Return to [MDM upgrade tasks on page 835](#)

Performing an MDM backup

During the upgrade the contents of the /opt/MagellanMDP/data and the /opt/MagellanMDP/cfg subdirectories can be overwritten. The /opt/MagellanNMS/data and /opt/MagellanNMS/cfg are affected as well. Therefore, you must back up the entire disk partition on which the MDM software resides. If a disk partition backup has not been done recently, back up the directories listed in the table below. Save the indicated directories to a location on another workstation or on a temporary storage device so that if you encounter problems during the upgrade, you can restore the information stored in those directories.

MDM directories to save

Directory	Description
/opt/MagellanNMS/cfg	MDM base software configuration.
/opt/MagellanNMS/data	MDM base software data.
/opt/nortel/EPIC/cfg	Supports the Enhanced MSS Interface Controller.
/opt/nortel/config	Supports the Admin Server
/opt/nortel/data	Supports the Admin Server
/opt/nortel/logs	Supports the Admin Server
/opt/MagellanMDP/cfg	MDP base software configuration. Backup is only required if MDP is installed.
/opt/MagellanMDP/data	MDP base software data. Backup is only required if MDP is installed.

Before performing a backup, remove extraneous data. Refer to [Ensuring that there is enough disk space on the servers on page 864](#) to identify obsolete software and data.

Performing an MDM backup

At the MDM server

- 1 Log in to the MDM workstation as the root user.
- 2 Back up the MDM configuration and data information.
 - a Back up the MDM software configuration files.

cd /opt/MagellanNMS/cfg

```
tar cvfp mdmcfg_<release>.tar ./*
```

```
mv mdmcfg_<release>.tar <safe directory>
```

where

<release> is the MDM software release (for example, 143)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- b** Back up the MDM software data files.

```
cd /opt/MagellanNMS/data
```

```
tar cvfp mdmdata_<release>.tar ./*
```

```
mv mdmdata_<release>.tar <safe directory>
```

where

<release> is the MDM software release (for example, 143)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- c** If this MDM workstation includes the Management Data Provider (MDP) software, back up the MDP software configuration files.

```
cd /opt/MagellanMDP/cfg
```

```
tar cvfp mdpcfg_<release>.tar ./*
```

```
mv mdpcfg_<release>.tar <safe directory>
```

where

<release> is the MDM software release (for example, 143)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- 3** If this MDM workstation includes the Management Data Provider (MDP) software, back up the MDP data files.

```
cd /opt/MagellanMDP/data
```

```
tar cvfp mdpdata_<release>.tar ./*
```

```
mv mdpdata_<release>.tar <safe directory>
```

where

<release> is the MDM software release (for example, 143)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- 4** If this MDM workstation uses MDM 15.1 or above, back up additional MDM software configuration files.

a cd /opt/nortel/config**tar cvfp nortelconfig_<release>.tar ./*****mv nortelconfig_<release>.tar <safe directory>**

where

<release> is the MDM software release (for example, 152)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- b**
- If this MDM workstation uses MDM 15.2 or above, back up additional MDM software data files.

cd /opt/nortel/data**tar cvfp norteldata_<release>.tar ./*****mv norteldata_<release>.tar <safe directory>**

where

<release> is the MDM software release (for example, 152)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- c**
- If this MDM workstation uses MDM 15.2 or above, back up the MDM log files.

cd /opt/nortel/logs**tar cvfp nortellogs_<release>.tar ./*****mv nortellogs_<release>.tar <safe directory>**

where

<release> is the MDM software release (for example, 152)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- 5**
- If this MDM workstation uses MDM 14.1 or above, back up the EPIC configuration files.

cd /opt/nortel/EPIC/cfg**tar cvfp nortelEPICcfg_<release>.tar ./*****mv nortelEPICcfg_<release>.tar <safe directory>**

where

<release> is the MDM software release (for example, 152)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- 6** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Ensuring that there is enough disk space on the servers

Ensure that you have sufficient disk space to accommodate the downloaded software.

Increase the available disk space by removing obsolete MDM software and data. Some of the MDM directories that can contain obsolete software and data are listed in the following table.

Attention: To avoid loss of data required for an upgrade, ensure that you do not remove software or data for the release currently installed.

Obsolete software and data

Directory	Description
Pre-current versions of MDM software	/opt/MagellanNMS/loads/<software_loadname>/
Pre-current Passport data models	/opt/MagellanNMS/cfg/PassportSchema/
Pre-current Network Models	/opt/MagellanNMS/data/model/nmf/
RTAC alarm files	/opt/MagellanNMS/data/rtac/data
Pre-current backup data	/opt/MagellanNMS/data/Backup_Data
MDM software patch temporary files	files located in /tmp

Checking server disk space

From the MDM server

- 1 Log in.
- 2 Determine how much disk space is available on each of the servers:

df -k

The system indicates in kilobytes how much disk space is used in each of the disk partitions.

Note: MDM data directories (/opt/MagellanNMS/data/) should not be part of the root (/) partition. A separate /data partition with a soft-link to /opt/MagellanNMS/data/ or an NFS mount to a separate physical medium is recommended.

- 3 Ensure that adequate disk space is allocated for MDM installation. Typically, 2000 Mb of disk space is required for the software. However, an additional 3000 Mb will temporarily be required to untar the software.
- 4 Compare the space available under / with the value in step 3.
- 5 If you need more disk space on the server, investigate the following strategies:
 - Remove older, unwanted MDM software versions
 - List the software version currently available:
ls /opt/MagellanNMS/loads
 - **Attention:** Before performing the following task, ensure that you do not select any packages whose names begin with NN.

Select loads that are no longer required and enter the following commands, where <release> is the name of the software load you wish to uninstall:

cd /opt/MDM<release>_INST
./uninstall_mdm<release>
 - remove old CSV files
 - remove core files
 - remove bdf files

Note: MDM software configuration is persistent. As a result, you will not lose your configuration when you delete MDM packages.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Verifying Solaris and its patch level

Before beginning the upgrade, determine if the Sun workstation OS is at the right level with the correct patches. Check the *Multiservice Data Manager 15.4 Release Supplement* to determine which Sun OS patches to upgrade. The supplement is available at the Electronic Software Distribution (ESD) page at www.nortel.com.

Verifying Solaris and its patch level

From the MDM server

- 1 Log in.
- 2 Open an xterm session.
- 3 Check what release of OS is currently running on the workstation:

cat /etc/release

An example of a Solaris 8 OS output is as follows:

```
Solaris 8 HW 7/03 s28s_hw3wos_05a SPARC
```

In the example, the OS version is Solaris 8 with a version date of 7/03.

- 4 Compare the output with the Solaris Maintenance Releases as specified in the *Multiservice Data Manager 15.4 Release Supplement*.
- 5 If the OS version is equal to or greater than the OS version as specified in the *Multiservice Data Manager 15.4 Release Supplement*, an upgrade is not required.

If the OS version is less than the version specified in the *Multiservice Data Manager 15.4 Release Supplement*, you must upgrade the OS Maintenance release to the correct version of the specified Solaris OS. Refer to the *Multiservice Data Manager 15.4 Release Supplement* for information on where to find the Solaris Maintenance release software.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Retrieving MDM software

After verifying that the server has sufficient disk space, you can begin to download Nortel MDM software.

Downloading MDM software from Nortel website

One method is to download the required software from Nortel website. When you download the software from this website, a copy of the software is placed in the directory you specify.

Prerequisites

The prerequisites are follows:

- Refer to the software downloads area of Nortel website, www.nortel.com, to determine the software load that you need.
- Download all the software files that belong to the release you require. The software you need to download can be composed of more than one file.

From the MDM server

- 1 Log in.
- 2 Change directories to the / directory: **cd /**
- 3 Create a directory to which you can download the software:
mkdir MDM154
- 4 On the web, go to www.nortel.com.
- 5 In the Support & Training section of the window, select Software Downloads.
- 6 In the Product Family section of the Software Downloads window, select Preside.
- 7 Under the Multiservice Data Manager for Succession PT/UA-AAL1 section, click Software.

Note: This link is used for all solutions, IP and PT/UA-AAL1.

The Software Downloads window opens.

- 8 The loads and patches for the release are identified at www.nortel.com.

Note: Software loads are contained in zip files, while each patch is contained in a single file. The software is found under the Software tab.

- 9 Select the version of the release of the software you want to download. Download the following software:
 - MDM 154 CD1
 - MDM 154 CD2
 - MDM 154 CD3
 - Carrier VoIP SN09 Security Software CD (if required)
- 10 Enter the following directory to indicate where you want the software load files placed: /MDM154.
- 11 When prompted, enter your user name and password for the log in.
- 12 Click Save.
- 13 On the MDM server, change directories to the directory containing the software:
cd /MDM154
- 14 Uncompress the software load file:
uncompress <swload_name>.tar.Z
- 15 Untar the software load file: **tar xvf <swload_name>.tar**
- 16 Repeat step [14](#) through step [15](#) for every software file you downloaded.
- 17 Delete each tar file: **rm -r <swload_name>.tar**
- 18 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Retrieving software from a drop box

Prerequisites

The prerequisites are as follows:

- You need a dropbox and an account with a user name and password. Contact your Nortel customer representative for more information on accessing Nortel website.
- Refer to the software downloads area of the Nortel website (www.nortel.com) to verify that the drop box contains the software files you need to retrieve. If there are no patches listed for this release, then there are no patches currently required for this release.

From the MDM server

- 1 Log in.

- 2** Retrieve the required software files and patches according to your retrieval procedure:
 - MDM 15.4 CD1
 - MDM 15.4 CD2
 - MDM 15.4 CD3
 - Carrier VoIP SN09U Security Software CD (if the MDM Enhanced Security package is ordered)
- 3** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Downloading MDM patches

During an upgrade, you may need to download patches from the Nortel website to the Multiservice Data Manager (MDM) server. When you download the patches from this website, a copy of the patches is placed in the directory you specify.

Prerequisites

The prerequisites are as follows:

- Acquire a dropbox and an account with a user name and password. Contact your Nortel customer representative for more information on accessing Nortel website.
- Refer to the software downloads area of the website www.nortel.com to determine which patches you need to download. Consult the Release Notes for the current release and for the new release to which you are upgrading in order to identify the most current list of patches you require. MDM patches are jumbo patches that include all previous patches. As a result, you only need to download the most current version of a patch.

From the MDM server

- 1 Log in.
- 2 Change directories to the / directory:
cd /
- 3 Create a directory to hold the patches that you download:
mkdir <patch directory>
where
<patch directory>
is the name of a directory you want to create. Ensure that you create a directory to hold patches for the current release and also a directory to hold patches for the release to which you are upgrading. For example, when you are upgrading to release MDM154, a directory named patch153 should be created for the current release, MDM153 and a directory named patch154 should be created for MDM154.
Note: Remove this directory after the patches have been installed.
- 4 On the web, go to www.nortel.com.

- 5 In the Support & Training section of the window, select Software Downloads.
- 6 In the Product Family section of the Software Downloads window, click Preside.
- 7 Under the Multiservice Data Manager for Succession section, click Software.

Note: This link is used for all solutions, IP and PT/UA-AAL1. The Software Downloads window opens.

- 8 Refer to the software downloads area of Nortel website (www.nortel.com) to determine which patches you want to download.
- 9 Download the MDM, MDP, and DVR patches for the release, if they exist. For example, MDM154, MDP154, and DVR 154.
- 10 When prompted, log in.
- 11 Click the file listed beside the File Download heading.
- 12 Enter the following directory to indicate where you want the patch placed:

/<patch directory>

where

<patch directory>

is a directory you created in step [3](#)

- 13 Click Save.
- 14 Repeat steps [12](#) through [13](#) for the other patches you need.
- 15 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Setting the shared memory size

Before beginning the upgrade, set the shared memory size to the value 256.

Setting the shared memory size

From the MDM server

- 1 Log in.
- 2 Check the shared memory size configured on the workstation:
grep shminfo_shmmax /etc/system

If	Do
the value in the system output is equal to or greater than 268435456	Step 6
the value in the system output is less than 268435456	Step 3

- 3 Issue the following command:
/opt/MagellanNMS/system/config/config_sys_shmem 256
The system prompts you to confirm the change in shared memory size.
- 4 Confirm the change:
yes
- 5 If the system prompts you to reboot, do not confirm the reboot.
no
Note: A reboot is required later during the installation; therefore, it is not necessary to reboot at this time.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Upgrading the Solaris operating system

The operating systems on the MDMs must be upgraded from Solaris 8 to Solaris 9 before upgrading to SN09U. The Solaris 9 upgrade must be performed before:

- deploying MDM Admin Servers for centralized authentication and authorization in an Operator Client environment
- activating any Carrier Voice over IP or MDM base features, including security

Upgrading with Live Upgrade

Use Live Upgrade to upgrade Solaris operating systems. MDM is a flexible system that supports different deployments, therefore, the migration needs to be performed on each MDM in each set. The following server sets and client-sets are deployed as redundant pairs:

- distributed server and client-set server
- separate server and client-set server
- stand-alone (combined server and client)

Note: Upgrade the client-sets followed by the server sets.

The Live Upgrade feature provides both a command-line interface (CLI) and a character-based interface (CUI). Use the command-line interface to perform the upgrade. The CUI does not have the full feature set of the CLI and there are limitations on using it remotely.

In normal operation the Solaris operating system runs in one boot environment (BE). Live Upgrade creates a clone of the BE for an upgrade. The two BEs are the active boot environment (BE) and the alternate boot environment (ABE). The upgrade uses the (ABE), which is a clone of the current OS, to perform the OS upgrade without any impact on the OS that is running in the BE. The main requirement is that each BE have enough disk space for its own root partition.

The naming convention used to identify the two BEs is as follows:

`Solaris<release number>_<mmyy>`

As an example, `Solaris8_0703` corresponds to the Solaris 8 release dated 07/2003. The Live Upgrade utilities make use of the two logical names to identify the BE that is being manipulated.

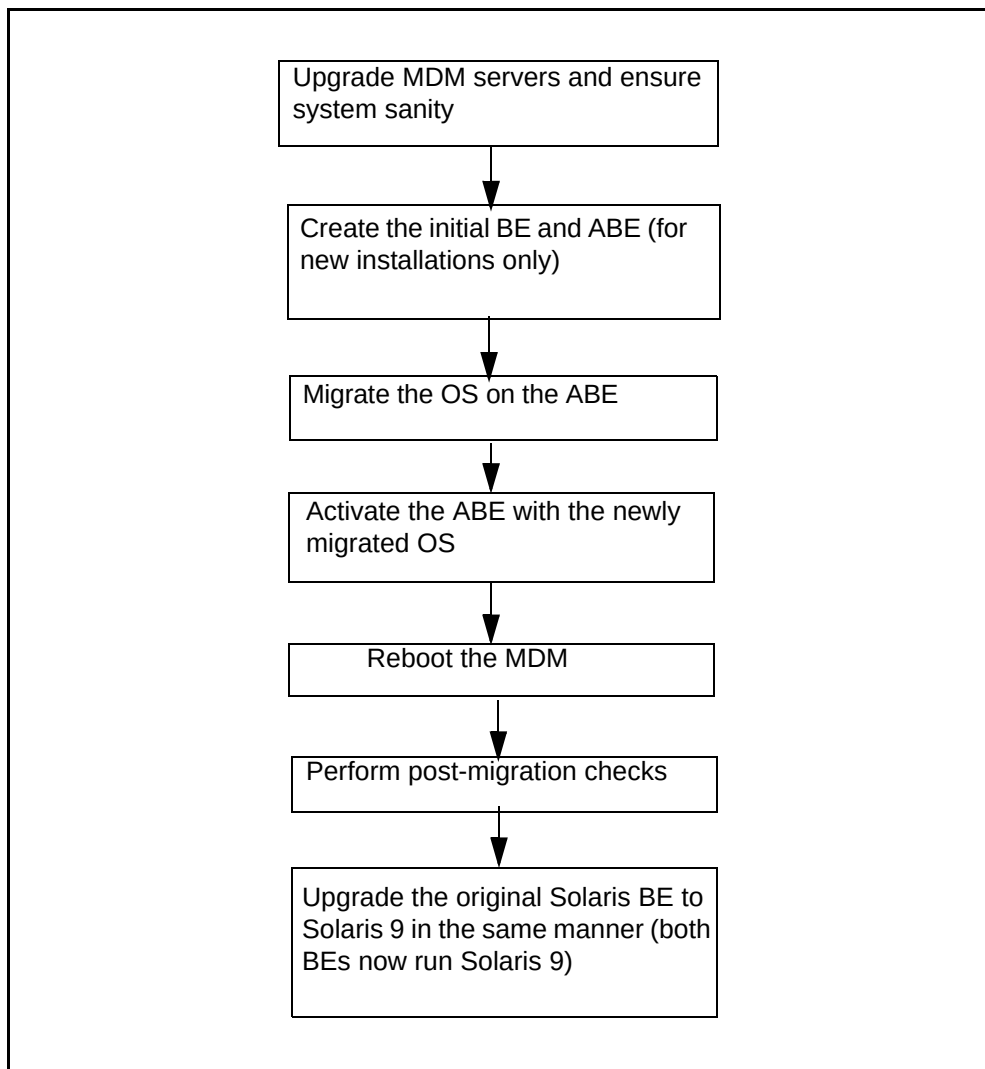
All the new Solaris OS software is installed in the ABE while the current Solaris OS continues operating in the boot environment (BE). Once the

new Solaris OS is installed in the ABE, it is activated in the ABE. At this point you must test the ABE to see if there are any problems.

Make sure that all the [Post migration checks on page 880](#) have passed in the BE before upgrading the ABE. If there are no problems, reboot (init 6) the ABE. The new Solaris OS does not become functional until after a reboot. If you find there is a problem after both BEs are at the new version of Solaris OS, uninstall the new version and re-install the old version in the BEs, then start the upgrade again.

The workstation is fully available to users throughout this entire procedure with the exception of the reboot. See the [Workflow for Solaris 9 upgrade on page 877](#) strategy.

Workflow for Solaris 9 upgrade



CAUTION

Rolling back after an MDM software upgrade

Once both boot environments have been updated to Solaris 9, you can only rollback to an earlier MDM release by re-installing Solaris 8.

When you create an initial BE from the current OS, two boot environments are created:

- one for the current OS named Solaris8_0703 for example
- one clone of the current OS named Solaris9_0404 for example, which is used for the upgrade

In subsequent upgrades, this step is omitted. The ABE created here can be used to perform the upgrade.

Prerequisites to performing the Solaris upgrade

Ensure the following prerequisites are performed prior to the upgrade:

- Verify the current OS (must be at least Solaris 8):
cat /etc/release
- Both MDM servers must be sane and operating without any errors:
 - Both servers must be in service, operating in a redundant capacity, and capable of supporting traffic and network management functions with no major or critical alarms.
 - Check the Alarm Display and the System Log Display tools and ensure there are no serious or unexplained logs or alarms.
 - Ensure that the second server (the one not being upgraded) is sane before you proceed with the upgrade.
 - Verify that you can access the MSS/MG15000 using Command Console.
 - If using disk mirroring, it must be enabled on both servers and operating without any errors.
- Both MDM servers must have been upgraded to the latest MDM release.
- Disable disk mirroring using the Sun documentation for disk mirroring provided in “Solaris Live Upgrade 2.0 Guide”, Sun Microsystems, 2004
[http:// www.sun.com/software/solaris/liveupgrade](http://www.sun.com/software/solaris/liveupgrade)
- Disable volume managers using the vendor information and Sun information provided in “Solaris Live Upgrade 2.0 Guide”, Sun Microsystems, 2004
[http:// www.sun.com/software/solaris/liveupgrade](http://www.sun.com/software/solaris/liveupgrade)
- Create disk partitions using the Sun documentation (if required).
- Unharden the OS.
- Back up system and user data.

- Install patches for the current OS (if required). See the *Multiservice Data Manager Release 15.4 Supplement* to determine the latest set of patches.
- Install Live Upgrade packages using the Sun documentation, go to the Sun Microsystems Documentation Center at:
<http://www.sun.com/documentation>

Upgrading to Solaris 9

- 1 Obtain the required software from Sun Microsystems Inc.
- 2 Install the Solaris 9 operating system according to the instructions provided in “Solaris Live Upgrade 2.0 Guide”, Sun Microsystems, 2004
[http:// www.sun.com/software/solaris/liveupgrade](http://www.sun.com/software/solaris/liveupgrade).

Note: If the documentation is not available or to ensure that the latest documentation was provided, go to the Sun Microsystems Documentation Center at <http://www.sun.com/documentation>.

ATTENTION

When installing Solaris 9, choose Entire distribution plus oem support 2.2 to ensure that SSH and IPsec are installed. The End User system support 2.3 option does not include these packages. IPsec and SSH are required for the Security feature.

Post migration checks

Ensure the following post migration checks are performed after the upgrade:

- Verify that the OS is at the new version of the Solaris operating system:
cat /etc/release
- Verify the system sanity as follows:
 - Both servers must be in service, operating in a redundant capacity, and capable of supporting traffic and network management functions with no major or critical alarms.
 - Check the Alarm Display and the System Log Display tools and ensure there are no serious or unexplained logs or alarms.
 - Verify that you can access the MSS/MG15000 using the Command Console.
 - If using disk mirroring, it must be enabled on both servers and operating without any errors.
- Test the BE in case you are required to revert back to the previous OS.
- Enable disk mirroring using the Sun documentation. Refer to “Solaris Live Upgrade 2.0 Guide”, Sun Microsystems, 2004 ([http:// www.sun.com/software/solaris/liveupgrade](http://www.sun.com/software/solaris/liveupgrade)).

- Enable volume managers using the vendor information and Sun information. Refer to “Solaris Live Upgrade 2.0 Guide”, Sun Microsystems, 2004 ([http:// www.sun.com/software/solaris/liveupgrade](http://www.sun.com/software/solaris/liveupgrade)).
- Harden the OS, if necessary. Refer to NN10180-612 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*.

Rollback to previous Solaris version before activation of the new Solaris version

If testing indicates that there are problems with the new OS, activate the BE that hosts the old version of the Solaris OS and then reboot according to the Sun documentation. Refer to “Solaris Live Upgrade 2.0 Guide”, Sun Microsystems, 2004 ([http:// www.sun.com/software/solaris/liveupgrade](http://www.sun.com/software/solaris/liveupgrade)).



CAUTION

Do not perform a manual OS sync.

Differences between Solaris OS versions can be destructive. Do not perform a manual OS sync and make sure that you use init 6 or shutdown for reboots.

Verifying that MDM servers and processes are running

The state of Nortel Multiservice Data Manager (MDM) servers will be one of the following:

- Not started, which indicates that the server has not been started since the SVMMDN process was started or since it was added to the list.
- Running, which indicates that the server has been started automatically by the SVMMDN process or by an administrator.
- Exited, which indicates that the server has exited unexpectedly and is awaiting a restart. When a server is in this state, information about the server is displayed on a yellow background.
- Quit, which indicates that the server has shut itself down. No restarts are being attempted. When a server is in this state, information about the server is displayed on a red background.
- Failed, which indicates that the server has exceeded all restart limits and that no further attempts to restart it automatically are being made. When a server is in this state, information about the server is displayed on an orange background.

Verifying the servers and processes are running

From the MDM server

- 1 Log in.
- 2 Open a MDM window:
/opt/MagellanNMS/bin/nmstool
- 3 From the MDM window, choose System > Administration > Server Administration.
- 4 Scan the server list and verify that all of the servers are in a Running state.
- 5 To view more detailed information about the server, click the name of the server whose information you want to view.
- 6 From the Edit menu, select View.
The server name in the Server Administration dialog indicates the descriptive name assigned to the server.
- 7 Click OK when you have finished with the dialog.
- 8 Close the Server Administration tool.

- 9** From the MDM window choose System -> Administration -> GMDR Administration.
- 10** Ensure that there are two FMDR servers for every distinct Carrier Voice over IP office, and two OAMC servers (total) listed. Ensure that each server is associated with a different workstation, and that all are in a connected state.
- 11** Close the GMDR Administration window.
- 12** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Verifying that the MDM toolset is functioning

Perform the following procedure to verify that Nortel Multiservice Data Manager (MDM) processes are working correctly.

Verifying that the MDM toolset is functioning

From the MDM server

- 1 Log in.
- 2 Open a MDM window:
/opt/MagellanNMS/bin/nmstool
- 3 Click OK to close the copyright dialog.
- 4 Verify that the Alarm display opens and displays alarms.
 - a From the MDM window, choose Fault > Alarm Display: Active
 - b When the Alarm Display window opens, verify that the alarms are being received.
- 5 Verify that the Network Viewer opens and displays the nodes.
 - a From the MDM window, select Fault > Network Viewer.
 - b When the Network Viewer window opens, double-click the group icon to expand it.

Right-click on the icons to see the node name. Select the node(s) you wish to check.
- 6 Confirm that the viewer displays the status of the nodes.
- 7 Verify that the Nodal Provisioning tool opens. From the MDM window, select the default menu **Configuration > MSS > Nodal Provisioning**.

Note: Customers who have "Set up MDM Toolset restricted access" as per NTP *MSS 15000*, *MG 15000* and *MDM in VoIP Networks - Securing Network Elements*, NN10180-612, will only see menu **Configuration->Nodal Provisioning**.
- 8 If more than one Configuration Manager server is specified in the configuration file, a Select Server dialog box opens. Otherwise, go to step [10](#).
- 9 If required, select a valid host in the Select Server dialog and click OK.
- 10 In the Nodal Provisioning Device Selection dialog, select a valid device and click OK.

- 11** In the Authenticating dialog, log on to the network destination by entering a valid user ID and password.

- 12** In the Open View dialog, select the Access Mode and the desired View Mode.

The Nodal Provisioning window opens with a component hierarchy.
- 13** From the MDM toolset, select the help menu and choose the On Window menu item. Ensure that the Help system opens.
- 14** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Installing MDM software

The following procedure provides the steps you need to upgrade the MDM.

**CAUTION**

Failure to restore contents of /etc/pam.conf and /etc/nsswitch.conf before installing new MDM software can cause MDM server lock-up.

If you are upgrading an MDM server that uses Integrated EMS as the central authentication and authorization server, you must restore the files /etc/pam.conf and /etc/nsswitch.conf to their pre-security activation versions.

Failure to do so can cause the MDM server to lock up, requiring on site access to restore operation.

Installing MDM software

Installing MDM software

From the MDM server

- 1 Open a UNIX xterm as the root user.
- 2 Stop the MDM server processes on the server you are upgrading, by entering the following command:

/etc/init.d/nmssvm.server stop

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

If	Do
you are installing the MDM software from CD-ROM	step 4
you are installing software downloaded from the Nortel ESD site	step 7

- 4 Insert the software disk 1 of 3 for the release to which you are upgrading into the CD-ROM drive, pattern side up. If your drive uses a disk caddy, insert the disk into the caddy pattern side up, then slide the disk caddy into the CD-ROM drive.

Note: Do not change directories (cd /cdrom/cdrom0) before executing the command install_mdm. Changing directories will cause problems when attempting to eject and load the CD-ROM.

- 5 Launch the MDM Installer:

/cdrom/cdrom0/install_mdm

- 6 Proceed to step [8](#).

- 7 Launch MDM Installer from the directory that contains the software that you downloaded in Retrieving MDM software

<MDM_software_pathname>/install_mdm

- 8 You are prompted for a DISPLAY environment variable. The default is to use a console local to the MDM workstation.

Enter the environment DISPLAY to launch the MDM Installer GUI [:0.0]

If your console is not local to the workstation, type the DISPLAY environment value (for example, BELTOR32:0.0)

The Nortel splash screen opens, a countdown occurs, then the window closes.

The Introduction window opens.

The left panel of the window indicates the current phase of the installation. As selections are made, the indicator for each phase changes color. The contents of the right panel changes as each installation phase is presented.

Note: The MDM Installer can be stopped at anytime before you press the Install button. Do not attempt to stop the software installation after the installation process has begun.

If you make a mistake while selecting installation options, you can uninstall the MDM software after completing the installation process and then re-install the MDM software. For information about uninstalling MDM software, see [Uninstalling MDM software on page 911](#).

To stop the MDM Installer, click Cancel.

9 Click Next.

The License agreement window opens.

10 Review the license information.

Click I accept the terms of the License Agreement, then click Next.

Another window opens requesting that you wait while the workstation is examined.

The System information window opens.

This window indicates:

- details about the Solaris operating system currently installed on this workstation
- the sizes of the disk partitions on this workstation and the disk partition sizes recommended for Carrier Voice over IP MDM software
- the MDM software (by release) currently installed on this workstation
- the MDM software licenses currently installed on this workstation

11 If the actual sizes of the partitions are equal to, or larger than, the partition sizes recommended in *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics*, NN10028-111, click Next.

The MDM Install Options window opens.

- 12** Select the MDM and MDP software packages to install on this workstation.

13

ATTENTION

Do not install Operator Client on server-sets. Server-set servers are dedicated to providing fault and PM information.

Operator Client (OC) is an optional feature in the VoA solution.

- a** To install Operator Client in a VoA solution, select the software package MDM Operator Client and User Administration.

This enables the Security Server and the Java Web Start Server.

If you do not want OC in your VoA solution, do not make a selection for this attribute.

- b** Operator Client is a mandatory feature in a secure VoIP solution.

To install Operator Client in a VoIP solution, select the software package MDM Operator Client and User Administration.

Deselect the Security Server.

If the software package MDM Operator Client and User Administration is selected and the package Security server is not selected, a data entry box is displayed beside the Java Web Start server option.

In the data entry box, SunONE IS, type the name of the Integrated EMS server.

Note: Do not select the Security Server option for VoIP.

- 14** Click Next.

The MDM Installation Source Path window opens.

- 15** If the indicated directory corresponds to the location of the software, click Next.

If you are installing from a directory other than the indicated directory, click Choose, select the appropriate folder, click Select, then click Next.

If the software packages are located in different directories, you are provided with prompts to select the appropriate directory for each package selected in step [12](#).

- If the MDM CD-ROMs are available, the default source path is: /cdrom/cdrom0
- If the MDM CD-ROMs are not available, the default source path is the directory that contains the MDM Installer: /MDM153

- 16** If the <host name>.<domain name> of this workstation cannot be automatically resolved, the Enter domain name window opens.

Type the domain name required to locate this MDM workstation on the network. If you do not know the domain name, contact your network or system administrator.

If the MDM workstation does not belong to a domain, you must assign a domain name in the /etc/hosts file. For example:

Example

Old file

Internet host table

127.0.0.1 localhost

10.17.1.2 MDM01 loghost

Modified file

Internet host table

127.0.0.1 localhost

10.17.1.2 MDM01 MDM01.XYZ.COM loghost

Note: If you do not know your domain name, contact your Nortel system administrator.

- 17** Click Next.

- 18** The Network Viewer Background Pixmaps window opens.

This window allows you to select optional bitmap images to use as the background for the Network Viewer (for example, the map of the world as the background).

Click No.

- 19** The Pre-installation summary window opens.

This summary identifies the software packages that will be installed and the disk space requirement for each package.

If the list of software packages to install is incorrect, click Previous to return to the MDM install options window and select the correct software packages.

If the amount of disk space required to install the software exceeds the amount of available disk space, click Cancel to stop the installation and ensure there is enough disk space on the servers (see [Ensuring that there is enough disk space on the servers on page 864](#)).

20 Click Install.

The MDM Installer displays the name of each software package as the package is installed.

If you are installing from a CD-ROM, the MDM Installer prompts for additional CD-ROMs until all of the selected software is installed. To eject the current disk, from the command prompt in the terminal screen, type:

```
eject cdrom
```

Insert the next disk and click OK.

Note: Do not attempt to stop the software installation after the installation process has begun.

If you made a mistake while selecting installation options, you can uninstall the MDM software after completing the installation process and then re-install the MDM software. For more information about uninstalling MDM software see [Uninstalling MDM software on page 911](#).

21 The Enter new license window opens after the software is installed if a valid license key is not located on this workstation.

Type a new MDM software license in the provided data entry box and click Next.

If you do not enter a software license key, a temporary software license is generated. The license key is valid for all of the MDM software for a maximum of 30 days. When you have a permanent software license, manually apply the new license using the appropriate procedure in *Nortel Multiservice Data Manager Customization and Server Administration*, 241-6001-303.

The Install complete window opens.

MDM software installation is now complete.

22 Click Done.

The MDM Installer window closes.

Note: Do not reboot the MDM at this point.

23

ATTENTION

You must check the logs for any errors in the installation. If the installation logs indicate failure to install any of the MDM packages, follow the instructions in “Recovering from an incomplete MDM software installation” in *Nortel Multiservice Data Manager*, 241-6001-123.

Examine the MDM software installation logs for any errors. The logs are located in the directory:

/opt/MagellanNMS/data/log/<release>_Install_logs

Variable definitions

Variable	definition
hostname.domain name	the fully qualified host name of this workstation
domain name	the domain name used on this network
MDM_software_pathname	the absolute pathname of the directory that contains the MDM Installer

MDM Installer logs

Log	Description
Install_summary.log	This file contains the following information for each software package: package - version added or replaced - installation success or failure

MDM Installer logs

Log	Description
stopServers	This file identifies the Multiservice Data Manager servers that were stopped by the MDM Installer during a Multiservice Data Manager software upgrade.
Package_logs	This file contains each package installation or package removal.

- 24 Reboot the workstation.
shutdown -i 6 -y
- 25 Repeat this procedure for the other MDM servers in their deployment.
- 26 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Installing MDM patches

Before and after installing Nortel Multiservice Data Manager (MDM) software, you may need to install the patches for MDM and MDP. MDM patches are jumbo patches that include all previous patches. As a result, only install the most current versions of each of the patches you need. You cannot install multiple versions of the same patch since you must remove the older version of a patch before you can install a newer version.

From the MDM server

- 1 Log in.
- 2 Display the patches that are currently installed on the system:
cd /var/sadm/patch
ls
showrev -p | grep MDM
showrev -p | grep MDP
Note: This step and the next two steps are not required if you are performing this procedure immediately after a software migration because there are no previously installed patches.
- 3 If there are any patches for previous releases listed, uninstall them. Uninstall the patches from the highest (numerically) to the lowest.
patchrm <patch_name>
- 4 If prompted to either reboot or re-initialize the NMS servers, do not reboot the servers at this time. You will reboot the server after completely installing the new patches.
- 5 Change directories to the directory containing the patches:
cd /<patch directory>
Note: The <patch directory> name you enter was created in [Downloading MDM patches on page 871](#).
- 6 Display the available patches:
ls
- 7 Uncompress the first patch that you need:
uncompress <patch name>.tar.Z
where

<patch name> is the name of the patch that you want to remove or install. The patch names have the MDM, MDP, or DVR release number followed by the patch number. For example, MDM153-01.

- 8 Untar the patch:

tar xvf <patch name>.tar

- 9 Remove the tar file:

rm -r <patch name>.tar

- 10 Change directories to the specific patch subdirectory:

cd /<patch directory>/<patch name>

- 11 In that subdirectory, open the README file associated with the patch and follow the instructions to install the patch. In the README file, however, ignore the steps that have you uncompress, tar and reboot (init 6).

- 12 Repeat steps [7](#) through step [12](#) for each of the patches you need to install.

- 13 To ensure that all changes have been applied, synchronize the file systems by issuing the sync command three times, pressing Enter after each one:

sync

sync

sync

- 14 Return the server to service and apply the changes by rebooting it:

init 6

After the reboot, the MDM server should return to service without any problem.

- 15 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Verifying that MDM servers and processes are running post-migration

From the MDM server

- 1 Log in.
- 2 Open an MDM window. See Opening the MDM Toolset.
- 3 From the window, choose System > Administration > Server Administration.
- 4 Scan the server list and verify that all of the servers are in a Running state.
- 5 To view more detailed information about the server, click the name of the server whose information you wish to view.
- 6 From the Edit menu, select View.
The server name in the Server Administration dialog indicates the descriptive name assigned to the server.
- 7 Click OK when you have finished with the dialog.
- 8 Close the Server Administration tool.
- 9 From the MDM window choose System > Administration > GMDR Administration.
- 10 Highlight GMDR Subserver "GMDR_LOWER" and then select the toolbar menu item "Options->Connect to selected sub GMDR"
- 11 Ensure that there are two FMDR servers for every distinct Carrier Voice over IP office, and two OAMC servers (total) listed. Ensure that each server is associated with a different workstation, and that all are in a connected state.
- 12 Close the GMDR Administration window.
- 13 Verify that the installation was successful. From the Toolset icon, select any tool, select the Help menu from the tool bar, and select the Help on Window menu item.
- 14 If the installation was successful, enter the following commands to remove the software download directory and to remove the software patch directory:

rm -r /<software download directory>

rm -r /<patch directory>

Example

rm -r /MDM154

rm -r/patch154

- 15** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Activating new features for MDM when updating from SN09 to SN09U

Configuring Network Model surveillance

At your MDM

- 1 Log in.
- 2 Launch the NMS toolset by typing
`/opt/MagellanNMS/bin/nmstool`
and press enter.
- 3 Launch the Server Administration tool by selecting System > Administration > Server Administration
- 4 Select Security > Authorize and provide the password
- 5 Select NM Surv Updater from the list of servers.
- 6 From the Edit menu, select Edit server to launch the SVM Edit Server dialog.
- 7 In the SVM Net Server dialog that appears, enter the following as the Startup command:
`/opt/MagellanNMS/bin/surnup -A ~t`
- 8 Click OK.
- 9 When you are prompted to save the new server definition, click Yes.
- 10 This procedure is complete. Return to [step 4](#) in [Upgrading an MDM server from SN09 to SN09U on page 855](#).

Activating new features for MDM when upgrading from SN08 to SN09U

The following features must be activated in SN09U:

- IS client for Integrated EMS central AAA access
- Network Model surveillance

IS client for Integrated EMS central AAA access

For secured networks using Integrated EMS central AAA services, the software used for communication with the Integrated EMS central AAA server must be activated to enable user authentication and authorization.

Note: Re-activation of access to Integrated EMS central AAA services must be done before other feature activations.

Installing and configuring user authentication and authorization interfaces to Integrated EMS

At your MDM

- 1 If you received MDM software from CD, install the PAM Radius and NNSwitch SAML software modules from the MDM installation CDs:

```
pkgadd -d /cdrom/cdrom0 NNnssaml
```

```
pkgadd -d /cdrom/cdrom3 NNpamradclt
```

- 2 If you received MDM software from the Nortel website, install the PAM Radius and NNSwitch SAML software modules:

```
pkgadd -d /<download_directory> NNnssaml
```

```
pkgadd -d /<download_directory> NNpamradclt
```

and pressing the Enter key.

where

download_directory

is the directory where you have downloaded the software for the MDM

- 3 Activate the PAM Radius client software on the MDM Server:

```
cd
```

```
/opt/nortel/applications/security/pamradclt_1.2.0/swmgmt/bin
```

```
./activate_pamradclt.sh
```

The following sample output should display:

NOTE: Upgrading pamradclt component from 1.1.0 to 1.2.0.

NOTE: Operation succeeded.

4 Activate the NSSwitch SAML software on the MDM Server:

```
cd  
/opt/nortel/applications/security/nsssaml_1.2.0/swmgmt/bin  
./activate_nsssaml.sh
```

The following sample output should display:

NOTE: Upgrading nsssaml component from 1.1.0 to 1.2.0.

NOTE: Operation succeeded.

5 Configure the PAM Radius client software on the MDM Server:

```
cd  
/opt/nortel/applications/security/pamradclt_1.2.0/swmgmt/bin  
./configure_pamradclt.sh -subcomponent libs
```

The following sample output should display:

NOTE: Configuring component pamradclt

NOTE: Configuring libs subcomponent

Linking /etc/raddb/server to
/opt/nortel/config/applications/security/pamradclt/pam_radius_auth.conf

Deploying version 1 of shared library
/opt/nortel/applications/security/pamradclt_1.2.0/lib/pam_radius_auth.so

Linking /usr/lib/security/pam_radius_auth.so.1 to
/opt/nortel/applications/security/current_pamradclt/lib/pam_radius_auth.so.1

Linking /usr/lib/security/pam_radius_auth.so to
/usr/lib/security/pam_radius_auth.so.1

Deploying version 1 of shared library
/opt/nortel/applications/security/pamradclt_1.2.0/lib/pam_mkhome.so

```
Linking /usr/lib/security/pam_mkhomedir.so.1 to
/opt/nortel/applications/security/current_pamr
adclt/lib/pam_mkhomedir.so.1
```

```
Linking /usr/lib/security/pam_mkhomedir.so to
/usr/lib/security/pam_mkhomedir.so.1
```

6 Configure the NSSwitch SAML software.

```
cd
/opt/nortel/applications/security/current_nsss
aml/swmgmt/bin
./configure_nsssaml.sh -subcomponent nsssaml
```

The configuration application will prompt for input. Default values for each prompt are shown in brackets, and can be accepted by pressing Enter. For the prompts shown below, however, enter the value shown after the colon (:).

- Enter the SAML servlet server Protocol [http]: https
- Enter the SAML servlet server Port [58080]: 58081
- Enter the SAML servlet server Host (ft1400-2.ca.nortel.com): <IEMS FQDN>

7 Copy the /etc/pam.conf and /etc/nsswitch.conf files from the Carrier VoIP Security Software CD. If these files were installed during a previous release, create backup copy in case you need to revert back to the previous release.

```
cp /etc/pam.conf /etc/pam.conf.<release_id>
cp /etc/nsswitch.conf
/etc/nsswitch.conf.<release_id>
cp <Carrier VoIP Succession Security Software
CD>/pam.conf /etc/pam.conf
cp <Carrier VoIP Succession Security Software
CD>/nsswitch.conf /etc/nsswitch.conf
```

8 Copy the tsets.tar file from the Carrier VoIP Security Software CD. If this file was installed during a previous release, tar the directory and save it with a release-specific name in case you need to revert back to the previous release.

```
cd /opt/MagellanNMS/cfg
tar cvf tsets_<release_id>.tar tsets
cp <Carrier VoIP Succession Security Software
CD>/tsets.tar /opt/MagellanNMS/cfg
```

After you have finished copying the tsets.tar file, untar the file in its new location.

- 9 Test that the NSSwitch software is working by executing the following command for both a locally defined userid and a userid defined on Integrated EMS and verify the output:

id <userid>

The following shows a sample command output:

```
> id chrisro      ← Integrated EMS userid
uid=10003(chrisro) gid=1024
> id root         ← local userid
uid=0(root) gid=1(other)
```

If the command response User not found is received, the authentication path with the Integrated EMS is not working. Verify the configuration on the Integrated EMS.

Network Model surveillance

Configuring Network Model surveillance

At your MDM

- 1 Log in.
- 2 Launch the Server Administration tool by selecting System > Administration > Server Administration
- 3 Select Security > Authorize and provide the password
- 4 Select NM Surv Updater from the list of servers.
- 5 From the Edit menu, select Edit server to launch the SVM Edit Server dialog.
- 6 In the SVM Net Server dialog that appears, enter the following as the Startup command:

`/opt/MagellanNMS/bin/surnup -A ~t`
- 7 Click OK.
- 8 When you are prompted to save the new server definition, click Yes.
- 9 This procedure is complete. Return to step [6](#) in [Upgrading the MDM](#).

Setting the solution release name identification

Setting the solution release name on the MDM

From the MDM server

- 1 Log in.
- 2 The file /opt/MagellanNMS/cfg/.SuccessionEnabled must exist. If this file doesn't exist, execute the following command:
touch /opt/MagellanNMS/cfg/.SuccessionEnabled
Note: A period appears as the first character in the .SuccessionEnabled filename shown in the command above.
If the /opt/MagellanNMS/cfg/.SuccessionEnabled file was just created, changes will only appear the next time the MDM toolset is launched. To proceed with the next step, re-launch the toolset.
- 3 From the MDM window, choose System > Administration > Succession Release Update: MDM.
The Succession MDM Software Migration window opens and displays the current MDM release.
- 4 Enter the Carrier Voice over IP release name using the format: SN09U
The Succession MDM Software Migration window opens displaying the current MDM release.
- 5 Click OK.
The file /opt/Magellan/NMS/system/info/release.name is changed and the MDM toolset icon displays the MDM release name followed by the Carrier Voice over IP (in the format SN09U) release name.
If you click Cancel, the process is cancelled and the file /opt/MagellanNMS/system/info/release.name is unchanged. If nothing is entered into the Succession Release field, the information is removed from the MDM toolset.
Note: The updated release name will not appear until you exit the tool and re-start it.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Downgrading MDM software

Downgrading to a previous MDM software version consists of the following steps:

- uninstalling the latest version of the MDM software
- uninstalling any remaining packages from the previous MDM software version
- re-installing the previous MDM software version
- restoring the configuration and data information that was backed up prior to the upgrade

If the downgrade is being performed on an SPFS-based server, and if the release to which you are downgrading supports the use of the SPFS backup utility to backup the entire file system, including the MDM software and configuration, this backup CD can be used to restore the previous software release.

Prerequisites

Perform the following tasks before you downgrade MDM software to a previous version:

- Verify that the MSS/MG core network has been downgraded. Although MDM software is backwards-compatible and can manage the current and previous releases of MSS/MG, it is not necessarily forward-compatible.
- Consult the *Multiservice Data Manager (MDM) 15.4 Release Supplement* and note any special considerations related to rolling back to a previous release. Contact your Nortel service representative to obtain the most up-to-date version *Multiservice Data Manager (MDM) 15.4 Release Supplement*.

ATTENTION

Possible service outage! Performing an end-to-end Carrier Voice over IP network downgrade requires downgrading individual component software in a specific order. Failing to follow the required order can result in a service outage.

ATTENTION

To ensure that one MDM server remains in contact with the CS 2000 Core Manager, Integrated EMS, CBM or the OSS at all times and continues to provide OAM&P information, isolate and completely downgrade one server using the following procedure while the other server remains fully operational. Following the successful downgrade of the first server, isolate and downgrade the second server, also using the following procedure.

ATTENTION

For an MDM16.1 OC client, if the MDM server downgrade to pre 16.1 version, on the OC client side, user must:

1. Uninstall J2SE 5.0 Upgrade 6 version so that OC client can connect to a 15.x OC server that uses JRE1.4x.
2. In JRE1.4.x Java WebStart, File -> Preference, select Java tab in Preferences: Select the 1.5.x platform version entry, then click Remove action button to remove the entry

Failure to do both can result in **Login Failed** pop-up message shown after OC displayed authentication dialog to allow login.

Action

Downgrading MDM software

At your MDM

- 1 Disable central authentication and authorization for the MDM server with IEMS, if applicable. See “Disabling central user authentication and authorization for an MDM server” in *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration - Securing Network Elements*, NN10180-612.
- 2 Unharden the OS, if applicable. See “Disabling security features on MSS15K, MG15K, and MDM components” in *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration - Securing Network Elements*, NN10180-612.
- 3 Back up the current software. See [Performing an MDM backup on page 860](#)

Attention: Backing up current MDM data and configuration is essential to being able to rollback and restore the MDM successfully.

- 4 To perform a complete system backup on SPFS-based workstations, see [Performing a backup of file systems on an SPFS-based server on page 379](#)
- 5 Uninstall the current version and all previous versions of the MDM software. Perform [Uninstalling MDM software on page 911](#)
- 6 Revert to the previous OS and patch level, if applicable. Review the *Multiservice Data Manager (MDM) 15.4 Release Supplement*.
- 7 Install the previous MDM and MDP release and patches. Perform [Installing MDM software on page 887](#) and [Installing MDM patches on page 895](#).
- 8 Restore MDM and MDP information. Perform [Restoring MDM and MDP information on page 914](#).
- 9 For a complete system restore on an SPFS-based server, see "Performing a full system restore on an SPFS-based server," in *ATM/IP Solution-level Fault Management* NN10408-900.
- 10 Reboot the workstation.
shutdown -i 6 -y
- 11 Activate MDM features. Review the *Multiservice Data Manager (MDM) 15.4 Release Supplement* for release-specific features.
- 12 Reset the Carrier VoIP release name on the MDM using the method appropriate for the release version. Perform [Setting the solution release name identification on page 905](#)
- 13 Harden the OS if required. See "Preparing to secure the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager network elements," in *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration - Securing Network Elements*, NN10180-612.
- 14 Enable central authentication and authorization for the MDM server with IEMS, if applicable. See "Migrating MDM Unix userids to IEMS" and "Configure the PAM interfaces on the MDM server" in "Preparing to secure the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager network elements," in *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice*

over IP Networks Security and Administration - Securing Network Elements, NN10180-612.

- 15** This procedure is complete. If you haven't performed this procedure for both MDM units, perform the procedure for the second MDM unit now. If you have performed this procedure for both MDM units, return to the higher-level task flow or procedure that directed you to this procedure.

Uninstalling MDM software

Prerequisites

ATTENTION

Deployments using central user authentication must have the PAM interfaces disabled prior to uninstalling the MDM software.

Action

Perform the following procedures in the order listed:

- [Uninstalling MDM software on page 911](#)
- [Removing MDM software patch on page 913](#)

Uninstalling MDM software

At the MDM

- 1 Open a UNIX xterm as the root user.
- 2 Change to the uninstaller directory applicable to the release you want to remove:
cd /opt/MDM<release>_INST
- 3 Start the software removal tool InstallAnywhere Uninstaller.
./uninstall_mdm[134 or 141] (for release 13.4 or 14.1)
./uninstall_mdm (for any release above 14.1)
The InstallAnywhere Uninstaller window opens.
- 4 Select Uninstall.
A window opens that shows the MDM packages available for removal.
- 5

ATTENTION

If you have upgraded to MDM15.4 or higher prior to uninstalling a previous release, do not select any packages whose names begin with NN during the uninstall process. Otherwise, software required for current release will be removed.

Select the MDM packages to remove and click Uninstall Selected Packages.

A progress bar indicates the stage of removal for each package.

A popup window indicates completion.

6 Click Ok.

7 Click Done.

8 To verify the success of the software removal, review any uninstaller logs. The uninstaller logs are located in the directory `/opt/MagellanNMS/data/log/<release>_Install_logs/Uninstall_summary.log`

9 If the Secure Shell (SSH) software was installed on this workstation, you may need to remove the SSH software. Type the following commands in sequence and respond to the prompts.

For Solaris 9 workstations, enter the following commands:

```
/bin/pkgrm MagSTRM
```

```
/bin/pkgrm SSHinit
```

For Solaris 8 workstations, enter the following command:

```
/bin/pkgrm MagOSSH
```

For SPFS-based workstations, do not remove SSH. SSH is installed as part of the SPFS operating system.

10 Remove the NNpamradclt and NNnssaml packages for the previous release.

Attention: Before performing this step, check the package version using the following command and ensure the old packages are being removed and not the current version.

```
pkginfo -1 <pkg_name>
```

Remove the old packages by typing

```
pkgrm NNpamradclt
```

```
pkgrm NNnssaml
```

11 If a previous version of PAM Radius Client 1.0.0 or 1.1.0 is installed, it must be removed manually.

```
rm -rf
```

```
/opt/nortel/applications/security/pamradclt_1.0.0
```

or

```
rm -rf
```

```
/opt/nortel/applications/security/pamradclt_1.1.0
```

Note 1: In the commands shown above, there is only a space between -rf and /opt

Note 2: For upgrade from PAM Radius Client 1.0.0 if the file /etc/pam.conf.radius has been modified or replaced, it should be saved before removing the NNpamradclt version 1.0.0 and restored after the uninstallation is complete if necessary. Removing NNpamradclt 1.0.0 will unconditionally remove the file /etc/pam.conf.radius.

- 12 If the software package cannot be successfully removed, contact your Nortel service representative (GNTS).
- 13 This procedure is complete. Proceed to [Removing MDM software patch on page 913](#)

Removing MDM software patch

At the MDM

- 1 Open a UNIX xterm as the root user.
- 2 Run the Sun Microsystems Inc. patch removal utility.
patchrm <release>-<patch>
The software patch is removed. You are informed of a successful patch removal.
- 3 Review the MDM Release Supplement or the README file included with the installed software patch. Determine the actions required to restore the MDM software to its previous state.
- 4 This procedure is complete. Return to step 6 in [Downgrading MDM software](#)

Restoring MDM and MDP information

Restoring MDM and MDP information

At your MDM

- 1 Log in to the MDM workstation as user ID root.
- 2 Restore the MDM configuration and data information.
 - a Restore the MDM software configuration files.

```
cd /opt/MagellanNMS/cfg
rm -R *
cp <safe directory>/mdmcfg_<release>.tar
/opt/MagellanNMS/cfg
tar xvpf mdmcfg_<release>.tar
```

where
<release> is the MDM software release (for example, 143)
<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)
 - b Restore the MDM software data files.

```
cd /opt/MagellanNMS/data
rm -R *
cp <safe directory>/mdmdata_<release>.tar
/opt/MagellanNMS/
data
tar xvpf mdmdata_<release>.tar
```

where
<release> is the MDM software release (for example, 143)
<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)
 - c If this MDM workstation includes the Management Data Provider (MDP) software, restore the MDP software configuration files.

```
cd /opt/MagellanMDP/cfg
rm -R *
cp <safe directory>/mdpcfg_<release>.tar
/opt/MagellanMDP/cfg
```

```
tar xvpf mdpcfg_<release>.tar
```

where

<release> is the MDM software release (for example, 143)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- 3 If this MDM workstation includes Management Data Provider (MDP) software, restore the MDP data files.

```
cd /opt/MagellanMDP/data
```

```
rm -R *
```

```
cp <safe directory>/mdpdata_<release>.tar  
/opt/MagellanMDP/  
data
```

```
tar xvpf mdpdata_<release>.tar
```

where

<release> is the MDM software release (for example, 143)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- 4 If this MDM workstation uses MDM 15.1 or above, restore additional MDM software configuration files.

```
cp <safe  
directory>/nortelconfig_<release>.tar/opt/nortel/config  
cd /opt/nortel/config
```

```
tar xvpf nortelconfig_<release>.tar
```

where

<release> is the MDM software release (for example, 152)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- a If this MDM workstation uses MDM 15.1 or above, restore additional MDM software data files.

```
cd /opt/nortel/data
```

```
rm -R *
```

```
cp <safe  
directory>/norteldata_<release>.tar/opt/nortel/data  
tar xvpf norteldata_<release>.tar
```


where

<release> is the MDM software release (for example, 152)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- b If this MDM workstation uses MDM 15.1 or above, restore the MDM log files.

```
cp <safe
directory>/nortellogs_<release>.tar/opt/nortel/logs
```

```
cd /opt/nortel/logs
```

```
tar xvpf nortellogs_<release>.tar
```

where

<release> is the MDM software release (for example, 152)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- 5 If this MDM workstation uses MDM 14.1 or above, restore the MDM EPIC configuration files.

```
cd /opt/nortel/EPIC/cfg
```

```
rm -R *
```

```
cp <safe
directory>/nortelEPIC_<release>.tar/opt/nortel/EPIC/cfg
```

```
tar xvpf nortelEPIC/cfg_<release>.tar
```

where

<release> is the MDM software release (for example, 152)

<safe directory> is any directory that will not be removed using the MDM uninstall (for example, /opt)

- 6 Enable the PAM interfaces for the release that has just been restored. Refer to “Adding or restoring network elements in a secured network” in *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration - Securing Network Elements*, NN10180-612.

- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



Multiservice Switch (MSS) 15000 upgrade

This chapter describes how to upgrade the software on the Nortel Multiservice Switch 15000 (MSS15k) nodes.

New in this release

This section describes changes in MSS15k upgrades in (I)SN09U.

Feature changes

None

Other changes

None

Upgrade paths

Nortel Networks supports the following upgrade paths:

- SPCR 6.1 or PCR 7.1 to PCR 7.2 within the context of a Packet Trunking - AAL1 (PT-AAL1) or Universal Access - AAL1 (UA-AAL1) solution upgrade from SN08 or SN09 to SN09U, or from one SN09U software version to another SN09U software version.
- SN08 or SN09 to a SN09U software version, or from one SN09U software version to another SN09U software version within the context of a PacketTrunking - IP (PT-IP), Packet Trunking - AAL2, (PT-AAL2), Universal Access - Internet Protocol (UA-IP), Integrated Access Cable (IAC), or Integrated Access Wireline (IAW) solutions.

Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

Time to complete an upgrade

The following table lists the tasks to upgrade the software on a MSS15k node and the estimated time to complete each task. The time varies depending on the node being upgraded. The maximum time estimate applies to the upgrade of the first node as it includes the activities performed once (e.g. reviewing release nodes, backing up the views, etc.) for all the MSS15K nodes.

Table 1 Estimated time to complete a software upgrade

Task	Time
Preparing for the upgrade	00:30 to 02:00
Upgrading the software	00:35 to 00:60
Completing the upgrade	00:15 to 00:20
Total estimated upgrade time	01:20 to 03:20

Service impacts

The upgrade of MSS15k software creates the following service impacts:



CAUTION

Calls in the process of being set up are dropped

This strategy removes inactive control and function processors from service. As a result, redundancy in the event of failure of the active shelf components is not available and some calls in the process of being set up (known as transient calls) are dropped. Stable calls are unaffected by the migration.



CAUTION

Loss of stable SVC connections can occur

When you perform the hitless software migration, a loss of SVC connections can occur. Although stable SVC calls should remain active in a redundant processor configuration, exercise caution when performing this upgrade.

Additional information

To perform the procedures discussed in this document, you should have a basic knowledge of Unix, Multiservice Data Manager (MDM), Multiservice Switch (MSS) software configuration, and Carrier Voice over IP portfolio architecture.

An upgrade of a Nortel Multiservice Switch 15000 node is also known as a hitless software migration (HSM). An operator performs a software migration using either the MDM Succession ATM Software Migration (SASM), or Succession IP Software Migration (SISM) tool. Once the HSM completes, the new functionality is added to the Nortel Multiservice Switch 15000 nodes by activating a new version of software.

An upgrade of a Nortel Multiservice Switch 15000 node is also known as a hitless software migration (HSM). An operator performs a software migration using the MDM Succession IP Software Migration (SISM) tool. Once the HSM completes, the new functionality is added to the Nortel Multiservice Switch 15000 nodes by activating a new version of software.

During a HSM, the node logically splits into two shelves: the service shelf and the migration shelf. The service shelf contains the active FPs and is controlled by the active CP. The migration shelf contains the standby FPs and is controlled by the standby CP. The standby cards that are being loaded with the new version of software are referred to as the migrating cards.

Complete all the upgrade tasks before installing additional hardware and configuring additional capabilities.

In the event you need or want to downgrade the MSS15k, refer to [Rollback of MSS 15000/MG 15000 nodes on page 995](#).

System capacity

The software upgrade procedure can impact the system capacity.

System performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade.

System limitations during upgrade

The following limitations apply:

- During the migration, the active CP and FPs continue to operate using the old version of software while a new version of software is

being loaded and provisioned on the migrating CP and FPs. The active cards remain active until the migrating cards have finished migrating to the new software and are ready to take over.

- The Multiservice Switch 15000 nodes in your network must be upgraded one at a time to ensure that no service interruption occurs. For in-band OAM configurations, Nortel Multiservice Switch 15000 nodes need to be upgraded in the sequence as listed in the section.

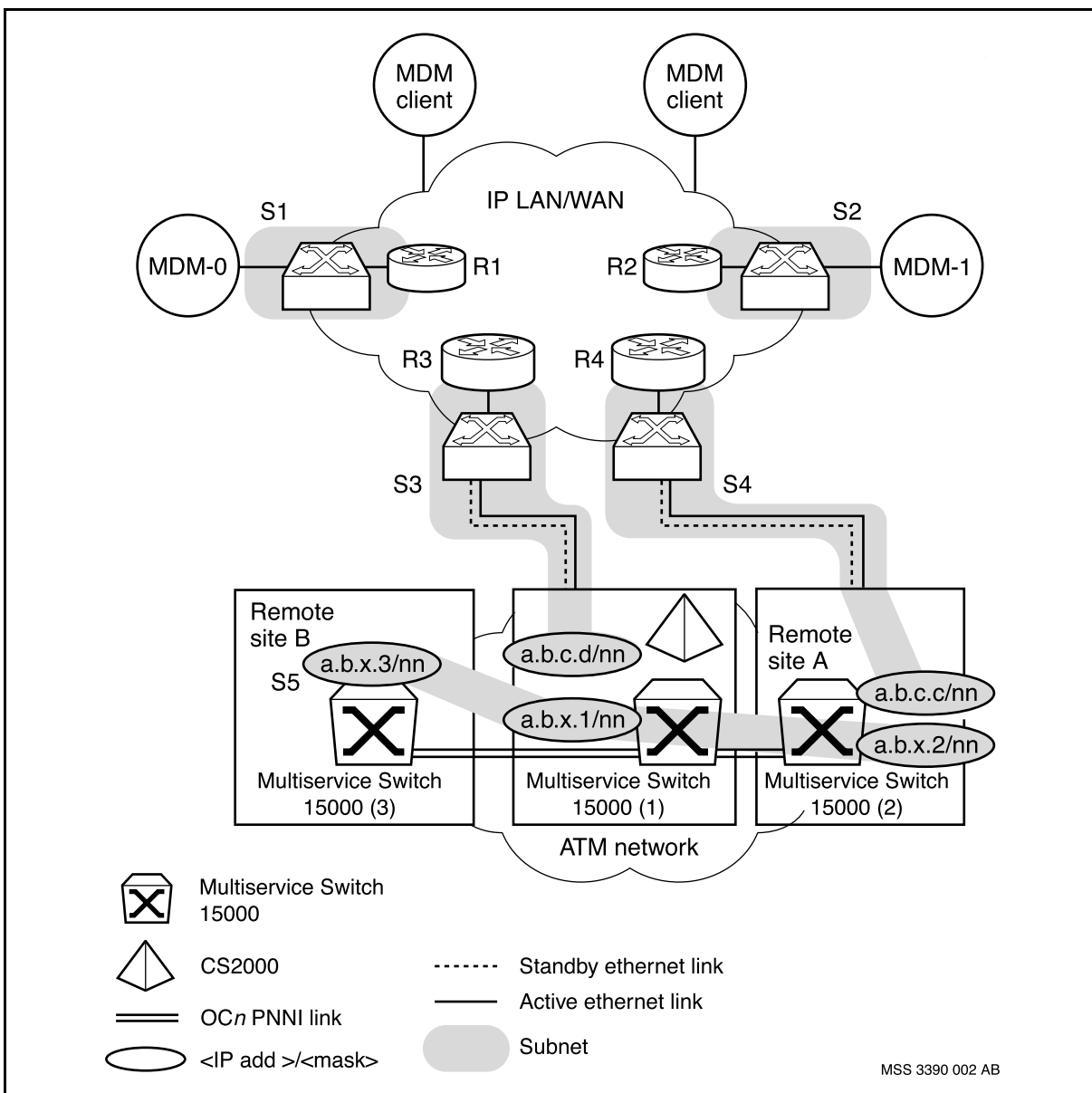
Node upgrade order for in-band OAM configurations

The Multiservice Switch 15000 nodes in your network must be upgraded one at a time to ensure that no service interruption occurs. For in-band OAM topologies, you must upgrade the nodes in the following sequence:

- upgrade all the remote nodes first
- upgrade the Multiservice Switch 15000 Gateway node that is not preferred. For more information about preferred and non-preferred gateways, see NN10028-111 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP*.
- upgrade the preferred Multiservice Switch 15000 Gateway node last. For more information about preferred and non-preferred gateways, see NN10028-111 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP*.
- For all out-of-band OAM configurations, upgrade all the Nortel Multiservice Switch 15000 nodes:
 - not physically co-located with the CS2K first
 - physically co-located with the CS2K next

The following is a quick reference to key relationships you need to understand for in-band OAM migration. For a complete description of in-band OAM, see NN10028-111 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP*. The figure [Sample in-band connectivity topology on page 921](#), illustrates a typical in-band OAM configuration. A brief description of the items in this diagram and their relationship to each other are provided below.

Figure 1 Sample in-band connectivity topology



MDM-0 and MDM-1

These Nortel Multiservice Data Manager servers are used to manage the Nortel Multiservice Switch network.

The chosen server is the MDM server that the operator uses as a launching point for MDM applications, such as SIS or Command Console.

The alternate server is the other MDM server that could have been used to perform the same set of tasks, except that it was not chosen.

Multiservice Switch -1

This Multiservice Switch 15000 node is in the Office and is a Gateway node using out-of-band connectivity.

From the perspective of MDM-0, S3 represents subnet to the preferred Multiservice Switch 15000 node.

Multiservice Switch-2

This Multiservice Switch 15000 node is in a remote office and is a Gateway node using out-of-band connectivity.

From the perspective of MDM-0, S4 represents the subnet to the alternate Multiservice Switch 15000 node.

Multiservice Switch-2 and Multiservice Switch-3

These Multiservice Switch 15000 nodes are Remote nodes using in-band connectivity with Multiservice Switch-1.

S5 represents the in-band OAM subnet. Multiservice Switch-1 has a direct ATMMPE ATM (PVC) connection to every other Multiservice Switch 15000 node.

Preparing to upgrade the MSS 15000

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

This procedure has the following prerequisites:

- you have completed the tasks under [Preparing to upgrade the Carrier Voice over IP Network on page 9](#)
- you have upgraded all components that precede the MSS 15000 under [Component Upgrade order on page 5](#)
- MDM GUI-based applications launched through a remote session must be launched on a trusted workstation. To start a trusted session, or to learn more about the MDM toolset, operator client interfaces, and processes that are common to all MDM tools, refer to 214-6001-122, *Using Toolset and Operator Client Interfaces*.

Action

Perform the following tasks to prepare for the MSS upgrade. Once all the listed tasks are complete, you can proceed with the software upgrade.

Nortel recommends that you perform the tasks involving commands issued from the command line using MDM Command Console tool rather than a Telnet session. For more information on using the

Command Console, see 241-6001-804 *Nortel Multiservice Data Manager Utilities*.

1. Ensure you have the following user IDs:
 - user ID for Nortel web support.
 - user ID for MDM software download
 - user ID for general access to MDM
 - Multiservice Switch user ID configured for local access, and access to FTP, FMIP, Telnet and MDM server
 - Multiservice Switch user ID with a minimum command scope of device and a command impact of configuration.

To determine your command scope and impact, type **me**. Information about your user ID is displayed.

2. Collect information to identify and avoid any compatibility issues that can prevent a software migration from completing successfully. For this task, use the procedures in the section:

[Information collection on page 932](#)

3. Download the new software version and patches and back up the current view of the MSS software. For this task, use the procedures in the section:

[Downloading and backing up MSS 15000/MG 15000 software on page 938](#)

4. If Internode ESA is configured for your network, you must also complete the procedure:

[Pre-work for HSM with AAL1 support of MG9000 Internode ESA on page 925](#)

5. Before performing the upgrade, ensure that all journal files are either used or purged by issuing this command: *display ProvisioningSystem restorePossible*.

If the response is yes, purge the files by issuing the *commit force prov* command. Then re-issue the *display ProvisioningSystem restorePossible disk* to verify the files have been purged. To restore these journal files, see the Restore Prov command section in NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*.

6. If you have DS-1 IMA interfaces using the Edgelink100 MUX, ensure that you use Edgelink100 MUX software (R3.3) during the SN09U upgrade.

For detailed steps, refer to the procedure [Determining the software version of the Edgelink 100 MUX on page 928](#).

7. Ensure that all configuration changes from the Global Bulletin System (GBS) and any associated Method of Procedure (MOP) are reflected on the node before performing the upgrade.
8. Ensure that all components supporting the service intended to be hitless are enabled. Check all the components prior to activating the migration provisioning to minimize any impacts to associated services.
9. Ensure nodes are connected to MDM servers. The nodes must also be in service and capable of supporting traffic and network management functions. In addition, the nodes must not have any major or critical alarms raised on them.
10. Ensure that you have an alternate way to access the node in case you lose IP connectivity during the migration.

For example, you can connect an operator terminal as described in the section “Connecting an operator terminal” in the *NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*. You can also use a modem or some other mode of out-of-band connectivity that was in place during the initial installation of the node.
11. If upgrading an ATM application, log into the MSS15k and determine if there are Pbg components configured by executing the **display Pbg/*** command. These components require some additional attention during the pause in the SASM HSM.
12. You have completed the pre-upgrade tasks. Proceed to [Upgrading the MSS15k](#).

Pre-work for HSM with AAL1 support of MG9000 Internode ESA

If the MSS15000 is configured to support MG9000 InterNode ESA, you must also check the state of the following additional components:

1. Verify that all VirtualRouter components are unlocked, enabled and active:

display Vr/* osistate

The following shows sample output for this command:

```
> display Vr/* osistate

Vr/*
-----
|          Vr          |osiAd|osi0|osiUs|Response
|          |          | min |per | age |
-----
|0            |unlck|ena |activ|
|ESA          |unlck|ena |activ|
```

- 2 Verify that all ProtocolPorts components are unlocked, enabled and active:

display Vr/* Pp/* osistate

The following shows sample output for this command:

```
> display Vr/* Pp/* osistate

Vr/* Pp/*
+-----+-----+-----+-----+-----+
|          Vr          |          Pp          |osiAd|osi0|osiUs|
|          |          | min |per | age |
+-----+-----+-----+-----+-----+
|0            |ATMMPE                |unlck|ena |activ|
|0            |OAMENET0              |unlck|ena |activ|
|ESA          |9K_1_ESA              |unlck|ena |activ|
|ESA          |9K_2_ESA              |unlck|ena |activ|
|ESA          |9K_3_ESA              |unlck|ena |activ|
|ESA          |9K_4_ESA              |unlck|ena |activ|
|ESA          |PP_D6_1000_ESA        |unlck|ena |activ|
|ESA          |PP_D6_1001_ESA        |unlck|ena |activ|
|ESA          |PP_D7_800_ESA         |unlck|ena |activ|
```

- 3 Verify that all Ip components are unlocked, enabled and active:

display Vr/* Ip osistate

The following shows sample output for this command:

```
> display Vr/* Ip osistate

Vr/* Ip
-----
|          Vr          |osiAd|osi0|osiUs|Response
|          |          | min |per | age |
-----
|0            |unlck|ena |activ|
|ESA          |unlck|ena |activ|
```

4 Verify that the static routes are up.

The osiOper (operational state) of all static routes are ena (enabled).

display Vr/* Ip static routeEntry/* operationalState

The following shows sample output for this command:

```
> display Vr/* Ip static routeEntry/* operationalState
Vr/* Ip Static Route/*,*,*
-----
|      Vr      |      addr      |      mask      | tos | osiO
|              |                |                |     | per
|-----|-----|-----|-----|
| ESA          | 10.0.16.0      | 255.255.240.0  | 0   | ena
| ESA          | 10.0.32.0      | 255.255.240.0  | 0   | ena
```

5 Verify that all Nexthop components under static routes have an operational status of enabled:

display Vr/ESA Ip static route/*Nh/* operationalState

The following shows sample output for this command:

```
>
Vr/ESA Ip Static Route/*,*,* Nh/*
-----
|      addr      |      mask      |      tos      |      Nh      | osiO
|                |                |               |              | per
|-----|-----|-----|-----|
| 10.0.16.0      | 255.255.240.0  | 0             | 10.48.0.2    | ena
| 10.0.32.0      | 255.255.240.0  | 0             | 10.48.0.10   | ena
```

6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Determining the software version of the Edgeline 100 MUX

From the Command Console

- 1 Log into the Edgeline 100

Example response

```
EDGELINK100
ROOT MENU
1) CONFIGURATION MANAGEMENT
2) PERFORMANCE MANAGEMENT
3) FAULT MANAGEMENT
4) DIAGNOSTICS
5) SYSTEM CONFIGURATION STATUS
6) SYSTEM ADMINISTRATION
```

- 2 Select the number beside system configuration status (5).

Example response

```
EDGELINK100
SYSTEM CONFIGURATION STATUS
1) DS3 INTERFACE STATUS
2) DS1 INTERFACE STATUS
3) SYSTEM STATUS
4) IP ADDRESSES
5) CARD INVENTORY
6) PEER LAPD DATA
```

- 3 Select the number next to card inventory (5).

Example response

```
CARD INVENTORY
M13 CCA420          = G10
M13 CCA             = E
M13 CCB             = E
M13 CCP             = E
M13 SERIAL#         = 642010271
MANUFACTURE DATE    = 11/22/01
CLEI                = M3CMUN08AA
M13 SOFTWARE REV    = 3.3
SW RELEASE DATE     = 11/20/02
MAC ADDRESS         = 00001F10C97A
```

- 4 The software version is listed on the 8th line (M13 SOFTWARE REV). Confirm it is version 3.3.

If the software version is not 3.3, contact your next level of support.

- 5 Log off the Edgeline 100 by pressing control + E (Ctrl E).

- 6** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Upgrading the MSS15k

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

You have completed the tasks in [Preparing to upgrade the MSS 15000 on page 923](#).

Action

Perform the following procedures to upgrade the component.

1. Perform the HSM.

If performing HSM on a MSS15k node configured for UA/PT - AAL1 applications, use the procedure:

[HSM \(MDM SASM tool\) activation on page 956](#)

If performing HSM on a MSS15k node configured for UA/PT - IP applications, use the procedure:

[HSM \(MDM SISM tool\) activation on page 968](#)

2. The software upgrade is complete. Proceed to [Completing the MSS 15000 upgrade on page 931](#).

Completing the MSS 15000 upgrade

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

The HSM has completed successfully.

Action

Perform the following procedures to complete the component upgrade.

1. Activate and provision new features. For this task, use the procedures in the section:
[Feature activation on MSS 15000/MG 15000 nodes on page 984](#)
2. Create a backup of the current view of the newly upgraded node(s). For this task, use the procedure [Back up the current view on page 952](#)
3. Upgrade the next component in the end-to-end upgrade. Refer back to [Component Upgrade order on page 5](#).

Information collection

Collect information to identify and avoid any compatibility issues that can prevent a software migration from completing successfully. This procedure is applicable to upgrades of MSS 15000/MG 15000 nodes.

Prerequisites to information collection

The prerequisites are as follows:

- Determine the order in which you will upgrade the Nortel Multiservice Switch nodes (MSS 15000 or MG 15000) in your network. The criteria for determining this order is left to your migration prime's discretion. Criteria such as switch utilization, geographic location, need for new software features or need for corrective content are just some suggestions the migration prime may wish to consider when determining the upgrade order of all the MSS15000 or MG15000 nodes in your network.
- Determine that the Nortel MDM servers have already been upgraded. From the MDM Toolset GUI, look for the MDM software version displayed just below the Nortel banner. The MDM software version should be R15.4.
- Confirm which release of software is active on the node. On the MG15K node type:
d sw avl
- Confirm that the node is operating without known errors or failures. From the MDM toolset GUI, select Fault -> Alarm Display : Active. If any components on the node have alarms, investigate the cause and correct the problem before proceeding.

Information collection tasks

Perform the following information collection tasks:

- [Download release notes on page 932](#)
- [Verify hardware compatibility on page 934](#)
- [Verify node feature compatibility.](#)
- [Complete the software upgrade checklist on page 935](#)

Download release notes

Download the release notes for Nortel Multiservice Switch in Carrier Voice over IP PT/UA-AAL1 solutions to collect specific information affecting hardware and services for each of Multiservice Switch equipment software release (PCRs) and Multiservice Switch for Carrier Voice over IP software releases involved in the migration.

Review *Nortel Multiservice Switch Release Notes* to determine the following:

- how the data model has changed for this release and how you must adjust your configuration to compensate for these changes
- which features and services are required by this release and by each of the processor cards, and which software files and applications you need to download to support these features and services
- if the software you are installing is compatible with the other software already on the node

From a workstation with access to the external network

- 1 Go to the Nortel public website.
<http://www.nortel.com/>
- 2 From Support & Training, select Technical Support, then Technical Documentation.
- 3 Under the Find Products heading, click Families.
- 4 Under the Browse Product Support heading, select Passport.
- 5 Scroll down to the MSS15k version applicable to the your nodes from the list of products.
 - For AAL1 applications, select Multiservice Switch 15000 for Carrier VoIP PT/UA-AAL1.
 - For IP applications, select Multiservice Switch 15000/20000.
- 6 Click Documentation.
- 7 Click Filter and sort.
- 8 Select Release Notes from the by Documentation Type menu.
- 9 Click the Go button.
- 10 Select the release notes for the specified release.
A security screen may appear requesting your user ID and password for web support.
- 11 If prompted, enter your user ID and password.
- 12 This opens a new window, where the document can be downloaded. To open it, click on the document title. Right-click on the document title and select Save Target As... to download it.

Repeat this steps [10](#) through [12](#) for each Release Notes document you need to download.

- 13 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Verify hardware compatibility

Verify hardware compatibility to confirm that your hardware configuration will support all the software versions that will be used in the migration.

From the MDM command console

- 1 Log onto the MSS 15000/ MG 15000 node.
- 2 Note the product engineering codes (PECs) of all the processor cards used in your node.

d shelf card/* prc

From your browser

- 3 Go to the Nortel public website.
<http://www.nortel.com/>
- 4 From Support & Training, select Technical Support, then Technical Documentation.
- 5 Under the Find Products heading, click Families.
- 6 Under the Browse Product Support heading, select Passport.
- 7 Scroll down to the MSS15k version applicable to the your nodes from the list of products.
 - For AAL1 applications, select Multiservice Switch 15000 for Carrier VoIP PT/UA-AAL1.
 - For IP applications, select Multiservice Switch 15000/20000.
- 8 Click Documentation.
- 9 Click Filter and sort.
- 10 Under Documentation type, select Planning. Then hit the green Go button.
- 11 Select the Multiservice Switch 15000 Hardware Baseline document.

A security screen may appear requesting your user ID and password for web support.
- 12 If prompted, enter your user ID and password.
- 13 This opens a new window, where the document can be downloaded. To open it, click on the document title. Right-click

on the document title and select Save Target As... to download it.

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

Verify node feature compatibility

Verify the node's compatibility with the new software to confirm that your configuration of services and features will not be negatively affected by the software migration.

From the MDM command console

- 1 Log onto the MSS 15000/MG 15000 node.
- 2 Create a list of all the applications loaded on the node.
d -p sw lpt/* fl, log
- 3 Refer to the *Nortel Multiservice Switch Release Notes*, Chapter 2, "Upgrading From Previous Releases", for each PCR in your migration path to confirm there are no known compatibility issues.
- 4 If you have any doubt about the compatibility between your existing features and your migration path, contact your Nortel Service Representative before beginning the migration.
- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Complete the software upgrade checklist

Complete this software upgrade checklist to confirm that all potential complications have been considered and eliminated. Use the information gathered while performing the [Information collection tasks on page 932](#).

Multiservice Switch software upgrade checklist

Task	Yes	No	Date and Comments
A migration order has been established for all the MSS 15000/MG 15000 nodes in the network.			
Migration plan has been created including acceptance criteria and fall back strategy (backup and restore).			

Multiservice Switch software upgrade checklist

Task	Yes	No	Date and Comments
Migration plan has been reviewed and verified by migration prime as well as operational and engineering resources.			
Migration operator has complete knowledge of MSS 15000/MG 15000 applications, features and software.			
Migration operator has complete knowledge of all software versions in the migration.			
The <i>Nortel Multiservice Switch Release Notes</i> for all releases in the migration path have been reviewed for potential impacts to the migration plan.			
Network health has been analyzed to verify that no known problems exist.			
Network management platform meets minimum hardware requirements.			
Network management software is compatible with each release in the migration plan.			
Network statistical data is collected. (Install NetRx if required. See http://www.nortel.com)			
MSS 15000/MG 15000 hardware is compatible with all releases in the migration plan.			
MSS 15000/MG 15000 software is compatible with all releases in the migration plan.			
All provisioning files have been saved (backed up).			
Network configuration changes have been prohibited.			

Multiservice Switch software upgrade checklist

Task	Yes	No	Date and Comments
The software version you are migrating to has been downloaded and installed on the MDM server acting as an SDS.			
All configuration changes from the Global Bulletin System (GBS) and the Method of Procedure (MOP) are reflected on the node before performing the upgrade.			
The file system is synchronized and the migration operator knows which software versions are applicable to the migration plan.			
For networks using in-band OAM, is this node a gateway node or a remote node?			
Enter “display software avlist” to find the software version. The software version currently running on the node is:			
Enter “display software patch” to find the current patches. The current patches running on the node are:			
The intended software after the migration is:			
The software patches you are applying during the upgrade are:			
The PCRs between the intended software release and the current PCR operating on the node are:			

Downloading and backing up MSS 15000/MG 15000 software

Application

Use this procedure to download and backup MSS 15000/MG 15000 software prior to an upgrade.

Prerequisites

Ensure that:

- one of the Nortel MDM servers has been configured as a software distribution site (SDS). The server acting as the SDS manages, stores, and provides access to MSS 15000/MG 15000 software and patches. To upgrade your MSS 15000/MG 15000 nodes, you must download the required software from this server to the nodes.
- the download of the software and patches onto the server acting as the SDS and the download of the software and patches from this server to the nodes can be done at any time prior to the hitless software migration. Unless there are specific operational requirements, perform these tasks before the upgrade period begins.
- the application version list must contain the following applications: base, networking, atmNetworking, ip, and patch. If your nodes have been configured with in-band OAM or support for MG9000 Internode ESA, you will also have the wanDte application. If patches have been applied, you will also have the patch application provided you are starting at SN08. The application version list must not contain any additional applications.

Action

Perform the following procedures to complete the software download and backup tasks.

1. [Verify there is enough disk space on the MDM server on page 939](#)
2. [Download the software from the Nortel website and transfer to MDM on page 940](#)
or
[Install the software on the server from a CD-ROM on page 943](#)
3. [Download software patches from the Nortel website and transfer to MDM on page 944](#)
4. “Determining what software is already on the node” in *Nortel Multiservice Switch 7400/15000/20000 Software Installation*, NN10600-270.

5. "Removing unused software from the node" in *Nortel Multiservice Switch 7400/15000/20000 Software Installation*, NN10600-270.
6. [Verify there is enough free space on the node on page 947](#)
7. [Download the software to the node from the MDM on page 949](#)
8. [Back up the current view on page 952](#)
9. These tasks are complete. Return to the higher level task flow or procedure that directed you to this procedure.

Verify there is enough disk space on the MDM server

Before downloading the required software and patches to the Nortel MDM acting as the SDS, verify that the server has sufficient disk space to hold the software release and/or patches. The software requires approximately 350 Mbytes of space. See *Nortel Multiservice Switch Release Notes* to verify the amount of disk space required by this release.

Note: Keep the patch AV on the SDS. Nortel recommends that at least one SDS be available with the current software on the MSS.

From the MDM acting as the SDS

- 1 Log in.
- 2 Determine how much disk space is available on the partition containing the Multiservice Switch software:

df -k /localdisk/pp15ksw/software

Note: This directory path assumes that the user ID configured to access the software on the SDS has a home directory of /localdisk/pp15ksw. If the user ID has a different home directory, adjust the directory accordingly. For more information, refer to NN10180-611 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL 1/UA-AAL 1/UA-IP*.

The system indicates (in kilobytes) how much disk space is available in the disk partition.

- 3 Verify that the space available is more than 350 Mbytes.
- 4 If there is not 350 Mbytes of space, remove files from the server, as required. You can safely remove software from the SDS after all subtending nodes are upgraded to a new release.

Software is located among multiple directories (base, atm, ip). Each release subdirectory must be located and removed. The directory structure on the SDS includes the following directories:

- a user-defined home directory which is the default log in directory. The home directory must have a subdirectory called software.
- application directories, which contain the software application version directories
- software application version directories, which contain all the control files and object files for a particular version of an application

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Download the software from the Nortel website and transfer to MDM

ATTENTION

In the CVoIP network, the MDM does not connect to the external network. If you are obtaining your software from the Nortel website, you first need to download the software to an intermediary server with access to both the external and your internal network. The software can then be transferred to the MDM from this intermediary server.

Prerequisites

The prerequisites are as follows:

- You need a Nortel Web access account with a user name and password. Contact your Nortel customer representative for more information on accessing the site.
- Refer to the software downloads area of the website (www.nortel.com) to determine the software load that you must install.
- The software you need to download can be composed of more than one file. Ensure that you download all software files that belong to the release you require.
- Ensure that there is enough disk space on both the intermediary and MDM server based on the information gathered from the release notes.

From an intermediary server with external network access

- 1 Log in.

- 2 On the web, go to www.nortel.com.
- 3 From Support and Training, select Software Downloads.
- 4 Under the Product Families link, select the family Passport.
- 5 Select the application for your solution.
 - For AAL1 applications, under the Passport 15000 for Succession PT/UA-AAL1 (Now known as: Multiservice Switch 15000 for Succession PT/UA-AAL1 section), select Software.
 - For IP applications, an UA-IP solution from SN08 or SN09 to SN09U or, from one version of SN09U to another SN09U version in a PT-IP, PT-AAL2, IAC, or IAW solution network, scroll down to the Passport Packet Voice Gateway (PVG) section and select Software.

The Software Downloads window opens.

- 6 Select the version of the release software you want to download.
A Log In window opens.
- 7 When prompted to log in, enter your user name and password for the web access log in.

Note: The software you want to download can be composed of more than one file. Ensure that you download all software files that belong to the release you require.

The Software Downloads: Software Detail Information window opens.

- 8 Click the load name listed beside the File Download heading.
A Save As dialog opens.
- 9 Specify a directory on the intermediary server where you want the software placed.
- 10 Click **Save**.

From the MDM acting as the SDS

- 11 Log into MDM.
- 12 Change to the directory where the software will be placed.
cd /localdisk/pp15ksw
- 13 Establish an FTP session to the intermediary server.
ftp <intermediary_server>
where

<intermediary_server>

is the host name or IP address of the intermediary server.

- 14 Log in to the intermediary server.
- 15 Navigate to the directory where the MSS15k/MG15k load files are located on the intermediary server.

cd <software_directory>

where

<software_directory>

is the directory that contains the software load files.

- 16 Set the local directory.

lcd /localdisk/pp15ksw

This directory (pp15ksw) must match the user ID for MDM software download confirmed in [step 1](#) of procedure [Preparing to upgrade the Media Gateway 15000 on page 2093](#). It must also match the user ID specified in the "start software download" command issued in [step 7](#) of [Download the software to the node from the MDM on page 949](#).

- 17 Change the transfer mode to binary.

bin

- 18 Turn Interactive mode off.

prompt off

- 19 Transfer the load files to the /localdisk/pp15ksw/software directory.

mget *

- 20 Exit from the FTP session.

quit

- 21 Uncompress each of the software files.

uncompress <load_name>.tar.Z

where

<load_name>

is the name of a software load file

- 22 Untar each of the software files.

tar -xvf <load_name>.tar

- 23 Delete the tar files.

rm *.tar

- 24 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Install the software on the server from a CD-ROM

An alternative to downloading the software from the server acting as the SDS is to install the software from Nortel Multiservice Switch CD-ROM using the installation program.

Prerequisites

The prerequisites are as follows:

- You need a copy of Nortel Multiservice Switch PCR7.1 software CD. Contact your Nortel customer representative for information on how to order a CD.
- You need the IP address of the Nortel MDM server acting as the SDS.
- After installing the required software release from the CD-ROM, download the required patches.

From the MDM server that is the acting SDS

- 1 Log in to the server.
- 2 Insert the software CD in the server's CD-ROM drive.
- 3 Create a directory for mounting the CD:
cd /
mkdir /cdrom
Note: If the mountable CDs have been used for other applications, you may not have to create this directory.
- 4 Start the installation program:
/cdrom/cdrom0/install
- 5 Follow the installation program's prompts.
- 6 When the installation program prompts you for a product, select Multiservice Switch 15000.
- 7 When the installation program prompts you, select Install software.
- 8 When the installation program prompts you for a directory in which to place the software, type the following:

/localdisk/pp15ksw

The installation program indicates when the installation is complete. At this time, the software has been installed in the

- directory you defined when prompted by the installation program.
- 9 Once the software has been successfully installed, log back into the MDM server.
 - 10 Eject the CD from the CD-ROM drive:
eject cdrom
 - 11 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Download software patches from the Nortel website and transfer to MDM

ATTENTION

In the CVoIP network, the MDM does not connect to the external network. If you are obtaining your patches from the Nortel website, you first need to download the patches to an intermediary server with access to both the external and your internal network. The patches can then be transferred to the MDM from this intermediary server.

All MSS 15000/MG 15000 patches are delivered as a single application version (Av), the Patch Av. The Patch Av includes all the patches associated with a given software version. Reset and TAP patches are delivered with the Patch Av. If you have enabled Patch auto-application, MSS TAP patches will be automatically applied; however, reset patches are not eligible for auto-application and must be manually applied. The Patch Av must not be confused with a patched Av; however, a Patch Av can include any patches that have been built specifically for a patched Av based on the release.

The Patch Av ensures that switches have access to the complete set of TAP and Reset patches at a given level. The Patch Av does not need to be provisioned in the Sw avList to view the patches contained within it; however, it must be provisioned in the Sw avl to be added to the Sw patchList. If you choose to display the patches for the patch Av, all the patches for all the Avs (base, atmNetworking, ip, and so forth) are displayed. If you choose to display the patches for the base Av, all the patches on the CP disk for that SW level will be displayed.

The Patch Av tracks patches for each software level. The AD file contains a list of Patch Version files for that software level. Each Patch Version (PV) file reflects the status of patches when the PV file is created and displays which patches are calculated and applied. The

status of the patches on the switch is tracked in version files within the Patch Av. Refer to *Nortel Multiservice Switch 7400/15000/20000 Upgrading Software*, NN10600-272 for more information about patching.

Prerequisites

The prerequisites are as follows:

- You need an account with a user name and password. Contact your Nortel customer representative for more information on accessing the website.
- Refer to the software downloads area of the website (www.nortel.com) to determine the software patches that you must install on the node. If there are no patches listed for this release, it means that there are no patches currently required for this release.
- Ensure that there is enough disk space on both the intermediary and MDM server based on the information gathered from the release notes.
- Ensure regular software has been downloaded.

From an intermediary server with external network access

- 1 Log in.
- 2 On the web, go to www.nortel.com.
- 3 From Support & Training, select Software Downloads.
- 4 Under the Product Families link, select either the family Passport or Succession.
- 5 Select the MSS15k application for your solution.
 - For AAL1 applications, under the Passport 15000 for Succession PT/UA-AAL1 (Now known as: Multiservice Switch 15000 for Succession PT/UA-AAL1) section, select Software
 - For MSS patches in an UA-IP solution, or to obtain patches for MG 15000/20000 from SN08 or SN09 to SN09U, or from one version of SN09U to another SN09U version in a PT-IP, PT-AAL2, IAC, or IAW solution network, scroll down to the Passport Packet Voice Gateway (PVG) section and select Software.

The Software Downloads window opens.

- 6 Click the patch that you want to download.

The Software Downloads: Software Detail Information window opens.

- 7 When prompted to Login, enter your user name and password for the web access log in.
Note: If there are no patches listed for this release, there are no patches currently required for this release. You can move on to the next task in the upgrade process.
- 8 Select the patch name listed beside the File Download heading. A Save As dialog is displayed.
- 9 Specify a directory on the intermediary server where you want the software placed.
- 10 Click Save.

From the MDM acting as the SDS

- 11 Log into MDM.
- 12 Change to the directory where the software will be placed.
cd /localdisk/pp15ksw
- 13 Establish an FTP session to the intermediary server.
ftp <intermediary_server>
where
<intermediary_server>
is the host name or IP address of the intermediary server.
- 14 Log in to the intermediary server.
- 15 Navigate to the directory to where the MSS15k/MG15k patch files are located on the intermediary server.
cd <software_directory>
where
<software_directory>
is the directory that contains the software load files.
- 16 Set the local directory.
lcd /localdisk/pp15ksw/software
- 17 Change the transfer mode to binary.
bin
- 18 Turn Interactive mode off.
prompt off

- 19 Transfer the load files to the /localdisk/pp15ksw/software directory.
mget *
- 20 Exit from the FTP session.
quit
- 21 Uncompress the patch file.
uncompress <patch_name>.tar.Z
where
<patch_name>
is the name of a software load file
- 22 Untar each of the software files.
tar -xvf <patch_name>.tar
- 23 Delete the tar files.
rm -r *.tar
- 24 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Verify there is enough free space on the node

Before downloading MSS 15000/MG 15000 software and patches from the MDM server, ensure the node has sufficient disk space to download the software applications.

Because of the amount of time required to remove old software releases, remove old software several days before beginning the upgrade. In particular, running the command tidy Software can take several hours to complete. As a result, consider running it overnight.

Prerequisites

The prerequisites are as follows:

- Ensure that there is sufficient space to download the software files for the following applications: base, networking, atmNetworking and ip. If your nodes have been configured with in-band OAM or support for MG9000 Internode ESA, you will also have the wanDte application. If patches have been applied, you will also have the patch application. The application version list must not contain any additional applications. The amount of space required for the (up to) six applications is approximately 250 Mbyte.

Note: Applications wanDte, ethernet, pvg, and aal1Ces are not mandatory for all configurations. Download and activate these in

SN09U only if they were present in the pre-SN09U release. For an SN08 to SN09U upgrade, the ipsec application can also be present.

- If you need to upgrade the fabric card firmware with this release, you will also need to download the fabric application. Allocate additional space for this application.
- If you need to download patches, allocate additional space for the patches.
- See the *Nortel Multiservice Switch Release Notes* and the software downloads area of Nortel website (www.nortel.com) to determine the software load and patches that you must install, and the amount of disk space required. See the section on determining which software is already on the node in NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*.

From the node

- 1 Log in to the node using the appropriate permissions.
- 2 Determine the space currently available on the file system:
display FileSystem freeSpace
The number of bytes available on the system is displayed.
- 3 Verify that the space available is more than 250 Mybte.
Note 1: If your nodes have been configured with in-band OAM, you need to allocate additional space for the wanDte application.
Note 2: If you need to install patches, you need to allocate additional space for the patches.
- 4 If the file system does not have enough available space, remove any unused software and provisioning files using the **tidy Software** command. See the section on removing unused software in NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*.
Note: Removing unused software will usually free up sufficient disk space. However, it is possible that a significant amount of disk space is being used by spooling files if they are not being removed often enough by the Management Data Provider (MDP). If this is the case, use MDP to retrieve and delete spooling files. See 241-6001-309 *Nortel Multiservice Data Manager Management Data Provider*.
- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Download the software to the node from the MDM

Before beginning the hitless software migration, download the software from the Nortel MDM server acting as the SDS to the nodes.

Prerequisites

The prerequisites are as follows:

- Refer to the software downloads area of Nortel (www.nortel.com) website to determine the software load and patches that you must install on the MG15K node. If there are no patches listed for this release, it means that there are no patches currently required for this release.
- Ensure the required software applications and patches are available on the MDM acting as the SDS.
- Download the software files for the following applications: base, networking, atmNetworking, ip, and patch. If your nodes have been configured with in-band OAM or support for MG9000 Internode ESA, you will also have the wanDte application. If patches have been applied, you will also have the patch application. The application version list must not contain any additional applications.

Note: Applications wanDte, ethernet, pvg, and aal1Ces are not mandatory for all configurations. Download and activate these in SN09U only if they were present in the pre-SN09U release. For an SN08 to SN09U upgrade, the ipsec application can also be present.

- You need the IP address of the MDM server acting as the SDS.
- You need the MDM user ID and password for software download.
- You need the MG15K user ID and password for software download. In order to download software you need a user ID on the MG15K node with a minimum command scope of 'device' and a command impact of 'configuration'.

To determine your user ID command scope and impact, log in to the MG15K node using this user ID and password and then type **me**. Information about your user ID is displayed.

From the node

- 1 Log in to the MG15K node using the appropriate permissions.

Note: You need a user ID with a minimum command scope of device and a command impact of configuration.

- 2 Verify that the downloader is inactive:

display Software Download status

The value of the status attribute must be inactive.

- 3 Set the processor target type for the application versions:

set Software Download processorTargets PPC i960

- 4 List the set of software applications currently being used:

display software avl

- 5 Create a SN09U version of the list of the same software applications for download:

**set Software Download avListToDownload !
<application_versions>**

You must download the software files for the following applications:

- base_CG02xxx
- networking_CG02xxx
- atmNetworking_CG02xxx
- ip_CG02xxx
- fabric_CG02xxx (only if a fabric upgrade is necessary)
- patch_CG02xxx (only if patches are required)

Applications wanDte, ethernet, pvg, and aal1Ces are not mandatory for all configurations. Download and activate these in SN09U only if they were present in the pre-SN09U release. For an SN08 to SN09U upgrade, the ipsec application can also be present.

Sample output

```
> set Software Download avListToDownload ! base_CG02S1E
networking_CG02S1E ip_CG02S1E wanDte_CG02S1E
atmNetworking_CG02S1E
Sw Dld

ok                               2005-01-07 14:46:46.14
```

- 6 Verify that the software applications that you want to download are in the list of software that will be downloaded:

display Software Download avListToDownload

- 7 Start downloading the software:

**start -host(<ipAddress>) -user(<userId>)
-password(<password>) Software Download**

where

<ipAddress> is the IP address of the MDM acting as the SDS

<userId> is the user ID for MDM software download confirmed in Step 1 of "Preparing to upgrade the Media Gateway 15000" on page 1098

<password> is the password for the user ID above

The download process begins.

- 8** Monitor the progress of the download:

display Software Download

When the status attribute is inactive and the files To Transfer attribute is 0, the download is complete.

- 9** Verify that the software listed in step [5](#) was downloaded:

list Software ApplicationVersion/*

- 10** If patches are required for this release, verify that the patches listed in the software downloads area of the Nortel website (www.nortel.com) were downloaded:

list Software ApplicationVersion/patch_CG02xxx Patch/***Variable values**

Variable	Value
<application_version>	A space-separated, case sensitive list of application versions. Download the new version of the base, networking, atmNetworking and ip. If your nodes have been configured with in-band OAM or support for MG9000 Internode ESA, you will also have the wanDte application. If patches have to be applied, you will also have the patch application. The application version list must not contain any additional applications. If you need to upgrade the fabric card firmware with this release, download the fabric application.
i960	An attribute indicating that the i960 processor type is being used. This attribute is always required.

Variable values

Variable	Value
<ipAddress>	The IP address of the MDM server acting as the SDS.
<password>	The password for the <userid> of the MDM server acting as the SDS.
PPC	An attribute indicating that the PowerPC processor type is being used. This attribute is always required.
<userid>	The <userid> for a MDM account that contains the Multiservice Switch software to be downloaded. The value is usually pp15ksw.

- 11 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Back up the current view

Use this procedure to save the current view of a node using the MDM Backup and Restore tool. This tool copies service data and application version information from the node(s) to a reliable data storage site. This view can be used to restore provisioning on a node in case of file corruption.

Prerequisites

The prerequisites are as follows:

- The view to be saved must be either a committed or portable view.
- You must have write permissions on the node, with a minimum impact of service, a minimum scope of device, and a minimum access of ftp and fmip.
- The backup site can be the MDM server or another node. It can also be a Software Distribution Site (SDS) configured to store backed-up node service data.
- Verify that the backup site has enough space to accommodate the backup. For more information, see *Nortel Multiservice Switch 7400/15000/20000 Upgrading Software*, NN10600-272.
- The MDM Backup and Restore tool uses the /tmp directory to perform some of its file processing (for example, archive, compress, and uncompress). Your local disk needs to have twice the amount

of space as the actual size of the files you are transferring for back up. Clean up the local disk if errors are raised (for example, No space left on device). In this case, you can mount the /tmp directory from a lower-usage disk on a selected file server.

- The MDM Backup and Restore tool backs up only the node's configuration data. It does not back up the software.
- The Backup server, the Restore server, the Backup Provider, and the Restore Provider must all be running on the MDM server for the MDMBackup and Restore tool to function properly. Using the MDM Server Administration tool, verify that these four servers are running. If they are not, or if you need more information, see *Nortel Multiservice Data Manager Network Backup and Restore*, 241-6001-807.
- Using the **display -o prov** command, ensure that the committed view, the current view, the edit view, and the last used view are identical. If these views are not the same, see *Nortel Multiservice Switch 7400/15000/20000 Software Installation*, NN10600-270 for information on making them the same.
- If a view is not saved prior to an upgrade attempt and you have to revert to a previous software load, then you must re-configure the old software release manually.



CAUTION

This procedure backs up all views currently stored on each node and should be done during a maintenance window.

From the node

- 1 Log in with the appropriate permissions.
- 2 Display on-switch provisioning to determine which files you need to back up:

display -o prov

The committedFileName is the view you need to save. The committedFileName and the currentViewFileName should be the same.

If they are not the same, you need to execute a commit prov. For more information, please refer to NN10600-550 *Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.

Sample output

```
1> display -o prov
Prov
adminState = unlocked
operationalState = enabled
usageState      = idle
provisioningActivity = none
activityProgress    = n/a
standbyCpActivity   = none
standbyCpActivityProgress = n/a
committedFileName  = BASE_ENG01_7_0_9.full.005
currentViewFileName = BASE_ENG01_7_0_9.full.005
lastUsedFileName    = BASE_ENG01_7_0_9.full.005
provisioningSession =
provisioningUser     = none
checkRequired        = no
confirmRequired       = no
editViewName          = BASE_ENG01_7_0_9.full.005
editViewAddedComponents = 0
editViewDeletedComponents = 0
editViewChangedComponents = 0
```

- 3 Log in to an MDM server using a root user ID.
- 4 Open an MDM window:
/opt/MagellanNMS/bin/nmstool
The copyright dialog and the MDM window open.
- 5 Click **OK** to close the copyright dialog.
- 6 From the MDM window, select Configuration > MSS > Administration > MSS Service Data Backup/Restore.
The MSS Service Data Backup/Restore window opens.
- 7 Click **Add**
- 8 Select the device(s) to be backed up by selecting the groups and/or nodes located in the Device Groups panel.
- 9 From the Mode pop-up menu, select the value full to ensure that the default for the backup is to do a full backup and not an incremental one.
- 10 Enter the appropriate user ID and password to authenticate for the selected device(s).
- 11 Click **OK**.
The added devices now appear in the **Device List** of the main MSS Backup and Restore window.

- 12** Click **Backup** to start the backup procedure for all the devices listed in the Device List of the main MSS Backup and Restore window.

This will proceed to back up all the views currently stored on each node, and should be done during a maintenance window.
- 13** Alternatively, specific views can be backed up as follows. For each device in the Device List:

 - change the parameter under the Mode column from full to selective.
 - select the specific view to backup from the Configuration column.
 - click **Backup** to start the backup of the selected view for each node in the Device List.
- 14** Exit out of the Backup and Restore window by selecting **File -> Exit**.
- 15** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

HSM (MDM SASM tool) activation

Application

Use this procedure to upgrade a MSS 15000/MG 15000 node using the MDM tool Succession ATM Software Migration (SASM) tool.

Prerequisites

The prerequisites are as follows:

- Have the correct software load and patches downloaded to the MDM server.
- For in-band OAM topologies, upgrade all MSS 15000/MG 15000 nodes in the network in the following sequence:
 - upgrade all the remote nodes first
 - upgrade the non-preferred Gateway node next
 - upgrade the preferred Gateway node last

Action

Perform the following procedure to perform a HSM using the MDM SASM tool.

To stop the HSM any time BEFORE the migration switchover go to [Stop the HSM using MDM SASM tool on page 967](#). To back out AFTER the migration switchover go to the procedure [Rollback of MSS 15000/MG 15000 nodes on page 995](#).

Performing HSM using the MDM SASM tool

From the MDM window

- 1 Log into MDM.
- 2 The file /opt/MagellanNMS/cfg/.SuccessionEnabled must exist. If this file doesn't exist, execute the following command:

```
touch /opt/MagellanNMS/cfg/.SuccessionEnabled
```

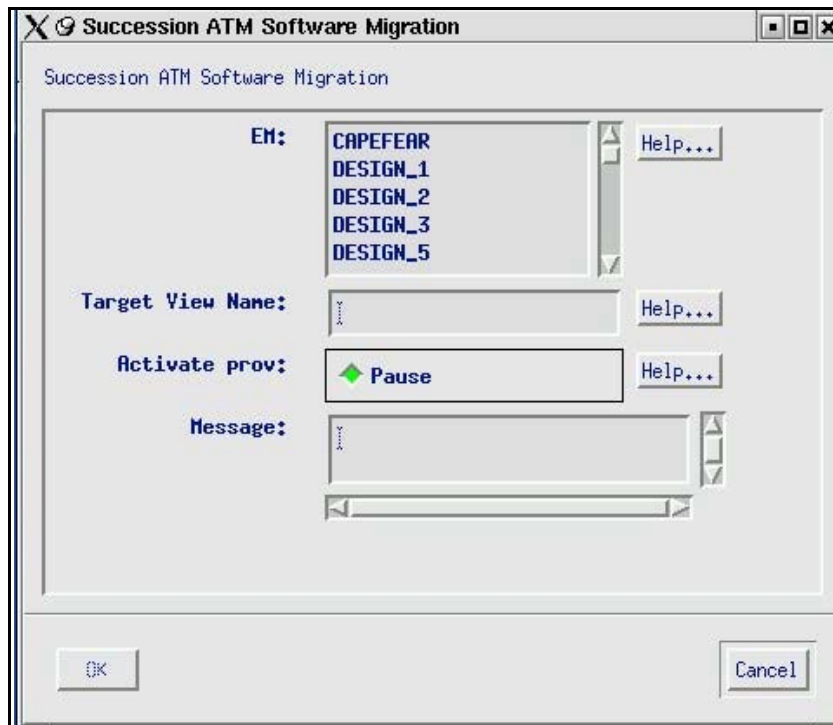
Note: A period appears as the first character in the .SuccessionEnabled filename shown in the command above.

- 3 Choose **Configuration > Administration > Succession ATM Software Migration**.

Alternatively, from the MDM Command Console, type:

```
$ /opt/MagellanNMS/bin/succession_atmsw_migr
```

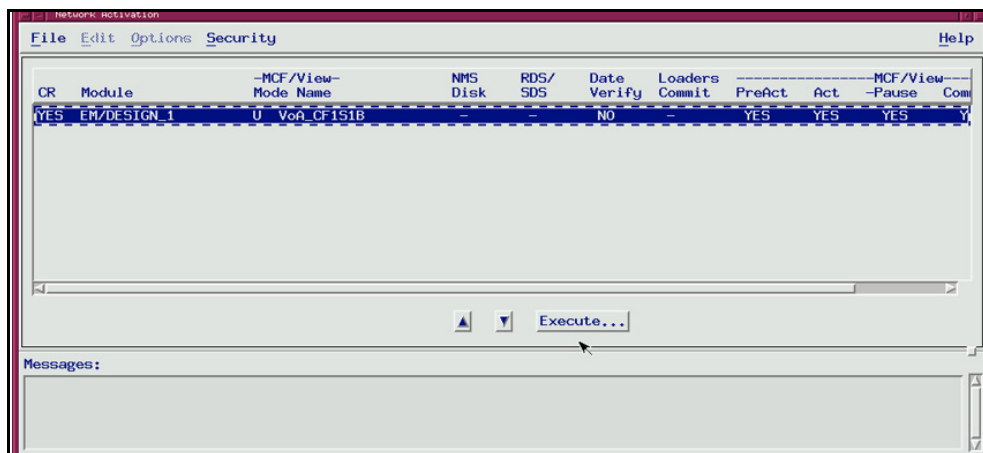
The Succession ATM Software Migration window opens.



- 4 In the EM field, select the name of the node you want to upgrade.
- 5 In the View field, enter the new target view name without the view type or version in the name (for example, CG01S1B_April_24).

The target view name must be 20 characters or less and be composed of numbers, letters and underscore. Use a consistent naming convention because this name is used when saving the current view and to create the view that will be activated for the software migration.

- 6 Click **OK**.
The Component Information Viewer opens.
The Network Activation window opens.



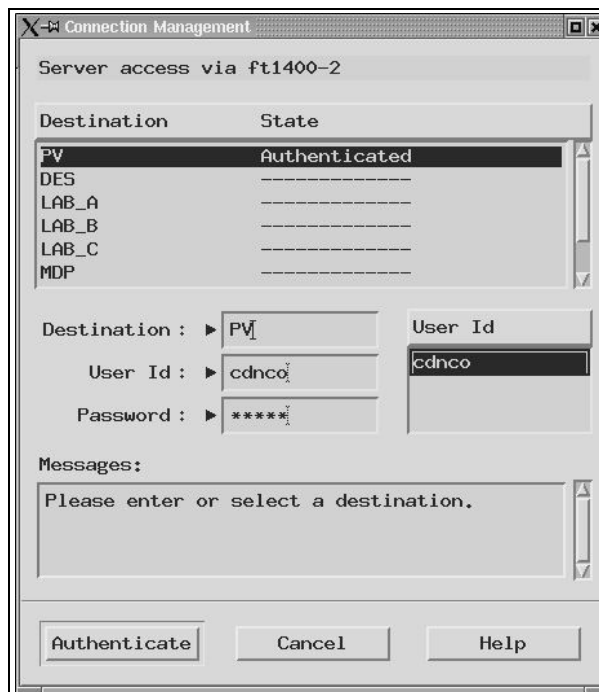
The Network Activation tool launches automatically in Hitless Software Migration mode with the network activation file already loaded.

- 7 Select the network activation record.
The network activation file contains one network activation record defined specifically for Carrier Voice over IP software migration activation.
DO NOT click **execute** yet.
- 8 From the MDM window, choose **Fault > Alarm Display: Log**.
The Alarm Display window opens.
- 9 Ensure the appropriate filters are turned on, including the filter for the target node, and that Format is set to full. Set filter to on. For more information on how to filter alarms, see “Filtering alarms” in 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.
- 10 From the MDM window, choose **Fault > Alarm Display: Active**.
The Alarm Display window opens.
- 11 Ensure the appropriate filters are turned on, including the filter for the target node, and that Format is set to full. Set filter to on. For more information on how to filter alarms, see “Filtering alarms” in 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.

Note: Monitor any alarms against the prov component (specifically 7000 0033, 7000 0034, and 7000 0035) and the prov migration component. Also monitor 7012 0204 against the Lp component. This alarm indicates that the LP cannot achieve its expected migration switchover behavior.

- 12 From the Network Activation tool, select **Group Authenticate** from the Security menu.

The Connection Management Dialog opens.



- 13 Enter or select the node's group name, and enter a valid user ID and password for the group. (The user ID must have a minimum impact of System Admin and minimum scope of network.)

- 14 Click **Authenticate**.

Authentication takes place. If authentication is successful, the dialog closes.

Note: If your user ID does not have sufficient permissions to perform the upgrade, exit and restart the SASM tool using an ID that has a minimum impact of System Admin and minimum scope of network.

After you authenticate with the group that contains the node to be migrated, use the Component Information Viewer to display the attributes of the provisioned components and later after the migration starts, monitor the progress of the migration. See 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.

- 15 In the Network Activation tool window, click **Execute**.

A confirmation dialog opens.

16 Click **OK** to proceed with the activation.

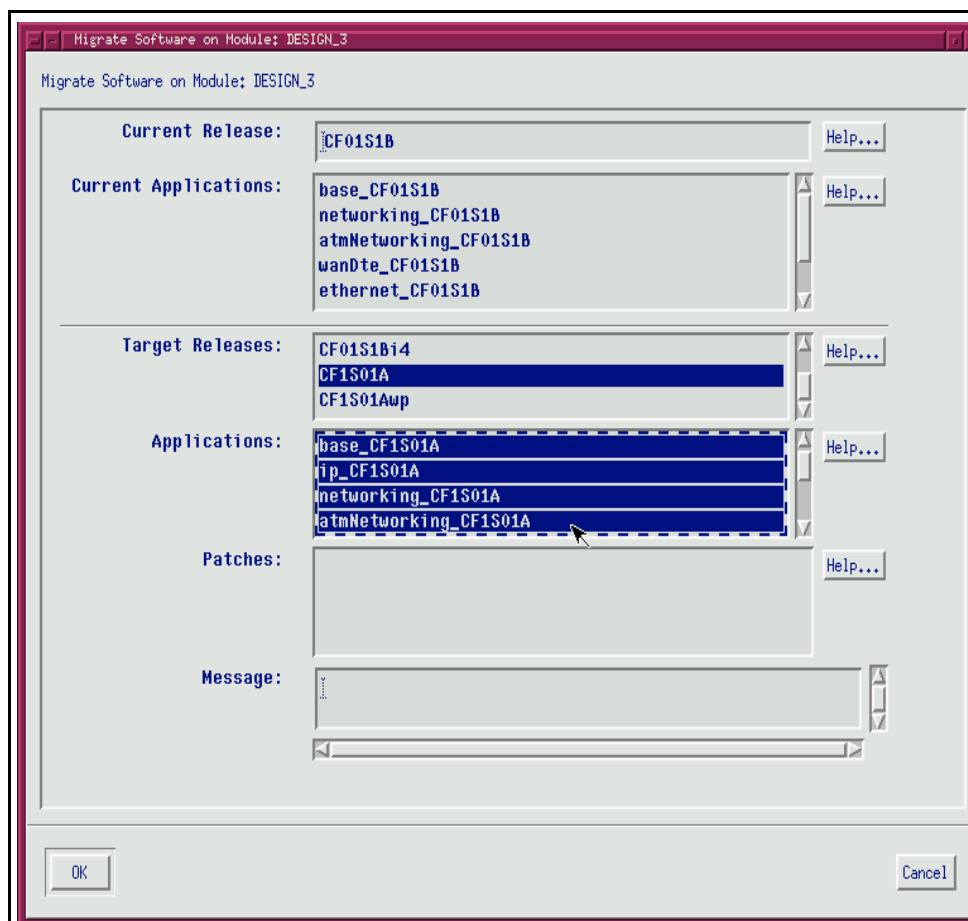
On the Network Activation tool, the **Execute** button is replaced by a **Stop** button that can be used to halt execution.

The activation begins. Information about the activation is written into the log file: `/opt/MagellanNMS/data/log/nat/nat_<nodename>_<timestamp>.log`.

As each process is performed, the corresponding field in the record turns from blue to green. If the action completes successfully, the field turns from green to blue and the next field turns green. If an action fails, the entire record turns red or yellow according to the severity of the error.

A window opens displaying the results of the pre-check and post-check commands. If a fault is found, the operator can stop the script (for example, if there is a fault on a component and the operator wants to fix it), fix the problem and repeat the process until all problems are corrected.

The Migrate Software on Module window opens.



- 17 In the Migrate Software on Module window, select the target release.
- 18 In the Migrate on Software Module window, select the destination software version from Target Releases and select applications matching the Current Release applications.
- 19 Select the required patches from the patch list.
- 20 To proceed with the migration, click **OK**.
- 21 The script progresses to the pre-activation stage and executes pre-HSM verification checks.

Note: Monitor the prov component using the Component Information Viewer. While the activation is in progress, monitor for alarms from the node using the MDM alarm display. Stop the migration if unexpected warnings or alarms appear.

- 22 Monitor the pre-HSM verification.

While the record is executing the pre-HSM portion of the script, information is displayed and you will be prompted to continue with the software migration or to abort the software migration.

While the activation is in progress, monitor for alarms from the node using the MDM alarm display. Stop the migration if unexpected warnings or alarms appear.

- 23 At the completion of the pre-activation portion of the script, you are asked if you want to continue with the software migration. To proceed, press **Enter**.

The migration takes place. The number of calls and components that have been provisioned on the node determine how long the activation takes.

Monitor the status of the node and the status of the migration. To monitor the progress of the migration, use the Component Information Viewer to display the attributes of the provisioning component. You can continue to do this until you lose connectivity to the node, which is when the originally active CP begins to load the new software. The MDM server automatically reconnects to the node when possible.

While the activation is in progress, monitor the alarms from the node using the MDM Alarm Display. If unexpected warnings or alarms appear, stop the migration.

- 24** When the software migration pauses, you are prompted to either stop the migration or continue the migration.

The software migration will pause because the **-pause** option is mandatory or, there is something wrong with the application during the software migration phase.

- a** When the software migration has paused and Pbg components have been provisioned, perform the following sub-steps. If the CS2000 and SAM21 connections have returned to service, click **Continue**.
 - i** Verify that the Laps components are enabled, unlocked, and free of alarms:
display Laps/* osistate
The osiAdmin column should contain only unlk values. The osiAvail column should contain degrad. All of the Laps components must be enabled and free of alarms.
 - ii** Verify that the sfs/0 component is enabled, unlocked, and free of alarms:
display pbg/* sts/0 osiState
 - iii** Verify that the Pbg components are enabled, unlocked, and free of alarms:
display pbg/* osiState
- b** Review the Migration Visible Alarms to determine whether to continue the migration. Click the appropriate button to continue or stop.

**CAUTION**

Contact GNTS before continuing during a migration pause

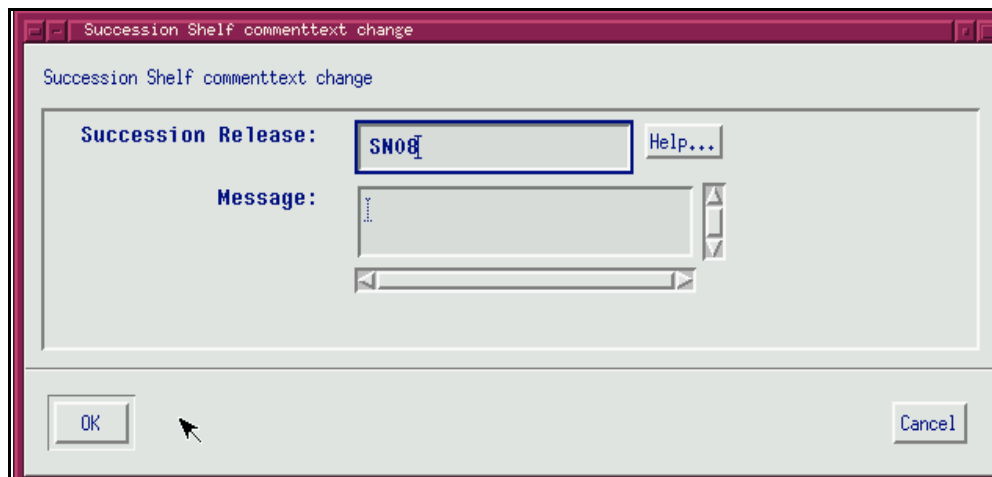
Contact Nortel Global Networks Technical Support (GNTS) for advice or assistance before continuing if the software migration pauses due to a Migration Visible Alarm.

- 25** After the HSM activation phase and commit phase are complete, the Network Activation tool starts the post-HSM verification portion script. While the record is executing the post-HSM portion of the script, information is displayed and you will be prompted to continue with the software migration. When prompted, press the Enter key.

After the record has executed the post-HSM verification, a fabric card firmware upgrade is performed on each fabric card if required.

Information on the result of the fabric card firmware upgrade and fabric card test is written to the log file. If the first fabric card firmware upgrade does not complete successfully, the second fabric card firmware upgrade is not attempted.

- 26 The SASM tool post-activation script prompts you for the new Carrier Voice over IP release name to display in the MSS 15000/MG 15000 Shelf CommentText. Use the format: SN09U.



If you click **Cancel**, the update is cancelled before execution and the MSS 15000/MG 15000 Shelf CommentText remains unchanged.

- 27 Click **OK**.

A NAT record is created and the NAT window is displayed for a second time since the start of SASM.

This time it activates the service data (the only change is the Shelf CommentText) with no pre- and post checks.

The Shelf CommentText attribute on the target node is updated with the Solution release name being displayed before the rest of the information in the Shelf CommentText field.

- 28 When all actions in the record have completed successfully, the entire record turns blue

Double-click the executed record in the record list to display and review the logged information. Alternatively you can choose Show Status from the record list pop-up menu.

- 29 Select **Exit** from the File menu to close the Network Activation Tool.
- 30 Select **Exit** from the File menu to close the Component Information Viewer tool.
- 31 If you have configured in-band OAM, use the following steps to view the status of the Atmmpe.
- a Ensure that the MDM servers can display OAM data received by way of both the preferred and non preferred Gateway nodes.
 - b View the status of the Atmmpe components.
display Atmmpe/* osiState
 - c View the status of the Ac components.
display Atmmpe/* Ac/* osiState
 - d View the accessibility of the chosen MDM server from the node. In conjunction with this step, ensure that both MDM servers are connected by way of different Gateway nodes.
ping -trace -ip(<MDM1 IP>) Vr/0 Ip Icmp
 - e View the accessibility of the alternate MDM server from the node. In conjunction with this step ensure that both MDM servers are connected by way of different Gateway nodes.
ping -trace -ip(<MDM2 IP>) Vr/0 Ip Icmp
- 32 If **display -o prov** shows a different version number for the `editViewName` from the `committedFileName`, execute the following comments through the `commandConsole`:
- ```
PROV 3> st pr
Prov
ok 2004-06-01 10:36:06.01

PROV 4> load -file(<committedFileName>) pr
Prov
 Loaded or applied file <committedFileName>.
ok 2004-06-04 10:20:47.36

PROV 5> end pr
Prov
ok 2004-06-01 10:36:09.45
```

The following output shows an example of misaligned `editViewName` and `committedFileName`.

```
Prov
 adminState = unlocked
 operationalState = enabled
 usageState = idle
 provisioningActivity = none
 activityProgress = n/a
 standbyCpActivity = none
 standbyCpActivityProgress = n/a
 committedFileName = CG0124F_April_27.full.001
 currentViewFileName = CG0124F_April_27.full.001
 lastUsedFileName = CG0124F_April_27.full.001
 provisioningSession =
 provisioningUser =
 checkRequired = no
 confirmRequired = no
 editViewName = CG0124F_April_27.full.001
 editViewAddedComponents = 0
 editViewDeletedComponents = 0
 editViewChangedComponents = 0
 currentJournal = 0
 journalDisabledReason = not disabled
 restorePossible = no
ok 2003-08-08 11:07:54.16
```

- 33** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Stop the HSM using MDM SASM tool

At any decision point during the software migration before the activation phase has begun, the operator can select **Cancel** and the migration stops. The Network Activation and MDM Component Information Viewer windows can be closed by selecting **File** and then **Exit**.

During the pre-script phase, you can stop the process by entering **<Ctrl> -C** in the pre-script window.

After the software activation has started, you can stop the software migration hitlessly by clicking **STOP** in the Network Activation tool's (NAT) main window. The NAT sends a **stop prov** command to the node and all the tool's processes stop. The success of the stop depends on timing. If the node enters the migration switchover phase before processing the **stop prov** command, it is too late to stop the hitless software migration.

If the system detects a problem during the software migration, then the hitless software migration automatically pauses before migration switchover occurs. This pause allows you to review the migration visible alarms before continuing or stopping the migration.

To stop the process after the Migration switchover phase has started, click the **Stop** button in the Network Activation Tool main window. Further processing stops on the HSM SASM tool (but not on the node).

close the SASM tool after stopping an HSM.

- Select **Exit** from the File menu to close the NAT.
- Select **Exit** from the File menu to close the Component Information Viewer window.

To back out after the migration switchover, follow the steps in [Rollback of MSS 15000/MG 15000 nodes on page 995](#).



### CAUTION

#### Non-hitless process

Stopping the process after the HSM switchover is not a hitless process.

---

## HSM (MDM SISM tool) activation

---

### Application

Use this procedure to upgrade a MSS 15000/MG 15000 node using the MDM Succession IP Software Migration (SISM) tool.

**Note:** The following pre-checks apply to Multiservice Switch 15000/Media Gateway 15000 nodes in a UA-IP solution. Solutions using AAL2, SPVCs for VoIP, and/or electrical TDM cards will require additional pre-checks of the related components.

### Prerequisites

The prerequisites are as follows:

- Download the correct software load and patches to the MG15K node.
- For in-band OAM topologies, upgrade all MSS 15000/MG 15000 nodes in the network in the following sequence:
  - Upgrade all the remote nodes first.
  - Upgrade the non-preferred Gateway node next.
  - Upgrade the preferred Gateway node last.

### Action

Perform the following procedure to execute a HSM using the MDM SISM tool.

To stop the HSM at any time BEFORE the migration switchover go to [Stop the HSM using MDM SISM tool on page 982](#). To back out AFTER the migration switchover go to the procedure [Rollback of MSS 15000/MG 15000 nodes on page 995](#).

#### Performing HSM using the MDM SISM tool

##### *From the MDM window*

- 1 Using the root user ID and password, log in to the MDM server.  
For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 The file /opt/MagellanNMS/cfg/.SuccessionEnabled must exist.  
Execute the following command:

```
touch /opt/MagellanNMS/cfg/.SuccessionEnabled
```

**Note:** A period appears as the first character in the .SuccessionEnabled filename shown in the command above.

The purpose of this file is to enable Succession specific features such as "succession\_ipsw\_migr". If this file does not exist and you attempt to execute the Succession specific feature for software migration, you will see the following error message:.

**Example**

```
/opt/MagellanNMS/bin/succession_ipsw_migr
```

MDM is not running in a Succession environment.

- 3 Launch the MDM toolset by typing

**/opt/MagellanNMS/bin/nmstool**

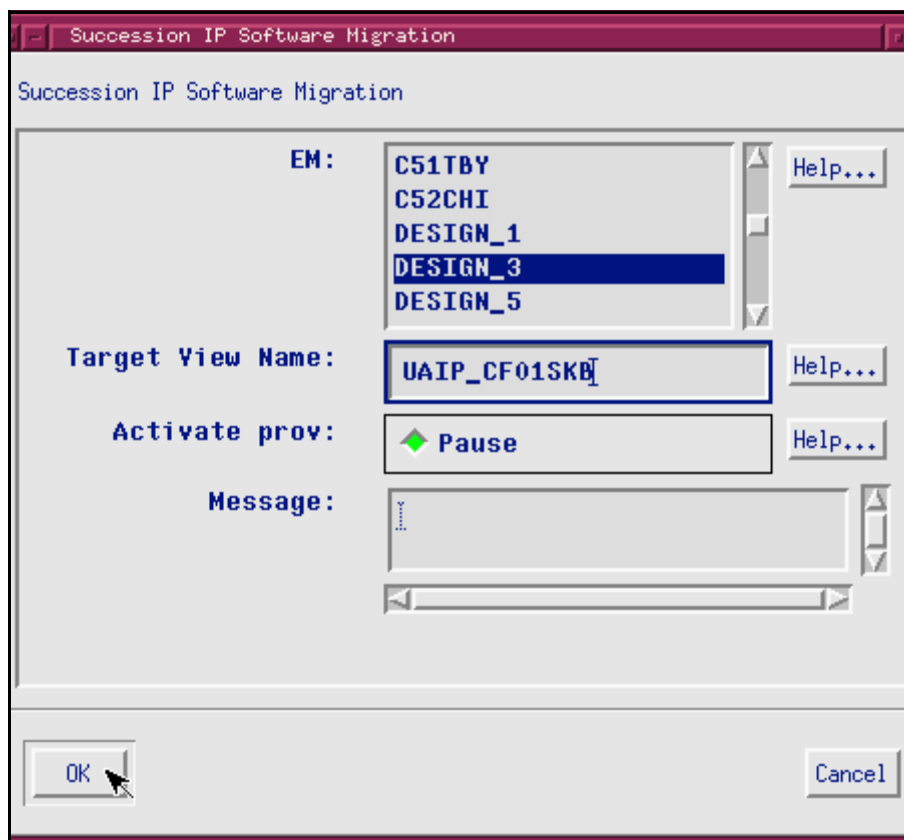
From the MDM Toolset GUI, choose **Configuration > MSS > Administration > Succession IP Software Migration**

Alternatively, from the MDM Command Console, type:

```
$ /opt/MagellanNMS/bin/succession_ipsw_migr
```

**Note:** The DISPLAY may have to be exported, otherwise the tool will not launch.

The Succession IP Software Migration window opens.



- 4 In the EM field, select the name of the node to upgrade.
- 5 In the Target View Name field, enter the new target view name without the view type or version in the name (for example, CG01S1B\_April\_24).

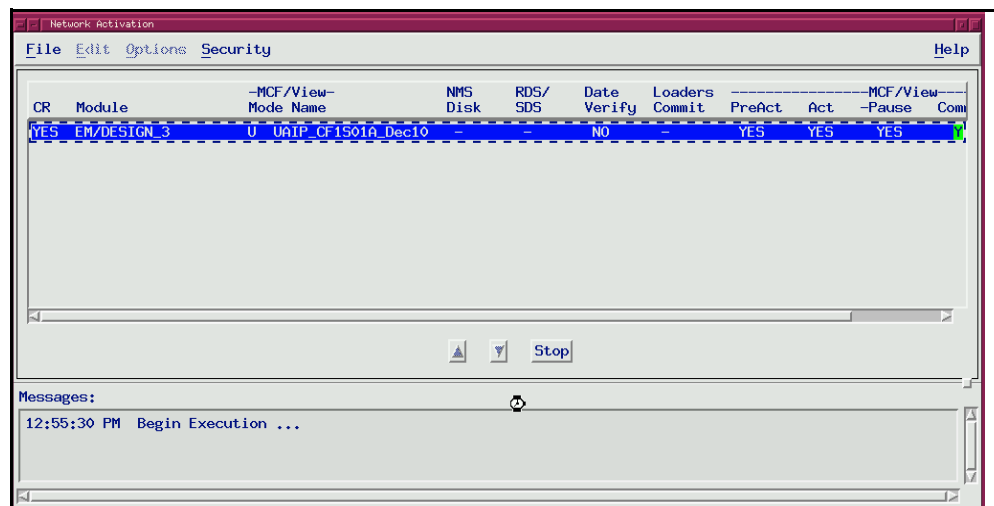
The target view name must be 22 characters or less and be composed of numbers, letters and underscore. Use a consistent naming convention because this name is used when saving the current view and to create the view that will be activated for the software migration.

Pause is the default setting for Activate Prov.

- 6 Click **OK**.

The Component Information Viewer (CIV) opens.

The Network Activation window opens.



The Network Activation tool launches automatically in Hitless Software Migration mode with the network activation file already loaded. The network activation file contains one network activation record defined specifically for Carrier Voice over IP software migration activation. The record is already selected.

- 7 From the MDM Toolset GUI, choose **Fault > Alarm Display: Log**  
The Alarm Display window opens in log mode.
- 8 Ensure the appropriate filters are turned on, including the filter for the target node, and that Format is set to full, then click **Filter**. For more information on how to filter alarms, see “Filtering alarms” in 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.

- 9 From the MDM Toolset GUI, choose **Fault > Alarm Display: Active**  
The Alarm Display window opens in active alarm mode.
- 10 Ensure the appropriate filters are turned on, including the filter for the target node, and that Format is set to full, then click **Filter**. For more information on how to filter alarms, see “Filtering alarms” in 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.  
**Note:** Monitor any alarms against the prov component (specifically 7000 0033, 7000 0034, and 7000 0035) and the prov migration component. Monitor 7012 0204 against the Lp component. This alarm indicates that the LP cannot achieve its expected migration switchover behaviour.
- 11 From the Network Activation tool, select **Group Authenticate** from the Security menu.  
The Connection Management Dialog opens.



| Destination    | State |
|----------------|-------|
| C8             | ----- |
| C9             | ----- |
| <b>CENTRAL</b> | ----- |
| CR_TEST        | ----- |
| LAB_VOA        | ----- |
| MDP            | ----- |

Destination : ▶ CENTRAL

User Id : ▶ dominicr

Password : ▶ \*\*\*\*\*

User Id

Messages:

Please enter or select a destination.

Authenticate Cancel Help

- 12 Enter or select the node's group name, and enter a valid user ID and password for the group. (Your user ID must have a minimum impact of System Admin and minimum scope of network.)

- 13 Click **Authenticate**.

Authentication takes place. If authentication is successful, the dialog closes.

**Note:** If your user ID does not have sufficient permissions to perform the upgrade, exit and restart the SISM tool using an ID that has a minimum impact of System Admin and minimum scope of network.

After you authenticate with the group that contains the node to be migrated, use the Component Information Viewer to display the attributes of the provisioned components and later after the

migration starts, monitor the progress of the migration. See 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*.

- 14 In the Network Activation tool window, ensure the activation record is selected and click **Execute**.

A confirmation dialog opens.

- 15 Click **OK** to proceed with the activation.

On the Network Activation tool, **Execute** is replaced by a Stop button (grey) which is not available for selection.

The activation begins.

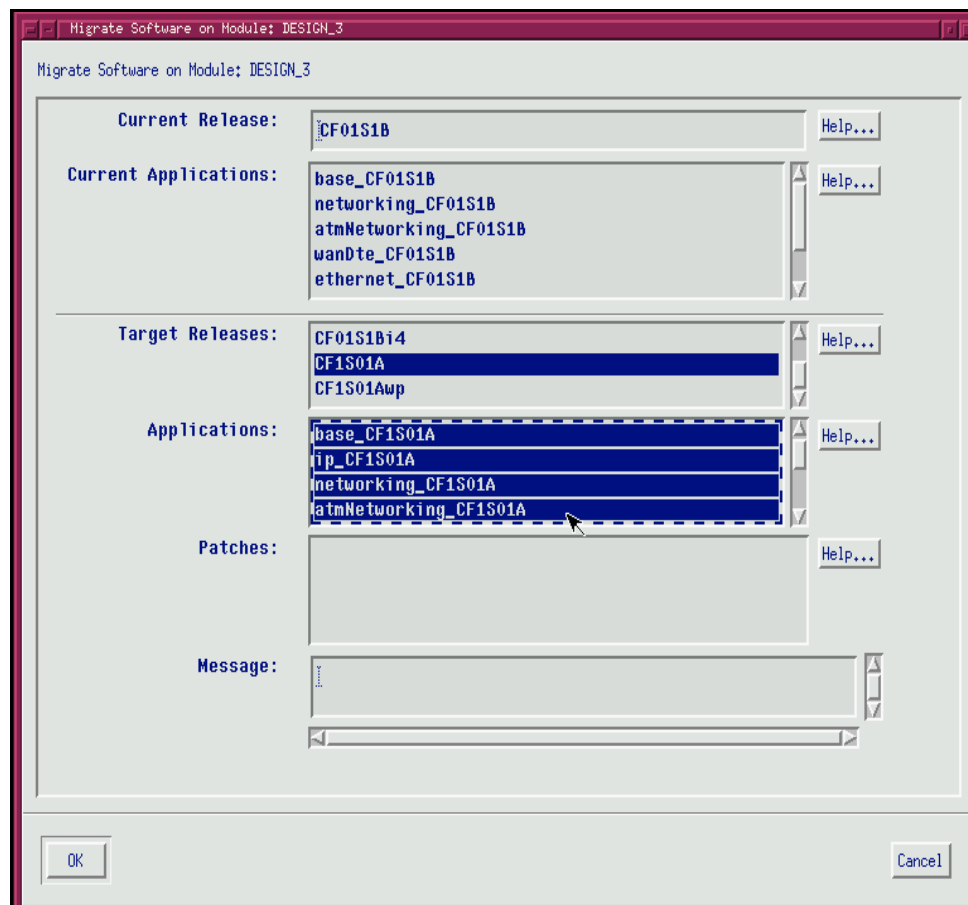
A pre-check terminal window and a Migrate Software on Module window opens.

Information about the activation is written into the log file:

```
/opt/MagellanNMS/data/log/nat/
nat_<nodename>_<timestamp>.log.
```

As each process is performed, the corresponding field in the record turns green. If the action completes successfully, the field turns from green to blue and the next field turns green. If an action fails, the entire record turns red or yellow according to the severity of the error. During this process, **Execute** is replaced by **Stop** that can be used to halt execution.

A window opens displaying the results of the pre-check and post-check commands. If a fault is found, the operator can stop the script (for example, if there is a fault on a component and the operator wants to fix it), fix the problem and repeat the process until all problems are corrected.



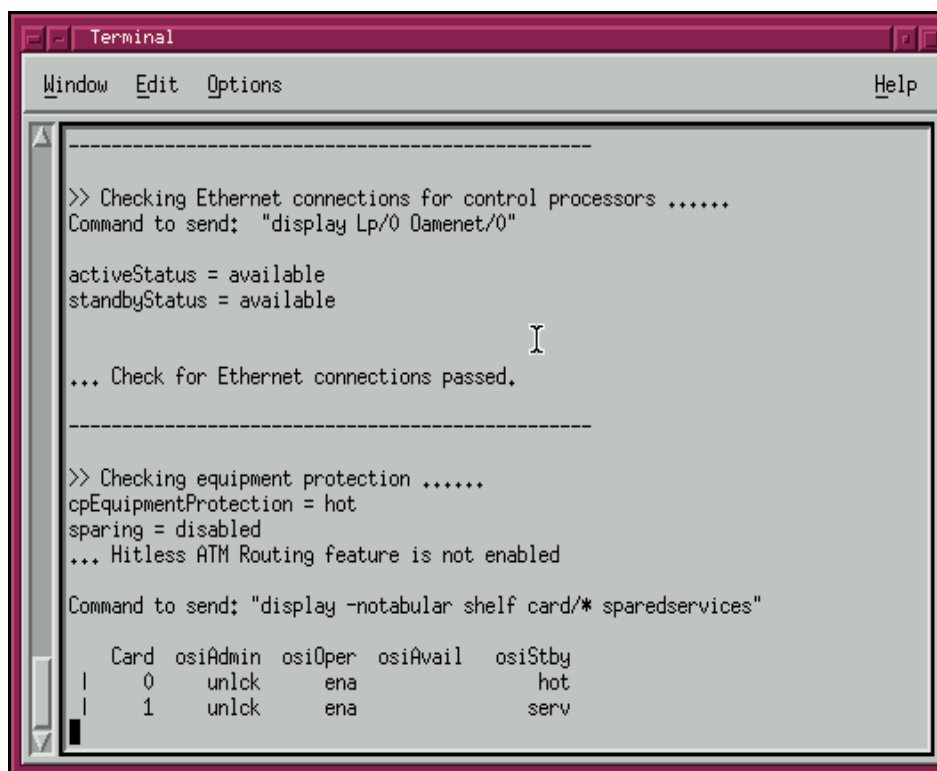
- 16 In the Migrate Software on Module window, select the destination software version from Target Releases and select applications matching the Current Release applications.
- 17 Select the required patches from the patch list.

**Note:** Only patches specific to the applications selected in the previous step can be applied from the patch list. For example, if the wanDte\_CG02xxx application has not been selected, then do not select any wanDte patches.

To determine which patches to select, refer to the readme file that accompanies the patch software on [www.Nortel.com](http://www.Nortel.com). In section 2 of the readme file, you will see a list of the "patches that comprise the MSS 15000/20000 patch baseline". Nortel recommends that each of these patches be applied, as appropriate (see note above about dependency on matching patches to applications), in order to remain patch current.

- 18 To proceed with the migration, click **OK**.

- 19 The script progresses to the pre-activation stage and executes pre-HSM verification checks.

A screenshot of a terminal window titled "Terminal" with a menu bar containing "Window", "Edit", "Options", and "Help". The terminal displays the following text:

```
>> Checking Ethernet connections for control processors
Command to send: "display Lp/0 Oamenet/0"

activeStatus = available
standbyStatus = available

... Check for Ethernet connections passed.

>> Checking equipment protection
cpEquipmentProtection = hot
sparing = disabled
... Hitless ATM Routing feature is not enabled

Command to send: "display -notabular shelf card/* spareservices"

Card osiAdmin osiOper osiAvail osiStby
| 0 unlk ena hot
| 1 unlk ena serv
```

- 20 Monitor the pre-HSM verification.

While the record is executing the pre-HSM portion of the script, information is displayed and you will be prompted to continue with the software migration or to cancel the software migration.

Monitor the prov component using the Component Information Viewer. While the activation is in progress, monitor for alarms from the node using the MDM alarm display. Stop the migration if unexpected warnings or alarms appear.

- 21 At the completion of the pre-activation portion of the script, you are asked if you want to continue with the software migration. To proceed, press **Enter**.

The migration takes place. The number of calls and components that have been provisioned on the node determine how long the activation takes.

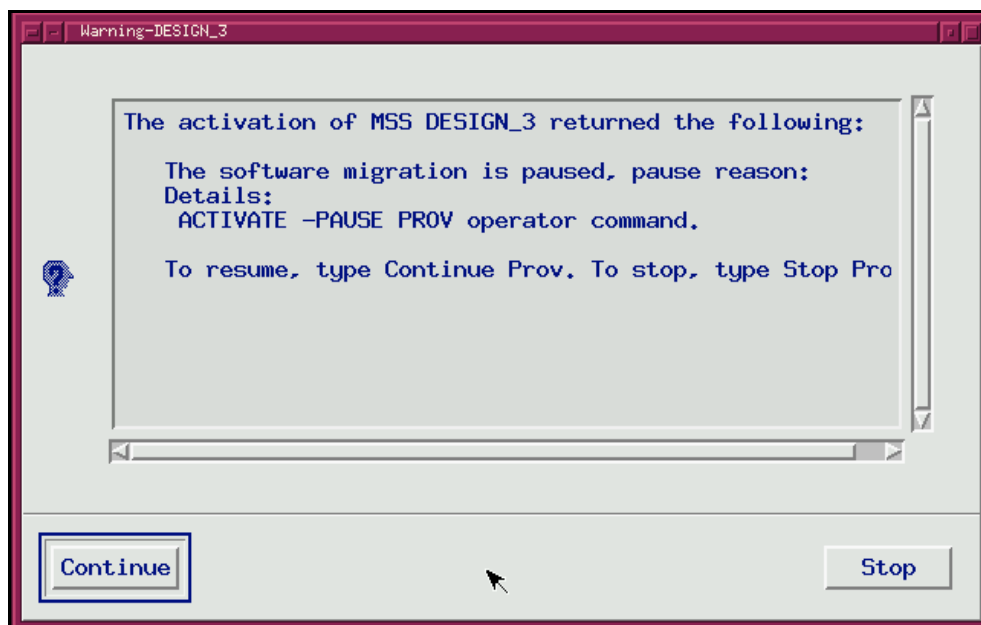
Monitor the status of the node and the status of the migration. To monitor the progress of the migration, use the Component Information Viewer to display the attributes of the provisioning component. You can continue to do this until you lose

connectivity to the node, which is when the originally active CP begins to load the new software. The MDM server automatically reconnects to the node when possible.

While the activation is in progress, monitor the alarms from the node using the MDM Alarm Display. If unexpected warnings or alarms appear, stop the migration.

- 22** When the software migration pauses, you are prompted to either stop the migration or continue the migration.

The software migration will pause because the **-pause** option has been chosen, or there is something wrong with the application during the software migration (Phases 1 to 3).



#### **CAUTION**

##### **Contact GNTS before continuing during a migration pause**

Contact Nortel Global Networks Technical Support (GNTS) for advice or assistance before continuing if the software migration pauses due to a Migration Visible Alarm.

Review the Migration Visible Alarms to determine whether to continue the migration. Click **Continue** or **Stop**.

When you have used the **-pause** option and the system has paused prior to the switchover, and you select **Continue** to continue HSM, the HSM will not pause again to allow you to make the checks outlined previously (unless the system finds a fault).

- 23** At the completion of the pre-activation portion of the script, you are asked if you want to continue with the software migration. To proceed, press **Enter**.

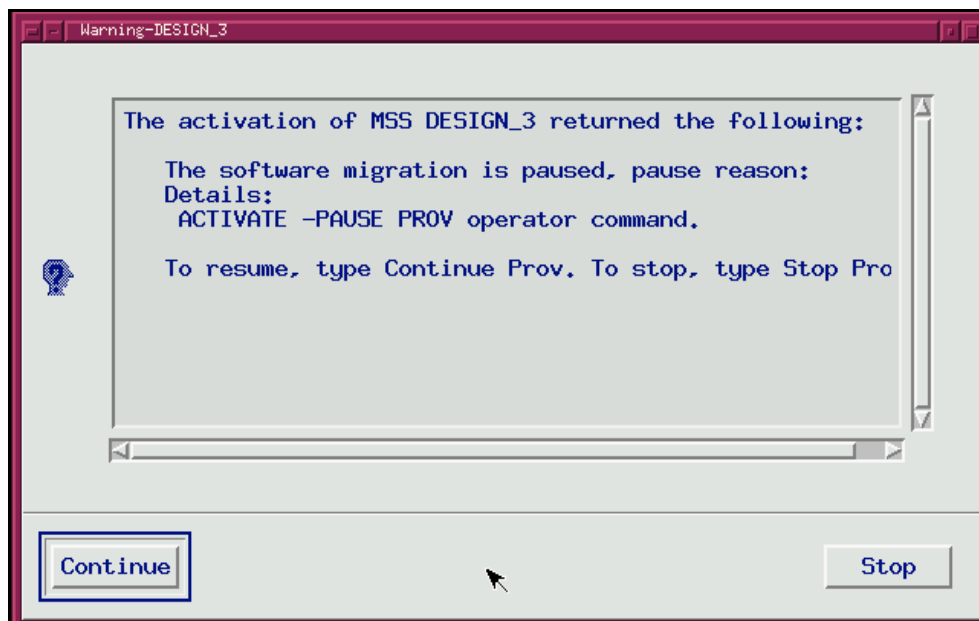
The migration takes place. The number of calls and components that have been provisioned on the node determine how long the activation takes.

Monitor the status of the node and the status of the migration. To monitor the progress of the migration, use the Component Information Viewer to display the attributes of the provisioning component. You can continue to do this until you lose connectivity to the node, which is when the originally active CP begins to load the new software. The MDM server automatically reconnects to the node when possible.

While the activation is in progress, monitor the alarms from the node using the MDM Alarm Display. If unexpected warnings or alarms appear, stop the migration.

- 24** When the software migration pauses, you are prompted to either stop the migration or continue the migration.

The software migration will pause because the **-pause** option has been chosen, or there is something wrong with the application during the software migration.



#### **CAUTION**

##### **Contact GNTS before continuing during a migration pause**

Contact Nortel Global Networks Technical Support (GNTS) for advice or assistance before continuing if the software migration pauses due to a Migration Visible Alarm.

Review the Migration Visible Alarms to determine whether to continue the migration. Click **Continue** or **Stop**.

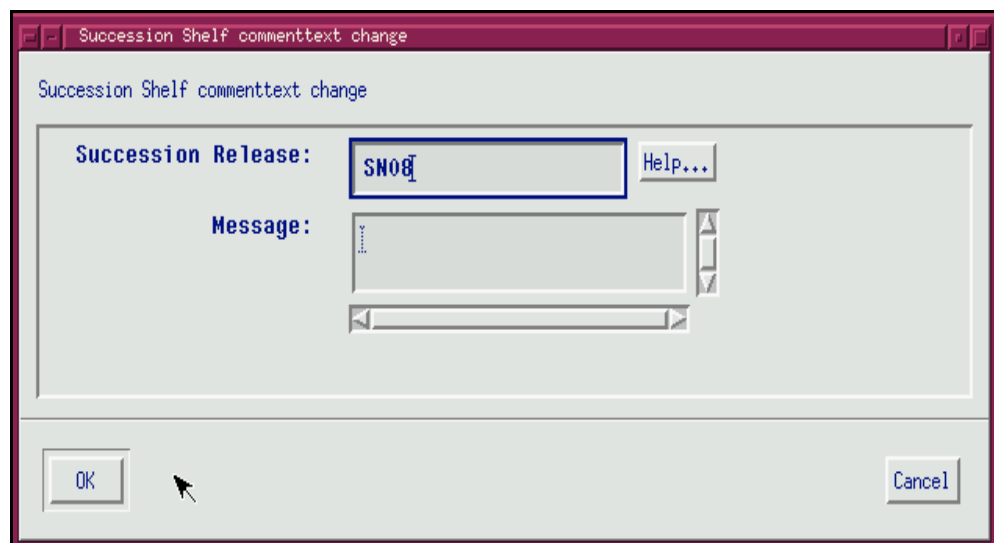
When you have used the **-pause** option and the system has paused prior to the switchover, and you select **Continue** to continue HSM, the HSM will not pause again to allow you to make the checks outlined previously (unless the system finds a fault).

- 25 After the HSM activation phase and commit phase are complete, the Network Activation tool starts the post-HSM verification portion script. While the record is executing the post-HSM portion of the script, information is displayed and you will be prompted to continue with the software migration. When prompted, press the Enter key to continue.

After the record has executed the post-HSM verification, a fabric card firmware upgrade is performed on each fabric card if required.

Information on the result of the fabric card firmware upgrade and fabric card test is written to the log file. If the first fabric card firmware upgrade does not complete successfully, the second fabric card firmware upgrade is not attempted.

- 26 The SISM tool post-activation script prompts you for the new solution (Carrier Voice over IP) release name to display in the MSS/MG15000 Shelf CommentText. Use the format: SN09U.



If you click **Cancel**, the update is cancelled before execution and the MSS/MG15000 Shelf CommentText remains unchanged.

- 27 Click **OK**.

A NAT record is created and the NAT window is displayed for a second time since the start of SISM.

This time it activates the service data (the only change is the Shelf CommentText) with no pre- and post checks.

The Shelf CommentText attribute on the target node is updated with the solution (Carrier Voice over IP) release name being



displayed before the rest of the information in the Shelf CommentText field.

- 28** When all actions in the record have completed successfully, the entire record turns blue.

Double-click the executed record in the record list to display and review the logged information. Alternatively, choose Show Status from the record list pop-up menu.

- 29** Select **Exit** from the File menu to close the Network Activation Tool.

- 30** Select **Exit** from the File menu to close the Component Information Viewer tool.

- 31** If you have configured in-band OAM, compare the status of the Atmmpe components with the information gathered during the HSM preperation.

- a** If the node being migrated relies on OAM Ethernet connectivity, compare the status of the active control processor with the status recorded before the HSM. For VSP3-0 FPs use the command:

**display Lp/0 Oamenet/0 activeStatus**

- b** If the node being migrated relies on OAM Ethernet connectivity, compare the status of the standby control processor with the status recorded before the HSM.

**display Lp/0 Oamenet/0 standbyStatus**

- 32** If **display -o prov** shows a different version number for the editViewName from the committedFileName, execute the following comments through the commandConsole:

```
PROV 3> st pr
```

```
Prov
```

```
ok 2004-06-01 10:36:06.01
```

```
PROV 4> load -file(<committedFileName>) pr
```

```
Prov
```

```
Loaded or applied file <committedFileName>.
```

```
ok 2004-06-04 10:20:47.36
```

```
PROV 5> end pr
```

```
Prov
```

```
ok 2004-06-01 10:36:09.45
```

The following output shows an example of misaligned editViewName and committedFileName.

```
Prov
adminState = unlocked
operationalState = enabled
usageState = idle
provisioningActivity = none
activityProgress = n/a
standbyCpActivity = none
standbyCpActivityProgress = n/a
committedFileName = CG0124F_April_27.full.001
currentViewFileName = CG0124F_April_27.full.001
lastUsedFileName = CG0124F_April_27.full.001
provisioningSession =
provisioningUser =
checkRequired = no
confirmRequired = no
editViewName = CG0124F_April_27.full.001
editViewAddedComponents = 0
editViewDeletedComponents = 0
editViewChangedComponents = 0
currentJournal = 0
journalDisabledReason = not disabled
restorePossible = no
```

- 33** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Stop the HSM using MDM SISM tool

At any decision point during the software migration before the activation phase has begun, you can select **Cancel** and the migration will stop. The Network Activation and MDM Component Information Viewer windows can be closed by selecting **File** and then **Exit**.

During the pre-script phase, you can stop the process by entering **<Ctrl> -C** in the pre-script window.

After the software activation has started and while the migration is in the Pause state, you can abort the software migration hitlessly by clicking **STOP** in the Network Activation tool's (NAT) main window. The NAT sends a **stop prov** command to the node and all the tool's processes stop. The success of the stop depends on timing. You can abort the software migration hitlessly before the migration switchover phase starts by clicking **STOP** in the NAT but success here also depends on timing. If the node enters the migration switchover phase before processing the **stop prov** command, it is too late to stop the hitless software migration.

If the system detects a problem during the software migration, the hitless software migration automatically pauses before migration switchover occurs to allow you to review the migration visible alarms before continuing or stopping the migration.

To stop the process after the Migration switchover phase has started, click **Stop** in the Network Activation Tool main window. Further processing stops on the HSM SISM tool (but not on the node).

In all of the previous cases, close the SISM tool after stopping an HSM.

- Select **Exit** from the File menu to close the NAT.
- Select **Exit** from the File menu to close the Component Information Viewer window.

If the Terminal Window is open, click **Close** from the Terminal Window menu.

Issue **start prov; copy prov; end prov** from the Command Console before restarting SISM.

To back out after the migration switchover, follow the steps in [Rollback of MSS 15000/MG 15000 nodes on page 995](#).

**CAUTION****Non-hitless process**

Stopping the process after the HSM switchover is not a hitless process.

---

## Feature activation on MSS 15000/MG 15000 nodes

---

Use the tasks in this section to activate features following the upgrade of MSS 15000/MG 15000 to SN09U.

To provision the optional Media Gateway 15000 periodic routine exercise (REX) feature, see NN10600-783 *Nortel Media Gateway 7480/15000 Periodic Routine Exercise*.

### Prerequisites

The HSM is complete.

### Feature activation task flow

The following shows the sequence of tasks to perform to activate new features:

- [Generating an initial NP template log for audit comparison on page 984](#)
- [Provisioning the hitless activation of critical attributes on page 991](#)
- [Release specific feature activation procedures on page 992](#)

### Generating an initial NP template log for audit comparison

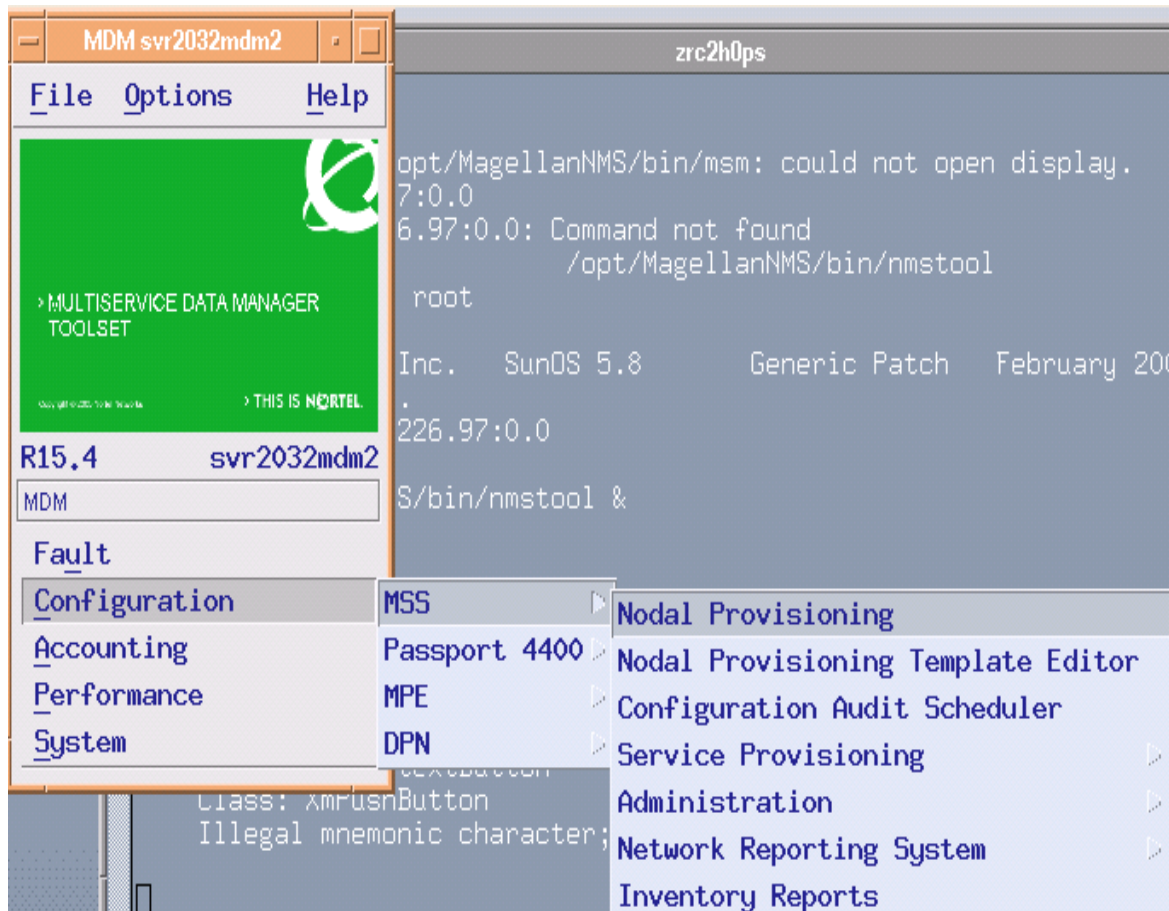
Generate a NP template log for a node to set a baseline against which an audit is run. The NP template log is a list of templates that have been applied to a provisioning view. The MSS/MG configuration data is compared against a template log and the discrepancies between the current configured view and the view represented by the NP template log are reported in the Node Level Audit report. If an in-service node does not have a template log, use the following procedure to generate an initial NP template log.

## Generating an initial NP template log

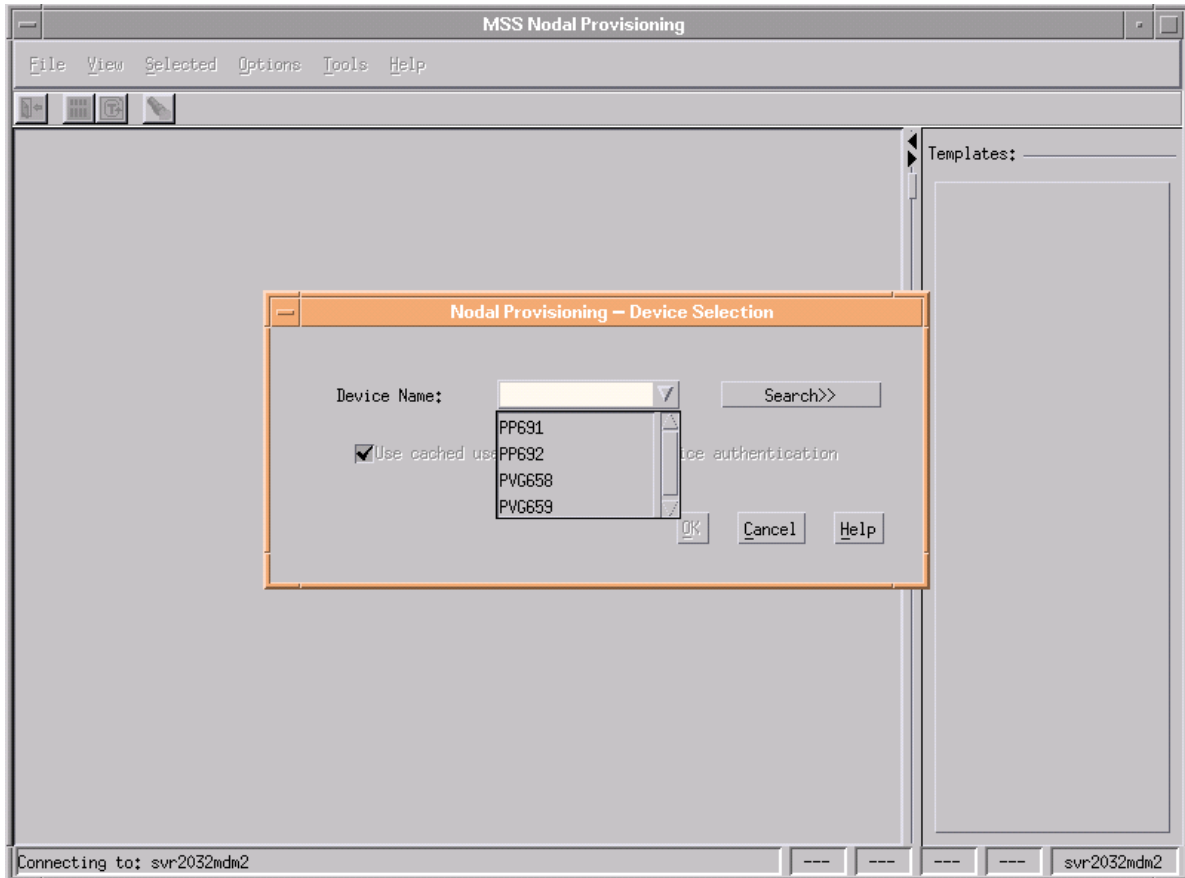
- 1 Launch the MDM Nodal Provisioning tool by typing  
`/opt/MagellanNMS/bin/nmstool &`



- 2 Access the Nodal Provisioning menu using the following navigation: **Configuration > MSS > Nodal Provisioning**

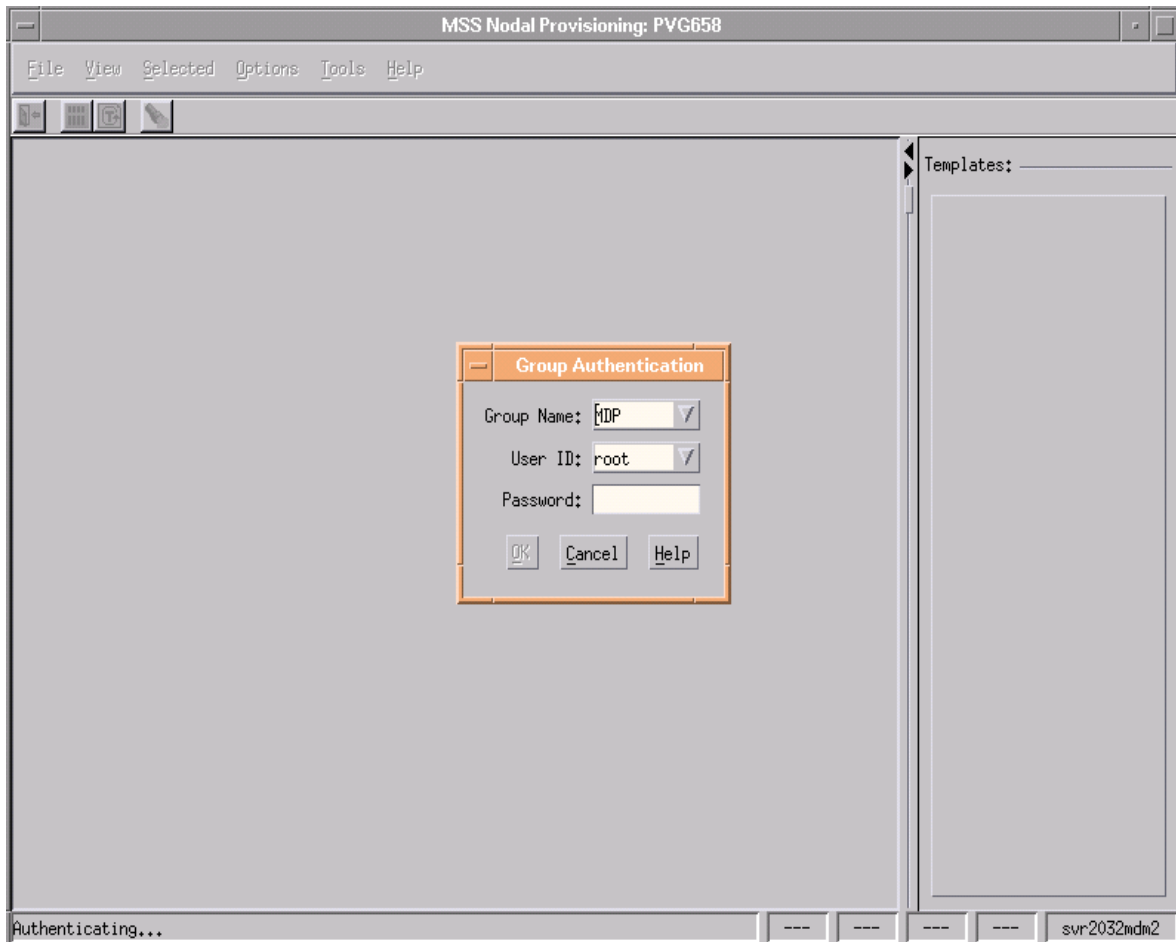


- 3 The Nodal Provisioning-Device Selection window opens. Select a device.





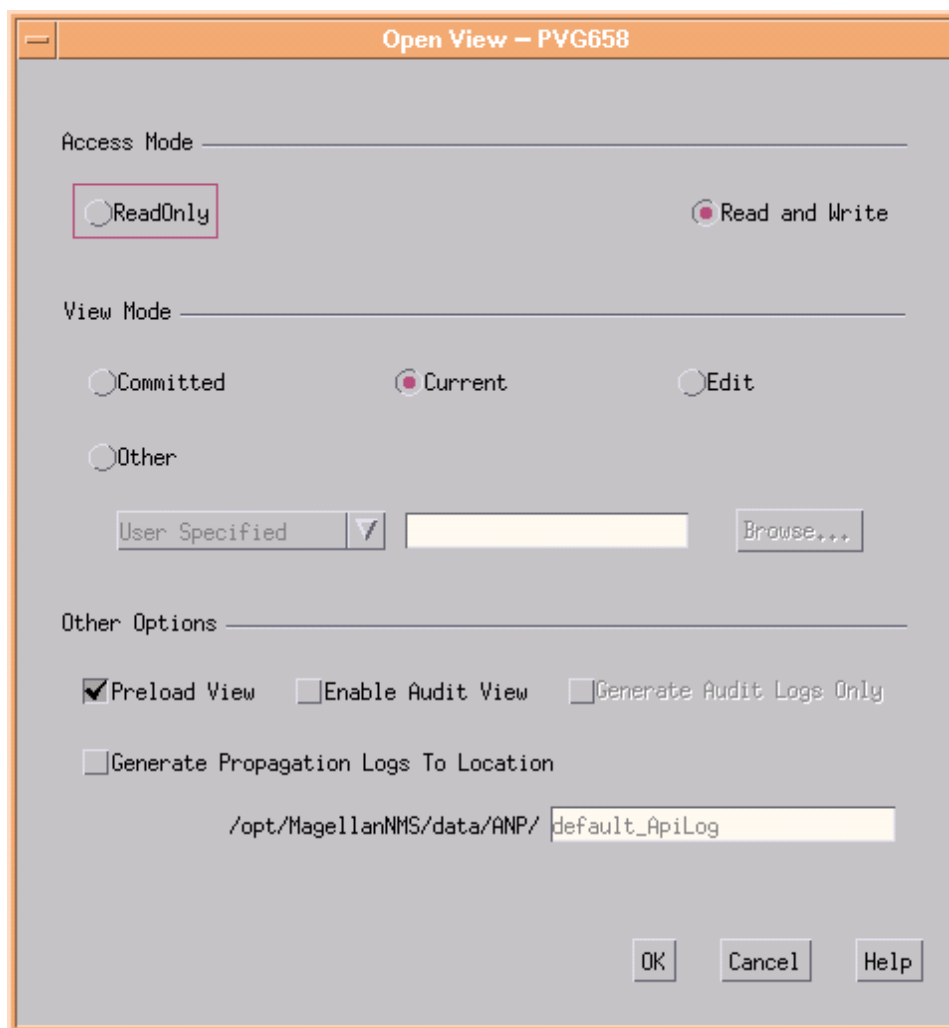
- 4 When prompted for a password, enter it, and select Ok.



- 5 The Open View-PVGnnn window opens up. Select **Read and Write** access mode and select **Enable Audit View** option. Once the Enable Audit View option has been selected the Generate Audit Logs Only becomes available and has to be selected.

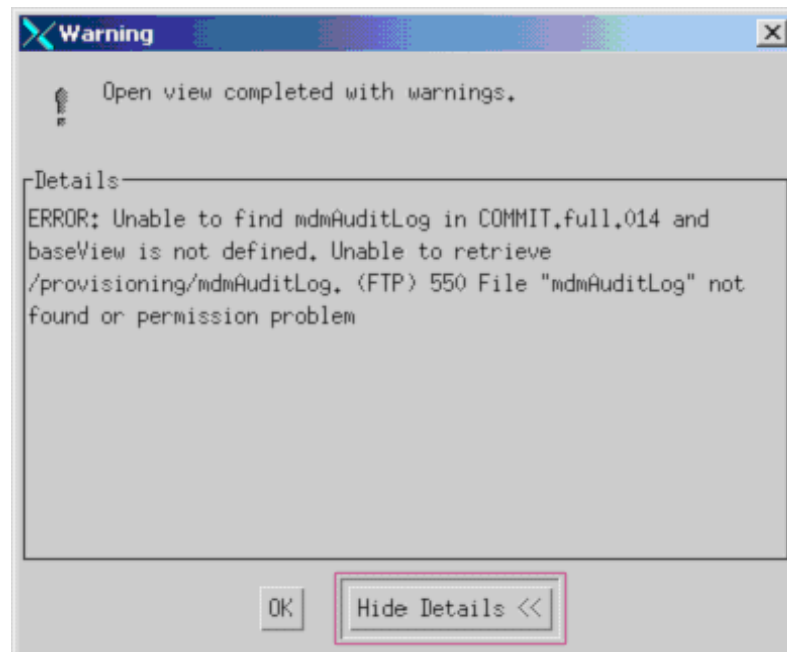
Open View-PVGnnn will open up only when "Always Prompt before Open View" is checked in User Preference dialog (Options->User Preferences...).

Open View-PVGnnn will display either the default values or user preference values, if you set them in User Preference.



- 6 The following dialog appears when Generate AuditLogs is used for the first time.

**Note:** Press the **Show Details** button on the Warning window in order to see the full message. This dialog can be safely ignored and is normal for the first time using audit logs. Proceed to [step 7](#).



- 7 If instead of the above Warning window you get a "Confirmation" window, press "**No**" because this is an indication that the mdmAuditLog file already exists. Close the view (**File > Close View**). Go to [step 10](#)
- 8 After the Nodal Provisioning tool opens the view on the MSS/MG, apply templates. Refer to "Auditing a Multiservice Switch service using a template", in *Multiservice Data Manager Configuration Tools*, NTP 241-6001-023.
- 9 Close the view (**File > Close View**).
- 10 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Provisioning the hitless activation of critical attributes

When hitless activation of critical attributes (HCA) is enabled, it helps prevent operators from making provisioning changes that can cause service outages on MSS/MG nodes after a change to a critical attribute (CA) is activated. Operators must provision whether CA activation is permitted for an attribute by adding the component called Prov ActivationMode (it is not added by default) and enabling it. The following procedure describes how to add and enable the component. If further provisioning changes are required, you must disable the component before doing further provisioning and enable it after the provisioning is complete.

For information on enabling HCA, or making changes after HCA has been enabled, or information on halting and continuing HCA, , see the NN10114-511 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP/PT-AAL2* guide.

See the NN10600-550 *Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures* guide for information on monitoring HCA.

### Provisioning hitless activation of critical attributes

- 1 Log in with the appropriate permissions.
- 2 Enter provisioning mode so that you can issue the appropriate commands:  
**start prov**
- 3 Add the ActivationMode component:  
**add Prov ActivationMode**  
**Note:** The default for ActivationMode hitlessActivation is enabled.
- 4 Perform a semantic check:  
**check prov**
- 5 Activate, confirm and commit the change:  
**activate prov**  
**confirm prov**  
**save prov**  
**commit prov**

- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Release specific feature activation procedures

Perform the following provisioning if applicable to your solution

- For all MSS15k/MG15k solutions, perform the following procedure to enable provisioning auto confirmation. Once enabled, a “confirm prov” is no longer required after activation in order to prevent the node from resetting after 20 minutes.

[Enable autoconfirm on page 992](#)

- If you have a MG15k PT-IP or UP-AIP over Gig E solution, then perform the following procedure:

[Enable static heartbeat on MG15000 on page 993](#)

- If you have a MG15k as a host device for PT-IP over Gig E solution, then perform the following procedure:

[Set the local host topology for MG15000 on page 993](#)

### Enable autoconfirm

- 1 Log in with the appropriate permissions.
- 2 Enter provisioning mode so that you can issue the appropriate commands:  
**start prov**
- 3 Enable provisioning autoconfirm attribute:  
**set prov autoconfirm on**
- 4 Perform a semantic check:  
**check prov**
- 5 Activate, confirm and commit the change:  
**activate prov**  
**save prov**  
**commit prov**
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Enable static heartbeat on MG15000

- 1 Log in with the appropriate permissions.
- 2 Enter provisioning mode so that you can issue the appropriate commands:  
**start prov**
- 3 Repeat the following for all instances of Vrs supporting voice traffic.  
**set Vr/VOIP ip static hbDeadInt 4**  
**set vr/VOIP ip static route/0.0.0.0,0.0.0.0,0 heartbeat enabled**  
where  
    **VOIP**  
        is the name of a Vr supporting the MG voice traffic.
- 4 Perform a semantic check:  
**check prov**
- 5 Activate, confirm and commit the change:  
**activate prov**  
**confirm prov**  
**save prov**  
**commit prov**
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Set the local host topology for MG15000

- 1 Log in with the appropriate permissions.
- 2 Enter provisioning mode so that you can issue the appropriate commands:  
**start prov**
- 3 Repeat the following for all instances of Vrs supporting voice traffic.  
**set vr/VOIP custSpec localHostDeviceTopology layer2**  
where

**VOIP**

is the name of a Vr supporting the MG voice traffic.

- 4 Perform a semantic check:  
**check prov**
- 5 Activate, confirm and commit the change:  
**activate prov**  
**confirm prov**  
**save prov**  
**commit prov**
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Rollback of MSS 15000/MG 15000 nodes

### Application

Use this procedure to back out of an upgrade in which software has already been activated. Once this procedure is completed, the software on the node is reverted to provisioning view that was saved while running a previous version of the software.

After successfully completing the rollback, use the MDM toolset to change the solution release name.

### Prerequisites

**CAUTION****Reverting to an earlier software version is not hitless**

After the originally-active CP and FPs have been reset, reverting back to the old configuration view is not hitless. At this point, any downgrade to the old configuration view results in a loss of call processing. While loading the old software and configuration view, the following events occur: call processing is initially maintained while the previous software load is loaded into one of the control processors. The function processors then go out of service, resulting in a loss of calls.

**CAUTION****Loss of provisioning changes**

If you revert the node to an earlier version of the software, provisioning changes made to the upgraded version are lost.

The prerequisites are as follows:

- Contact Nortel GNTS before initiating a rollback to verify that a rollback is necessary.
- Ensure the FPs and CPs on the shelf are compatible with the level of software to which you are reverting. To verify the minimum software requirements of the FPs, see NN10600-551 *Nortel Multiservice Switch 7400/15000/20000 FP Configuration Reference*. To verify the software requirements of the CPs, see



*NN10600-120 Nortel Multiservice Switch 15000/20000 Hardware Description.*

- To revert to a saved view of an older Nortel Multiservice Switch software version, when the MSS 15000/MG 15000 node restarts, it restarts in the operational state it was in when you saved the current view.
- The Backup server, the Restore sever, the MSS Backup provider, the MSS Restore provider, the FMDR server, and the GMDR server must all be running on the Multiservice Data Manager (MDM) server for the MDM Backup and Restore tool to function properly. See 241-6001-807 *Nortel Multiservice Data Manager Network Backup and Restore* for information on how to check these servers.
- Nortel recommends that you perform this rollback using the MDM Command Console. For more information on opening the Command Console, see 241-6001-804 *Nortel Multiservice Data Manager Utilities*.

## Action

To roll back a MSS 15000/MG 15000 configured for AAL1 applications, use the procedure:

- [Rollback to SN08 of a node configured for AAL1 applications on page 996](#)

To rolling back a MSS 15000/MG 15000 configured for IP applications, use the procedure:

- [Rollback to SN08 of a node configured for IP applications on page 997](#)

### Rollback to SN08 of a node configured for AAL1 applications

#### *From the node*

- 1 Log in with the appropriate permissions.
- 2



#### **CAUTION**

##### **Possible loss of calls**

After activating the previously saved view, the following events occur: call processing is initially maintained while the previous software load is loaded into one of the control processors. The function processors then go out of service, resulting in a loss of calls.

Activate the previously saved view:

```
activate -force -file(<committedViewName>) prov
```

where

<committedViewName> is the name of the previously saved committed view

Network connectivity is lost and the node starts reloading the old software.

- 3 When the MDM server reconnects to the node, confirm the provisioning changes:

```
confirm prov
```

- 4 Commit the provisioning changes:

```
commit prov
```

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### **Rollback to SN08 of a node configured for IP applications**

#### ***From the node***

- 1 Log in with the appropriate permissions.

- 2 Enter provisioning mode:

```
start prov
```

- 3



#### **CAUTION**

##### **Possible loss of calls**

After activating the previously saved view, the following events occur: call processing is initially maintained while the previous software load is loaded into the control processors. The function processors then go out of service, resulting in a loss of calls.

Activate the previously saved view:

```
reloadcp -force -file(<committedViewName>) lp/0
```

where

<committedViewName> is the name of the previously saved committed view

- Network connectivity is lost and the node begins reloading the old software.
- 4 When the server reconnects to the node, confirm the provisioning changes:  
**confirm prov**
  - 5 Save the view:  
**save prov**
  - 6 Commit the provisioning changes:  
**commit prov**
  - 7 Exit provisioning mode after the commit is complete:  
**end prov**
  - 8 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Peripheral Module upgrade

### ATTENTION

MG 4000, IW SPM ATM, and DPT SPM do not have new software loads for SN09 or SN09U. Ensure these components are patch and MR current. No upgrades are required for these components.

Peripheral module upgrades use the PANTHER automated upgrade tool for the following components:

- Legacy Peripheral Modules:
  - LCM
  - XPM
  - XPMs hosted by MG 9000 ABI cards
  - DMS SPM (PT-AAL1)
  - LPP/FLPP
- IW SPM IP (IAC and PT-IP *plus International PT-AAL2*)
- IW SPM ATM (PT-AAL1 and UA-AAL1)
- MG 4000 (PT-AAL1 and UA-AAL1)
- DPT SPM (PT-AAL1 and UA-AAL1)

The following software delivery methods are available:

- DAT Tape Delivery - XA-Core tape drives
- CD-ROM - Call Agent CD drives
- Electronic Software Delivery

An SPM-based node upgrade consists of two different upgrade methods:

- Automated upgrades
- Manual upgrades

The automated method upgrades several circuit pack types at once. The manual method upgrades circuit pack types individually. This book describes the automated upgrade procedure.

For SPMs and IW SPMs, the Sync Resource Module (SRM) does not provide sparing therefore TDM offices that use SRMs for office synchronization must upgrade the SRMs prior to using the Automated Upgrade process. All SRMs must be upgraded manually before beginning the Automated Upgrade procedure. Each TDM office has two SRMs which can be located in the SYNCLK table.

SRMs configured in MG 4000 nodes use contain sparing and may be upgraded using the Automated Upgrade process.

## Upgrade strategies

Nortel Networks strongly recommends completely loading entire SPMs with a single maintenance release or milestone upgrade. Failure to load all RMs and CEMs in an SPM can result in inadvertently running unsupported mixed load SPM configurations. Mixed load configurations can, in turn, result in the reload of modules in an out-of-procedure sequence, which can be potentially service affecting. If unable to complete the loading of all SPMs in one session, plan to upgrade a limited number of SPMs in multiple sessions.

During the upgrade process SPMs not loaded with an upgrade load reflect an ISTB condition caused by a loadname mismatch in the MNCKTPAK table. The ISTB condition remains in effect until all IW SPMs have been upgraded.

Operating company personnel can upgrade more than one RM and more than one SPM at the same time.

To upgrade multiple at the same time on the same SPM, open a MAPCI session for each RM type.

To concurrently upgrade multiple SPMs, Nortel Networks recommends upgrading up to two SPMs at the same time. Open a MAPCI session for each RM type on each SPM.

Note that during in-service loading, which involves downloading from the computing module (CM), you can load a maximum of eight RMs at the same time. The restriction of in-service loading no more than eight RMs at the same time also applies to CEMs. During mate loading, up to sixty four RMs can be loaded from the mate at the same time.

Periodically checking the carrier status during the upgrade process provides a method for monitoring the upgrade integrity.

For nonpatchable loads, post-release software updates (PRSU) must be built into the load file.

## Automated Upgrades

An automated upgrade procedure, known as PANTHER, consists of:

- the PMUPGRADE tool
  - selects and copies the new PM load and patch files from the distribution media to the Core
  - produces the PM upgrade plan outlining the tasks required to upgrade the PMs with the new loads and patches
- the SWUPGRADE PM tool
  - automates task execution in the PM upgrade plan to load and patch the necessary PMs

Panther does not support the upgrade of unspared RMs therefore RM spares must be configured before beginning an automated upgrade.

PANTHER makes a set of eight SPMS for upgrade. It constructs an RM list that comprises the RM groups for all eight SPMs. The RM groups list contains RM groups of the first SPM in the current set sequentially followed by RM groups for the remaining SPMs.

Loading times for similar RM types vary only slightly, therefore PANTHER loads the RMs of similar protection groups concurrently to expedite the process without waiting for the slowest RM type to load. The loading times for the 8 RMs of similar RM protection type usually require the same amount of time and therefore the upgrade process does not wait for the slowest RM in the group to load.

PANTHER can concurrently mate load up to 64 RMs across 8 SPMs in the current upgrade set. The calculation for determining the maximum RMs available for mate loading is:

$$\text{New RM Mate Loading Concurrency limit} = 8(\text{SPMs}) * 8(\text{Prot group per SPM}) = 64$$

### \$XREF Patch Control File

The PMUPGRADE tool uses an \$XREF patch control file to select the required PRSUs for a load. An XA-Core tape cartridge labeled as *Patches:Yes* should contain the appropriate \$XREF file for the corresponding load. If the tape does not contain an \$XREF file, then the

PMUPGRADE tool bypasses the steps to select or copy PRSUs and generates the following MAP message:

*WARNING: No Patch Control File Found. No patch files selected.*

When an office receives an \$XREF file through an X.25 NOP link, the file must be placed on the Patch File Distribution volume and the corresponding PRSU files placed on temporary disk volumes specified as the ISN Patch Destination volume and the XPM Patch Destination volume. PRSUs cannot reside on the same volume as the \$XREF file.

The PMUPGRADE tool communicates the \$XREF file name and location to the SWUPGRADE PM tool during the automated PM update. The SWUPGRADE PM tool accesses and automatically applies the PRSUs to any designated PM load files.

When downloading patches and loads through file transfer protocol (FTP) or other electronic methods, an \$XREF file automatically generates if the following two conditions are met:

- all PM loads and corresponding patches are on a temporary disk volume
- no other \$XREF file is present on the distribution volume

Electronically downloading patches and loads automatically copies the PM loads and their corresponding patches from the disk distribution volume to the selected destination volumes and generates a new \$XREF file available for use by the SWUPGRADE tool.

## What's new in PM Upgrades in (I)SN09U

### Feature changes



#### **CAUTION**

##### **Possible service interruption**

UDP Signaling has to be enabled in table MNMGPIIP for IW-IP SPM, otherwise TABXFR will cause tuple fallout during upgrade.

For SN09 and later releases, enable UDP Signaling by changing SIGIPENA to Y before proceeding with the Upgrade.

Peripheral Modules do not have new software loads for SN09U. Maintaining the patch currency and upgrading to the most recent Maintenance Release ensures SN09U compatibility.

## Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U
- SN09U to SN09U

## Estimated upgrade times

The following table provides upgrade time estimates for the PMs.

| Component                                                             | Upgrade time (minutes)                                                                                                                             | Soak time (minutes) | Total (minutes)                        |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|----------------------------------------|
| For legacy Peripheral Modules, refer to the appropriate documentation | For legacy PMs, refer to the <i>Peripheral Module Release Document</i> , 297-9051-599 (intl), or 297-2663-599 (NA) in your Helmsman DMS collection |                     |                                        |
| IW SPM IP                                                             | 1 hour for concurrent upgrade up to 8                                                                                                              |                     | 1 hour for concurrent upgrade up to 8  |
| IW SPM ATM                                                            | 1 hour for concurrent upgrade up to 8                                                                                                              |                     | 1 hour for concurrent upgrade up to 8  |
| MG 4000                                                               | 3 hours for concurrent upgrade up to 8                                                                                                             |                     | 3 hours for concurrent upgrade up to 8 |
| DPT SPM                                                               | 3 hours for concurrent upgrade up to 8                                                                                                             |                     | 3 hours for concurrent upgrade up to 8 |

## System capacity

The software upgrade procedure can impact the system capacity. This means that additional disk space on the OAMP workstation is required for converting existing databases.

Each destination volume must have sufficient free space for the new peripheral module load or PRSU files and meet all office criteria.



## System performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade

The inactive or spare card that is being upgraded is out of service for up to 15 minutes per card.

There is no loss of CallP, billing or customer visibility to the switch as the traffic is load-shared with redundant components.

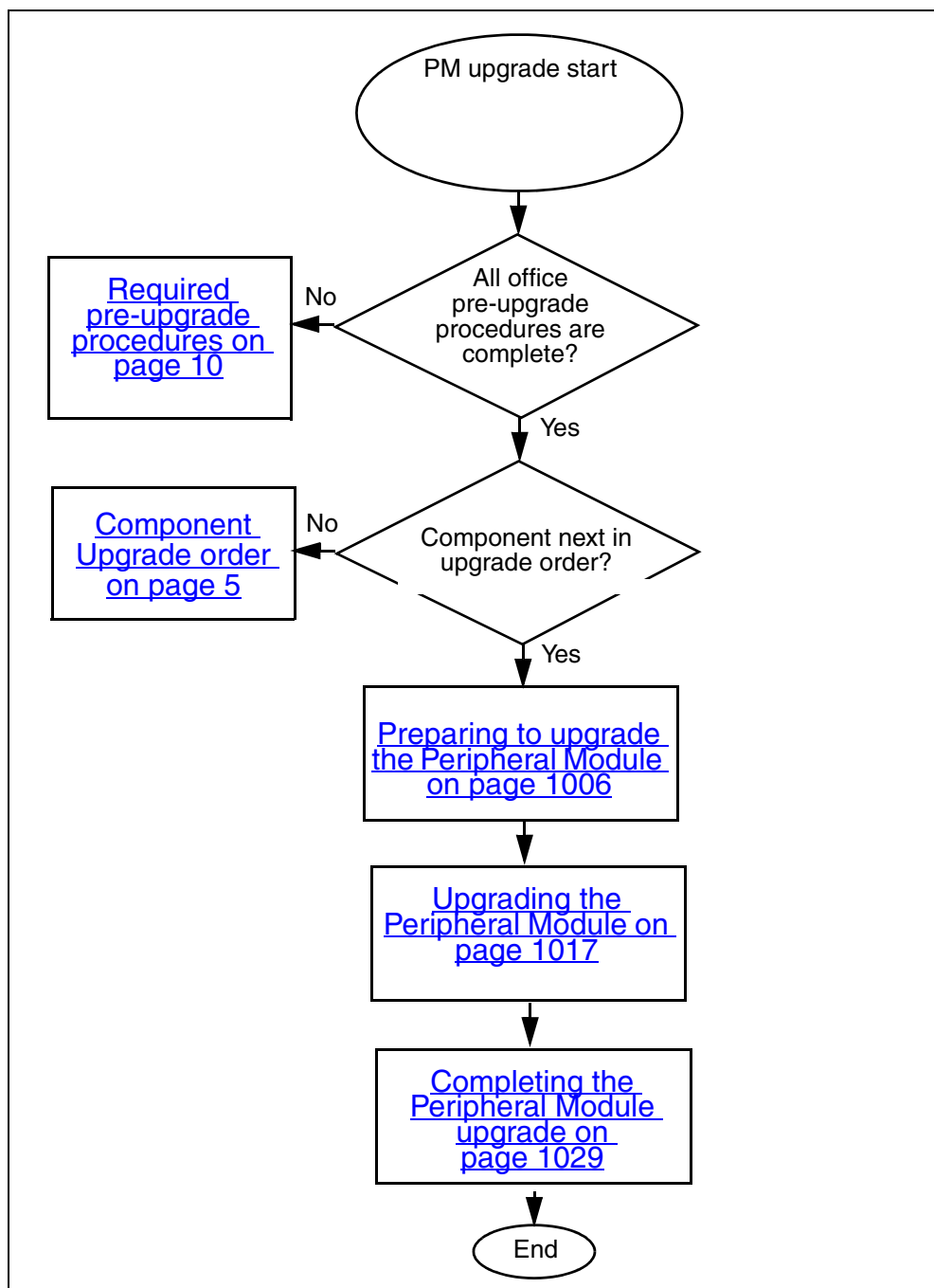
## System limitations during upgrade

During a software upgrade, the system prohibits the following actions:

- System administration
  - adding, deleting, or modifying users
  - setting the time of day
  - changing passwords
- System management
  - modifying the system name
  - adding or deleting system nodes
  - modifying the IP addresses

## PM upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

**Figure 1 PM upgrade tasks**

## Preparing to upgrade the Peripheral Module

The following procedure provides the steps you need to execute prior to upgrading the SPM-based Peripheral Modules. When applicable, a reference to the procedure that contains the detailed steps is provided.

### Prerequisites

You have completed the following tasks:

- all [Required pre-upgrade procedures on page 10](#)
- the upgrade of all components that precede the component in the [Component Upgrade order on page 5](#)

### Action

#### Upgrade Preparation

The [Variable Abbreviations](#) table defines the variables used in this procedure.

#### Variable Abbreviations

| Abbreviation        | Definition                                                                     |
|---------------------|--------------------------------------------------------------------------------|
| printer             | the printer name                                                               |
| dist_vol            | the name of the new Load File Distribution volume                              |
| ip_address          | the remote FTP volume server IP address for electronic software delivery (ESD) |
| pm_path             | the location of the PM loads files on the FTP server                           |
| patch_vol           | the name of the Patch Distribution volume                                      |
| patch_path          | the location of the patch files on the FTP server                              |
| load_number         | the number of the current load                                                 |
| load_name_1 (2) (n) | the names of the loads to be included or excluded (repeat variable as needed)  |

Perform the following procedures:

- ensure the circuit pack is in-service and the activity state is inactive
- suspend automatic routine exercise (REX) testing by typing

**REXTEST SUSPEND ALL**

and press enter

- if the network contains SPMs that require a Sync Resource Module (SRM) software upgrade, perform. [Manually upgrading an SRM on page 1035](#)
- [Preparing peripheral modules for an automated upgrade on page 1007](#)

**Preparing peripheral modules for an automated upgrade****ATTENTION**

Before beginning the automated upgrade, ensure that spares are configured for all RMs requiring an upgrade.

***At the CI level of the MAP display***

- 1 Send the terminal responses to a printer by typing  
**>RECORD START ONTO printer**
- 2 Enter the log utility and list devices for log output by typing  
**>LOGUTIL**  
**>LISTDEVS**

*Example of an active log output device*

| No. | Device | Status          | Rerouted | Format |
|-----|--------|-----------------|----------|--------|
| 0   | MAP121 | Outputting Logs | No       | STD    |

*Example of an inactive log output device*

| No.                | Device | Status    | Rerouted | Format |
|--------------------|--------|-----------|----------|--------|
| 1                  | MAP121 | Inactive. | No       | STD    |
| - End of devices - |        |           |          |        |

**If the device is****Do**

Inactive

[step 3](#)

Active (outputting logs)

[step 4](#)

- 3 Start the device by typing  
**>STARTDEV device**  
*Example of a MAP display*

```
>startdev map121
Log device MAP121 has been started.
Number of devices started : 1
```

- 4 Verify that all reports for the PRSM, SPM, NODE, and TUPL log types are configured for output by typing

```
>LISTREPS SPECIAL log_name
```

*Examples*

```
>LISTREPS SPECIAL PRSM
```

```
>LISTREPS SPECIAL SPM
```

```
>LISTREPS SPECIAL NODE
```

```
>LISTREPS SPECIAL TUPL
```

*Example of all log type reports configured for output*

| Log Name             | Rep. No. | Event Class | Type | Event Label | Suppressed/<br>Thresholded | Syslog |
|----------------------|----------|-------------|------|-------------|----------------------------|--------|
| -----                |          |             |      |             |                            |        |
| 67 report(s) printed |          |             |      |             |                            |        |

*Example of suppressed log type reports*

| Log Name | Rep. No. | Event Class | Type | Event Label         | Suppressed/<br>Thresholded | Syslog |
|----------|----------|-------------|------|---------------------|----------------------------|--------|
| -----    |          |             |      |                     |                            |        |
| SPM      | 650      | 0           | PASS |                     | *supp*                     |        |
| SPM      | 651      | 0           | FAIL |                     | *supp*                     |        |
| SPM      | 300      | 0           | TBL  | Device Fault Report | *supp*                     |        |

---

**If log reports are**

**Do**

suppressed

[step 5](#)

not suppressed

[step 6](#)

- 5 Resume any PRSM, SPM, NODE, and TUPL logs that have been suppressed by typing

```
>RESUME log_name log_#
```

*Example*

```
>resume spm 650
1 report(s) RESUMED
```

- 6 Identify the patch destination volume by typing

```
>TABLE PADNDEV;LIST ALL;QUIT
```

*Example*

```
TABLE: PADNDEV
TOP
DEVKEY DEVICE

 1 D030M17PTCH
 2 D030M15PTCH
 3 S01DIMAGE
```

BOTTOM

- 7 Access the PMUPGRADE utility by typing  
**>PMUPGRADE**
- 8 Set confirmation to ON by typing  
**>SET CONFIRMATION ON**
- 9 Carryover loads are load files on the tape that have the same version of the load currently used in the office. Operating company personnel can issue a SET CARRYOVER ON command to copy all peripheral module loads for the office. The default carryover setting is OFF.

| If the office                                                            | Do                      |
|--------------------------------------------------------------------------|-------------------------|
| requires all peripheral module loads for the office be copied            | <a href="#">step 10</a> |
| does not require all peripheral module loads for the office to be copied | <a href="#">step 11</a> |

- 10 Set carryover to ON by typing  
**>SET CARRYOVER ON**
- 11 Confirm the Load File Distribution setting is correct. If necessary, change the setting by typing

| If using | Do                                                                                               |
|----------|--------------------------------------------------------------------------------------------------|
| tape     | <b>&gt;SET LOADDISTRIB dist_vol</b><br><br><i>Example</i><br><b>&gt;SET LOADDISTRIB F02UTAPE</b> |
| ESD      | <b>&gt;SET LOADDISTRIB 'ftp://&lt;SDM_IP&gt;/&lt;directory_location&gt;'</b>                     |

| If using                                                                              | Do                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12                                                                                    | <i>Example</i>                                                                                                                                                                                                                                                                                                     |
|                                                                                       | >SET LOADDISTRIB<br>'ftp://11.22.33.44/swd/pmloads'                                                                                                                                                                                                                                                                |
|                                                                                       | Confirm the Load File Destination setting is correct. If necessary, change the setting by typing                                                                                                                                                                                                                   |
|                                                                                       | >SET LOADDEST dist_vol                                                                                                                                                                                                                                                                                             |
| 13                                                                                    | <i>Example</i>                                                                                                                                                                                                                                                                                                     |
|                                                                                       | >SET LOADDEST F02LPMLOADS                                                                                                                                                                                                                                                                                          |
|                                                                                       | Confirm the Patch File Distribution setting is correct. If necessary, change the setting by typing                                                                                                                                                                                                                 |
|                                                                                       | <b>If using      Do</b>                                                                                                                                                                                                                                                                                            |
| tape                                                                                  | >SET PATCHDISTRIB patch_vol                                                                                                                                                                                                                                                                                        |
| <i>Example</i>                                                                        |                                                                                                                                                                                                                                                                                                                    |
| >SET PATCHDISTRIB F02LPMLOADS                                                         |                                                                                                                                                                                                                                                                                                                    |
| ESD                                                                                   | >SET PATCHDISTRIB<br>'ftp://<SDM_IP>/<directory_location>'                                                                                                                                                                                                                                                         |
| <i>Example</i>                                                                        |                                                                                                                                                                                                                                                                                                                    |
| >SET PATCHDISTRIB<br>'ftp://11.22.33.44/swd/patchloads'                               |                                                                                                                                                                                                                                                                                                                    |
| 14                                                                                    | The ISN, XPM, and SPM Patch Destination settings must point to the patch file destination volume. Confirm the ISN, XPM, and SPM Patch Destination settings are correct based on the PADNDEV table listing obtained in <a href="#">step 6</a> . If necessary, change the setting by entering the following commands |
|                                                                                       | >SET ISNPATCH patch_vol                                                                                                                                                                                                                                                                                            |
|                                                                                       | >SET XPMPATCH patch_vol                                                                                                                                                                                                                                                                                            |
|                                                                                       | >SET SPMPATCH patch_vol                                                                                                                                                                                                                                                                                            |
| <b>Note:</b> The SPM patch destination volume should be entered in the PADNDEV table. |                                                                                                                                                                                                                                                                                                                    |
| <i>Example</i>                                                                        |                                                                                                                                                                                                                                                                                                                    |
| >SET ISNPATCH F02LPMLOADS                                                             |                                                                                                                                                                                                                                                                                                                    |
| >SET XPMPATCH F02LPMLOADS                                                             |                                                                                                                                                                                                                                                                                                                    |

**>SET SPMPATCH F02LPMLOADS**

- 15** Generate an office load report by typing

**>DISPLAY LOADS**

*Result*

PMUPGRADE compiles the PMUPGRADE Load Report from the PMLOADS table and the SPM inventory tables.

A load can have an empty “Tables Used” column. If office policy requires data in this column, perform the following steps:

- Exit PMUPGRADE
- Delete the out-dated load from the PMLOADS table
- Go to [step 7](#) of this procedure

- 16** Generate a node report for the office by typing

**>DISPLAY NODES**

*Result*

The PMUPGRADE Node Report is compiled from SPM inventory tables. The nodename information for the MNCKTPAK table is obtained from the MNNODE table.

- 17** Display the firmware information by typing

**>DISPLAY FWINFO**

- 18** Set the preferred load to the current load by typing

**>SET FWPREFERRED load\_number CURRENT**

The preferred load must be equal to the current load.

Repeat this step for each firmware load listed in [step 17](#).

- 19** Start the filecopy phase of the utility by typing

**>START FILECOPY**

*Time Requirements*

The FILECOPY process copies files to the destination volume and adds new loads to the PMLOADS table. The process requires approximately 40 minutes. The amount of time depends on the number of peripheral module loads and PRSU files.

- 20** When prompted to confirm a tape is in its appropriate drive, confirm the tape is physically inserted in the drive. Do not use the INSERTTAPE or IT commands on the tape.

If the tape cartridge label text indicates “Patches:Yes”, the tape includes the required PRSUs for peripheral module load files.



**21** At the prompt, continue by typing

&gt;Y

| If the response indicates                                                                      | Do                      |
|------------------------------------------------------------------------------------------------|-------------------------|
| that EXT files for datafill in the SPMLDVAL table are not available in the distribution volume | <a href="#">step 22</a> |
| the replacement loadname cannot be found                                                       | <a href="#">step 23</a> |
| Multiple replacements found for EXT file on the distribution volume                            |                         |
| or                                                                                             |                         |
| multiple replacement loadnames are found                                                       | <a href="#">step 24</a> |
| Possible one old replacement found on load distribution volume                                 |                         |
| or                                                                                             |                         |
| ready to continue                                                                              | <a href="#">step 25</a> |

**22** Stop the automated upgrade by typing

&gt;Q

Contact the next level of support to update the SPMLDVAL table.

**23** A response similar to the following example appears if PMUPGRADE cannot locate the replacement loadname.

No replacement loadname found on distribution volume for SM206BH1.  
Please enter replacement loadname, or "S" (Same) or "Q" (Quit FILECOPY)

| If                                                                            | Do                                                                                                   |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| A new load type replaces the current load type                                | Enter the new loadname. Ensure the loadname is typed accurately<br><br>Go to <a href="#">step 25</a> |
| The load is manufacture discontinued                                          | Enter "S"<br><br>Go to <a href="#">step 25</a>                                                       |
| The load is a filler RM load name, indicating an RM that does not have a load | Enter "S"                                                                                            |

|    |                                                                                                                                                                                                                                                                                                                          | If                                                              | Do                      |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|-------------------------|
|    |                                                                                                                                                                                                                                                                                                                          | Go to <a href="#">step 25</a>                                   |                         |
| 24 | <p>If a response indicates that multiple replacements are found on the load distribution volume, enter the appropriate replacement listed or just the load name.</p> <p>The load name appears before the underscore in the load file name. For example, DLC16DE is the load name for the load file DLC16DE_010082A3.</p> |                                                                 |                         |
| 25 | <p>Review the Load File Selection Report and determine if any loads need to be added or removed from the report.</p>                                                                                                                                                                                                     |                                                                 |                         |
|    |                                                                                                                                                                                                                                                                                                                          | If                                                              | Do                      |
|    |                                                                                                                                                                                                                                                                                                                          | one or more loads need to be added or removed from the report   | <a href="#">step 26</a> |
|    |                                                                                                                                                                                                                                                                                                                          | the report is complete and no loads need to be added or removed | <a href="#">step 31</a> |
| 26 | <p>Stop the file copy process by typing</p> <p><b>&gt;N</b></p>                                                                                                                                                                                                                                                          |                                                                 |                         |
|    |                                                                                                                                                                                                                                                                                                                          | If                                                              | Do                      |
|    |                                                                                                                                                                                                                                                                                                                          | one or more loads need to be removed from the report            | <a href="#">step 27</a> |
|    |                                                                                                                                                                                                                                                                                                                          | one or more loads need to be added to the report                | <a href="#">step 28</a> |
| 27 | <p>Remove the loads from the report by typing</p> <p><b>&gt;SET EXCLUDELOADS load_name_1 load_name_2 ... load_name_n</b></p> <p>Separate each load name with a space.</p> <p><i>Example</i></p> <p><b>&gt;SET EXCLUDELOADS BTMKA02 ECLI4BC</b></p>                                                                       |                                                                 |                         |
|    |                                                                                                                                                                                                                                                                                                                          | If                                                              | Do                      |
|    |                                                                                                                                                                                                                                                                                                                          | one or more loads need to be added to the report                | <a href="#">step 28</a> |
|    |                                                                                                                                                                                                                                                                                                                          | the report is complete and no loads need to be added or removed | <a href="#">step 29</a> |

- 28** Add the loads to the report by typing

```
>SET INCLUDELOADS load_name_1 load_name_2 ...
load_name_n
```

Separate the load names with a blank space.

*Example*

```
>SET INCLUDELOADS BTMKA02 ECLI4BC
```

| If                                                              | Do                      |
|-----------------------------------------------------------------|-------------------------|
| one or more loads need to be removed from the report            | <a href="#">step 27</a> |
| the report is complete and no loads need to be added or removed | <a href="#">step 29</a> |

- 29** Repeat the file selection phase of the utility by typing

```
>START FILECOPY
```

- 30** Confirm that the appropriate load names have been added or removed from the Load File Selection Report.

| If the Load File Selection Report                     | Do                      |
|-------------------------------------------------------|-------------------------|
| does not show the excluded and/or included load names | <a href="#">step 26</a> |
| shows the excluded and/or included load names         | <a href="#">step 31</a> |

- 31** Accept the Load Selection Report by typing

```
>Y
```

- 32** Confirm the patch file selection prompt by typing

```
>Y
```

PMUPGRADE uses the \$XREF patch control files to select PRSUs for copying. Depending on the method of PRSU delivery, this file may not be available. If the file is not available, PMUPGRADE generates a warning that no patch control file has been found. Contact your next level of support for instruction on how to proceed with the upgrade and a list of required PRSUs to be manually applied.

- 33** Create the list of files to copy by typing

```
>Y
```

*Time Requirements*

This final phase of the FILECOPY process requires approximately 20 minutes to complete adding new loads to the PMLOADS table. The amount of time depends on the number of peripheral module loads and PRSU files.

34

**ATTENTION**

Perform this step only if any offline peripheral modules are being installed or commissioned in the office.

Open a second window and update the LOAD field in the MNCKTPAK field to reflect the new software load for each RM type in all offline peripheral modules

35 Generate a PMUPGRADE load report for the office by typing

**>DISPLAY LOADS**

Confirm the selected new loads have been added to the report.

36 Start the generation of the PM upgrade plan by typing

**>START PLAN**

Only one PM upgrade plan can be executed at a time. A new plan cannot be started until an existing plan has been cancelled or completed.

37 Display the PM upgrade plan by typing

**>DISPLAY PLAN**

The PMUPGRADE Plan Report organizes the peripheral module upgrade by tasks and layers. A task is a set of peripheral modules of the same type at the same site with the same load requirements. A layer is a grouping of tasks.

38 Review the PMUPGRADE report.

- Confirm all peripheral modules that require upgrading are included in the plan report

For loads added to the Loadfile Selection Report with the SET INCLUDELOADS command, the associated peripheral modules must be manually upgraded.

- Confirm the correct loads are included with each task in the plan report.
- Confirm that the sequence of tasks in the plan report conforms to office policy.

If the sequence of tasks does not comply, use the RUNSTEP command during the automated upgrade to change the order of tasks.

- Confirm offline peripheral modules that are being installed or commissioned in the office are not included in the plan report. If an offline peripheral module is included in the plan
  - quit the PMUPGRADE process
  - update the appropriate peripheral module inventory table. Change the loadname field for that peripheral module to the new loadname from the loadfile selection report.
  - start this procedure again from [step 6](#)

**39** Exit the PMUPGRADE utility by typing

**>QUIT**

**40** Stop the terminal responses from printing by typing

**>RECORD STOP ONTO printer\_name**

**41** Remove the peripheral module load tape from the tape drive.

Check office policy concerning additional copies of peripheral module load and PRSU files. Some offices require additional copies of peripheral module load and PRSU files on a parallel device.

### ***At your desk***

**42** Any new hardware, identified by a Product Engineering Code (PEC), required for the software upgrade release must be installed.

---

#### **If each node**

#### **Do**

has the required hardware

[step 43](#)

does not have the required hardware

Contact your next level of support for more information.

---

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

---

## Upgrading the Peripheral Module

---

The following procedure provides the steps you need to execute to upgrade the PM. When applicable, a reference to the procedure that contains the detailed steps is provided.

### Prerequisites

You have completed procedure [Preparing to upgrade the Peripheral Module on page 1006](#).

### Action

Perform the following procedures:

- For CS 2000 - Compact/Call Agent applications, install SPM and IW SPM IP software that is delivered on CD-ROM [Peripheral Module CD-ROM based installation on page 1017](#)
- [Perform an automated upgrade for peripheral modules on page 1020](#)

### Peripheral Module CD-ROM based installation

For CS 2000 - Compact/Call Agent applications, use this procedure to install SPM and IW SPM IP software that is delivered on CD-ROM.

#### Installing SPM and IW SPM IP software from CD-ROM

##### ***SITE — At the CS 2000 Management Tools server***

- 1 Insert the disk into the drive.

##### ***SITE — At the CS 2000 Management Tools terminal***

- 2 Log into the Core Manager or CBM by typing  
`telnet <cbm_ip_address>`  
*Choose the username of Core0usr or Core1usr and enter the appropriate password.*
- 3 Change the directory to the PMLOADS volume by typing:  
`cd /3PC/<sd0x>/<pmloads_volume>`  
*Example*  
`[mtc@hostname mtc]$ cd /3PC/sd01/pmloads`
- 4 Open an FTP session to the CS 2000 Management Tools (CMT) server by typing:  
`ftp <cmt_ip_address>`

Log in using *maint* for the hostname and password.

*Example*

```
[mtc@10.40.44.67 pmloads]$ ftp <cmt_ip_address>
Connected to <cmt_ip_address>.
220 ProFTPD 1.2.8 Server (Authorized Use Only) [hostname]
Name (hostname:mtc): maint
331 Password required for maint.
Password:
230 User maint logged in.
ftp>
```

- 5 Change directory (*cd*), list (*ls*) the file size, change the mode to binary (*bin*), turn the prompt off (*prompt*), get the files (*mget*), and end the ftp session by typing the commands as indicated in the following example:

*Example*

```
ftp> cd /cdrom/cdrom0
250 CWD command successful.
ftp> ls
ERS20CE.img1020
ENX20CE.img1020
...
LRS20CE.img1020
MPF20CE.bin128
QLI20BT.img1020
ftp> bin
200 Type set to I.
ftp> prompt
Interactive mode off.
ftp> mget *
local:
200 PORT command successful.
150 Opening data connection for
ERS20CE.img1020 (binary mode) (5107140
byt
226 Transfer complete.
150 Opening data connection for
ENX20CE.img1020 (binary mode) (3913740
byt
226 Transfer complete.
.....
.....
ftp> bye
```

- 6 At the *core0* prompt, type *exit* to return to the CBM session.

*Example*

```
[mtc@hostname mtc]$ exit
```

- 7 At the CBM prompt, telnet to the CM session by typing.

```
telnet cm
```

When prompted type in the appropriate username and password.

- 8 Enter the DISKUT level by typing:

```
DISKUT
```

- 9 Import the PMLOADS file by typing

```
IMPORT sd01 <pmloads_volume>
```

*Example*

```
DISKUT:
```

```
>IMPORT SD01PMLoads
```

```
Attempting to import 24 files selected on SD01PMLoads.
```

```
Imported ERS20CE.img1020 as ERS20CE.IMAGE1020.
```

```
Imported ENX20CE.img1020 as ENX20CE.IMAGE1020.
```

```
...
```

```
Imported MPF20CE.bin128 as MPF20CE BIN128.
```

```
Imported QLI20BT.img1020 as QLI20BTIMAGE 1020
```

```
Imported 24 files successfully of 24 attempts on SD01PMLoads.
```

*The PM LOAD files are imported from the native file system into the call processing application file system. If the disk does not have enough space, a prompt to increase the volume size is presented.*

- 10 Once the IMPORT has completed quit and logout using the following commands:

```
quit all
logout
```

*This returns you to the CBM prompt.*

- 11 From the CBM prompt, log into the CMT by typing :

```
telnet <cmt_ip_address>
```

Log in using *maint* for the hostname and password.



- 12** Eject the disk from the drive by typing:

**eject cdrom**

Software on the CS 2000 Management Tools server unmounts the disk and opens the drive tray. If the eject command fails and indicates that the device is busy, ensure that the FTP session has ended and no users have changed the directory into /cdrom/... directory. Re-enter the eject command.

***SITE — At the CS 2000 Management Tools server***

- 13** Remove the disk from the drive.
- 14** This procedure is complete.

**Perform an automated upgrade for peripheral modules**

This procedure upgrades all of the peripheral modules in an office.

Use at least two devices with this procedure. Use one device to perform the automated peripheral module upgrade. Use the second device as a trace device to monitor the progress of the automated peripheral module upgrade.

Some offices use a third device during the automated upgrade. Use the third device as a MAP terminal. Post the peripheral modules and monitor peripheral module loading, patching, and service status.

Send the output of each device to a printer for record keeping.

SWUPGRADE PM disables the Spectrum Patching After RTS (SPARTS) tool during the automated upgrade. When SWUPGRADE PM is completed or aborted, SPARTS is automatically re-enabled.

The SPM601 log generates when SPARTS is disabled and enabled. No action is required when this log is generated.

**Variable Abbreviations**

| Abbreviation | Definition                                                                                 |
|--------------|--------------------------------------------------------------------------------------------|
| printer      | the printer name                                                                           |
| max_no       | the UNLIMITED or the maximum number of peripheral modules the system upgrades concurrently |
| dev_name     | the name of the new Patch Distribution volume                                              |

## Variable Abbreviations

| Abbreviation | Definition                               |
|--------------|------------------------------------------|
| spm_no       | the ID (number) of the peripheral module |
| step_name    | the name of the step                     |

MAP displays in this procedure are provided as reference examples and may not represent the actual screen display. Load versions and resource modules (RMs) listed on the screen may vary depending on the office configuration.

Throughout the upgrade procedure, the request to type a command requires pressing the Enter key on the keyboard after the command has been typed.

## Performing an automated upgrade for peripheral modules

### *At the CI level of the MAP display*

- 1 Send the terminal responses to a printer by typing  
**>RECORD START ONTO <printer>**
- 2 Enter the SWUPGRADE PM increment for automated upgrades by typing  
**>SWUPGRADE PM**
- 3 Establish a second device as a trace device by typing  
**>SET TRACE\_DEVICE dev\_name**  
The second device records SWUPGRADE PM operations during the automated upgrade.
- 4 The trace device must display a message indicating that the device is selected for TRACEing.

| If the device                | Do                                                                                                        |
|------------------------------|-----------------------------------------------------------------------------------------------------------|
| displays the message         | <a href="#">step 5</a>                                                                                    |
| does not display the message | Confirm the correct device is selected as the trace device. If necessary, repeat <a href="#">step 3</a> . |

- 5 Start the upgrade shift by typing  
**>SET SHIFT STARTED**

| If unspared SRMs         | Do                     |
|--------------------------|------------------------|
| included in the plan     | <a href="#">step 6</a> |
| not included in the plan | <a href="#">step 8</a> |
- 6 A list of SPMs with unspared SRMs appears with the option to stop or continue PMUPGRADE.  
 Either stop PMUPGRADE and manually upgrade the SRMs before resuming PMUPGRADE or continue PMUPGRADE and upgrade all components in the plan except for the non-spared SRMs.  
 The recommended choice is to stop PMUPGRADE, manually upgrade the SRMs and then resume the PMUPGRADE plan.
 

| If choosing to     | Do                                          |
|--------------------|---------------------------------------------|
| stop PMUPGRADE     | Press <b>Y</b> go to <a href="#">step 7</a> |
| continue PMUPGRADE | Press <b>N</b> go to <a href="#">step 8</a> |
- 7 PMUPGRADE has stopped. Manually upgrade the SRMs and return to [step 5](#).
- 8 SWUPGRADE PM checks for the availability of a \$XREF patch cross-reference file and processes patch cross-reference information.
- 9 Display the SWUPGRADE PM environment variables by typing  
**>DISPLAY VAR ALL**  
 The variable name TRACE\_DEVICE is the trace device established in [step 3](#). SHIFT indicates the status of the current upgrade shift. CONCURRENCY indicates the maximum number of concurrent upgrades.
- 10 Display HELP for the CONCURRENCY variable by typing  
**>HELP VAR CONCURRENCY**
- 11 Determine the maximum number of peripheral modules to upgrade concurrently. Note that a concurrency value set to UNLIMITED can exceed the maintenance window for the upgrade shift in large scale offices. The maximum value cannot

exceed eight. The value defaults to eight if entering a value of UNLIMITED or greater than eight.

| <b>If the value in CONCURRENCY</b> | <b>Do</b>               |
|------------------------------------|-------------------------|
| needs to be changed                | <a href="#">step 12</a> |
| does not need to be changed        | <a href="#">step 14</a> |

- 12 Set the concurrency value by typing  
**>SET CONCURRENCY max\_no**
- 13 Display the environment variables and confirm the change by typing  
**>DISPLAY VAR ALL**
- 14 Set prompting to on by typing  
**>PROMPTING ON**  
 PROMPTING ON is the recommended method of operation. Set PROMPTING ON forces a pause after each automated step. This allows user intervention for the next required step. The remainder of this procedure assumes prompting is enabled.
- 15 From a second terminal, post the nodes designated for an upgrade by typing  
**>MAPCI;MTC;PM;POST SPM spm\_no**  
*Example*  
**>MAPCI;MTC;PM;POST SPM 23**
- 16 Display alarms on the RMs on the peripheral modules by typing  
**>QUERYPM FLT REASON**
- 17 Display and note any alarms on the nodes by typing  
**>LISTALM**
- 18 Display and note the carrier statuses on the nodes by typing  
**>MAPCI;MTC;TRKS;CARRIER;POST SPM spm\_no 1**  
*Example*  
**>MAPCI;MTC;TRKS;CARRIER;POST SPM 23 1**
- 19 Determine the impact of the current alarm status on the upgrade.

| <b>If there are</b>          | <b>Do</b>               |
|------------------------------|-------------------------|
| alarms other than ISTB alarm | <a href="#">step 20</a> |

|    | If there are                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Do                      |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
|    | no alarms or all alarms are ISTB alarms                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">step 21</a> |
| 20 | Perform the appropriate alarm clearing procedures. After completing the required procedures, go to <a href="#">step 21</a> .                                                                                                                                                                                                                                                                                                                                                             |                         |
| 21 | From the SWUPGRADE device, begin the automated upgrade by typing<br><b>&gt;START</b>                                                                                                                                                                                                                                                                                                                                                                                                     |                         |
| 22 | Display and review the upgrade steps by typing<br><b>&gt;DISPLAY STEPS</b><br>A step with an “_A_” identifies the step as an automated step. An “_M_” identifies the step as a manual step.<br>After an automated step has been completed the status changes from NEEDED to COMPLETED.<br>The columns marked as PERM, ACT, and PROC are used by other platforms and do not apply to an SPM upgrade.<br>Steps proceed automatically, however the option exists to manually select a step. |                         |
| 23 | Display HELP on the step you wish to execute by typing<br><b>&gt;HELP STEP step_name</b><br>SWUPGRADE PM displays a brief description of the step including <ul style="list-style-type: none"> <li>the nodes affected by the step</li> <li>the load(s) and PRSU(s) required by the step</li> <li>the steps required prior to the step</li> </ul>                                                                                                                                         |                         |
| 24 | Based on your office requirements, determine if you wish to upgrade or not upgrade (override) the step.                                                                                                                                                                                                                                                                                                                                                                                  |                         |
|    | If                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Do                      |
|    | not upgrading a step                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">step 25</a> |
|    | upgrading a step                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <a href="#">step 27</a> |
| 25 | Override the step by typing<br><b>&gt;OVERRIDE step_name</b>                                                                                                                                                                                                                                                                                                                                                                                                                             |                         |
| 26 | At the prompt, accept the override by typing<br><b>&gt;Y</b>                                                                                                                                                                                                                                                                                                                                                                                                                             |                         |

After overriding a step, the option to reinstate that step exists by typing **>RESET step\_name**.

- 27** Ensure that the HELP STEP command has been performed for every step\_name.

| <b>If all step_names have</b> | <b>Do</b>               |
|-------------------------------|-------------------------|
| not been verified             | <a href="#">step 23</a> |
| been verified                 | <a href="#">step 28</a> |

- 28** Execute the upgrade process sequentially or out of sequence through one of the following commands:

| <b>If executing the upgrade</b> | <b>Do</b>                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| sequentially                    | Type<br><b>&gt;GO</b>                                                                                                                           |
| out of sequence                 | To run a step, type<br><b>&gt;RUNSTEP step_name</b><br><b>ATTENTION</b><br>Do not choose to RUNSTEP a step_name that was selected for override. |

- 29** Monitor the automated upgrade progress through the following:

- the trace device response
- the status of each node
- a log device

SWUPGRADE PM stops executing if:

- nodes are not ready for upgrading
- all nodes have been successfully upgraded
- An upgrade failure occurs.
- The SWUPGRADE PM shift exceeds the 14 hour time limit.
- a SET SHIFT FINISHED or SET SHIFT ABORTED command has been entered

SET SHIFT FINISHED stops the step after the full upgrade for the nodes in the step has completed

SET SHIFT ABORTED stops the step after the current maintenance action for node(s) has completed.

- 30** After SWUPGRADE PM completes a step, the trace device displays an upgrade status report for each node.

| If                                                                       | Do                      |
|--------------------------------------------------------------------------|-------------------------|
| every node in the step passed and you want to continue the upgrade shift | <a href="#">step 32</a> |
| a node in the step failed                                                | <a href="#">step 31</a> |
| every node in the step passed and you want to finish the upgrade shift   | <a href="#">step 33</a> |

Use the QUERYPM FILES command from the MAP display to confirm each node is correctly loaded and in-service.

- 31** Possible reasons for a node failure are:
- The peripheral module status, or one of its units, changed due to a maintenance problem not related to the automated upgrade.
  - The peripheral module load file or required PRSU files are not in the Destination Volume.
  - The node encountered a hardware problem.

Review logs PM703, SPM650, SPM651, SPM300, SPM500, SPM335 and NODE500, plus the trace device output to determine why the node failed the automated upgrade.

| If you can                        | Do                                                                                                                                                                                                                                      |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| determine why the node failed     | Correct the problem and return to <a href="#">step 28</a>                                                                                                                                                                               |
| not determine why the node failed | Contact your next level of support.<br><br>If the problem is resolved, go to <a href="#">step 28</a><br><br>To continue the upgrade shift, go to <a href="#">step 22</a><br><br>To end the upgrade shift, go to <a href="#">step 32</a> |

- 32** At the ALIGN\_RMS prompt, choose to align the RMIDs and PWIDs of all resource RMs in the office by typing

>Y

| If                                     | Do                      |
|----------------------------------------|-------------------------|
| you want to continue the upgrade shift | <a href="#">step 22</a> |

|           | If                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Do                      |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
|           | you want to finish the SPM upgrade shift                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <a href="#">step 33</a> |
| <b>33</b> | Finish the automated SPM upgrade shift by typing<br><b>&gt;SET SHIFT FINISHED</b><br><i>Result</i><br>A Summary Report for PM Software Upgrade containing the following information: <ul style="list-style-type: none"> <li>• the step name</li> <li>• the elapsed time between the previous and current step</li> <li>• the time the step began</li> <li>• the elapsed time to execute the step</li> <li>• the final result status</li> </ul> A result status of STEP NOT COMPLETE indicates SWUPGRADE PM did not perform the step. This could indicate a step that was overridden and performed manually.<br>The SET SHIFT FINISHED command can generate a PM700 log that indicates the SPM upgrade shift has finished. No action is required for this log. |                         |
| <b>34</b> | Display the step of the automated upgrade by typing<br><b>&gt;DISPLAY STEPS</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                         |
|           | <b>If all steps</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>Do</b>               |
|           | except UPGRADE_COMPLETE are complete or overridden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <a href="#">step 35</a> |
|           | are not complete or overridden and you do not intend to continue <sup>1</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <a href="#">step 38</a> |
|           | <sup>1</sup> .If all steps are not complete and overridden the upgrade can be resumed at a later date by restarting this procedure at <a href="#">step 1</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                         |
| <b>35</b> | Execute the UPGRADE_COMPLETE step by typing<br><b>&gt;GO</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                         |
| <b>36</b> | Obtain the final record of all completed steps by typing<br><b>&gt;DISPLAY STEPS</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                         |
| <b>37</b> | Complete the UPGRADE_COMPLETE step by typing<br><b>&gt;GO</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                         |



- 38 Quit the SWUPGRADE PM utility by typing  
**>QUIT**
- 39 Stop the terminal responses from printing by typing  
**>RECORD STOP ONTO printer**
- 40 You have completed this procedure.

## Completing the Peripheral Module upgrade

The following procedure provides the high-level steps to complete the SPM-based PM upgrade. Where applicable, a reference to the step-by-step procedure is provided.

The procedure consists of the following tasks:

- Deleting the old file names from the PMLOADS table.
- Deleting the old load and patch files from disk volumes.
- Dumping an image to disk after completing maintenance shift upgrade or downgrade activities.

### Prerequisites

You have completed procedure [Upgrading the Peripheral Module on page 1017](#)

### Action

Follow the link associated upgrade you wish to complete.

- [Completing the SPM upgrade or downgrade process on page 1029](#)

The [Variable abbreviations](#) table defines the variables used in this procedure.

#### Variable abbreviations

| Abbreviation | Definition                                                           |
|--------------|----------------------------------------------------------------------|
| load_name    | the name of the old load (as it appears in the PMLOADS table)        |
| disk_vol     | the name of the backup disk volume                                   |
| act_load     | the name of the new active load (as it appears in the PMLOADS table) |

### Completing the SPM upgrade or downgrade process

#### *At the MAP*

- 1 Access the PMLOADS table by typing  
**>TABLE PMLOADS**

- 2 Position on each old load name designated for deletion in the PMLOADS table by typing  
**>POS load\_name**  
*Example*  
**>POS GEM19AF**
- 3 Initiate the tuple deletion by typing  
**>DEL**
- 4 At the confirmation prompt, delete the tuple by typing  
**>Y**
- 5 Access the disk utility by typing  
**>DISKUT**  
*Response*  
Disk utility is now active
- 6 List the active PMLOADS volume by typing  
**>LF disk\_vol**  
*Example*  
**>LF F0LPMLOADS**
- 7 Delete each load file from the active disk volume by typing  
**>DDF act\_load**  
*Example*  
**>DDF CEM19CD\_010064A1**
- 8 List the loads on the active volume to ensure that all loads have been deleted by repeating [step 6](#).  
Follow [step 7](#) for any files that have not been deleted.
- 9 Repeat [step 1](#) through [step 7](#) for the backup and patch volumes.  
When all active, backup, and patch files have been deleted, continue to [step 10](#).
- 10 Quit the disk utility by typing  
**>QUIT**
- 11 Store an image of the completed upgrade or downgrade to a disk volume by typing  
**DUMP act\_file image\_vol ACTIVE RETAIN NOSDM**

*Example*

```
>DUMP DSP16AF_010005 S00DIMAGE ACTIVE RETAIN
NOSDM
```

The route action to turn off SDM spooling option (nosdm) reduces CI lockout time. Without specifying a route action, the default value is leave SDM spooling on (usesdm).

- 12 This procedure is complete. If applicable, return to the higher-level procedure or task flow that directed you to this procedure.

Proceed to upgrade legacy PMs using the appropriate *Peripheral Module Release Document*, 297-9051-599 (International) or *Peripheral Module Release Release Document*, 297-2663-599 (North America) available from a Helmsman DMS collection.

## Peripheral Module CD-ROM based installation

For CS 2000 - Compact/Call Agent applications, use this procedure to install SPM and IW SPM IP software that is delivered on CD-ROM.

### ***SITE — At the CS 2000 Management Tools server***

- 1 Insert the disk into the drive.

### ***SITE — At the CS 2000 Management Tools terminal***

- 2 Log into the Core Manager or CBM by typing  
**telnet <cbm\_ip\_address>**  
*Choose the username of Core0usr or Core1usr and enter the appropriate password.*
- 3 Change the directory to the PMLOADS volume by typing:  
**cd /3PC/<sd0x>/<pmloads\_volume>**  
*Example*  
**[mtc@hostname mtc]\$ cd /3PC/sd01/pmloads**
- 4 Open an FTP session to the CS 2000 Management Tools (CMT) server by typing:  
**ftp <cmt\_ip\_address>**  
Log in using *maint* for the hostname and password.  
*Example*

```
[mtc@10.40.44.67 pmloads]$ ftp <cmt_ip_address>
Connected to <cmt_ip_address>.
220 ProFTPD 1.2.8 Server (Authorized Use Only) [hostname]
Name (hostname:mtc): maint
331 Password required for maint.
Password:
230 User maint logged in.
ftp>
```

- 5 Change directory (cd), list (ls) the file size, change the mode to binary (bin), turn the prompt off (prompt), get the files (mget), and end the ftp session by typing the commands as indicated in the following example:

*Example*

```
ftp> cd /cdrom/cdrom0
250 CWD command successful.
ftp> ls
ERS20CE.img1020
ENX20CE.img1020
...
LRS20CE.img1020
MPF20CE.bin128
QLI20BT.img1020
ftp> bin
200 Type set to I.
ftp> prompt
Interactive mode off.
ftp> mget *
local:
200 PORT command successful.
150 Opening data connection for
ERS20CE.img1020 (binary mode) (5107140
byt
226 Transfer complete.
150 Opening data connection for
ENX20CE.img1020 (binary mode) (3913740
byt
226 Transfer complete.
.....
.....
ftp> bye
```

- 6 At the core0 prompt, type exit to return to the CBM session.

*Example*

```
[mtc@hostname mtc]$ exit
```

- 7 At the CBM prompt, telnet to the CM session by typing.

```
telnet cm
```

When prompted type in the appropriate username and password.

- 8 Enter the DISKUT level by typing:

```
DISKUT
```

- 9 Import the PMLOADS file by typing

```
IMPORT sd01 <pmloads_volume>
```

*Example*

DISKUT:

>**IMPORT SD01PMLoads**

Attempting to import 24 files selected on SD01PMLoads.

Imported ERS20CE.img1020 as ERS20CE.IMAGE1020.

Imported ENX20CE.img1020 as ENX20CE.IMAGE1020.

...

Imported MPF20CE.bin128 as MPF20CE BIN128.

Imported QLI20BT.img1020 as QLI20BTIMAGE 1020

Imported 24 files successfully of 24 attempts on SD01PMLoads.

*The PM LOAD files are imported from the native file system into the call processing application file system. If the disk does not have enough space, a prompt to increase the volume size is presented.*

- 10** Once the IMPORT has completed quit and logout using the following commands:

**quit all**

**logout**

*This returns you to the CBM prompt.*

- 11** From the CBM prompt, log into the CMT by typing :

**telnet <cmt\_ip\_address>**

Log in using *maint* for the hostname and password.

- 12** Eject the disk from the drive by typing:

**eject cdrom**

Software on the CS 2000 Management Tools server unmounts the disk and opens the drive tray. If the eject command fails and indicates that the device is busy, ensure that the FTP session has ended and no users have changed the directory into /cdrom/... directory. Re-enter the eject command.

***SITE — At the CS 2000 Management Tools server***

- 13** Remove the disk from the drive.
- 14** This procedure is complete.

## Manually upgrading an SRM



### CAUTION

Use this procedure before performing an automated upgrade only if the network contains DMS SPMs or IW SPMs that require a Sync Resource Module (SRM) software upgrade.

Both nodes with SRMs configured must be upgraded prior to performing an automated upgrade for the remaining nodes. After upgrading the first SPM/SRM, immediately upgrade the second SPM/SRM. It is important to upgrade the SPM/SRMs one after the other, not simultaneously.

The following [Variable Abbreviations](#) table defines the variables used in this procedure.

### Variable Abbreviations

| Abbreviation | Definition                      |
|--------------|---------------------------------|
| spm_no       | the number of the SPM (0 to 85) |
| rm_no        | the Sync RM number              |
| link_no      | the BITS link number (0 to 2)   |
| patch_id     | the PRSU name                   |

### ***At the CI level of the MAP display***

- 1 Access and monitor the switch timing links at the clock level of the MS to determine the STANDBY SRM by typing

**>MAPCI ;MTC ;MS ;CLOCK**

*Example of a MAP screen:*





- 4 Ensure that the SRM is in an ISTB condition with the new load listed as default, by typing.

**>QUERYMOD**

*Example of a MAP screen:*

```
SPM 23 SRM 0 Query: Request has been submitted.
SRM 0 ISTb Act Loc: Row D FrPos 1 ShPos 6 ShId 0 Slot 6

Default Load: SYN19EF Actual Load: SYN17EDD
```

- 5 Access the BITS link level by typing

**>BITS**

*Example of a MAP screen:*

```
SPM 23 SRM 0
LinkNo BitsName Status State SSM AlmSev
0 BITSA Act InSv PRS
1 BITSB InAct InSv PRS
2 BITSOUT . Uneq NIL
BITS:
```

- 6 Record the BITS link numbers associated with the SRM and the state of each link.

- 7 Manual busy (ManB) the inactive BITS links by typing

**>BSY link\_no**

*Example*

**>BSY 1**

*Response*

Busy:Request has been Submitted.

Busy:Command Completed.State Change has passed.

- 8 Force the active BITS links to ManB by typing

**>BSY link\_no FORCE**

*Example*

**>BSY 0 FORCE**

*Response*

WARNING: BITSB Link is a Timing Link.

Do you want to BUSY this Link.

Please confirm ("YES", "Y", "NO", or "N"):

- 9 At the confirmation prompt, type:  
>**Y**  
*Response*  
Busy:Request has been Submitted.  
Busy:Command Completed.State Change has passed.
- 10 Return to the SRM level by typing  
>**QUIT**
- 11 Force the SRM to ManB by typing  
>**BSY FORCE**  
*Response*  
WARNING: This RM provides timing information.  
Bsyng out this RM might result in loss of Synchronization.  
A Bsy action may impact services on this node.  
Do you wish to continue?  
Please confirm ("YES", "Y", "NO", or "N"):
- 12 At the confirmation prompt, type:  
>**Y**  
*Response*  
SRM Busy:Request has been Submitted.  
SRM Busy:Command Completed.
- 13 Load the SRM with the new load by typing  
>**LOADMOD**
- | If the loadname is        | Do                      |
|---------------------------|-------------------------|
| not in the SPMLDVAL table | <a href="#">step 14</a> |
| in the SPMLDVAL table     | <a href="#">step 15</a> |
- 14 At the confirmation prompt, continue by typing  
>**Y**

## Example of MAP response

>y

\*\*\* WARNING: Table SPMLDVAL is not datafilled for this loadname. Contact your next level of support before proceeding with upgrade. Do you want to continue without datafilling the table?

Please confirm ("YES", "Y", "NO", or "N"):

| If choosing to            | Do                                                     |
|---------------------------|--------------------------------------------------------|
| continue                  | <a href="#">step 15</a> <sup>1</sup>                   |
| update the SPMLDVAL table | stop the upgrade and contact the next level of support |

1.Continuing the upgrade when the loadname is not in the SPMLDVAL table prevents that load from being available in that table for future reference.

### 15 At the confirmation prompt, type:

>Y

#### *Response*

SRM Load:Request has been submitted.  
SRM Load: Command Completed. Command Passed

| If the SRM device is      | Do                      |
|---------------------------|-------------------------|
| the first for the office  | <a href="#">step 16</a> |
| the second for the office | <a href="#">step 23</a> |

### 16 Open a third window and access the PRSM tool by typing

>PRSM

### 17 Ensure that PRSM recognizes any pre-applied PRSUs and has found all applied PRSU files by typing

>DBAUDIT SPM spm\_no SRM rm\_no

#### *Example*

>DBAUDIT SPM 23 SRM 0

## Example of MAP response

Database audit submitted for 1 DESTs  
Auditing destination SPM 23 SRM 0....  
Database audit completed for 1 DEST  
Database audit completed for 1 DEST  
Database discrepancy found in 0 DESTs

### 18 Identify if PRSM found all patch files built into the PPSL by typing

>SELECT PRSUID CATEGORY STATUS BUILTIN FROM  
DESTSET SPM spm\_no SRM rm\_no

## Example of MAP response

```
>select prsuid category status builtin from destset spm 23 srm 0
PRSUID CAT ST BUILTIN

TAB51S0P GEN A Y
BUZ80S0P GEN A Y
CTC51S0P GEN A Y
DXH62S0P GEN A Y
DXH63S0P GEN A Y
JXM65S0P GEN A Y
KAA01S0P GEN A Y
KRI62S0P GEN A Y
LLH11S0P GEN A Y
SBF80S0P GEN A Y
SBF90S0P GEN A Y
TAV54S0P GEN A Y
```

**Note:** An empty list appears for a non-PPSL load (the load is not pre-patched).

An unknown category displayed as question marks (???) appears if PRSM cannot locate PRSU files in a PPSL during the first dbaudit of a newly loaded SPM device. This situation does not occur if all PRSU files have been placed in a PADNDEV table defined volume as instructed in the Upgrade Preparation procedure.

If this situation should occur use the validate command in PRSM for each PRSU with a category of ??? in at least one applicable DEST. For example: **VALIDATE ABC30S0Q IN SPM 23 SRM 0**

Also before proceeding to the next device type, ensure that all patch files are placed in the PADNDEV table defined volume according to the Upgrade Preparation procedure.

- 19 If required, patch the SRM device.

| If patches                         | Do                      |
|------------------------------------|-------------------------|
| are required for the load file     | <a href="#">step 20</a> |
| are not required for the load file | <a href="#">step 21</a> |

- 20 Apply the patches by typing

```
>APPLY `patch_id | patch_id | patch_id IN SPM
spm_no SRM rm_no
```

*Example*

```
>APPLY `ABC05513 | DEF10513 | GHI45513 IN SPM 23
SRM 0
```

**Note:** Repeat the command as necessary to apply additional patches.

- 21 Ensure that the SRM is correctly patched by typing

```
>REPORT DEST SPM spm_no SRM rm_no
```

*Example*

```
>REPORT DEST SPM 23 SRM 0
```

**Note 1:** For the first SRM, the output should be the combination of the PSRUs applied in [step 20](#) and the pre-applied PRSUs displayed in [step 18](#).

**Note 2:** For the second SRM, the list of patches should be identical to the list obtained in this step for the first SRM.

### Example of MAP response

```
REPORT DEST SPM 23 SRM 0
PRSUID STATDATE STATT CAT ACT ST LOADNAME H DESTID

ABC05S13 20020915 23:29 GEN A SRM17BU N SPM 23 SRM 0
DEF10S13 20020915 23:33 GEN A SRM17BU N SPM 23 SRM 0
GHI45S13 20020915 23:36 GEN A SRM17BU N SPM 23 SRM 0
TAB51S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
CTC51S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
BUZ80S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
DXH63S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
DXH62S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
JXM65S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
KAA01S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
KRI62S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
LLH11S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
SBF80S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
SBF90S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
TAV54S0P 20020915 23:10 GEN A SRM17BU N SPM 23 SRM 0
```

- 22 Exit the PRSM tool by typing

```
>QUIT
```

- 23 From the second window opened in [step 2](#), return the SRM to service by typing

```
>RTS
```

*Response*

```
SPM SRM RTS:Request has been submitted.
SPM SRM RTS: Command Completed.
```

- 24 Access the BITS level by typing

```
>BITS
```

- 25 Restore the BITS links to service by typing

```
>RTS link_no
```

*Example*

```
>RTS 0
```

**>RTS 1**

*Result*

The links change from InAct ManB to Act InSv and InAct InSv.

**26** Return to the SPM level by typing

**>QUIT**

**27** Return to the posted node level by typing

**>QUIT**

**28** Display alarms on the SPM by typing

**>QUERYPM FLT**

Display alarms on the SPM by typing

**>LISTALM**

If new alarms were introduced during this procedure, clear the alarms using procedures in the Fault Management section.

---

| <b>If the SRM device is</b> | <b>Do</b>               |
|-----------------------------|-------------------------|
| the first for the office    | <a href="#">step 29</a> |
| the second for the office   | <a href="#">step 31</a> |

---

**29** From the original window in [step 1](#), switch the SRM from ACTIVE to STANDBY by typing

**>SWCARR**

**30** Go to [step 1](#) and repeat the procedure for the second SRM.

**31** The SRM circuit pack protection group upgrade is completed.

---

## Prepare Peripheral Modules for an Automated Upgrade

---

This procedure prepares all of the peripheral modules in an office for an automated upgrade.

Each destination volume must have sufficient free space for the new peripheral module load or PRSU files and meet all office criteria.

The [Variable Abbreviations](#) table defines the variables used in this procedure.

### Variable Abbreviations

| Abbreviation        | Definition                                                                     |
|---------------------|--------------------------------------------------------------------------------|
| printer             | the printer name                                                               |
| dist_vol            | the name of the new Load File Distribution volume                              |
| ip_address          | the remote FTP volume server IP address for electronic software delivery (ESD) |
| pm_path             | the location of the PM loads files on the FTP server                           |
| patch_vol           | the name of the Patch Distribution volume                                      |
| patch_path          | the location of the patch files on the FTP server                              |
| load_number         | the number of the current load                                                 |
| load_name_1 (2) (n) | the names of the loads to be included or excluded (repeat variable as needed)  |

Throughout the upgrade procedure, the request to type a command requires pressing the Enter key on the keyboard after the command has been typed.

Before beginning the automated upgrade, ensure that spares are configured for all RMs requiring an upgrade.



## Prepare peripheral modules for an automated upgrade

### At the CI level of the MAP display

- 1 Send the terminal responses to a printer by typing  
**>RECORD START ONTO <printer>**
- 2 Enter the log utility and list devices for log output by typing  
**>LOGUTIL**  
**>LISTDEVS**

*Example of an active log output device*

| No. | Device | Status          | Rerouted | Format |
|-----|--------|-----------------|----------|--------|
| 0   | MAP121 | Outputting Logs | No       | STD    |

*Example of an inactive log output device*

| No.                | Device | Status    | Rerouted | Format |
|--------------------|--------|-----------|----------|--------|
| 1                  | MAP121 | Inactive. | No       | STD    |
| - End of devices - |        |           |          |        |

#### If the device is

#### Do

Inactive

[step 3](#)

Active (outputting logs)

[step 4](#)

- 3 Start the device by typing  
**>STARTDEV device**

*Example of a MAP display*

```
>startdev map121
Log device MAP121 has been started.
Number of devices started : 1
```

- 4 Verify that all reports for the PRSM, SPM, NODE, and TUPL log types are configured for output by typing  
**>LISTREPS SPECIAL <log\_name>**

*Examples*

**>LISTREPS SPECIAL PRSM**

**>LISTREPS SPECIAL SPM**

**>LISTREPS SPECIAL NODE**

**>LISTREPS SPECIAL TUPL**

*Example of all log type reports configured for output*

| Log Name | Rep. No. | Event Class | Type | Event Label | Suppressed/Thresholded | Syslog |
|----------|----------|-------------|------|-------------|------------------------|--------|
|----------|----------|-------------|------|-------------|------------------------|--------|

67 report(s) printed

### *Example of suppressed log type reports*

| Log Name | Rep. No. | Event Class | Type | Event Label         | Suppressed/Thresholded | Syslog |
|----------|----------|-------------|------|---------------------|------------------------|--------|
| SPM      | 650      | 0           | PASS |                     | *supp*                 |        |
| SPM      | 651      | 0           | FAIL |                     | *supp*                 |        |
| SPM      | 300      | 0           | TBL  | Device Fault Report | *supp*                 |        |

#### **If log reports are**

#### **Do**

suppressed

[step 5](#)

not suppressed

[step 6](#)

- 5** Resume any PRSM, SPM, NODE, and TUPL logs that have been suppressed by typing

**>RESUME <log\_name> <log\_#>**

#### *Example*

```
>resume spm 650
1 report(s) RESUMED
```

- 6** Identify the patch destination volume by typing

**>TABLE PADNDEV;LIST ALL;QUIT**

#### *Example*

```
TABLE: PADNDEV
TOP
DEVKEY DEVICE

 1 D030M17PTCH
 2 D030M15PTCH
 3 S01DIMAGE
BOTTOM
```

- 7** Access the PMUPGRADE utility by typing

**>PMUPGRADE**

- 8** Set confirmation to ON by typing

**>SET CONFIRMATION ON**

- 9** Carryover loads are load files on the tape that have the same version of the load currently used in the office. Operating company personnel can issue a SET CARRYOVER ON command to copy all peripheral module loads for the office. The default carryover setting is OFF.

**If the office****Do**

requires all peripheral module loads for the office be copied

[step 10](#)

does not require all peripheral module loads for the office to be copied

[step 11](#)

- 10** Set carryover to ON by typing

**>SET CARRYOVER ON**

- 11** Confirm the Load File Distribution setting is correct. If necessary, change the setting by typing

**If using****Do**

tape

**>SET LOADDISTRIB <dist\_vol >**

*Example*

**>SET LOADDISTRIB F02UTAPE**

ESD

**>SET LOADDISTRIB <ip\_address> <pm\_path>**

*Example*

**>SET LOADDISTRIB 123.123.123.123 /PMLOADS/**

- 12** Confirm the Load File Destination setting is correct. If necessary, change the setting by typing

**>SET LOADDEST <dist\_vol>**

*Example*

**>SET LOADDEST F02LPMLOADS**

- 13** Confirm the Patch File Distribution setting is correct. If necessary, change the setting by typing

**If using****Do**

tape

**>SET PATCHDISTRIB <patch\_vol>**

*Example*

**>SET PATCHDISTRIB F02LPMLOADS**

| If using | Do                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESD      | <p>&gt;SET PATCHDISTRIB &lt;ip_address&gt; &lt;patch_path&gt;</p> <p><i>Example</i></p> <p>&gt;SET PATCHDISTRIB 123.123.123.123<br/>/PATCHLOADS/</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 14       | <p>The ISN, XPM, and SPM Patch Destination settings must point to the patch file destination volume. Confirm the ISN, XPM, and SPM Patch Destination settings are correct based on the PADNDEV table listing obtained in <a href="#">step 6</a>. If necessary, change the setting by entering the following commands</p> <pre>&gt;SET ISNPATCH &lt;patch_vol&gt; &gt;SET XPMPATCH &lt;patch_vol&gt; &gt;SET SPMPATCH &lt;patch_vol&gt;</pre> <p><b>Note:</b> The SPM patch destination volume should be entered in the PADNDEV table.</p> <p><i>Example</i></p> <pre>&gt;SET ISNPATCH F02LPMLOADS &gt;SET XPMPATCH F02LPMLOADS &gt;SET SPMPATCH F02LPMLOADS</pre> |
| 15       | <p>Generate an office load report by typing</p> <pre>&gt;DISPLAY LOADS</pre> <p><i>Result</i></p> <p>PMUPGRADE compiles the PMUPGRADE Load Report from the PMLOADS table and the SPM inventory tables.</p> <p><b>Note:</b> A load can have an empty “Tables Used” column. If office policy requires data in this column, perform the following steps:</p> <ul style="list-style-type: none"> <li>• Exit PMUPGRADE</li> <li>• Delete the out-dated load from the PMLOADS table</li> <li>• Go to <a href="#">step 7</a> of this procedure</li> </ul>                                                                                                                |
| 16       | <p>Generate a node report for the office by typing</p> <pre>&gt;DISPLAY NODES</pre> <p><i>Result</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

The PMUPGRADE Node Report is compiled from SPM inventory tables. The nodename information for the MNCKTPAK table is obtained from the MNNODE table.

- 17** Display the firmware information by typing

**>DISPLAY FWINFO**

- 18** Set the preferred load to the current load by typing

**>SET FWPREFERRED <load\_number> CURRENT**

**Note 1:** The preferred load must be equal to the current load.

**Note 2:** Repeat this step for each firmware load listed in [step 17](#).

- 19** Start the filecopy phase of the utility by typing

**>START FILECOPY**

#### *Time Requirements*

The FILECOPY process copies files to the destination volume and adds new loads to the PMLOADS table. The process requires approximately 40 minutes. The amount of time depends on the number of peripheral module loads and PRSU files.

- 20** When prompted to confirm a tape is in its appropriate drive, confirm the tape is physically inserted in the drive. Do not use the INSERTTAPE or IT commands on the tape.

If the tape cartridge label text indicates “Patches:Yes”, the tape includes the required PRSUs for peripheral module load files.

- 21** At the prompt, continue by typing

**>Y**

| If the response indicates                                                                      | Do                      |
|------------------------------------------------------------------------------------------------|-------------------------|
| that EXT files for datafill in the SPMLDVAL table are not available in the distribution volume | <a href="#">step 22</a> |
| the replacement loadname cannot be found                                                       | <a href="#">step 23</a> |
| Multiple replacements found for EXT file on the distribution volume                            |                         |
| or                                                                                             |                         |
| multiple replacement loadnames are found                                                       | <a href="#">step 24</a> |
| Possible one old replacement found on load distribution volume                                 |                         |

|           | <b>If the response indicates</b>                                                                              | <b>Do</b>               |
|-----------|---------------------------------------------------------------------------------------------------------------|-------------------------|
|           | or<br>ready to continue                                                                                       | <a href="#">step 25</a> |
| <b>22</b> | Stop the automated upgrade by typing<br>>Q<br>Contact the next level of support to update the SPMLDVAL table. |                         |
| <b>23</b> | A response similar to the following example appears if PMUPGRADE cannot locate the replacement loadname.      |                         |

No replacement loadname found on distribution volume for SM206BH1.  
Please enter replacement loadname, or "S" (Same) or "Q" (Quit FILECOPY)

|           | <b>If</b>                                                                                                                                                                                                                                                                                                         | <b>Do</b>                                                                                            |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
|           | A new load type replaces the current load type                                                                                                                                                                                                                                                                    | Enter the new loadname. Ensure the loadname is typed accurately<br><br>Go to <a href="#">step 25</a> |
|           | The load is manufacture discontinued                                                                                                                                                                                                                                                                              | Enter "S"<br><br>Go to <a href="#">step 25</a>                                                       |
|           | The load is a filler RM load name, indicating an RM that does not have a load                                                                                                                                                                                                                                     | Enter "S"<br><br>Go to <a href="#">step 25</a>                                                       |
| <b>24</b> | If a response indicates that multiple replacements are found on the load distribution volume, enter the appropriate replacement listed or just the load name.<br><br>The load name appears before the underscore in the load file name. For example, DLC16DE is the load name for the load file DLC16DE_010082A3. |                                                                                                      |
| <b>25</b> | Review the Load File Selection Report and determine if any loads need to be added or removed from the report.                                                                                                                                                                                                     |                                                                                                      |
|           | <b>If</b>                                                                                                                                                                                                                                                                                                         | <b>Do</b>                                                                                            |
|           | one or more loads need to be added or removed from the report                                                                                                                                                                                                                                                     | <a href="#">step 26</a>                                                                              |
|           | the report is complete and no loads need to be added or removed                                                                                                                                                                                                                                                   | <a href="#">step 31</a>                                                                              |

**26** Stop the file copy process by typing**>N**

| If                                                   | Do                      |
|------------------------------------------------------|-------------------------|
| one or more loads need to be removed from the report | <a href="#">step 27</a> |
| one or more loads need to be added to the report     | <a href="#">step 28</a> |

**27** Remove the loads from the report by typing

```
>SET EXCLUDELOADS <load_name_1> <load_name_2>
... <load_name_n>
```

**Note:** Separate each load name with a space.

*Example*

```
>SET EXCLUDELOADS BTMKA02 ECLI4BC
```

| If                                                              | Do                      |
|-----------------------------------------------------------------|-------------------------|
| one or more loads need to be added to the report                | <a href="#">step 28</a> |
| the report is complete and no loads need to be added or removed | <a href="#">step 29</a> |

**28** Add the loads to the report by typing

```
>SET INCLUDELOADS <load_name_1> <load_name_2>
... <load_name_n>
```

**Note:** Separate the load names with a blank space.

*Example*

```
>SET INCLUDELOADS BTMKA02 ECLI4BC
```

| If                                                              | Do                      |
|-----------------------------------------------------------------|-------------------------|
| one or more loads need to be removed from the report            | <a href="#">step 27</a> |
| the report is complete and no loads need to be added or removed | <a href="#">step 29</a> |

**29** Repeat the file selection phase of the utility by typing

```
>START FILECOPY
```

- 30** Confirm that the appropriate load names have been added or removed from the Load File Selection Report.

---

| <b>If the Load File Selection Report</b> | <b>Do</b> |
|------------------------------------------|-----------|
|------------------------------------------|-----------|

---

|                                                       |                         |
|-------------------------------------------------------|-------------------------|
| does not show the excluded and/or included load names | <a href="#">step 26</a> |
|-------------------------------------------------------|-------------------------|

|                                               |                         |
|-----------------------------------------------|-------------------------|
| shows the excluded and/or included load names | <a href="#">step 31</a> |
|-----------------------------------------------|-------------------------|

---

- 31** Accept the Load Selection Report by typing  
**>Y**

- 32** Confirm the patch file selection prompt by typing  
**>Y**

**Note:** PMUPGRADE uses the \$XREF patch control files to select PRSUs for copying. Depending on the method of PRSU delivery, this file may not be available. If the file is not available, PMUPGRADE generates a warning that no patch control file has been found. Contact your next level of support for instruction on how to proceed with the upgrade and a list of required PRSUs to be manually applied.

- 33** Create the list of files to copy by typing  
**>Y**

*Time Requirements*

This final phase of the FILECOPY process requires approximately 20 minutes to complete adding new loads to the PMLOADS table. The amount of time depends on the number of peripheral module loads and PRSU files.

**34**

**ATTENTION**

Perform this step only if any offline peripheral modules are being installed or commissioned in the office.

Open a second window and update the LOAD field in the MNCKTPAK field to reflect the new software load for each RM type in all offline peripheral modules

- 35** Generate a PMUPGRADE load report for the office by typing  
**>DISPLAY LOADS**

Confirm the selected new loads have been added to the report.



**36** Start the generation of the PM upgrade plan by typing

**>START PLAN**

**Note:** Only one PM upgrade plan can be executed at a time. A new plan cannot be started until an existing plan has been cancelled or completed.

**37** Display the PM upgrade plan by typing

**>DISPLAY PLAN**

The PMUPGRADE Plan Report organizes the peripheral module upgrade by tasks and layers. A task is a set of peripheral modules of the same type at the same site with the same load requirements. A layer is a grouping of tasks.

**38** Review the PMUPGRADE report.

- Confirm all peripheral modules that require upgrading are included in the plan report

**Note:** For loads added to the Loadfile Selection Report with the SET INCLUDELOADS command, the associated peripheral modules must be manually upgraded.

- Confirm the correct loads are included with each task in the plan report.
- Confirm that the sequence of tasks in the plan report conforms to office policy.

**Note:** If the sequence of tasks does not comply, use the RUNSTEP command during the automated upgrade to change the order of tasks.

- Confirm offline peripheral modules that are being installed or commissioned in the office are not included in the plan report. If an offline peripheral module is included in the plan
  - quit the PMUPGRADE process
  - update the appropriate peripheral module inventory table. Change the loadname field for that peripheral module to the new loadname from the loadfile selection report.
  - start this procedure again from [step 6](#)

**39** Exit the PMUPGRADE utility by typing

**>QUIT**

**40** Stop the terminal responses from printing by typing

**>RECORD STOP ONTO <printer\_name>**

**41** Remove the peripheral module load tape from the tape drive.

Check office policy concerning additional copies of peripheral module load and PRSU files. Some offices require additional copies of peripheral module load and PRSU files on a parallel device.

***At your desk***

- 42** Any new hardware, identified by a Product Engineering Code (PEC), required for the software upgrade release must be installed.

---

| <b>If each node</b>                 | <b>Do</b>                                                |
|-------------------------------------|----------------------------------------------------------|
| has the required hardware           | <a href="#">step 43</a>                                  |
| does not have the required hardware | Contact your next level of support for more information. |

---

- 43** You have completed this procedure.

---

## Perform an automated upgrade for peripheral modules

---

This procedure upgrades all of the peripheral modules in an office.

Use at least two devices with this procedure. Use one device to perform the automated peripheral module upgrade. Use the second device as a trace device to monitor the progress of the automated peripheral module upgrade.

Some offices use a third device during the automated upgrade. Use the third device as a MAP terminal. Post the peripheral modules and monitor peripheral module loading, patching, and service status.

Send the output of each device to a printer for record keeping.

SWUPGRADE PM disables the Spectrum Patching After RTS (SPARTS) tool during the automated upgrade. When SWUPGRADE PM is completed or aborted, SPARTS is automatically re-enabled.

The SPM601 log generates when SPARTS is disabled and enabled. No action is required when this log is generated.

### Variable Abbreviations

| Abbreviation | Definition                                                                                 |
|--------------|--------------------------------------------------------------------------------------------|
| printer      | the printer name                                                                           |
| max_no       | the UNLIMITED or the maximum number of peripheral modules the system upgrades concurrently |
| dev_name     | the name of the new Patch Distribution volume                                              |
| spm_no       | the ID (number) of the peripheral module                                                   |
| step_name    | the name of the step                                                                       |

MAP displays in this procedure are provided as reference examples and may not represent the actual screen display. Load versions and resource modules (RMs) listed on the screen may vary depending on the office configuration.

Throughout the upgrade procedure, the request to type a command requires pressing the Enter key on the keyboard after the command has been typed.

## Performing an automated upgrade for peripheral modules

### *At the CI level of the MAP display*

- 1 Send the terminal responses to a printer by typing  
**>RECORD START ONTO <printer>**
- 2 Enter the SWUPGRADE PM increment for automated upgrades by typing

**>SWUPGRADE PM**

- 3 Establish a second device as a trace device by typing

**>SET TRACE\_DEVICE dev\_name**

The second device records SWUPGRADE PM operations during the automated upgrade.

- 4 The trace device must display a message indicating that the device is selected for TRACEing.

| If the device                | Do                                                                                                        |
|------------------------------|-----------------------------------------------------------------------------------------------------------|
| displays the message         | <a href="#">step 5</a>                                                                                    |
| does not display the message | Confirm the correct device is selected as the trace device. If necessary, repeat <a href="#">step 3</a> . |

- 5 Start the upgrade shift by typing

**>SET SHIFT STARTED**

| If unspared SRMs         | Do                     |
|--------------------------|------------------------|
| included in the plan     | <a href="#">step 6</a> |
| not included in the plan | <a href="#">step 8</a> |

- 6 A list of SPMs with unspared SRMs appears with the option to stop or continue PMUPGRADE.

Either stop PMUPGRADE and manually upgrade the SRMs before resuming PMUPGRADE or continue PMUPGRADE and upgrade all components in the plan except for the non-spaced SRMs.

The recommended choice is to stop PMUPGRADE, manually upgrade the SRMs and then resume the PMUPGRADE plan.

| If choosing to     | Do                                          |
|--------------------|---------------------------------------------|
| stop PMUPGRADE     | Press <b>Y</b> go to <a href="#">step 7</a> |
| continue PMUPGRADE | Press <b>N</b> go to <a href="#">step 8</a> |

- 7 PMUPGRADE has stopped. Manually upgrade the SRMs and return to [step 5](#).
  - 8 SWUPGRADE PM checks for the availability of a \$XREF patch cross-reference file and processes patch cross-reference information.
  - 9 Display the SWUPGRADE PM environment variables by typing  
**>DISPLAY VAR ALL**  
 The variable name TRACE\_DEVICE is the trace device established in [step 3](#). SHIFT indicates the status of the current upgrade shift. CONCURRENCY indicates the maximum number of concurrent upgrades.
  - 10 Display HELP for the CONCURRENCY variable by typing  
**>HELP VAR CONCURRENCY**
  - 11 Determine the maximum number of peripheral modules to upgrade concurrently. Note that a concurrency value set to UNLIMITED can exceed the maintenance window for the upgrade shift in large scale offices. The maximum value cannot exceed eight. The value defaults to eight if entering a value of UNLIMITED or greater than eight.
- | If the value in CONCURRENCY | Do                      |
|-----------------------------|-------------------------|
| needs to be changed         | <a href="#">step 12</a> |
| does not need to be changed | <a href="#">step 14</a> |
- 12 Set the concurrency value by typing  
**>SET CONCURRENCY max\_no**
  - 13 Display the environment variables and confirm the change by typing  
**>DISPLAY VAR ALL**
  - 14 Set prompting to on by typing  
**>PROMPTING ON**  
 PROMPTING ON is the recommended method of operation. Set PROMPTING ON forces a pause after each automated step. This allows user intervention for the next required step. The remainder of this procedure assumes prompting is enabled.
  - 15 From a second terminal, post the nodes designated for an upgrade by typing  
**>MAPCI;MTC;PM;POST SPM spm\_no**

*Example*

**>MAPCI;MTC;PM;POST SPM 23**

- 16** Display alarms on the RMs on the peripheral modules by typing

**>QUERYPM FLT REASON**

- 17** Display and note any alarms on the nodes by typing

**>LISTALM**

- 18** Display and note the carrier statuses on the nodes by typing

**>MAPCI;MTC;TRKS;CARRIER;POST SPM spm\_no 1**

*Example*

**>MAPCI;MTC;TRKS;CARRIER;POST SPM 23 1**

- 19** Determine the impact of the current alarm status on the upgrade.

| If there are                            | Do                      |
|-----------------------------------------|-------------------------|
| alarms other than ISTB alarm            | <a href="#">step 20</a> |
| no alarms or all alarms are ISTB alarms | <a href="#">step 21</a> |

- 20** Perform the appropriate alarm clearing procedures. After completing the required procedures, go to [step 21](#).

- 21** From the SWUPGRADE device, begin the automated upgrade by typing

**>START**

- 22** Display and review the upgrade steps by typing

**>DISPLAY STEPS**

A step with an “\_A\_” identifies the step as an automated step. An “\_M\_” identifies the step as a manual step.

After an automated step has been completed the status changes from NEEDED to COMPLETED.

The columns marked as PERM, ACT, and PROC are used by other platforms and do not apply to an SPM upgrade.

Steps proceed automatically, however the option exists to manually select a step.

- 23** Display HELP on the step you wish to execute by typing

**>HELP STEP step\_name**

SWUPGRADE PM displays a brief description of the step including

- the nodes affected by the step
- the load(s) and PRSU(s) required by the step
- the steps required prior to the step

- 24** Based on your office requirements, determine if you wish to upgrade or not upgrade (override) the step.

| If                   | Do                      |
|----------------------|-------------------------|
| not upgrading a step | <a href="#">step 25</a> |
| upgrading a step     | <a href="#">step 27</a> |

- 25** Override the step by typing

**>OVERRIDE step\_name**

- 26** At the prompt, accept the override by typing

**>Y**

After overriding a step, the option to reinstate that step exists by typing **>RESET step\_name**.

- 27** Ensure that the HELP STEP command has been performed for every step\_name.

| If all step_names have | Do                      |
|------------------------|-------------------------|
| not been verified      | <a href="#">step 23</a> |
| been verified          | <a href="#">step 28</a> |

- 28** Execute the upgrade process sequentially or out of sequence through one of the following commands:

| If executing the upgrade | Do                                                                                                                                              |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| sequentially             | Type<br><b>&gt;GO</b>                                                                                                                           |
| out of sequence          | To run a step, type<br><b>&gt;RUNSTEP step_name</b><br><b>ATTENTION</b><br>Do not choose to RUNSTEP a step_name that was selected for override. |

**29** Monitor the automated upgrade progress through the following:

- the trace device response
- the status of each node
- a log device

SWUPGRADE PM stops executing if:

- nodes are not ready for upgrading
- all nodes have been successfully upgraded
- An upgrade failure occurs.
- The SWUPGRADE PM shift exceeds the 14 hour time limit.
- a SET SHIFT FINISHED or SET SHIFT ABORTED command has been entered

SET SHIFT FINISHED stops the step after the full upgrade for the nodes in the step has completed

SET SHIFT ABORTED stops the step after the current maintenance action for node(s) has completed.

**30** After SWUPGRADE PM completes a step, the trace device displays an upgrade status report for each node.

| If                                                                       | Do                      |
|--------------------------------------------------------------------------|-------------------------|
| every node in the step passed and you want to continue the upgrade shift | <a href="#">step 32</a> |
| a node in the step failed                                                | <a href="#">step 31</a> |
| every node in the step passed and you want to finish the upgrade shift   | <a href="#">step 33</a> |

Use the QUERYPM FILES command from the MAP display to confirm each node is correctly loaded and in-service.

**31** Possible reasons for a node failure are:

- The peripheral module status, or one of its units, changed due to a maintenance problem not related to the automated upgrade.
- The peripheral module load file or required PRSU files are not in the Destination Volume.
- The node encountered a hardware problem.



Review logs PM703, SPM650, SPM651, SPM300, SPM500, SPM335 and NODE500, plus the trace device output to determine why the node failed the automated upgrade.

---

**If you can**


---

**Do**

determine why the node failed

Correct the problem and return to [step 28](#)

not determine why the node failed

Contact your next level of support.

If the problem is resolved, go to [step 28](#)

To continue the upgrade shift, go to [step 22](#)

To end the upgrade shift, go to [step 32](#)

- 
- 32** At the ALIGN\_RMS prompt, choose to align the RMIDs and PWIDs of all resource RMs in the office by typing

>Y

---

**If**


---

**Do**

you want to continue the upgrade shift

[step 22](#)

you want to finish the SPM upgrade shift

[step 33](#)

- 
- 33** Finish the automated SPM upgrade shift by typing

>**SET SHIFT FINISHED**

*Result*

A Summary Report for PM Software Upgrade containing the following information:

- the step name
- the elapsed time between the previous and current step
- the time the step began
- the elapsed time to execute the step
- the final result status

A result status of STEP NOT COMPLETE indicates SWUPGRADE PM did not perform the step. This could indicate a step that was overridden and performed manually.

The SET SHIFT FINISHED command can generate a PM700 log that indicates the SPM upgrade shift has finished. No action is required for this log.

- 34** Display the step of the automated upgrade by typing

**>DISPLAY STEPS**

| If all steps                                                                  | Do                      |
|-------------------------------------------------------------------------------|-------------------------|
| except UPGRADE_COMPLETE are complete or overridden                            | <a href="#">step 35</a> |
| are not complete or overridden and you do not intend to continue <sup>1</sup> | <a href="#">step 38</a> |

1.If all steps are not complete and overridden the upgrade can be resumed at a later date by restarting this procedure at [step 1](#).

- 35** Execute the UPGRADE\_COMPLETE step by typing

**>GO**

- 36** Obtain the final record of all completed steps by typing

**>DISPLAY STEPS**

- 37** Complete the UPGRADE\_COMPLETE step by typing

**>GO**

- 38** Quit the SWUPGRADE PM utility by typing

**>QUIT**

- 39** Stop the terminal responses from printing by typing

**>RECORD STOP ONTO printer**

- 40** You have completed this procedure.



## MG 9000 Manager upgrade

The MG 9000 Manager provides a network management system for the MG 9000. The MG 9000 Manager enables remote management of multiple MG 9000 network elements through a single graphical user interface (GUI).

**Note:** The MG 9000 element upgrade occurs after the MG 9000 Manager and Gateway Controller upgrades are completed.

The MG 9000 Manager runs on the SUN Microsystems servers which reside in the Cabinetized Operations Administration and Maintenance (COAM) cabinet. The Sun platform uses the Server Platform foundation software (SPFS) which is a high-performance, UNIX-based processing platform based on Sun Micro System's Netra line of NEBS compliant servers. The SPFS platform is used as the platform for OAM&P services.

The following software packages comprise the MG 9000 Manager

- SPFS
- MG 9000 server
- MG 9000 mid-tier

The following platforms are supported for the MG 9000 Manager tools:

- simplex server on which the MG 9000 server and MG 9000 mid-tier software run
  - one Sun Netra N240
  - one Sun t1400 server, one stand alone server for the MG 9000 Manager server and one for the MG 9000 Manager mid-tier
- duplex high availability server pair, two Sun Netra N240 servers

In the event you need or want to downgrade the MG 9000 Manager, refer to [Downgrading the MG 9000 and MG 9000 Manager from SN09U to SN08 or SN09 on page 2495](#).

## What's new in MG 9000 Manager Upgrades in (I)SN09U

### Feature changes

Modified procedures reflecting support for upgrade to SN09U.

### Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U
- SN09U to SN09U

### Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

### Time to complete an upgrade

The following table lists the tasks to upgrade MG 9000 Manager software and the estimated time to complete each task.

#### Estimated time to complete a software upgrade

| Task                                            | Application                                                  | Time                                               |
|-------------------------------------------------|--------------------------------------------------------------|----------------------------------------------------|
| Upgrading the SPFS software                     | SPFS - simplex configuration<br>SPFS - cluster configuration | 130 mins<br>160 mins                               |
| Preparing for the upgrade                       | MG 9000 Manager                                              | 30-50 mins                                         |
| Upgrading the software                          | MG 9000 Manager                                              | 30 mins                                            |
| Completing the upgrade                          | MG 9000 Manager                                              | 10 mins                                            |
| Total estimated time to upgrade MG 9000 Manager |                                                              | 90 mins                                            |
| Total time to upgrade all applications          |                                                              | 5.5 to 6 hours<br>(depending on the configuration) |
| Completing the upgrade                          |                                                              | 60 minutes                                         |
| Total estimated upgrade time                    |                                                              | 6.5 to 7 hours                                     |

**Service impacts**

The upgrade of MG 9000 Manager software has the following impact on service:

- OAM outage - the user cannot reach the server during upgrade of the MG 9000 Manager in t1400 and simplex N240 configurations.
- OM data collection is not performed during upgrades.
- OAM outage - during SWACT from earlier software release to new software release for an N240 HA cluster configuration.

**Note:** The high-availability (HA) cluster takes approximately five minutes to failover and bring up the standby server to active state.

**Additional information**

The following additional information applies to the upgrade of MG 9000 Manager software:

- After the SN09U MG 9000 Manager upgrade, the SN08 or SN09 MG 9000 Manager cannot be started against the same tablespace. The SN08 or SN09 server shuts down if the SN08 or SN09 MG 9000 Manager attempts to start up against a database schema that has been upgraded by the SN09U MG 9000 Manager. If this occurs, the following error message appears::

```
The application is trying to start up against a
database schema of a later release than the
application. This is not supported. The database
of the earlier release must be restored - or the
application must be taken up to the later release.
```

```
Application Version: >8.0< Database Schema
Version: >9.1<
```

- When upgrading the MG 9000 Manager from an earlier release to SN09U, earlier releases cannot run in tandem with the SN09U MG 9000 Manager. In addition, the SN09U MG 9000 Manager software is not compatible with earlier SPFS platform versions. The software release versions of the MG 9000 Manager and the SPFS platform cannot be mixed.
- Recommendations for limiting service impact: none

## Upgrade strategy

The following high-level strategy summarizes network upgrade procedures required when upgrading the MG 9000 Manager:

1. You have upgraded all components that precede the MG 9000 Manager as listed in table [Component Upgrade Order on page 6](#).
2. Remove the existing SN08 or SN09 software packages. Perform this activity just before upgrading the Server Platform Foundation Software (SPFS). SN09U MG 9000 Manager software cannot run on SN08 or SN09 SPFS software.
3. Upgrade the SPFS software. This includes the SPFS on the MG 9000 Manager master and mid-tier servers.
4. Upgrade the MG 9000 Manager software in the following order:
  - server
  - mid-tier

## When to use this document

Use this document to upgrade the MG 9000 Manager from SN08 or SN09 to SN09U.

When upgrading the MG 9000 Manager from SN08 to SN09U or SN09 to SN09U, the following activities take place in the following order:

- remove SN08 or SN09 software packages
- upgrade the Server Platform Foundation Software (SPFS)
- upgrade the MG 9000 Manager master server and mid-tier software

For a high level MG 9000 Manager upgrade summary, refer to either the [MG 9000 Manager SN08 or SN09 to SN09U upgrade checklist \(one-server\) on page 1073](#) or the [MG 9000 Manager SN08 or SN09 to SN09U upgrade checklist \(two-server\) on page 1074](#), depending on the appropriate upgrade path. These checklists reference detailed procedures that are provided later in the document.

Refer to the following related procedures:

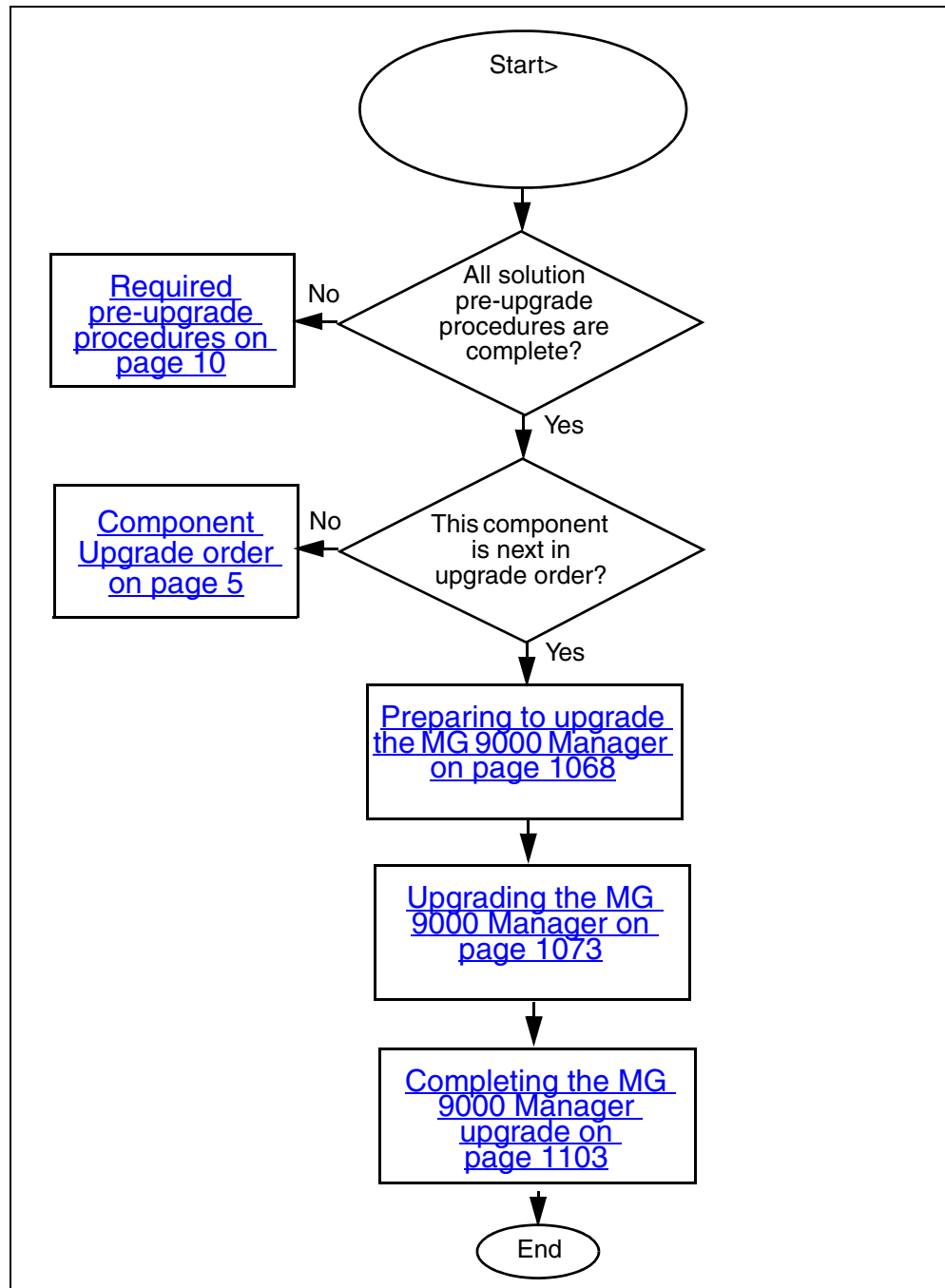
- [Downgrading the MG 9000 and MG 9000 Manager from SN09U to SN08 or SN09 on page 2495](#) for downgrading the MG 9000 Manager software
- [Upgrading the MG 9000 Manager software to a maintenance release on page 2512](#) for upgrading the MG 9000 Manager software to a maintenance release (MR)

## Tools and utilities

The MG 9000 Manager supports patching through the network patch manager (NPM). Patching procedures and information are located in [Carrier Voice over IP Network patching on page 2265](#).

## MG 9000 Manager upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

**MG 9000 Manager upgrade tasks**



---

## Preparing to upgrade the MG 9000 Manager

---

This section provides the information necessary for preparing to upgrade the MG 9000 Manager.

### Prerequisites

#### ATTENTION

Prior to the upgrade, verify your system has a minimum of 1800000 kilobytes of available disk space on the “/opt” file system, a minimum of 1200000 kilobytes of available disk space on the “/var” file system, and a minimum of 1550000 kilobytes of available disk space on the root (/) file system. If required, refer to procedure “Verifying disk utilization on an SPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.

Perform the previous required upgrade according to the order listed in the table [Component Upgrade order on page 5](#). The required upgrade is the previous component in the list according to your network configuration.

### Pre-upgrade requirements

Ensure the CS 2000 Manager has been upgraded to SN09U before upgrading any MG 9000 NEs to SN09U. Refer to [SN09U Upgrade Paths on page 5](#) to determine if the CS 2000 Manager upgrade is required.

The MG 9000 Manager must be upgraded to SN09U before upgrading MG 9000 NE cards to SN09U. This means the MG 9000 Manager running SN09U is capable of managing an MG 9000 NE operating at SN08, SN09 or, SN09U.

**Note:** All alarms on the MG 9000 Manager and MG 9000 NE must be cleared prior to proceeding with the SN08 or SN09 to SN09U upgrade process.

Do not provision any new data to the NEs during upgrade activities.

**Entry criteria**

The following information and tools are required during the software upgrade:

- host names and IP addresses required for:
  - the MG 9000 Manager mid-tier server
  - the MG 9000 Manager server
  - the CS 2000 Manager (Oracle database), required
  - the Security Authentication Host, typically the mid-tier IP address
  - the Imaging FTP Server Host, typically the SDM
- user id and password for the Imaging FTP Server Host must have overwrite privileges
- hardware and software baseline - MG 9000 Manager software must be at SN08 or SN09 with all patches applied and enabled
- tools required - database browser (optional)

**Upgrade interdependencies**

The following interdependencies are required during the upgrade process:

- SPFS on MG 9000 Manager master and mid-tier servers must be upgraded to SN09U ([Upgrading SPFS software on page 403](#)).
- CS 2000 Management Tools must be upgraded to SN09U prior to upgrading the MG 9000 Manager to SN09U.
- Ensure MG 9000 PSEs are configured correctly before the upgrade starts. This requires the following steps:

**Note:** If this is an N240 server, configure PSE on the workstation. If this is a t1400 server, configure PSE on the master and mid-tier servers.

- Telnet to the specific machine to be upgraded by typing
  - > **telnet <server ip address>**
- Change to the root directory by typing
  - \$ **su - root**
- Access the command line interface by typing
  - > **cli**
- To select Configurations, type
  - > **2**

- To select Succession Element Configuration, enter the number next to Succession Element Configuration option in the menu.
- To select PSE Configurations, enter the number next to the PSE Application Configuration option in the menu.
- To select View\_NPM\_host\_or\_ip, enter the number next to View\_NPM\_host\_or\_ip option in the menu.
- Ensure the PSE application points to the server which is hosting the NPM server. If it is not configured correctly, reconfigure accordingly. Refer to [Upgrading SPFS software on page 403](#) for more information.
- Run a getpatch to retrieve all SN09U patches before the upgrade starts. Refer to [Manually placing patches in the NPM database on page 2301](#), [Transferring patches delivered on CD to the NPM database on page 2297](#), or [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#) for more information.

**Exit criteria**

The following are the criteria for exiting from the SN08 or SN09 to SN09U upgrade process:

- The upgrade was successful after the MG 9000 Manager mid-tier server and server applications are running in SN09U.
- Additional exit criteria is determined later in the upgrade process, after upgrading the MG 9000 network element. Refer to MG 9000 NE [Exit criteria on page 1580](#).

**Applying software fixes**

When it is necessary to apply software fixes, the following methods are available:

- Maintenance Release upgrade process - Refer to procedure [Upgrading the MG 9000 Manager software to a maintenance release on page 2512](#).
- Patching - Refer to [Carrier Voice over IP Network patching on page 2265](#) for more information.

## MG 9000 Manager client system requirements

The following table provides recommended minimum configurations for the MG 9000 Manager client.

### MG 9000 Manager client minimum configurations

| Client platform | Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows client  | <ul style="list-style-type: none"><li>Windows NT 4.0 (SP5 or later), Windows 2000 (SP2 or later), or Windows XP</li><li>Pentium III 1 GHz or higher</li><li>display resolution of 1280 x 1024 with 256 colors</li><li>256 MB RAM</li><li>200 MB hard drive space</li><li>10BaseT/100BaseT Ethernet network connection</li><li>Java Web Start (JWS) 1.4.2_08 and higher</li></ul> <p>If the Windows PC supports more network client applications than just the MG 9000 Manager client application, the following minimum configuration is required:</p> <ul style="list-style-type: none"><li>Windows 2000 (SP2 or later), or Windows XP</li><li>Pentium III 2.5 GHz or higher</li><li>display resolution of 1280 x 1024 with 256 colors</li><li>1 Ghz RAM</li><li>30 Gb hard drive space</li><li>10BaseT/100BaseT Ethernet network connection</li><li>Java Runtime Environment (JRE) 1.4.2_08 and higher</li><li>Java Web Start (JWS) 1.4.2_08 and higher</li></ul> |
| Solaris client  | <ul style="list-style-type: none"><li>Solaris 7 or Solaris 8 with Sun recommended patches for Java Runtime Environment (JRE) 1.4.2_08</li><li>Ultra 5 400 MHz or higher</li><li>display resolution of 1280 x 1024 with 256 colors</li><li>256 MB RAM</li><li>200 MB hard drive space</li><li>10BaseT/100BaseT Ethernet network connection</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**MG 9000 Manager client minimum configurations**

| Client platform           | Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows or Solaris client | <p>Third party software</p> <ul style="list-style-type: none"><li>• Netscape 6.0 and higher or Internet Explorer 5.5, 6.0 and higher</li><li>• Java Web Start (JWS) 1.4.2_08 and higher</li></ul> <p><b>Note:</b> Access to some functions requires the use of SSH-compatible client software for access to secure telnet and ftp services (using SSH standard). Some operating systems contain SSH clients. Any missing SSH clients must be obtained separately. Sources for SSH clients include, but are not limited to, the following:</p> <ul style="list-style-type: none"><li>• PUTTY - freeware</li><li>• OpenSSH - freeware</li><li>• SSH Inc. - commercial</li><li>• Secure CRT - commercial</li><li>• WinSCP - freeware</li></ul> <p>Nortel does not supply or recommend a particular supplier.</p> |

**Action**

Use the following checklists to determine the steps for upgrading the MG 9000 Manager:

- [MG 9000 Manager SN08 or SN09 to SN09U upgrade checklist \(one-server\) on page 1073](#)
- [MG 9000 Manager SN08 or SN09 to SN09U upgrade checklist \(two-server\) on page 1074](#)

## Upgrading the MG 9000 Manager

The following checklists provide the high-level steps to upgrade the MG 9000 Manager. Where applicable, a reference to the step-by-step procedure is provided.

### SN08 or SN09 to SN09U t1400/N240 one-server (simplex) upgrade checklist

Use the following table as a checklist for upgrading the MG 9000 Manager from SN08 or SN09 to SN09U in a t1400/N240 single-server (simplex) configuration. Enter a check mark (✓) in the ✓column as each step or procedure is completed.

#### MG 9000 Manager SN08 or SN09 to SN09U upgrade checklist (one-server)

|   | Activity                                                                                                                          | Procedure                                                                                                                                                                                                                                                                                                                                                                                  | ✓ |
|---|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1 | Upgrade the MG 9000 Manager to SN09U.                                                                                             | 1. Refer to procedure <a href="#">Upgrading MG 9000 Manager software from SN08 or SN09 to SN09U on page 1076</a> . and the procedures referenced in the following steps to complete the MG 9000 Manager upgrade.                                                                                                                                                                           |   |
|   | <b>Note:</b> This is a safe stopping point                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                            |   |
| 2 | Update the version of the software registered in IEMS for the MG 9000 Manager.                                                    | Update the IEMS with the version number of the software now running in the MG 9000 Manager. Refer to either of the following procedures: <ul style="list-style-type: none"> <li>• <a href="#">Editing and viewing object properties using Web Client on page 2261</a></li> <li>• <a href="#">Editing and viewing object properties using Java Web Start Client on page 2255</a></li> </ul> |   |
| 3 | This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure. |                                                                                                                                                                                                                                                                                                                                                                                            |   |

## SN08 or SN09 to SN09U N240 two-server (cluster) upgrade checklist

Use the following table as a checklist for upgrading the MG 9000 Manager from SN08 or SN09 to SN09U in a two-server (cluster) configuration. Enter a check mark (✓) in the ✓ column as each step or procedure is completed.

### MG 9000 Manager SN08 or SN09 to SN09U upgrade checklist (two-server)

| Activity                                       | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | ✓ |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| <b>On the Inactive node</b>                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |   |
| <b>1</b> Upgrade the MG 9000 Manager to SN09U. | <ol style="list-style-type: none"> <li>1. Perform the following steps to complete the MG 9000 Manager upgrade.             <ol style="list-style-type: none"> <li>a. Telnet to the inactive node of the specific machine to be upgraded by typing<br/> <code>&gt; telnet &lt;server ip address&gt;</code></li> <li>b. Log in as root.</li> <li>c. To verify you are on the inactive node, type<br/> <code>&gt; bash</code></li> <li>d. To verify all applications have stopped, type<br/> <code>&gt; servquery -status all</code></li> <li>e. To verify if the node in the cluster is active or standby unit, type<br/> <code>&gt; ubmstat</code><br/>               If the system response is ClusterIndicatorSTBY, proceed to the next step. If the response is other than ClusterIndicatorSTBY, refer to <a href="#">Verifying the state of a cluster on page 400</a>.</li> <li>f. To verify the unit is in standby and is in a normal state<br/> <code>&gt; udstat</code><br/>               If the system response is STANDBY normal UP clean, proceed to the next step. If the response contains nodaemon, offline, down, or not mounted, refer to <a href="#">Verifying the state of a cluster on page 400</a>.</li> <li>g. Perform procedure <a href="#">Upgrading MG 9000 Manager software from SN08 or SN09 to SN09U on page 1076</a>.</li> </ol> </li> </ol> |   |
| <b>Note:</b> This is a safe stopping point     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |   |

**MG 9000 Manager SN08 or SN09 to SN09U upgrade checklist (two-server)**

| Activity                                                                                                                                   | Procedure                                                                                                                                                                                                                                                                                                                                                                               | ✓ |
|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| <b>2</b> Update the version of the software registered in IEMS for the MG 9000 Manager.                                                    | Update the IEMS with the version number of the software now running in the MG 9000 Manager. Refer to either of the following procedures: <ul style="list-style-type: none"><li>• <a href="#">Editing and viewing object properties using Web Client on page 2261</a></li><li>• <a href="#">Editing and viewing object properties using Java Web Start Client on page 2255</a></li></ul> |   |
| <b>3</b> This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure. |                                                                                                                                                                                                                                                                                                                                                                                         |   |

**Prerequisites**

You have completed the information in [Preparing to upgrade the MG 9000 Manager on page 1068](#)

If software is delivered to the customer using Electronic Software Delivery (ESD), ensure the MG 9000 Manager loads are available by performing procedure [Preparing MG 9000 Manager software delivered through ESD for an upgrade on page 1104](#).



## Action

Perform the following procedure to upgrade the MG 9000 Manager.

### Upgrading MG 9000 Manager software from SN08 or SN09 to SN09U

- 1 Perform a full system backup. Refer to procedure [Performing a backup of file systems on an SPFS-based server on page 379](#).

- 2 Use the following table to determine how to begin.

| If the master and mid-tier are on | Do                                                           |
|-----------------------------------|--------------------------------------------------------------|
| the same server                   | log into the active (physical IP) side of the cluster        |
| separate servers                  | log into the server hosting the mid-tier application as root |

- 3 For your reference, write down the existing configuration settings for the mid-tier server. To view these settings, type:  

```
> /opt/nortel/mg9kmtr_<release_number>/bin/mg9kconfig.sh
```

where  
release\_number is 08 for SN08, or 09 for SN09

When prompted, enter Y to keep the existing settings and exit from the script.

- 4 Log in as root on the master server.

**Note:** If this is an N240 cluster configuration, log in to the **active unit**.

- 5 For your reference, write down the existing configuration settings for the master server. To view these settings, type:

```
> /opt/nortel/mg9ksrv_<release_number>/bin/mg9kconfig.sh
```

where  
release\_number is 08 for SN08, or 09 for SN09

When prompted, enter Y to keep the existing settings and exit from the script.

- 6 From the **active** unit, make a backup of the SN08 or SN09 tablespace by typing
- ```
> /opt/nortel/mg9ksrv_<release_number>/bin/mgems_ora_ts_backup.sh $DB_HOST
```
- where**
release number is the number of the software such as 08 for SN08 or 09 for SN09
- Note:** The tablespace data will be written to /data/mg9kem/persistdata/tsBackup.
- 7 Use the following table to determine the next step.
- | If the MG 9000 Manager software to be upgraded runs on | Do |
|--|-------------------------|
| a t1400/N240 simplex (one-server) configuration | step 8 |
| an N240 cluster (two-server) configuration | step 15 |
- 8 Log in as root on each of the machines where the mid-tier and server reside and determine whether the applications are running by typing:
- ```
> servquery -status all
```
- 9 Use the following table to determine the next step.
- | If the mid-tier applications | Do                      |
|------------------------------|-------------------------|
| are running                  | step <a href="#">10</a> |
| are not running              | step <a href="#">11</a> |
- 10 Stop the mid-tier by typing
- ```
> servstop MG9KMIDTIER<_release number>
```
- where**
release number is a value such as 08 for SN08. Release number is not required for SN09.
- 11 Use the following table to determine the next step.
- | If the server applications | Do |
|----------------------------|-------------------------|
| are running | step 12 |
| are not running | step 13 |

- 12 Stop the server by typing

```
> servstop MG9KSERVER<_release number>
```

where
release number is a value such as 08 for SN08. Release number is not required for SN09.
- 13 To remove the master server SN08 or SN09 application packages, from the master server, log in as root and type

```
> pkgrm NTmg9ks<release_numbe>
```

where
release_number is 08 for SN08, or 09 for SN09

To continue, respond to the two prompts with Y.
- 14 To remove the mid-tier server SN08 or SN09 application packages, from the mid-tier server, log in as root and type

```
> pkgrm NTmg9km<release_number>
```

where
release_number is 08 for SN08, or 09 for SN09

To continue, respond to the two prompts with Y.

Go to step [18](#).
- 15 If upgrading an N240 cluster configuration, log in to the **inactive unit** to remove the master server SN08 or SN09 application packages by typing

```
> pkgrm NTmg9ks<release_number>
```

where
release_number is 08 for SN08, or 09 for SN09

To continue, respond to the two prompts with Y.
- 16 To remove the mid-tier server SN08 or SN09 application packages, log in as root on the **inactive node** and type

```
> pkgrm NTmg9km<release_number>
```

where
release_number is 08 for SN08, or 09 for SN09

To continue, respond to the two prompts with Y.

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

If the server being upgraded is	Do
an N240 one-server or t1400 configuration	step 18
an N240 cluster configuration	step 19

- 18 For the one-server or t1400 configuration, upgrade both the mid-tier server and the master server to the SN09U SPFS platform.

Note: At this time, do not execute the command SSPFS_Upgrade.accept. This command is the last step of the upgrade process.

Details about upgrading the SPFS platform are provided in procedure [Upgrading SPFS software on page 403](#). Go to step [20](#).

- 19 For the N240 cluster configuration, upgrade the inactive server to the SN09U SPFS platform.

Note: At this time, do not execute the command SSPFS_Upgrade.accept. This command is the last step of the upgrade process.

Details about upgrading the SPFS platform are provided in procedure [Upgrading SPFS software on page 403](#)

- 20 Obtain any patches you received with your software release, that are applicable to the components on the server, such as PSE, SPFS, MG 9000 Manager, and transfer them to the NPM database.

Use the following table to determine the next step.

If you received patches	Do
on a CD	step 24
in an ISO image file	step 21

- 21 On the SPFS server on which the NPM resides, transfer and mount the patch ISO image on the server. For detailed steps, refer to procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

- 22 Transfer the patches from the ISO image file to the NPM database. For detailed steps, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).

- 23** Unmount and remove the patch ISO image from the server. For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
Go to step [25](#).
- 24** Transfer the patches from the CD to the NPM database. For detailed steps, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).
- 25** Check for patch currency, for patches that are applicable to the components on the server, such as, PSE, SPFS, MG 9000 Manager, and transfer them to the NPM database. For detailed steps, refer to [Ensuring patch currency on page 12](#).
- 26** Execute steps [20](#) thru 24 to install the patches after the patches are downloaded.
- 27** Install any patches for SPFS using the NPM by performing procedure [Applying patches using the NPM on page 2319](#).

Upgrading the master server software

- 28** Install the SN09U master server application. Log in as root (superuser).

Note: If this is an N240 cluster (two-server) configuration, perform this step on the **inactive node**.

Use the following table to determine the next step.

If installing the master server software from	Do
CD-ROM	step 29
electronic software delivery (ESD)	step 32

- 29** Insert the Succession MG 9000 Manager software CD into the CD-ROM drive. This server is also running the OpenOrb NamingService.

Note: If this is an N240 cluster configuration, install the software on the inactive side.

- 30** List the available files on the Nortel Networks load disk. To list the files, change directory to the CD-ROM drive and list the contents by typing

```
> cd /cdrom/cdrom0
> ls
```

The system responds with the following example output:

```
# cd /cdrom/cdrom0
# ls
BWTool.exe NTMG9KS91_31_0.PKG
NTMG9KM91_31_0.PKG
```

- 31** At the prompt (#), use pkgadd to install the server portion (NTmg9ks91.pkg) of the software. To directly install the software from the CD, enter the following command:

```
# pkgadd -d /cdrom/cdrom0/<mgemserver package>
where
```

<mgemserver package> is the MG 9000 Manager server package name, for example NTMG9KS91_31_0.PKG

The system responds with the following:

The following packages are available:

```
1 NTmg9ks91 Succession MG 9000 Manager Server
(sparc) 9_1_44
```

```
Select package (s) you wish to process (or 'all'
to process all packages). (default: all)
[?,??,q]:
```

Go to step [33](#).

- 32** At the prompt (#), use pkgadd to install the server portion (NTmg9ks91.pkg) of the software from ESD by typing

Note 1: If this is an N240 cluster configuration, install the software on the inactive side.

Note 2: For information on retrieving software from ESD, refer to procedure [Preparing MG 9000 Manager software delivered through ESD for an upgrade on page 1104](#).

```
# pkgadd -d
/opt/nortel/<mgeserver_package>.pkg
```

where

<mgeserver package> is the MG 9000 Manager server package name, for example NTMG9KS_9_1_31_0.PKG

The following packages are available:

```
1 NTmg9ks91 Succession MG 9000 Manager Server
      (sparc) NTMG9KS_9_1_44_0
```

```
Select package(s) you wish to process (or 'all'
to process all packages).
(default: all) [?,??,q]:1
```

- 33** Enter 1 and press return to begin the server installation process.

The system responds with the following:

```
Processing package instance <NTmg9ks91> from
</NTmg9ks91.pkg>
```

```
Succession MG 9000 Manager Server (sparc) 7.44
```

```
Copyright (c) 1998-2003 Nortel Networks
All Rights Reserved
```

```
This product is protected by copyright and
distributed under licenses restricting copying,
distribution and decompilation.
```

```
## Executing checkinstall script.
Using as the package base directory.
## Processing package information.
## Processing system information.
    135 package pathnames are already properly
installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be
executed with super-user permission during the
process of installing this package.
```

```
Do you want to continue with the installation of
<NTmg9ks91> [y,n,?]
```

- 34** To continue, respond to the prompt with Y.

Note: Verify the installation of <NTmg9ks91> was successful. If there are any errors please contact your next level of support.

- 35** If applicable, eject the CD-ROM by typing

```
# eject cdrom0
```

Note: This is not necessary if the mid-tier and base server reside on the same server.

- 36** Obtain the hostname of the current master server by typing

```
# hostname
```

- 37** The steps for installing software in the master server are complete.

Configuring the master server software

38 To configure the MG 9000 Manager master server, type

Note: If this is an N240 cluster (two-server) configuration, perform this step on the inactive node.

```
> /opt/nortel/mg9ksrv_09_1/bin/mg9kconfig.sh
```

The system responds with the following:

```
Setup Server As : Master
Master Server IP Address : 47.xxx.xx.207
CS2M IP Address: 47.xxx.xx.220
Security Authentication Host : 47.xxx.xx.227
Get Northbound logs from IEMS : y
Oracle IP Address : 47.xxx.xx.220
Image Server : 47.xxx.xx.8
Image Server User ID : maint
SuperCore Gige Image Directory : /swd/mg9k
SuperCore IMA Image Directory : /swd/mg9k
SuperCore OC3 Image Directory : /swd/mg9k
ITP Image Directory : /swd/mg9k
ITX Image Directory : /swd/mg9k
ABI Image Directory : /swd/mg9k
DS1 Image Directory : /swd/mg9k
OM Collector CSV Directory : /data/oms/1
*****Is
the above information correct? Press the enter
key to accept the default (y/n)? Default : [n]
=>
```

Note 1: Accept the default values to continue with the upgrade. However if you want to change the settings, at this point in the upgrade process, use the prompts to change any values.

Note 2: If the IEMS is configured through /etc/syslog.conf , then set Get Northbound logs from IEMS to y , or if SDM is configured through /etc/syslog.conf , then set Get Northbound logs from IEMS to n.

- 39** The MG 9000 mid-tier GUI banner now displays the CM_CLLI. The CM_CLLI needs to be configured by performing the steps that follow while logged into the MG 9000 master server. These steps must be performed on the inactive unit. Once this is complete, log into the MG 9000 mid-tier and perform the same steps.

If the MG 9000 master server and mid-tier reside on the same IP, you need to perform this only once.

Log in as root by typing

```
$ su - root
```

The system responds with the following:

Password:

<enter the root password>

- 40** Access the command line interface by typing

```
# cli
```

The system responds with the following:

Command Line Interface

- 1 - View
- 2 - Configuration
- 3 - Other
- X - exit

- 41** Enter 2 to access the Configuration menu.

The system responds with the following:

Configuration

- 1 - NTP Configuration
- 2 - Apache Proxy Configuration
- 3 - OAMP Application Configuration
- 4 - CORBA Configuration
- 5 - IP Configuration
- 6 - DNS Configuration
- 7 - Syslog Configuration
- 8 - Remote Backup Configuration
- 9 - Database Configuration
- 10 - NFS Configuration
- 11 - Bootp Configuration
- 12 - Restricted Shell Configuration
- 13 - Security Services Configuration
- 14 - Disk Drive Upgrade
- 15 - Login Session
- 16 - Location Configuration
- 17 - Cluster Configuration

```
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
```

```
X - exit
```

42 Enter 3 to access the OAMP Application Configuration menu.

The system responds with the following:

```
OAMP Application Configuration
1 - sdm_conf (Configure SDM IP Address)
2 - sdm_unconf (Unconfigure SDM IP Address)
3 - sdmuser_conf (Configure SDM User)
4 - sdmuser_unconf (Unconfigure SDM User)
5 - cmClli_rediscovery (Re-discovery the CM
CLLI by SDM IP )
6 - cmClli_conf (Configure CM_CLLI Address)
7 - cmClli_unconf (Unconfigure CM_CLLI IP
Address)
8 - cm_conf (Configure CM IP Address)
9 - cm_unconf (Unconfigure CM IP Address)
```

```
X - exit
```

43 Enter 6 to configure the CM CLLI address.

Note: The CM CLLI address is determined by the customer based on the entire network and is an engineering parameter specific to the customer site. The CM CLLI is provisioned at the Core. Contact your next level of support for more information.

The system responds with the following:

```
=== Executing "cmClli_conf"
Enter CM_CLLI: <site CM_CLLI>
CM CLLI :      <site CM_CLLI>
```

44 Enter ok to accept current settings.

```
ok
```

```
Processing values....
```

```
CM_CLLI Configured
Please perform a logout and login so your shell
will reflect CLLI environment settings
=== "cmClli_conf" completed successfully
```

45 Quit this MG 9000 Manager telnet Unix shell and login again to inherit the new settings.

- 46** For additional help on available options, execute the following command.

```
# /opt/nortel/mg9ksrv_09_1/bin/mg9kserver help
```

- 47** Use the following table to determine the next step.

If the server being upgraded is	Do
an N240 cluster configuration	step 49
an N240 one-server or t1400 configuration	step 48

- 48** For simplex configuration only, start the SN09U master server application by typing

```
> servstart MG9KSERVER
```

Note: If messages appear indicating that a <file_name>_patch failed to stay up, these messages can be ignored.

Upgrading the mid-tier server software

- 49** Install the SN09U mid-tier server application. Log in as root (superuser).

Note: If this is an N240 cluster (two-server) configuration, perform this step on the inactive node.

- 50** Use the following table to determine the next step.

If installing the mid-tier server software from	Do
CD-ROM	step 51
electronic software delivery (ESD)	step 53

- 51** Insert the CD containing the MG 9000 Manager software into the CD-ROM drive.

Note: If this is an N240 cluster configuration, install the software on the inactive side.

- 52** At the prompt (#) use pkgadd to install the mid-tier portion (NTmg9km91.pkg) of the software. If you are directly installing from the CD-ROM use the following command to read the CD-ROM, and list the contents to read the release number:

```
# cd /cdrom/cdrom0/
# ls
# pkgadd -d /cdrom/cdrom0/NTMG9KM91_xx_0.pkg
```

where

xx is the build number.

The system responds with the following information.

The following packages are available:

```
1 NTmg9km91 Succession MG 9000 Manager Midtier
Server
```

```
(sparc) 9_1.44
```

```
Select package(s) you wish to process (or 'all'
to process all packages). (default: all)
[? , ?? , q]:
```

Go to step [54](#).

- 53 At the prompt (#) use pkgadd to install the mid-tier portion (NTmg9km91.pkg) of the software from ESD by typing

Note 1: If this is an N240 cluster configuration, install the software on the inactive side.

Note 2: For information on retrieving software from ESD, refer to procedure [Preparing MG 9000 Manager software delivered through ESD for an upgrade on page 1104](#).

```
# pkgadd -d /opt/nortel/NTMGKM91_XX_0.pkg
```

The following packages are available:

```
1 NTmg9km91 Succession MG 9000 Manager
    Midtier Server
    (sparc) NTMG9KM91_44_0
```

```
Select package(s) you wish to process (or 'all'
to process all packages).
(default: all) [?,??,q]:1
```

- 54 Enter 1 and press return to begin the server installation process.

The system responds as follows:

```
Processing package instance <NTmg9km91> from
</NTmg9km91.pkg>
```

```
Succession MG 9000 Manager Midtier Server
(sparc) 9_1.44
```

```
Copyright (c) 1998-2003 Nortel Networks
All Rights Reserved
```

```
This product is protected by copyright and
distributed under licenses restricting copying,
distribution and decompilation.
```

```
Executing checkinstall script.
Using </opt> as the package base directory.
Processing package information.
Processing system information.
1 package pathname is already properly
installed.
```

Note: If a message appears with a confirmation prompt to overwriting conflicting files, respond Y. If existing files are not overwritten, the MG 9000 Manager mid-tier server upgrade cannot continue.

```
Verifying disk space requirements.  
Checking for conflicts with packages already  
installed.Checking for setuid/setgid programs.
```

```
This package contains scripts which will be  
executed with super-user permission during the  
process of installing this package.
```

```
Do you want to continue with the installation of  
<NTmg9km91> [y,n,?]
```

```
# y
```

Note: Verify installation of <NTMG9KM91_xx_0> was successful. If there are any errors please contact your next level of support.

- 55** The installation continues automatically and installs all the mid-tier server files in /opt/nortel/mg9kmtr_91 subdirectory as noted in the system response.

```
Installing Succession MG 9000 Manager Midtier  
Server as <NTmg9km91>
```

```
## Installing part 1 of 1.
```

```
.  
.  
.
```

```
Configuring system, please wait ...
```

```
Installation of <NTmg9km91> was successful.
```

After the installation is complete, a message appears reporting that the installation was successful.

Configuring the mid-tier server software

- 56** To configure the MG 9000 Manager mid-tier server, type

Note: If this is an N240 cluster (two-server) configuration, perform this step on the inactive node.

```
# /opt/nortel/mg9kmtr_09_1/bin/mg9kconfig.sh
```

- 57** Accept the default values to continue with the upgrade.

- 58** Use the following table to determine the next step.

If the server being upgraded is	Do
an N240 cluster configuration	step 63
an N240 one-server or t1400 configuration	step 59

- 59** Start the SN09U mid-tier server application by typing

```
> servstart MG9KMIDTIER
```

Note: If messages appear indicating that a <file_name>_patch failed to stay up, these messages can be ignored.

- 60** Stop and start the Patching Server Element (PSE) application by typing

```
# pse stop
```

```
# pse start
```

- 61** Apply any MG 9000 Manager software patches. Refer to [Carrier Voice over IP Network patching on page 2265](#).

- 62** Perform a full backup on the new load. For detailed steps, refer to [Performing a backup of file systems on an SPFS-based server on page 379](#).

Go to step [70](#).

For cluster configuration**63****ATTENTION**

The patchUpToDate script should only be used when the NPM resides on the same server as that being upgraded. If the NPM does not reside on the same server, use the procedure [Applying patches using the NPM on page 2319](#).

Patch the inactive node of the cluster. Apply the SPFS patches to the inactive server by typing

patchUpToDate

and pressing the Enter key.

The system responds as follows:

Obtaining the list of devices that can be patched.

According to the current PSE configuration, "wnc0s00z" is the NPM host.

Is this correct? [yes]

Note: If this is a geographical redundant configuration, upgrade the standby server.

64 Press the Enter key to confirm that you want the patches applied.

Note: Typing no and pressing the Enter key causes the processing to stop.

A report is generated which contains all the console output from the patchUpToDate session.

The report that is produced contains a summary of the patching actions that occurred as well as any errors. The summary includes patches applied, any patches that were already applied when the patchUpToDate utility started, any patches that have been applied and removed when the patchUpToDate utility started, and any patches that were not applied because their prerequisite patches were not available.

65 Return the server to the cluster by performing the procedure [Returning a server to a cluster on page 456](#)

66 Stop the SN08 or SN09 MG 9000 client applications since earlier version cannot operate with an SN09U MG 9000 Manager.

To stop the client application on a PC or Unix workstation, close the SN08 or SN09 Subnet View.

- 67 Telnet to the active node through the console (port A) using the root user ID and password
- 68 Stop the cluster by typing
- ```
init 0
```
- and pressing the Enter key.
- Stopping a cluster causes the standby (inactive) server to take over and start providing OAM&P services as the new active server.
- Note:** The high-availability (HA) cluster takes approximately five minutes to failover and bring up the standby server to Active state.
- 69 Telnet to the cluster IP address and login to the newly active unit.

### ***For simplex and cluster configurations***

- 70 Install the SN09U GUI client application by performing the installation procedure based on the platform type used for the client, PC or Sun workstation. Refer to the [Installing the MG 9000 Sun client software on page 1099](#) or [Installing the MG 9000 Manager Windows PC client software on page 1097](#) procedure.
- 71 Use the following table to determine the next step.
- | <b>If a userid with appropriate permissions</b> | <b>Do</b>               |
|-------------------------------------------------|-------------------------|
| needs to be provisioned                         | step <a href="#">72</a> |
| does not need to be provisioned                 | step <a href="#">74</a> |
- 72 Provision a userid with appropriate privileges for the upgrade process. Add a new user to group succssn and emsadm. To allow access to the GUI, from the mid-tier server type
- ```
> useradd -g succssn -G emsadm [userid]
```
- where**
- emsadm is the privilege to be assigned to the userid. Refer to *MG 9000 Security and Administration*, NN10162-611 for details.
- Note:** For t1400 configurations where the mid-tier and master servers are on different machines, run this command on each machine.
- 73 To enter the password for this userid, type
- ```
>passwd [userid]
```

**Note:** The password must be entered twice.

- 74** Verify the health of the master and mid-tier servers by typing

> **servquery -status all**

**Note:** If the mid-tier and master server applications are on separate machines, perform this step on each machine. Please contact your next level of support if applications MG9KSERVER or MG9KMIDTIER is NOT RUNNING

- 75** Use the following table to determine the next step.

| If the MG 9000 Manager                              | Do                      |
|-----------------------------------------------------|-------------------------|
| needs to be configured for central security         | step <a href="#">76</a> |
| does not need to be configured for central security | step <a href="#">84</a> |

- 76** Configure the MG 9000 Manager for central security, configure the IEMS server to include the MG 9000 Manager in central security. Accessing the command line interface by typing

> **cli**

- 77** Enter the number that corresponds to “Configuration”.
- 78** Enter the number that corresponds to “Security Services Configuration”.
- 79** Enter the number that corresponds to Security Server Location Configuration”.
- 80** Enter the number that corresponds to “Configure Security Server IP”.
- 81** Enter the Server IP address.
- 82** Enter the Fully Qualified Domain Name.
- 83** If the output is correct, enter OK to commit changes.
- 84** Start any SN09U 3rd party application(s), especially those using the OSS alarm interface.
- 85** Launch SN09U GUI client software.
- During the upgrade process, when the user clicks on the SN09.1 link in the Application Launch Point, the SN09U application launches. At that point, the user must login. This allows the user into the SN09U application.

- 86 Use the following table to determine the next step.

| If the server being upgraded is           | Do                      |
|-------------------------------------------|-------------------------|
| an N240 cluster configuration             | step <a href="#">87</a> |
| an N240 one-server or t1400 configuration | step <a href="#">88</a> |

***For simplex and cluster configurations***

- 87 To confirm the upgrade on a cluster, at the active node console, log in to the active node through the console (port A) using the root user ID and password, if not already logged in.

- 88 Use the following table to determine the next step.

| If                                                       | Do                      |
|----------------------------------------------------------|-------------------------|
| you choose to accept the upgraded environment            | step <a href="#">89</a> |
| you choose to rollback to the state prior to the upgrade | step <a href="#">90</a> |

- 89 Accept the upgraded environment by typing

**# /SSPFS\_Upgrade.accept**

and pressing the Enter key.

Proceed to step [91](#) for a cluster configuration or step [94](#) for a simplex configuration.

- 90 Rollback to the state prior to the upgrade by performing procedure [Downgrading the MG 9000 and MG 9000 Manager from SN09U to SN08 or SN09 on page 2495](#).

The node is now restored as it was before the upgrade.

- 91 To verify the node is the active unit, type

**> ubmstat**

- 92 To check the health of the unit, type

**> servquery -status all**

- 93 Perform the procedure [Cloning the image of one server in a cluster to the other server on page 478](#).

**94** This procedure is complete.

If this is a simplex upgrade, return to step [2 on page 1073](#) of the [MG 9000 Manager SN08 or SN09 to SN09U upgrade checklist \(one-server\)](#) and continue with the SN08 or SN09 to SN09U upgrade process.

If this is a two-server upgrade, return to step [2 on page 1075](#) of the [MG 9000 Manager SN08 or SN09 to SN09U upgrade checklist \(two-server\)](#) and continue with the SN08 or SN09 to SN09U upgrade process.

## MG 9000 Manager client configuration

### Installing the MG 9000 Manager Windows PC client software

#### *At the Windows PC client*

- 1 From a web browser, launch Succession OAM&P Applications Launch Point page at:  
http://<SN09U MG9KEM Midtier Server IP or hostname>.

Click Application Launcher.

The Application Launch Point window appears. Click the MG9000 Element Manager [SN09.1] link. Enter the username and password in the login when prompted.

**Note:** When starting the MG 9000 Manager from a Microsoft Windows platform, Windows may ask for a Security Certificate Approval. Windows does not display the Security Certificate Approval window on top of all other open windows. It may become necessary to minimize all open windows to see the Security Certificate Approval window. The security settings in the browser determine if the user will be asked for certificate approval.

- 2 To verify the version of Java Web Start being executed, access the Java Web Start Application Manager by selecting Start->Programs->Java Web Start. The Java Web Start Application Manager appears.
- 3 From the JWS Application Manager, select Help->About Java Web Start.
- 4 If the version is not 1.4.2\_08, reinstall from the Client Software Installation page as noted in the following step.
- 5 Use the following figure and the information in the following table to determine the next step.

| If Java Web Start (JWS)<br>version 1.4.2_08 software                          | Do                      |
|-------------------------------------------------------------------------------|-------------------------|
| is already installed in the client machine                                    | step <a href="#">11</a> |
| is not installed in the client machine, as evidenced by the preceding message | step <a href="#">6</a>  |

- 6 Select the link Java™ Web Start Install Guide to go to the Client Software Installation page.
- 7 Go to Java 2 Runtime Environment Install Guide under Microsoft Windows section for online documentation.

- 8** Go to Java 2 Runtime Environment Software Download under the Microsoft Windows section to download Java Runtime Environment.
- 9** Save j2re-1\_4\_2\_08-windows-i586-i.exe and execute the JRE software.
- 10** Follow the instructions in JRE software to install JRE 1.4.2\_08.
- 11** The PC client is setup to launch MG 9000 Manager SN09U client applications.
- 12** Remove JWS cache by performing procedure [Removing an MG 9000 Manager JWS application from cache on page 1101](#).
- 13** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Installing the MG 9000 Sun client software

### *At the client workstation*

- 1 From a web browser, launch Succession OAM&P Applications Launch Point page at: `http://<SN09U MG9KEM Midtier Server IP or hostname>`. Click Application Launcher.  
The Application Launch Point window appears with a link for SN09U. Click the MG9000 Element Manager [SN09.1] link. Enter the username and password in the login when prompted.
- 2 To verify the version of Java Web Start being executed change directory to where the Java Web Start application is installed by typing  
`> cd <path/javaws>`
- 3 To launch the Java WebStart application manager, type  
`> javaws &`
- 4 From the JWS Application Manager, select Help->About Java Web Start. The application version is displayed.
- 5 If the version is not 1.4.2\_08, reinstall from the Client Software Installation page as noted in the following step.
- 6 Use the following figure and the information in the following table to determine the next step.

| If Java Web Start (JWS)<br>version 1.4.2_08 software                          | Do                      |
|-------------------------------------------------------------------------------|-------------------------|
| is already installed in the client machine                                    | step <a href="#">18</a> |
| is not installed in the client machine, as evidenced by the preceding message | step <a href="#">7</a>  |

- 7 Select the link Java™ Web Start Install Guide to go to the Client Software Installation page.
- 8 Go to the Java 2 Runtime Environment Install Guide under the Sun Solaris section for online documentation.
- 9 Go to the Java 2 Runtime Environment Software Download under the Sun Solaris section to download Java Runtime Environment.
- 10 Save `j2re-1_4_2_08-solaris-sparc.sh` to your home directory.
- 11 Change execute permissions.

```
$ chmod +x j2re-1_4_2_08-solaris-sparc.sh
```



- 12 Execute JRE, which will create a JRE subdirectory called j2re1.4.2\_08 in your home directory. Remember the path of this directory as you will need this path later when configuring JWS.  
**\$ ./j2re-1\_4\_2\_08-solaris-sparc.sh**
- 13 Follow the instructions in JRE software to install JRE 1.4.2\_08.
- 14 In your j2re1.4.2\_08 subdirectory there is a zip file called javaws-1\_2\_0\_02-solaris-sparc-i.zip. Copy this zip file to your home directory.
- 15 Install JWS by unzipping the zip file and executing install.sh.  
**\$ unzip ./javaws-1\_4\_2\_08-solaris-sparc-i.zip**  
**\$ ./install.sh**
- 16 Accept the license agreement and enter the path to JRE from step [12](#).
- 17 Follow the remaining online directions.
- 18 The Sun Solaris client is now setup to launch MG9KEM SN09U client applications.
- 19 Remove JWS cache by performing procedure [Accessing JWS application on a Sun workstation on page 1102](#).
- 20 Exit the browser and launch the browser again for settings to take effect.
- 21 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Removing an MG 9000 Manager JWS application from cache

### *At the MG 9000 Manager client PC*

- 1 Access the Java Web Start Application Manager by selecting Start->Programs->Java Web Start. The Java Web Start Application Manager appears.
- 2 Select View->Downloaded Applications from the menu bar.
- 3 Select an MG 9000 Manager JWS application to be deleted.
- 4 Select Application->Remove Application from the menu bar.
- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Uninstalling the Java client

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

| If uninstalling Java client from a | Do                     |
|------------------------------------|------------------------|
| Windows PC                         | step <a href="#">2</a> |
| Sun workstation                    | step <a href="#">3</a> |

- 2 To uninstall the Java 2 Runtime environment or Java 2 SDK from a Windows PC, use the Microsoft Windows Add/Remove Programs utility accessed from the Control Panel by selecting Start->Settings->Control Panel->Add/Remove Programs. Select the version to be removed and follow the prompts.  
Go to step [4](#).
- 3 To uninstall 1.4.x installation of Java 2 SDK, from a web browser access <http://java.sun.com/j2se/1.4.2/install-solaris.html> and refer to the instructions for uninstalling any 1.4.x installation of Java 2 SDK.
- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

The following procedure is provided as an optional method for accessing a JWS application on a Sun workstation.

### **Accessing JWS application on a Sun workstation**

#### ***At the client workstation***

- 1** Change directory to where the Java Web Start application is installed and enter the following command  

```
> cd <path/javaws>
```
- 2** To launch the Java WebStart application manager, type  

```
> javaws &
```
- 3** Select View->Downloaded Applications from the menu bar.
- 4** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Completing the MG 9000 Manager upgrade

---

Perform the next required upgrade according to the order listed in the table [Component Upgrade Order on page 6](#). The required upgrade is the next component in the list according to your network configuration.

## Preparing MG 9000 Manager software delivered through ESD for an upgrade

---

### Purpose of this procedure

These procedures describe how to prepare MG 9000 Manager software delivered through Electronic Software Delivery (ESD) for an upgrade of the MG 9000 Manager.

### When to use this procedure

Use this procedure after you perform the procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

### Prerequisites

Your operating company must have an ESD agreement with Nortel Networks. When the agreement was established, the operating company furnished Nortel Networks with the location of an electronic drop box and a user name and password pair for delivering software loads. When Nortel Networks delivers a software load to the drop box, an electronic mail notification is sent to the e-mail address specified by the telephone operating company when the ESD agreement was established.

### Action

#### Preparing MG 9000 Manager software delivered through ESD for an upgrade

##### *At the MG 9000 Manager server (if on a cluster, use the inactive unit)*

- 1 Make sure you are logged in as root. If necessary, perform the following steps.
  - a Change to the root user by typing  

```
$ su -
```

and pressing the Enter key.
  - b When prompted, enter the root password.
- 2 Copy the MG 9000 software packages to a permanent location.
  - a List the contents of the tmpmnt directory by typing  

```
ls -l /tmpmnt
```

- b Copy the packages in tmpmnt directory to a permanent location by typing

```
cp /tmpmnt/*.PKG /opt/nortel/
```
- 3 Verify the package files are on directory /opt/nortel by typing
  - a Change to the /opt/nortel directory by typing

```
cd /opt/nortel
```
  - b List the contents of all files with .PKG suffix by typing

```
ls -l *.PKG
```
- 4 Unmount the MG 9000 Manager ISO image by performing the following
  - a Enter the command line interface by typing

```
cli
```
  - b Enter the number next to the Other menu option.
  - c Enter the number next to the Un-mount a Generic Iso Image from the SSPFS Unit menu option.
  - d To exit each menu level, type

```
x
```
  - e Verify the MG 9000 Manager packages no longer exist in the tmpmnt directory by changing to the /tmpmnt directory and listing the contents

```
cd /tmpmnt
ls -l
```

The system responds with the following

```
total 0
```
  - f Login to the active server, if in a cluster configuration.  
Change to the directory where the ISO file is stored by typing

```
cd <iso_filename_directory>
```

where

```
iso_filename_directory
```

is the directory with the iso image file, for example,  
`/data/esd_iso`
  - g List the contents of the directory containing files with a .iso extension by typing

```
ls -l *.iso
```

**h** Remove the EM ISO file by typing

```
rm mg9kem_9_<version_number>.iso
```

**Example**

```
rm mg9kem_9_1_151.iso
```

- 5** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



Copyright © 2006, Nortel Networks

Nortel Networks Confidential

## Session Server-Lines upgrade

### **ATTENTION**

Due to the complexity of the upgrade for the MCS 5200, Border Control Point 7100/7200, and Session Server-Lines product, Nortel requires that all customers contact their Nortel Customer Service representative to engage the appropriate Nortel Software Delivery team to perform this upgrade.

There will be no service charges incurred for this activity.







## Session Server Trunks upgrade

The Session Server is a call media and signaling interoperability component deployed as two redundant hardware units housed in the SAM-F frame only and used in PT-IP solutions. The primary application introduced on the Session Server platform is the SIP Gateway application which facilitates interoperability between the CS 2000 network and 3rd party SIP-based Call Servers and Media Application Servers.

### **ATTENTION**

The Session Server Trunks does not have a new software load for SN09U, therefore no upgrade is required.

### **What's new in Session Server Trunks Upgrades in (I)SN09U**

#### **Feature changes**

Added procedures for acquiring and applying Session Server Manager patches.

Added procedure for enabling and disabling autopatching on the Session Server Trunks.

## Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U
- SN09U to SN09U

## Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

**Time to complete an upgrade**

The following table lists the tasks to upgrade Session Server Trunks software and the estimated time to complete each task.

**Table 1 Estimated time to complete a software upgrade**

| Task                         | Application                                                                                                                                                                                     | Time       |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| Preparing for the upgrade    | Making any necessary backups<br>Transferring the ISO file to the Session Server                                                                                                                 | 30 minutes |
| Upgrading the software       | Upgrading the platform software (NCGL) and rebooting.<br>Running the upgrade scripts so the SIP Gateway application software will upgrade and reboot.<br>Total time to upgrade all applications | 2 hours    |
| Completing the upgrade       | Synching with mate (occurs during the upgrade)                                                                                                                                                  | 30 minutes |
| Total estimated upgrade time |                                                                                                                                                                                                 | 3 hours    |
| Performing a rollback        |                                                                                                                                                                                                 | 2 hours    |

**Service impacts**

The upgrade of Session Server Trunks software does not impact service.

**Additional information**

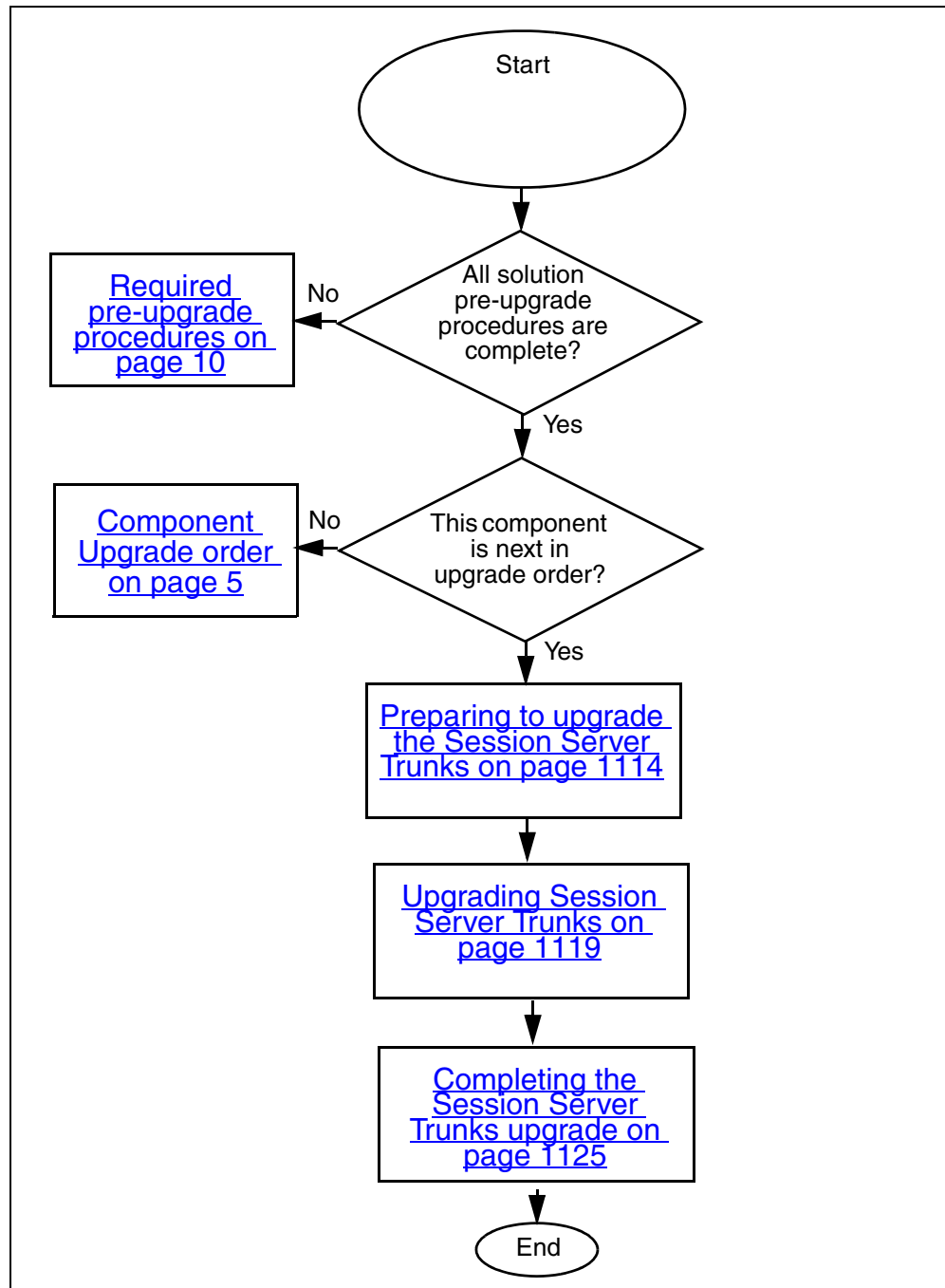
The following additional information applies to the upgrade of Session Server Trunks software:

- Patches can only be applied using the CLI (command line interface).
- Seamless upgrades involving Non-PacketCable compliant TLS certificates to PacketCable compliant TLS certificates are not supported.
- Performing a full rollback is an out-of-service activity. All call processing and billing information generation is terminated for part of the rollback activity.

In the event you need or want to downgrade the Session Server Trunks, refer to [Performing a rollback of Session Server Trunks software on page 2444](#).

**Session Server Trunks upgrade tasks**

This taskflow shows you the sequence of tasks you perform to upgrade this component.

**Session Server Trunks upgrade tasks**

---

## Preparing to upgrade the Session Server Trunks

---

The procedure in this section provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

Perform the previous required upgrade according to the order listed in the table [Component Upgrade Order on page 6](#). The required upgrade is the previous component in the list according to your network configuration.

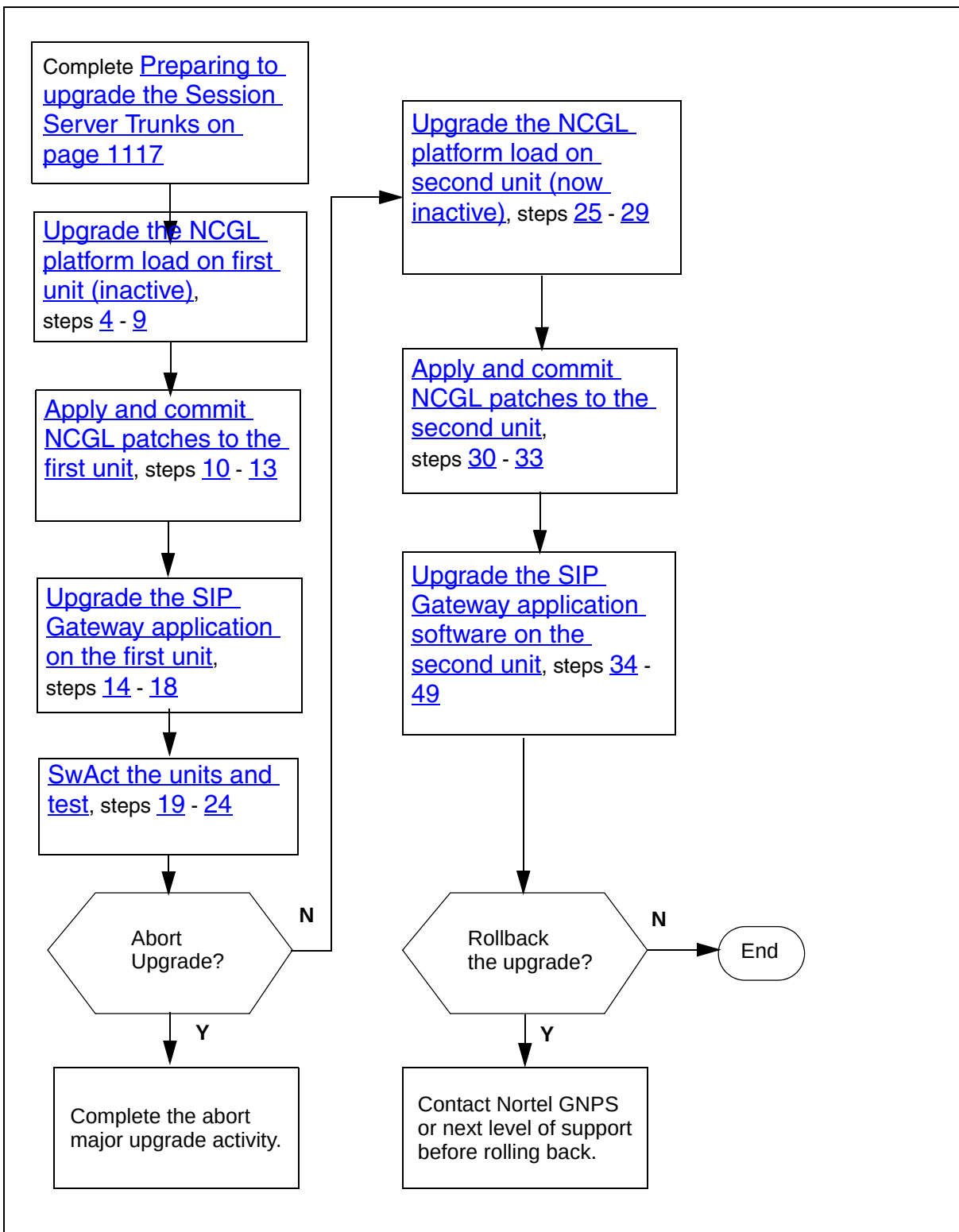
### Upgrade strategy

Software upgrade impacts both the NCGL platform software and the SIP Gateway application software.

- NCGL platform software release consists of CS 2000 NCGL Platform Manager software, NCGL software, and release notes. CS 2000 NCGL Platform Manager patches are delivered on a separate DVD-ROM, if available.
- SIP Gateway application software release consists of CS 2000 Session Server Manager software, and SIP Gateway application software. SIP Gateway application patches are delivered on separate DVD-ROM, if available.

Using both the CS 2000 NCGL Platform Manager and the NCGL command line interface (CLI), you can upgrade the NCGL platform software and the SIP Gateway application software.

Refer to the following activity diagram for a high-level view of the upgrade process for the Session Server - Trunks units.

**Session Server - Trunks upgrade overview**



## Software delivery methods

Software is delivered on a data CD/DVD disk or using Electronic Software Delivery (ESD). For ESD, a compressed ISO image is delivered to an electronic drop-box on the customer network from Nortel.

ESD delivery requires transferring the upgrade package to both Session Server - Trunks units and put in the `/opt/swd` directory using a secure file transfer program such as scp. After the upgrade of the NCGL platform, the bootload file is stored in the `/boot` directory.

To receive software using ESD, the operating company must have an ESD agreement with Nortel. When the agreement is established, the operating company furnishes Nortel with the location of an electronic dropbox, an e-mail address for notification and a username and password pair for delivering software loads. When Nortel delivers a software load to the dropbox, an electronic mail notification is sent to the e-mail address specified by the operating company.

## Software installation methods

You can upgrade the NCGL load from the local DVD-ROM drive, or from an ISO image located on a remote system, or copied to a local directory. The following upgrade protocols (methods) are selectable from the CS 2000 NCGL Platform Manager:

- Local CDROM - the local DVD-ROM drive (labeled in the software as the local CD-ROM).
- Local file - an iso image, or load.tgz file copied from the local DVD-ROM drive to the hard drive using the secure copy program, scp, to transfer the data.
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP service. If the workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in cleartext format across the network. This is not a recommended method.
- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service. This is not a recommended method.

You can upgrade the SIP Gateway application from the local DVD-ROM drive, or from an ISO image copied to a local directory. Most of the time the software load for the SIP Gateway application is on the

same CD/DVD disk or copied ISO image as the NCGL platform load; however, some customers receive a separate software load for the SIP Gateway application. Consult your release notes for details.

## Managing security certificates

### Upgrading from SN08

Upgrades from SN08 require no special consideration during the upgrade process, other than considering when the certificates expire. If the certificates are scheduled to expire within one month of completing the upgrade, use the cert\_mngt tool to renew the certificates. For more information, refer to

- [Back up security certificates on page 1126](#)
- [Import certificates and private key on page 1157](#)
- [Generate self-signed security certificates on page 1162](#)

## Action

Perform the following procedure to prepare the Session Server Trunks for upgrade.

### Preparing to upgrade the Session Server Trunks

- 1 Verify the component network order in which the Session Server - Trunks node will be upgraded for the end-to-end upgrade strategy.
- 2 Refer to section [Managing security certificates on page 1117](#) and determine the kind of certificates you currently have (customer self-signed or purchased from a certificate authority). You will need this information during the upgrade and after the upgrade is complete.
- 3 Back up the SIP Gateway application database on the active unit using procedure [Perform a backup on page 1128](#).
- 4 Acquire the appropriate major release software from Nortel either using ESD delivery to a customer dropbox/repository server or from a major release CD/DVD disk.
- 5 If you are performing a major release upgrade using an ISO image acquired using ESD, complete procedure [Extract an ISO image from an Electronic Software Delivery \(ESD\) on page 1134](#) to copy the ISO files to hard drive of each unit.
- 6 Use procedure [View release notes for a release on page 1132](#) to check release notes for upgrade issues.

- 7 Locate and have available the currently running release software CD/DVD disk along with a copy of the existing version of the SIP Gateway application installed on your system. The existing version can be from the last maintenance release image installed from a CD/DVD disk or an ESD downloaded image file.
- 8 Monitor logs and alarms. Clear all alarms and verify normal functioning of both units before continuing.
- 9 You have completed this high-level activity.

---

## Upgrading Session Server Trunks

---

The following procedure provides the high-level steps to upgrade the Session Server Trunks. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

Complete the following task

- [Preparing to upgrade the Session Server Trunks on page 1114](#)

### Action

Perform the following procedures to upgrade the component.

#### Upgrading the Session Server Trunks

- 1 Ensure that you have completed section [Preparing to upgrade the Session Server Trunks on page 1114](#) before continuing.
- 2 Enable pop up windows in the web browser. Several activities performed at the CS 2000 Session Server Manager require acknowledging prompts on pop-up dialog windows.

**Note:** If pop up windows are not enabled in the web browser, the Session Server Trunks upgrade will not function.

- 3 Ensure the console ports are accessible to support monitoring upgrade activities on the NCGL.

#### Upgrade the NCGL platform load on first unit (inactive)

- 4 Determine what version of the NCGL platform load is currently installed on your Session Server Trunks node by going to the System Information page of the CS 2000 NCGL Platform Manager and using procedure [Determine the currently running software load on page 1137](#).

If this is an MR upgrade, the NCGL platform software version probably has not changed. If it has not, skip the sections about upgrading the NCGL platform load.

Determine what version of the SIP Gateway application software (listed as Session Server load info) is currently installed on your Session Server Trunks node using procedure [Determine the currently running software load on page 1137](#).

- 5 If using a CD/DVD disk, insert the disk into the drive of the **inactive** unit.
- 6 At the **active** unit, use procedure [Inhibit a system SwAct \(Jam\) on page 1141](#) to jam the inactive unit.

- 7 At the CS 2000 NCGL Platform Manager for the physical unit which is **inactive**, upgrade the NCGL platform software using procedure [Upgrade NCGL platform software on page 1144](#). Ensure that you set the new NCGL load as the default boot load.  
  
For instance, if unit 0 is the active unit, log in to the CS 2000 NCGL Platform Manager for unit 1.
- 8 From the **active** unit, use procedure [Reboot a unit on page 1151](#) to perform a RebootMate of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.
- 9 Log in to the **inactive** unit CS 2000 NCGL Platform Manager and go to the System Information page. Use procedure [View the operational status of the NCGL platform on page 1172](#) for assistance with this task. If you can access the CS 2000 NCGL Platform Manager, then the security certificates are properly installed.

**Note:** If you cannot access the CS 2000 NCGL Platform Manager, then there is a problem with your security certificates. Contact your next level of support, Nortel GNPS or Nortel's emergency response team.

#### Apply and commit NCGL patches to the first unit

- 10 Use procedure [View release notes for a release on page 1132](#) to identify the required NCGL platform patches (if any) for the new release.
- 11 Log onto the **active** unit and use procedure [Inhibit a system SwAct \(Jam\) on page 1141](#) to verify that the units are jammed. If they are not, then jam the units.
- 12 Use procedure [Acquire patch files on page 1189](#) to copy all required patches from the CD/DVD disk or the ESD delivered ISO image file to the patching holding directory on the unit.
- 13 Use procedure [Apply and commit an NCGL patch on page 1191](#) to apply and commit NCGL patches to the inactive unit.

#### Upgrade the SIP Gateway application on the first unit

- 14 If the **inactive** unit is not jammed, jam it now as described in procedure [Inhibit a system SwAct \(Jam\) on page 1141](#).  
  
If necessary, use procedure [View web proxy settings in SPFS for Session Server - Trunks on page 1193](#) to determine the tag name you are using for this Session Server Trunks node.  
  
On the **inactive** unit, upgrade the SIP Gateway application software using procedure [Upgrade/rollback/reinstall a Session Server - Trunks application on page 1196](#).

- 15 After the **inactive** unit completes rebooting, log in to the inactive unit's CLI and verify that the current version of the SIP Gateway application matches the expected version by executing the following command:
- cat /opt/apps/webint/version\_info.txt**
- Refer to procedure [Determine the currently running software load on page 1137](#) for assistance with this task.
- 16 From the **active** unit, verify that the SIP Gateway application databases on both units have synchronized using procedure [Verify synchronization status on page 1215](#).
- 17 Use procedure [Enable a system SwAct \(Unjam\) on page 1217](#) to unjam the units.
- 18 As applicable to your site, check the new software on upgraded unit, still inactive.
- Monitor logs and alarms. Clear all alarms and verify normal functioning of both units before continuing.

#### SwAct the units and test

- 19 From the **active** unit, perform a SwAct using procedure [Invoke a maintenance SWACT of the Session Server Trunks platform on page 1219](#). All calls will continue to be processed on the (non-upgraded) active unit up to the time that the active IP address is switched to the inactive (upgraded) unit.
- 20 After the first unit is upgraded to NGSS\_09.1 and made **active**, use procedure [Acquiring Session Server Trunks patch files on page 1202](#) to identify and download Session Server Trunks patches.
- 21 Use procedure [Applying a Session Server Trunks patch to the active unit on page 1206](#) to apply emergency application patches to the **active** unit.
- 22 From the **active** unit, re-verify that the SIP Gateway application databases on both units have synchronized using procedure [Verify synchronization status on page 1215](#).
- 23 As applicable to your site, test new software on upgraded unit, now active. Testing includes:
- placing test calls according to your site upgrade guidelines
  - applying a minimum live traffic soak time for the unit according to your site upgrade guidelines
  - Refer to the *Session Server Trunks Fault Management*, NN10332-911, and use procedures "View Session Server -

Trunks alarms” and “View Session Server - Trunks logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.

- 24 If all software tests are successful, continue with the next step in this procedure to upgrade the second (mate) unit (now inactive).

Otherwise, if the active unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure and complete [Abort an upgrade on page 2449](#) and contact your next level of support or Nortel GNPS.

### Upgrade the NCGL platform load on second unit (now inactive)

- 25 Verify that all applicable activities in Section [Preparing to upgrade the Session Server Trunks on page 1114](#) have been completed for the second unit.
- 26 If applying a major upgrade using a CD/DVD disk, insert the disk into the disk drive of the **inactive** unit.
- 27 At the **active** unit use procedure [Inhibit a system SwAct \(Jam\) on page 1141](#) to jam the units.
- 28 On the NCGL Platform Manager for the physical unit that is **inactive**, upgrade the NCGL platform software using procedure [Upgrade NCGL platform software on page 1144](#). Ensure that you set the new NCGL load to be the default boot load.
- For instance, if unit 0 is the active unit, log in to the CS 2000 NCGL Platform Manager for unit 1.
- 29 From the **active** unit, use procedure [Reboot a unit on page 1151](#) to perform a RebootMate of the inactive unit. Monitor the reboot progress from **active** unit CS 2000 NCGL Platform Manager.

When the inactive unit boots, the SIP Gateway application can be in an Unlocked/Disabled state. If this occurs, a SIPM301 SIP Gateway Application System Busy alarm will be raised, as well as a SIPM301 SIP Gateway Application Mtc Out Of Sync alarm. This does not affect service on the active unit and the alarms will probably clear after the SIP Gateway application on the inactive unit is upgraded in step [34](#).

### Apply and commit NCGL patches to the second unit

- 30 Use procedure [View release notes for a release on page 1132](#) to identify the required NCGL platform patches for the new release.



- 31 Log on to the **active** unit and use procedure [Inhibit a system SwAct \(Jam\) on page 1141](#) to verify that the units are jammed. If they are not, then jam the units.
- 32 Use procedure [Acquire patch files on page 1189](#) to copy all required patches from the CD/DVD disk or the ESD delivered ISO image file to the patching holding directory on the unit.
- 33 Use procedure [Apply and commit an NCGL patch on page 1191](#) to apply and commit NCGL patches to the inactive unit.

#### **Upgrade the SIP Gateway application software on the second unit**

- 34 If the **inactive** unit is not jammed, jam it now.  
At the **inactive** unit, upgrade the SIP Gateway application software using procedure [Upgrade/rollback/reinstall a Session Server - Trunks application on page 1196](#).
- 35 After the **inactive** unit completes rebooting, log in to the inactive unit's CLI and verify that the current version of the SIP Gateway application matches the expected new version by executing the following command:  
**cat /opt/apps/webint/version\_info.txt**
- 36 Use procedure [Applying a Session Server Trunks patch to the inactive unit on page 1209](#) to apply all application patches using the ALL option to the **inactive** unit.
- 37 Use procedure [Applying a Session Server Trunks patch to the active unit on page 1206](#) to apply all remaining patches using the ALL option to the **active** unit.
- 38 From the **active** unit, verify that the SIP Gateway application databases on both units have synchronized using procedure [Verify synchronization status on page 1215](#).
- 39 Use procedure [Enable a system SwAct \(Unjam\) on page 1217](#) to unjam the units.
- 40 As applicable to your site, check the new software on the upgraded unit, still inactive.  
Monitor logs and alarms. Clear all alarms and verify normal functioning of both units before continuing.
- 41 From the **active** unit perform a SwAct of the units using procedure [Invoke a maintenance SWACT of the Session Server Trunks platform on page 1219](#).



- 42 As applicable to your site, test new software on the upgraded unit, now active. Testing includes:
  - placing test calls according to your site upgrade guidelines
  - applying a minimum live traffic soak time for the unit according to your site upgrade guidelines
  - Monitor logs and alarms. Clear all alarms and verify normal functioning of both units before continuing.
- 43 If all software tests are successful, continue with the next step in this activity to upgrade.

Otherwise, if the active unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure. Go to and complete procedure [Performing a rollback of Session Server Trunks software on page 2444](#), and contact your next level of support, Nortel GNPS or Nortel's emergency response team.
- 44 From the **active** unit, verify that the SIP Gateway application databases on both units have synchronized using procedure [Verify synchronization status on page 1215](#).
- 45 Monitor the system for an appropriate period according to your site guidelines before declaring this major upgrade complete.
- 46 Edit the object properties in the IEMS for the Session Server Trunks network elements you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the Device Version field.
  - [Editing and viewing object properties using Java Web Start Client on page 2255](#)
  - [Editing and viewing object properties using Web Client on page 2261](#)
- 47 Back up the SIP Gateway application database on the **active** unit using procedure [Perform a backup on page 1128](#).
- 48 If autopatching is to be enabled, perform procedure [Enabling/disabling autopatching on Session Server - Trunks application on page 1211](#).
- 49 You have completed the upgrade activity. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Completing the Session Server Trunks upgrade

---

Perform the next required upgrade according to the order listed in the table [Component Upgrade Order on page 6](#). The required upgrade is the next component in the list according to your network configuration.

---

## Back up security certificates

---

### Purpose of this procedure

Use the following procedure to create backup copies of security certificates to a folder on the unit and make copies to a remote server location, chosen by the customer.

Use this procedure anytime new security certificates are created or when the system is changed from using self-signed certificates to CA-signed certificates. This procedure is also used as part of a major release upgrade activity.

### Limitations and Restrictions

There are no limitations on performing this procedure.

### Prerequisites

There are no prerequisites for this procedure.

### Action

Perform the following steps to complete this procedure.

#### ***At the NCGL CLI or IEMS client***

- 1 Log on to the Session Server unit that has the security certificates you need to back up, and change to the root user.  
  
If you are performing this procedure outside of a high-level task, back up the security certificates on both units. Otherwise, back up the security certificates on the unit indicated in the high-level task that directed you to this procedure.

- 2 Change directories to the /opt/base/share/ssl directory:

```
cd /opt/base/share/ssl
```

- 3 Create a new directory to store backup copies of the certificate files:

```
mkdir <SNxx_ddmmyyyy>
```

where

**SNxx\_ddmmyyyy**

is the name of the new directory based on the currently installed release of the system software (for example SN08) and the current date in the format ddmmyyyy

- 4 Copy the certificates to the newly created backup directory:

```
cp * <SNxx_ddmmyyyy>
```

#### ATTENTION

Completing this step ensures that you have valid backup copies of the security certificates for restoring in case of an upgrade abort or rollback or for disaster recovery purposes.

- 5 Use the following table to determine your next step:

| If                                                                                    | Do                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you want to make backup copies of the security certificates to a remote server        | Ensure that the remote host that will store the security related files is secure, that the host is unavailable to general users, and offers restricted access to personnel with security related responsibilities. Proceed to <a href="#">step 6</a> |
| you do not want to make backup copies of the security certificates to a remote server | This procedure is complete.                                                                                                                                                                                                                          |

- 6 Secure copy the files to the remote server:

```
cd <SNxx_ddmmyyyy>
scp * <user>@<remote_server>:</path>
```

where

**user**

is a valid user ID on the remote server

**remote\_server**

is the IP address of the remote server

**/path**

is where the file will be located on the remote server

*The files are copied to the remote server.*

- 7 You have completed this procedure.

## Perform a backup

### Purpose of this procedure

Use this procedure to perform a backup before beginning an upgrade.

### Limitations and Restrictions

#### ATTENTION

SIP Gateway application provisioning activities must be suspended during the time of the database backup in order to ensure that an accurate and complete copy of the active unit database is created. However, call processing is not affected.

### Prerequisites

#### ATTENTION

The SIP Gateway application database must be in sync with the CS 2000 to ensure an accurate copy of the active unit database is created. Verify this condition using procedure [Verify synchronization status on page 1215](#).

### Action

#### *At the NCGL CLI or IEMS client*

- 1 Log in to the active unit and change to the root user.
- 2 The next action depends on the currently running software load:

| If the running software load is | Do                     |
|---------------------------------|------------------------|
| SN09, SN09U                     | <a href="#">step 3</a> |
| SN08                            | <a href="#">step 5</a> |

- 3 Use this step only when backing up a unit that is running SN09 or SN09U software.

Run the bkup\_ngss.sh command:

```
/opt/apps/db_install/sd/bkup_ngss.sh
```

*A backup is created in /data/bkresmgr/backup and ends in a .tgz suffix.*

- 4 Copy the database file to a remote device such as CBM/SDM or CMT to support the ability to restore the system at a later time

**Note:** This copy action overwrites any file with the same name in that location. If any files must be kept, consider making a copy and saving it to another location.

Secure copy the files to the remote server:

```
cd /data/bkresmgr/backup
scp * <user>@<remote_server>:</path>
```

where

**user**

is a valid user ID on the remote server

**remote\_server**

is the IP address of the remote server

**/path**

is where the file will be located on the remote server

The files are copied to the remote server.

Go to step [7](#).

- 5 This step applies when upgrading from SN08.

Copy the database file to a remote device such as CBM/SDM or CMT to support the ability to restore the system at a later time.

**Note:** This copy action overwrites any file with the same name in that location. If any files must be kept, consider making a copy and saving it to another location.

Secure copy the files to the remote server:

```
cd /opt/apps/database/solid/dbfiles
scp * <user>@<remote_server>:</path>
```

where

**user**

is a valid user ID on the remote server

**remote\_server**

is the IP address of the remote server

**/path**

is where the file will be located on the remote server

**Note:** Confirm the overwrite if a backup file already exists.

The files are copied to the remote server.

- 6 Copy the database file to a backup directory:  
**`cp solid.db /opt/apps/database/solid/backup`**  
and press the Enter key.  
**Note:** This may overwrite previous backups.  
The database file is copied.
- 7 This procedure is complete.

## Backup security related files

### At the NCGL CLI or IEMS client

- 1 Log in to the active unit and change to the root user by typing  
**`$ su -`**  
and pressing the Enter key.
- 2 Enter the root password when prompted.
- 3 Change directory to the /opt/base/share/ssl directory:  
**`cd /opt/base/share/ssl`**
- 4 Create a new directory to store backup copies of the certificate files:  
**`mkdir <SNxx_ddmmyyyy>`**  
where  
**SNxx\_ddmmyyyy**  
is the name of the new directory based on the currently installed release of the system software (for example SN09) and the current date in the format ddmmyyyy
- 5 Copy the certificates to the newly created backup directory:  
**`cp * <SNxx_ddmmyyyy>`**

#### ATTENTION

Completing this step ensures that you have valid backup copies of the security certificates for restoring in case of an upgrade abort or rollback or for disaster recovery purposes.

**6** Use the following table to determine your next step:

| If                                                                                    | Do                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you want to make backup copies of the security certificates to a remote server        | Ensure that the remote host that will store the security related files is secure, that the host is unavailable to general users, and offers restricted access to personnel with security related responsibilities. Proceed to <a href="#">step 7</a> |
| you do not want to make backup copies of the security certificates to a remote server | <a href="#">step 8</a>                                                                                                                                                                                                                               |

**7** Secure copy the files to the remote server:

```
cd <SNxx_ddmmyyyy>
scp * <user>@<remote_server>:</path>
```

where

**user**

is a valid user ID on the remote server

**remote\_server**

is the IP address of the remote server

**/path**

is where the file will be located on the remote server

*The files are copied to the remote server.*

**8** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



---

## View release notes for a release

---

### Purpose of this procedure

Use this procedure to view the release notes.

### Limitations and Restrictions

Release notes are not included for all software releases and may only be available for maintenance release software versions.

### Prerequisites

If reading release notes from a CD/DVD disk, ensure that the maintenance release or major release CD/DVD-ROM disk is inserted into the inactive unit DVD-ROM drive.

### Action

#### *At the NCGL CLI or IEMS client*

- 1 Log on to the inactive Session Server unit and change to root user.
- 2 Use the following table to determine your first step.

| If media is delivered by | Do                      |
|--------------------------|-------------------------|
| ESD                      | <a href="#">step 3.</a> |
| CD/DVD disk              | <a href="#">step 4.</a> |

- 3 Ensure the software archive file, which includes the release notes, has been extracted and put in the /opt/swd directory on the inactive unit, and that the image file has been mounted to mount point /cdrom. If required, refer to procedure [Extract an ISO image from an Electronic Software Delivery \(ESD\) on page 1134.](#)  
When complete, return to this procedure, and proceed to [step 7.](#)
- 4 Insert the CD/DVD-ROM disk into the DVD-ROM disk drive of the inactive unit.
- 5 At the prompt, type  
**cd /**
- 6 Mount the DVD-ROM drive by typing  
**mount /cdrom**
- 7 Change directories to the mounted filesystem by typing  
**cd /cdrom**

- 8 Locate the release notes file by typing  
**ls**  
*If release notes are available, they are listed as a .pdf file with the rest of the files.*
- 9 Transfer the release notes file from the unit and then open the file with a viewer that reads .pdf format files.  
**Note:** It may be necessary to ftp the release notes .pdf file (/cdrom/pdf) to an OAMP node and then transfer the pdf to a PC with Adobe Acrobat Reader.
- 10 When you have finished reviewing the release notes file, change directories out of the mounted DVD-ROM filesystem by typing  
**cd /**
- 11 Unmount the DVD-ROM drive by typing  
**umount /cdrom**
- 12 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Extract an ISO image from an Electronic Software Delivery (ESD)

---

### Purpose of this procedure

Use this procedure to extract an ISO image, patch files and release notes for a major upgrade or maintenance release archive file retrieved from an electronic software delivery dropbox.

### Prerequisites

Ensure that the ESD software archive file has been transferred from the dropbox on the repository server. The repository server is the machine owned by the operating company that was selected to be the destination for the ESD software files.

To secure copy the ISO image from the dropbox into the target directory type

```
scp <ISO_filename> mtc@<Session_Server_IP>:/opt/swd
```

This command assumes the customer has logged onto the dropbox and is in the target directory that contains the ISO file before the command is executed. The system prompts for a password before the file transfer can commence. If the transfer fails, delete any older ISO files in the /opt/swd directory to ensure enough space exists for the new ISO file.

Your existing Regional Customer Service Team has knowledge of your ESD implementation methodology. You can also contact the technical assistance support (TAS) hotline after hours for any urgent issues related to ESD.

For more information about how your site's ESD is implemented, contact your site network administrator.

### Restrictions and Limitations

This procedure must be completed on both the active and inactive units.

### Action

#### *At the Session Server CLI or IEMS client*

- 1 Log on to either unit and change to the root user.
- 2 Change directory to the location of the ESD software archive file by typing

```
cd /opt/swd
```

- 3 Ensure that enough disk space is available for the extracted ISO image by typing

**df -k /opt/swd**

*Ensure that the value in field Avail is at least 350. This ensures that at least 350 Megabytes are available. In the example that follows, 1013 Megabytes are available.*

```
[root@hostname swd]# df -k /opt/swd
Filesystem Size Used Avail Use% Mounted on
/dev/ntvg/_opt_sw 1014M 364k 1013M 1% /opt/swd
[root@hostname swd]#
```

- 4 Uncompress the ESD software load from the ESD archive file by typing

**tar xvzf <ESD\_ISOfilename>.tar.gz**

**Example**

tar xvzf NGSS0090.90.P.NCL.NAP.VAULT.6.D.tar.gz

*The ESD software load is unarchived, and a new directory named after the ESD software filename is created. The directory name is the name of the ESD filename without the .tar.gz suffix. The contents of the ESD software load are placed in this new directory.*

- 5 Change directory to the newly created directory by typing

**cd <ESD\_ISO\_directory>**

**Example**

cd NGSS0090.90.P.NCL.NAP.VAULT.6.D

- 6 Verify that the image file exists in the directory by typing

**ls -l**

*The system responds by listing the ISO image in the directory.*

```
[root@hostname NGSS090.90.P.NCL.NAP.VAULT.6.D]# ls -l
total 282272
```

*The command prompt returns upon success and the contents of the image are available from the /cdrom mount point.*

- 7 Mount the image file to mount point `/cdrom` by typing

```
mount -o loop <iso image> /cdrom
```

**Example**

```
mount -o loop NGSS09.x_NCL.iso /cdrom
```

*The command prompt returns upon success and the contents of the image are available from the `/cdrom` mount point.*

- 8 List the contents of the ISO by typing

```
cd /cdrom
```

```
ls -l
```

*The system responds with a list of files in the ISO image including any applicable patch files and the release notes file.*

```
[root@hostname cdrom]# ls -l
total 19361
-r-xr-xr-x 1 208126 4848 5005 Mar 22 17:36 InstallApps
drwxrwxrwx 2 208126 4848 6144 Mar 22 17:36 Tools
-r-xr-xr-x 1 208126 4848 33 Feb 23 18:09 buildversion
drwxrwxrwx 2 208126 4848 2048 Feb 23 18:09 isolinux
-r-xr-xr-x 1 208126 4848 19810925 Feb 23 18:09 load.tgz
```

- 9 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

The NCGL software is available for install by selecting Local File from the Software Upgrade area of the Services web page.

The SIP Gateway application software is available for install by logging in to the unit and running the InstallApps script from the `/cdrom` directory.

**Note:** Repeat this procedure on the second unit before beginning the software upgrade.

---

## Determine the currently running software load

---

### Purpose of this procedure

Use this procedure to determine the version of the currently running software load on the active unit.

### Limitations and Restrictions

This procedure has no limitations or restrictions.

### Prerequisites

This procedure has no prerequisites.

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

- 1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 At the Session Server folder, click Version Info.



*The version information page opens in the right side frame.*

## Version Information

```
=====
Session Server Load Info
=====
Release = NGSS_09_Bld_int
Version = NGSS_09_Bld_20_b
Build Date = Wed May 28 22:44:28 EST 2005
=====

=====
NCGL Platform Load Info
=====
BUILDVERSION=8.20.1.0.0506281015
=====
```

This value is not accurate if a maintenance release has been applied.

- 3 Review and record the software load version information for the SIP Gateway application (top).

**Note:** The version information for the NCGL platform load is only accurate if a maintenance release has not been applied to the load.

***At the CS 2000 Session Server Manager or IEMS client***

- 4 Select Succession Communication Server 2000 NCGL Platform Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 5 Review the Platform Information table for the running NCGL software version:

| Platform Information    |                                               |
|-------------------------|-----------------------------------------------|
| Date:                   | Tuesday April 05th 2005 08:43:51 AM EDT       |
| Time since last reboot: | 11 days, 20 hours, 12 minutes, 31 seconds     |
| System Power-On Time:   | 1 years 28 days 6 hours                       |
| System booted from:     | Hard disk drive                               |
| Last restart cause:     | Last restart due to soft reset                |
| Last power event cause: | Last power down caused by loss of power feed. |
| Current version:        | 8.20.1.0.0506281015                           |

- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Alternate command line interface method

### At the NCGL CLI

- 1 Log in to the unit using a secure shell (ssh).
- 2 Verify the installed software versions for this unit by typing  
**cat /opt/apps/webint/version\_info.txt**  
*The system responds:*

```
=====
Session Server Load Info
=====
Release = NGSS_09_Bld_int
Version = NGSS_09_Bld_20_b
Build Date = Sat May 28 14:47:17 EST 2005
=====
=====
NCGL Platform Load Info
=====
BUILDVERSION=8.20.1.0.0506281015
=====
```
- 3 Verify the NCGL platform software versions for this unit by typing  
**ncglversion**  
*The system responds:*

```
ncgl_samxts_8.20.1.0_0506281015
```



- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Inhibit a system SwAct (Jam)

---

### Purpose of this procedure

The jam command is used to manually prevent a SwAct (switch of activity) of the active and stand-by units by inhibiting the toggling of operational states of both units, thereby preventing the stand-by unit from going active.

### Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as in cases of a replacing a faulty standby unit or upgrading the software for a standby unit.

#### ATTENTION

This procedure can be performed only from the active unit. You cannot Jam the active unit if the inactive unit is out of service.



#### CAUTION

##### Loss of redundancy

This procedure prevents the node from operating in a duplex, fault-tolerant mode and prevents the SIP Gateway application from being able to SwAct as needed. Keep a jam in effect only as long as is necessary.

### Prerequisites

There are no prerequisites for performing this procedure.

## Action

### ***At the CS 2000 Session Server Manager or IEMS workstation***

- 1 Select Succession Communication Server NCGL Platform Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Click the Node Maintenance link.  
*The Node Maintenance page opens in the right side frame.*
- 3 Determine if the Jam State of the standby unit is Yes or No. If it is Yes, then the unit is already jammed and you are done with this procedure. If it is No, then continue with the next step.

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | no        |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Jam"/> <input type="checkbox"/> Force |

- 4 Click the Jam button. If the button is disabled, then this is the inactive unit; reconnect to the active unit.  
*A confirmation dialog window opens.*

- 5 Click OK to proceed with the jam activity.
- 6 If the system responds with a message box click OK to close the dialog box.  
*A dialog window indicates that the Jam passed. The Node Maintenance window refreshes and the Jam State for the inactive unit becomes yes.*
- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Force Jam information

The Jam action does not work if critical faults exist on the active unit. Using the Jam command with the Force option overrides any pre-checks. A Forced Jam forces a Jam of the inactive unit even if critical faults exist on the active unit, in which case, a full service outage on the Session Server - Trunks node could occur if the active unit fails.

---

## Upgrade NCGL platform software

---

### Purpose of this procedure

This procedure describes how to use the CS 2000 NCGL Platform Manager to apply an upgrade to an NCGL platform load.

### Limitations and Restrictions

You can upgrade the NCGL platform load from the local DVD-ROM drive or from an ISO image located on the system disk drive. The following upgrade protocols (methods) are selectable from the CS 2000 NCGL Platform Manager:

- Local CDROM - the local DVD-ROM drive (labeled in the software as the local CD-ROM)
- Local file - an iso image, or load.tgz file copied from the local CD/DVD disk to the hard drive using the secure copy program, scp, to transfer the data
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the FTP service. If the workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in cleartext format across the network.
- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service.

### Prerequisites

For the prerequisites of performing any upgrade, refer to [Preparing to upgrade the Session Server Trunks on page 1114](#).

## Action

### ***At the CS 2000 NCGL Platform Manager or IEMS client***

- 1 If software is delivered in CD/DVD, then insert the disk in the drive of the inactive unit now.

If software is delivered by ESD, ensure the image is mounted. Refer to [Extract an ISO image from an Electronic Software Delivery \(ESD\) on page 1134](#) for assistance.

**Note:** If one unit has been upgraded and this procedure is being performed on the second unit, the ISO image does not need to be untarred. Perform only step 7 of [Extract an ISO image from an Electronic Software Delivery \(ESD\) on page 1134](#) and return to this step.

- 2 Select Succession Communication Server 2000 NCGL Platform Manager from the launch point menu.

**Note:** Access the **inactive** NCGL Platform Manager GUI using the IP address of the **inactive** NGSS unit.

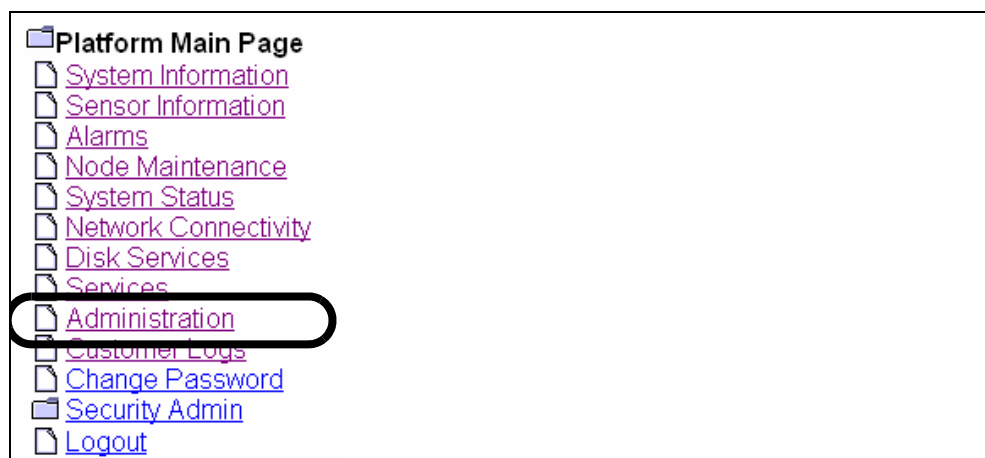
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

*The Platform Main Page menu is displayed.*

- 3 Click the Administration link.



*The Administration page opens in the right side frame.*

- 4 Click the Protocol drop down menu and select an upgrade protocol. Refer to the following table to help you determine the appropriate protocol:

The screenshot shows the 'Software Upgrade' section of the Nortel NMS. A dropdown menu for 'Protocol' is open, showing the following options: Anonymous FTP, FTP, HTTP, HTTPS, Local File, and Local CDRom. The 'Protocol' dropdown is highlighted with a black border. The background interface includes sections for 'Bootload Management', 'Software Upgrade', and 'Server Maintenance'. Under 'Server Maintenance', 'Unit 0 - Active' is highlighted in green, and 'Unit 1 - Inactive' is shown below it. Buttons for 'Reboot', 'Halt', and 'Force' are visible for each unit.

**If the Protocol selection is**

**Do**

Anonymous FTP

Enter the IP address of the remote server which has the bootload image in the IP address text box.

Enter the location (as a relative path on the remote server) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`.

then continue with [step 5](#)

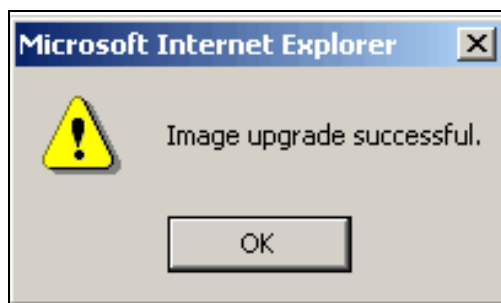
| If the Protocol selection is | Do                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FTP                          | <p>Enter your username in the Login ID text box.</p> <p>Enter your password in the Password text box.</p> <p>Enter the IP address of the remote server which has the bootload image in the IP address text box.</p> <p>Enter the location (as a relative path) of the bootload image file <code>load.tgz</code> in the File text box. For example, <code>/opt/swd/load.tgz</code>.</p> <p>then continue with <a href="#">step 5</a></p> |
| HTTP or HTTPS                | <p>Enter the IP address of the remote server which has the bootload image in the IP address text box.</p> <p>Enter the location (as a relative path on the remote server) of the bootload image file <code>load.tgz</code> in the File text box. For example, <code>/opt/swd/load.tgz</code>.</p> <p>then continue with <a href="#">step 5</a></p>                                                                                      |
| Local File                   | <p>If the ISO file is mounted, put in the local file and path as <code>/cdrom/load.tgz</code> instead of using <code>/opt/swd/&lt;load.iso&gt;</code> where the actual load name must be known.</p> <p>then continue with <a href="#">step 5</a></p>                                                                                                                                                                                    |
| Local CDROM                  | <p>Ensure that the CD/DVD disk is inserted into the drive or that an image is mounted on <code>/cdrom</code>.</p> <p>then continue with <a href="#">step 5</a></p>                                                                                                                                                                                                                                                                      |



- 5 Click the Upgrade button.

| Password             | IP address           | File                 | Action                                 |
|----------------------|----------------------|----------------------|----------------------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="button" value="Upgrade"/> |

- 6 Verify that the load files were successfully copied by clicking OK on the pop-up window.



**ATTENTION**

Refer to the [Troubleshooting Upgrades on page 1149](#) section if the popup window does not indicate a successful image upgrade.

- 7 Click the Set Default button to the right of the new (upgraded) bootloader.

| Bootload Management |                                                                                  |
|---------------------|----------------------------------------------------------------------------------|
| Bootload            | Maintenance                                                                      |
| 8.08.1.0.0502231439 | <input type="button" value="Set default"/> <input type="button" value="Delete"/> |
| 7.09.1.0.0502281015 | Default Bootload                                                                 |
| 5.36.2.1.0411021023 | <input type="button" value="Set default"/> <input type="button" value="Delete"/> |

*The system responds by setting the newly installed load as the default load, as shown in the following figure.*

| Bootload Management |                  |        |
|---------------------|------------------|--------|
| Bootload            | Maintenance      |        |
| 8.08.1.0.0502231439 | Default Bootload |        |
| 7.09.1.0.0502281015 | Set default      | Delete |
| 5.36.2.1.0411021023 | Set default      | Delete |

- 8 Verify that you have set the correct bootload to be the default.
- 9 If you upgraded using the Local CD-ROM protocol, remove the CD/DVD disk from the drive. If you are going to upgrade the SIP Gateway application from the same CD/DVD, leave it in the drive until the SIP Gateway application has been upgraded.
- 10 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

**Note:** The unit is not yet running the upgrade software. The unit must be rebooted so that it can boot the upgrade software that has just been set as the Default Bootload.

## Troubleshooting Upgrades

For [step 6](#) of this procedure, review the message in the pop-up window. The following possible error messages and their meaning are described:

- Error: Failed to update image /usr/bin/copy\_boot\_image -f /opt/swd/load.tgz Invalid load file content. Exiting  
Indication: If the bootload file is corrupt, the system software indicates that the bootload contains invalid content.
- Error: Failed to update image /usr/bin/copy\_boot\_image -u https://10.40.5.62/tmp/load.tgz: Failed to retrieve file from the network.  
Indication: The user has attempted to perform a software upgrade where the file path or the IP address used is not correct. Validate that the IP address is correct, also, make sure the file path is correct.
- Error: Failed to update image /usr/bin/copy\_boot\_image -u ftp://mtc:mtc@10.40.5.59/usr/load.tgz: Failed to retrieve file from the network.

Indication: The user has attempted to perform a software upgrade where the file path or the user ID or password used is not correct. Validate that the file path is correct and make sure to check the user ID and password.

- Error: Failed to update image /usr/bin/copy\_boot\_image -u ftp://mtc:mtc@10.40.5.59//usr/load.tgz: 10.40.5.59 IP address is not responding.

Indication: The user has attempted to perform a software upgrade from a host that is not responding. Check that the host IP address is available and try again.

- Error: Failed to update image /usr/bin/copy\_boot\_image -f load.tgz: Could not find load.tgz

Indication: The user has attempted to perform a software upgrade where the file path is not correct. Validate that the file path is correct.

- Error: Failed to update image /usr/bin/copy\_boot\_image -c : Failed to mount the cdrom RC=32

Indication: If the CD-ROM is not placed in the CD-ROM drive and an attempt is made to upgrade software with the Local CDROM option, the previous message appears. Verify that the CD-ROM is in the drive. If the CD-ROM is inserted, verify that the drive is functioning properly.

or

The user has attempted to perform a software upgrade where there is a problem with mounting the CD-ROM drive. Mount or remount the CD-ROM drive before attempting another software upgrade process.

- Error: Failed to update image /usr/bin/copy\_boot\_image -u https://10.40.5.62/load.tgz : Unable to decompress /opt/base/upgrade/29335/load.tgz Exiting

Indication: The user has attempted to perform a software upgrade, which uses filesystem (/opt/base) that is full. Remove unwanted files and make sure there is enough space in the targeted filesystem.

---

## Reboot a unit

---

### Purpose of this procedure

Use this procedure to perform a graceful shutdown and reboot of a unit. Use this procedure only as part of a high-level activity such as maintenance or fault clearing activities or as part of a software upgrade activity.

**ATTENTION**

This procedure causes a three to four minute service interruption of the affected unit. Use this procedure only when recommended by Nortel support personnel.

### Limitations and Restrictions

**ATTENTION**

Nortel recommends performing this procedure only on the standby unit; however, this procedure can be performed only from the active unit.

**CAUTION****Loss of redundancy**

This procedure halts all call processing activity and billing record generation on the affected unit and prevents the node from operating in a fault-tolerant mode.

### Prerequisites

Use procedure [View the operational status of the NCGL platform on page 1172](#) to check for any disk array rebuilds in progress. Wait for the rebuild to complete before executing this procedure.

Ensure that you have your bootable software installation CD/DVD disk available, in case you have trouble rebooting the unit.

## Action

### ***At the CS 2000 NCGL Platform Manager or IEMS client for the active unit***

- 1 Select Succession Communication Server NCGL Platform Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Click the Administration link.  
*The Administration page is displayed.*
- 3 Review the status of the unit you want to reboot.
- 4 Reboot the Session Server unit indicated in the high-level activity that directed you to this procedure, using the corresponding Reboot or RebootMate button. Use
  - RebootMate to reboot the inactive unit on a duplex system, or
  - Reboot to reboot the active unit on a simplex system only

**Note 1:** If you want to override any pre-reboot queries including a pre-check by applications running on the unit, click the Force check box.

**Note 2:** If the buttons are disabled, then this is the inactive unit. Reconnect to the active unit.

The screenshot shows a web interface with two main sections. The top section, titled "Software Upgrade", contains four input fields: "Protocol", "Login ID", "Password", and "IP address". The bottom section, titled "Server Maintenance", lists two units. "Unit 0 - Inactive" is highlighted with a black border and contains two buttons: "RebootMate" (circled in black) and "HaltMate", each followed by a "Force" checkbox. "Unit 1 - Active" is highlighted with a green border and contains two buttons: "Reboot" and "Halt", each followed by a "Force" checkbox.

*The system responds with the following message box. If pop up windows are disabled in the web browser, the message box does not appear.*



5

**CAUTION**

Wait for the reboot to complete. If the unit is powered down, the firmware may be left in an unrecoverable state.

Any upgrade from a pre-NCGL9 platform load or the first NCGL9 platform load (9.11.1.0) to any NCGL9-based platform load (including 9.11.1.0 and higher) requires a longer upgrade time. When the Session Server is rebooted with the new load, a firmware upgrade occurs, and this greatly increases the time required for this reboot. The reboot may now take more than 20 minutes to complete.

Do not power down the Session Server during this time, as it may leave the firmware in an unrecoverable state. Monitor the reboot progress using the console port.

Click OK to confirm the reboot operation.

The NCGL and all call activity on the affected unit are shutdown and the unit begins to reboot. The system responds with the following message box:



- 6 Click OK to close the dialog box.
- 7 Monitor the recovery of the rebooting unit using procedure [View the operational status of the NCGL platform on page 1172](#) to confirm the recovery of the unit after reboot. Continue monitoring the active unit until the simplex alarm clears in the state field.

| Unit | Activity | Jam | State          | Connectivity | Host Name      | Last Update Time |
|------|----------|-----|----------------|--------------|----------------|------------------|
| 1    | Active   | no  | simplex<br>3M+ | MatCon<br>M  | rtpsngss1unit1 | 01:52:38         |

- 8 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Alternate command line interface (CLI) method



### CAUTION

#### Loss of redundancy

This procedure halts all call processing activity and billing record generation on the affected unit and prevents the node from operating in a fault-tolerant mode.

Halting the active unit will cause the loss of all call processing and billing generation for the entire node.

### ATTENTION

All prerequisites and restrictions shown on page [1151](#) apply when using this procedure.

### At NCGL CLI or IEMS client

- 1 Log on to the active unit and change to the root user.
- 2 Reboot the selected unit by typing  

```
mtccli rebootmate (to reboot the inactive unit)
```

or

```
mtccli reboot (to reboot the active unit operating in simplex mode)
```
- 3 Use procedure [View the operational status of the NCGL platform on page 1172](#) to confirm the recovery of the unit after reboot.
- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Troubleshooting reboots

The following possible error messages received during a reboot attempt and their meaning are described:

**Error: Command failed. Reason: Mate not available.**

Reboot the unit using the [Alternate command line interface \(CLI\) method on page 1155](#).

**Error: Reboot - Command rejected. Reason: Mate is available.**

The user has attempted to reboot the active server when the inactive server is available.

**Error: Halt - Command rejected. Reason: Mate is available.**

The user has attempted to halt the active server when the inactive server is available.

**Error: Command failed. Reason: PRECHECK FAILED: application rejected request.**

The user has attempted a rebootmate or haltmate command and the application rejected the request. Check /var/log/designlog to determine the name of the application that rejected the maintenance command.

**Actions:**

- Using the Force option overcomes a pre-check failure by any application running on the unit.
- Try the operation again later. If the problem persists, then contact Nortel Networks support personnel for assistance.

---

## Import certificates and private key

---

### Purpose of this procedure

This procedure uses the certificate management tool to import the CA-signed certificate, the user certificate and the RSA private key to the appropriate directory.

### Limitations and restrictions

The following restrictions apply to migrating CA-signed certificates:

- You must be a root user to use the certificate management tool.
- Only PEM formatted, CA-signed certificates are supported on Session Server - Trunks.
- CA chain is required in PEM format in a `trusted.crt` file, top down with the root CA at the top.

### Prerequisites

Ensure `server.crt`, `trusted.crt`, and `server.key` files are located in a temporary directory such as `/users/mtc`.

### Action

#### *At the NCGL CLI or IEMS client*

- 1 Log on to the inactive unit and change to the root user.
- 2 Change directory to the location of the certificate and key files:  
`cd /users/mtc`
- 3 Start the certificate management tool by typing  
`/sbin/cert_mgnt`

*After a few seconds the Introduction screen is displayed.*

| X509 Certificate Setup. Copyright 2004 Nortel Networks, All Rights Reserved |                                                                              |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Stages                                                                      | X509 Certificate Setup                                                       |
| CertType                                                                    |                                                                              |
|                                                                             | Welcome to the X509 Certificate Setup tool.                                  |
|                                                                             | 1) Generate Self-Signed Certificate                                          |
|                                                                             | 2) Generate Certificate Signing Request                                      |
|                                                                             | 3) Import Certificates and Private Key                                       |
|                                                                             | Option:                                                                      |
|                                                                             | <input type="checkbox"/>                                                     |
|                                                                             | -----                                                                        |
|                                                                             | Abort                                                                        |
|                                                                             | -----                                                                        |
|                                                                             | Next>>                                                                       |
|                                                                             | -----                                                                        |
|                                                                             | This tool will help you to bring your SSL/TLS-based application into service |
|                                                                             | Use the <TAB> key to move and select fields                                  |

- 4 Press 3 for the option to import certificates and private key.  
Use the Tab key to position the cursor on the Next button and press Enter.

**Note:** In general, use the Tab key or the < and > keys to navigate between fields on the screen and use Enter to select a field or entry.

*The Configure the Certificate Authority certificate filename screen appears.*

```
X509 Certificate Setup. Copyright 2004 Nortel Networks. All Rights Reserved

Stages |
 | Configure the Certificate Authority certificate filename
 |-----
CertType |
CAFile |
CertFile | Please enter a CA certificate filename
KeyFile |
Summary |
 |
 |
 |
 |-----
 | | <<Back | | Next>> |
 |-----
 | Use '<' and '>' keys to move if left and right arrows don't work
```

**5** Enter the filename of the CA certificate by typing

**trusted.crt**

position the cursor on the Next button and press Enter.

**Note 1:** The tool will not proceed unless the CA certificate trusted.crt file exists in the location specified.

**Note 2:** If migrating self-signed certificates, then enter server.crt here and in [step 6](#).



- 7 Review the information summary. Position the cursor on the Proceed button and press Enter, otherwise click Back to make revisions.

*The tool validates the certificates chain and the trusted certificate files. Upon success, the tool displays the following:*

```
Provisioning CA Certificate
Verifying certificate/key pair
spawn openssl verify -CAfile trusted.crt server.crt
server.crt: OK
Certificate validation succeeded
Exporting certificate/key pair to PKCS#12 keystore
Committing trusted certificate to /opt/base/share/ssl
Committing server certificate to /opt/base/share/ssl
Committing private key to /opt/base/share/ssl
Certificate/key pair has been successfully exported to PKCS#12
format
Changing permissions on key file
Changing permissions on keystore file
```

- 8 The procedure is complete. The cert\_mgnt tool automatically copies the files to the /opt/base/share/ssl directory and sets the correct file permissions. If applicable return to the higher level task flow or procedure that directed you to this procedure.

## Troubleshooting

The private key in the server.key file must correspond to the certificate in the server.crt file for validation to be successful. If you require assistance with completing this procedure, please contact Nortel GNPS.

---

## Generate self-signed security certificates

---

### Purpose of this procedure

This procedure uses the certificate management tool to generate self-signed security certificates used for both units. Use this procedure only as part of a high-level task for updating security certificates.

A successful completion of this procedure creates a self-signed certificate composed of the following files:

- server.crt - contains the local certificate
- server.key - contains the private key corresponding to the local certificate
- trusted.crt - is an empty file if it did not already exist before the certificate management tool was run
- certificate.keystore - contains the private key and local certificate

### Limitations and restrictions

You must be a root user to use the certificate management tool.

#### **ATTENTION**

The certificate management tool sets the appropriate file permissions when the certificate files are generated. Do not change these file permissions.

If the permissions are modified, the private key can be compromised. A compromise of the private key forces a re-issuing of the certificate with a new private key and re-datafilling the certificate as necessary on peer remote SIP servers.

### Prerequisites

Please read the complete disclaimer, found in section [Self-signed certificate security disclaimer on page 1170](#).

## Action

### ***At the NCGL CLI or IEMS client***

- 1 To check the node maintenance status and the unit activity, refer to "View the operational status of the NCGL platform" in *Session Server - Trunks Security and Administration*, NN10346-611.
- 2 Log on to the standby unit and change to the root user.
- 3 Start the certificate management tool by typing

**`/sbin/cert_mgnt`**

*After a few seconds the Introduction screen is displayed.*

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved

Stages |
CertType | X509 Certificate Setup

 |
 | Welcome to the X509 Certificate Setup tool.
 |
 | 1) Generate Self-Signed Certificate
 | 2) Generate Certificate Signing Request
 | 3) Import Certificates and Private Key
 |
 | Option:
 | ☐
 | -----
 | | Abort | | Next>> |
 | -----
 |
 | This tool will help you to bring your SSL/TLS-based application
 | into service
 | Use the <TAB> key to move and select fields

```



- 4 Type 1 for the option to generate a self-signed certificate type, position the cursor on the Next button and press Enter.

**Note:** In general, use the Tab key or the < and > keys to navigate between fields on the screen and use Enter to select a field or entry.

*A security disclaimer screen appears.*

| X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stages                                                                      | X509 Certificate Setup                                                                                                                                                                                                                                                                                                                                                                                                           |
| CertType                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                                             | <p>PLEASE REVIEW THE FOLLOWING TERMS AND CONDITIONS REQUIRED FOR THE USE OF DIGITAL SELF-SIGNED CERTIFICATES. MOVE BETWEEN PAGES BY USING THE 'C' AND 'B' KEYS. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS BELOW, YOU ARE NOT AUTHORIZED TO USE A DIGITAL SELF-SIGNED CERTIFICATE.</p> <p>BY PRESSING 'Y' BELOW, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS BELOW</p> <p>Type (c) to continue <input type="text"/></p> |

- 5 Carefully read the series of screens displaying the terms and conditions of the security certificate tool. Press c to continue to the next disclaimer page or press b to go back to the previous disclaimer page.
- 6 At the final disclaimer page, accept the terms and conditions of the security certificate tool by pressing y.

Otherwise you can reject the terms and conditions of the security disclaimer by pressing n. You are returned to the main menu.

*The RSA modulus size screen appears.*

| X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved |                                 |
|-----------------------------------------------------------------------------|---------------------------------|
| Stages                                                                      | Configure RSA modulus size      |
| CertType                                                                    |                                 |
| RSAModulus                                                                  | Please enter a RSA modulus size |
| ExpiryDays                                                                  | <input type="text"/>            |
| CountryName                                                                 |                                 |
| State                                                                       |                                 |
| LocalityName                                                                |                                 |
| OrgName                                                                     |                                 |
| OrgUnit                                                                     |                                 |
| CommonName                                                                  |                                 |

- 7 Enter the RSA modulus (key) size, position the cursor on the Next button and press Enter. Supported values are 1024, 1536 or 2048 bits. (1024 is recommended)

**Note:** The larger the key size, the stronger the private key. There can be a performance impact when using larger key sizes.

- 8 Use the following table to determine your next step:

| If                                                                                                   | Do                                        |
|------------------------------------------------------------------------------------------------------|-------------------------------------------|
| you receive the message that the RSA private key already exists and you do not want to reuse the key | <a href="#">step 9</a>                    |
| you receive the message that the RSA private key already exists and you want to reuse the key        | Press y and go to <a href="#">step 13</a> |
| you do not receive any message that an RSA private key already exists                                | <a href="#">step 13</a>                   |

- 9 If you do not want to reuse the key, press n.  
*The system prompts that the RSA key is about to be deleted.*

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

| If                                                                          | Do                                                                        |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------|
| you do not want to delete the existing RSA key                              | Press n to abort the delete operation and go to <a href="#">step 11</a> . |
| you are sure you want to proceed with deleting the existing RSA private key | Go to <a href="#">step 12</a> .                                           |

- 11 Press any key and return to [step 7](#).
- 12 If you want to delete the existing RSA key, press y.  
*A backup of the existing key is made to a file in the same directory and a customer log is generated. The expiration configuration screen appears.*

| X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved |                                       |
|-----------------------------------------------------------------------------|---------------------------------------|
| Stages                                                                      | Configure the certificate expiry days |
| CertType                                                                    |                                       |
| RSAModulus                                                                  |                                       |
| ExpiryDays                                                                  | Please enter a expiry days value      |
| CountryName                                                                 |                                       |
| State                                                                       | <input type="text"/>                  |
| LocalityName                                                                |                                       |

- 13** At the certificate expiry days screen, enter the number of days you want the certificate to be valid, position the cursor on the Next button and press Enter. Supported expiration values range from 30 (30 days from the date of creation) to 7300 (20 years from the date of creation).

*The country name configuration screen appears.*

| X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved |                                                        |
|-----------------------------------------------------------------------------|--------------------------------------------------------|
| Stages                                                                      | Configure the country name                             |
| CertType                                                                    |                                                        |
| RSAModulus                                                                  |                                                        |
| ExpiryDays                                                                  | Please enter a country name (2 letter code) (optional) |
| CountryName                                                                 | <input type="text"/>                                   |
| State                                                                       | <input type="text"/>                                   |
| LocalityName                                                                |                                                        |
| OrgName                                                                     |                                                        |
| OrgUnit                                                                     |                                                        |
| CommonName                                                                  |                                                        |
| EmailAddress                                                                |                                                        |
| Summary                                                                     |                                                        |

- 14** If applicable, enter the optional ISO 3166-1-alpha-2 two-letter country code, position the cursor on the Next button and press Enter.

**Note:** This entry helps identify the node to a remote entity.

*The state/province configuration screen appears.*

| X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved |                                               |
|-----------------------------------------------------------------------------|-----------------------------------------------|
| Stages                                                                      | Configure the state or province name          |
| CertType                                                                    |                                               |
| RSAModulus                                                                  |                                               |
| ExpiryDays                                                                  | Please enter a state/province name (optional) |
| CountryName                                                                 |                                               |
| State                                                                       | <input type="text"/>                          |
| LocalityName                                                                |                                               |
| OrgName                                                                     |                                               |
| OrgUnit                                                                     |                                               |
| CommonName                                                                  |                                               |
| EmailAddress                                                                |                                               |
| Summary                                                                     |                                               |

- 15** If applicable, enter the optional state or province name, position the cursor on the Next button and press Enter.

**Note:** This entry helps identify the node to a remote entity.

*The locality configuration screen appears.*

| X509 Certificate Setup. Copyright 2004 Nortel Networks. All Rights Reserved |                                                    |
|-----------------------------------------------------------------------------|----------------------------------------------------|
| Stages                                                                      | Configure the locality name                        |
| CertType                                                                    |                                                    |
| RSAModulus                                                                  |                                                    |
| ExpiryDays                                                                  | Please enter a locality name, e.g. city (optional) |
| CountryName                                                                 |                                                    |
| State                                                                       | <input type="text"/>                               |
| <b>LocalityName</b>                                                         |                                                    |
| OrgName                                                                     |                                                    |
| OrgUnit                                                                     |                                                    |
| CommonName                                                                  |                                                    |
| EmailAddress                                                                |                                                    |
| Summary                                                                     |                                                    |

- 16** If applicable, enter the optional name of the locality or city, position the cursor on the Next button and press Enter.

**Note:** This entry helps identify the node to a remote entity.

*The organizational configuration screen appears.*

| X509 Certificate Setup. Copyright 2004 Nortel Networks. All Rights Reserved |                                                             |
|-----------------------------------------------------------------------------|-------------------------------------------------------------|
| Stages                                                                      | Configure the organizational name                           |
| CertType                                                                    |                                                             |
| RSAModulus                                                                  |                                                             |
| ExpiryDays                                                                  | Please enter a organizational name, e.g. company (optional) |
| CountryName                                                                 |                                                             |
| State                                                                       | <input type="text"/>                                        |
| LocalityName                                                                |                                                             |
| <b>OrgName</b>                                                              |                                                             |
| OrgUnit                                                                     |                                                             |
| CommonName                                                                  |                                                             |
| EmailAddress                                                                |                                                             |
| Summary                                                                     |                                                             |

- 17** If applicable, enter the optional name of the organization, position the cursor on the Next button and press Enter.

**Note:** This entry helps identify the node to a remote entity.

*The organizational unit configuration screen appears.*

| X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved |                                                       |
|-----------------------------------------------------------------------------|-------------------------------------------------------|
| Stages                                                                      | Configure the organizational unit name (e.g. section) |
| CertType                                                                    |                                                       |
| RSAModulus                                                                  |                                                       |
| ExpiryDays                                                                  | Please enter a organizational unit name (optional)    |
| CountryName                                                                 |                                                       |
| State                                                                       | <input type="text"/>                                  |
| LocalityName                                                                |                                                       |
| OrgName                                                                     |                                                       |
| <b>OrgUnit</b>                                                              |                                                       |
| CommonName                                                                  |                                                       |
| EmailAddress                                                                |                                                       |
| Summary                                                                     |                                                       |

- 18** If applicable, enter the optional name of the organizational unit, position the cursor on the Next button and press Enter.

**Note:** This entry helps identify the node to a remote entity.

*The server common name configuration screen appears.*

| X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved |                                                 |
|-----------------------------------------------------------------------------|-------------------------------------------------|
| Stages                                                                      | Configure the server common name                |
| CertType                                                                    |                                                 |
| RSAModulus                                                                  |                                                 |
| ExpiryDays                                                                  | Please enter a common name for this certificate |
| CountryName                                                                 |                                                 |
| State                                                                       | <input type="text"/>                            |
| LocalityName                                                                |                                                 |
| OrgName                                                                     |                                                 |
| OrgUnit                                                                     |                                                 |
| <b>CommonName</b>                                                           |                                                 |
| EmailAddress                                                                |                                                 |
| Summary                                                                     |                                                 |

- 19** Enter a common name for the Session Server - Trunks node to which this certificate applies using one of the following methods:

- use the active IP address for the node in the format:  
xxx.xxx.xxx.xxx
- use a hostname of up to 64 alphanumeric characters, with hyphens, underscores and periods allowed. The hostname used must be in FQDN (fully-qualified domain name) format. If you chose to use a host name, this same hostname must also be used as in the mgcHostName field when datafilling the SIP Gateway application configuration parameters.

**Note:** Using special characters in the mgcHostName other than "-" and "." may lead to issues with other third

party vendor equipment that strictly adhere to the RFC recommendation.

To datafill the mgcHostName, refer to procedure “Configure SIP Gateway application parameters” in *Session Server - Trunks Configuration Management*, NN10338-511.

**Note:** The common name value is used for mutual authentication between the node and the remote application server. There is no validation of the common name at this stage of the configuration operation.

- 20** Position the cursor on the Next button and press Enter.

*An email configuration screen appears.*

| X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved |                                          |
|-----------------------------------------------------------------------------|------------------------------------------|
| Stages                                                                      |                                          |
|                                                                             | Configure an email address               |
| CertType                                                                    |                                          |
| RSAModulus                                                                  |                                          |
| ExpiryDays                                                                  | Please enter an email address (optional) |
| CountryName                                                                 |                                          |
| State                                                                       | <input type="text"/>                     |
| LocalityName                                                                |                                          |
| OrgName                                                                     |                                          |
| OrgUnit                                                                     |                                          |
| CommonName                                                                  |                                          |
| EmailAddress                                                                |                                          |
| Summary                                                                     |                                          |

- 21** If applicable, enter the optional email address of the organization, position the cursor on the Next button and press Enter.

**Note:** This entry helps identify the node to a remote entity. There is no validation of the email address.

*A certificate summary information screen appears.*

| X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved |                                             |
|-----------------------------------------------------------------------------|---------------------------------------------|
| Stages                                                                      | Confirm the certificate information         |
| CertType                                                                    |                                             |
| RSAModulus                                                                  |                                             |
| ExpiryDays                                                                  | Select 'Proceed' or 'Back' to make changes. |
| CountryName                                                                 |                                             |
| State                                                                       | Modulus Size: 1024                          |
| LocalityName                                                                | Expiry Days: 7300                           |
| OrgName                                                                     | Country Name: CA                            |
| OrgUnit                                                                     | State/Province: Ontario                     |
| CommonName                                                                  | Locality Name: Ottawa                       |
| EmailAddress                                                                | Org. Name:                                  |
| Summary                                                                     | Org. Unit:                                  |
|                                                                             | Common Name: 172.16.182.16                  |
|                                                                             | Email Address:                              |

- 22** Review the information summary. Position the cursor on the Proceed button and press Enter. Otherwise, click Back to make revisions.

*The system responds by creating the security certificate:*

```
Exporting certificate/key pair to PKCS#12
keystore
Certificate/key pair has been successfully
exported to PKCS#12 format
Changing permissions on key file
Changing permissions on keystore file
```

- 23** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Self-signed certificate security disclaimer

The following text contains the complete security disclaimer for using self-signed certificates. It is recommended that you read and understand this disclaimer before creating self-signed certificates.

“PLEASE REVIEW THE FOLLOWING TERMS AND CONDITIONS REQUIRED FOR THE USE OF DIGITAL SELF-SIGNED CERTIFICATES. MOVE BETWEEN PAGES BY USING THE 'C' AND 'B' KEYS. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS BELOW, YOU ARE NOT AUTHORIZED TO USE A DIGITAL SELF-SIGNED CERTIFICATE.”;

“DISCLAIMER OF WARRANTY: THIS DIGITAL SELF-SIGNED CERTIFICATE IS PROVIDED BY NORTEL 'AS IS' AND NEITHER NORTEL NOR ANY OF ITS SUPPLIERS MAKE, AND SPECIFICALLY DISCLAIM, ANY AND ALL REPRESENTATIONS, WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, STATUTORY,

ARISING BY USAGE OF TRADE OR OTHERWISE, INCLUDING WITHOUT LIMITATION, REPRESENTATIONS, WARRANTIES AND CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK OF THE USE OF ANY DIGITAL SELF-SIGNED CERTIFICATE SHALL BE BORNE SOLELY BY YOU.”;

“LIMITATION OF LIABILITY: IN NO EVENT SHALL NORTEL OR ANY OF ITS SUPPLIERS AND THEIR RESPECTIVE, EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, RELIANCE, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS OR BUSINESS OPPORTUNITIES, LOSS OF GOODWILL, PROFITS OR DATA, BUSINESS INTERRUPTION, LOST SAVINGS OR OTHER SIMILAR PECUNIARY LOSS, ARISING FROM OR IN CONNECTION WITH THE USE, PERFORMANCE OR NON-PERFORMANCE OF THE DIGITAL SELF-SIGNED CERTIFICATE, WHETHER ARISING IN LAW OR EQUITY, ARISING FROM CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE) OR ANY OTHER THEORY OF LIABILITY AND REGARDLESS OF WHETHER NORTEL OR ITS SUPPLIERS WERE AWARE OF THE POSSIBILITY THEREOF. BY ENTERING 'Y', YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS JUST REVIEWED. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS JUST REVIEWED, ENTER 'N' BELOW. IF YOU DO NOT ACCEPT THESE TERMS AND CONDITIONS, YOU ARE NOT AUTHORIZED TO USE A DIGITAL SELF-SIGNED CERTIFICATE.”;



---

## View the operational status of the NCGL platform

---

### Purpose of this procedure

Use the following procedure to view the service status of the hardware and NCGL operating system using the CS 2000 NCGL Platform Manager. This procedure can be used as a standalone task or as part of a high-level activity.

### Limitations and restrictions

This procedure provides instructions for determining the service status of the Session Server - Trunks NCGL platform only. For instructions on determining the status of the SIP Gateway application, refer to procedure "View the operational status of the SIP Gateway application" in *Session Server - Trunks Configuration Management*, NN10338-511.

Although some activities described in this procedure can be accomplished using the CS 2000 Session Server Manager, they are described instead using the more complete CS 2000 NCGL Platform Manager.

This procedure does not describe how to view customer logs or alarms. For detailed instructions on viewing customer logs or alarms, refer to procedures in *Session Server - Trunks Fault Management*, NN10332-911.

### Prerequisites

There are no prerequisites for using this procedure.

## Action

### ***At the CS 2000 NCGL Platform Manager or IEMS client***

- 1 Select Succession Communication Server 2000 NCGL Platform Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

*The Platform Main Page menu is displayed.*

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

| If                                                                                                                                                                                            | Do                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| you want to review the version of the platform software load, boot statistics and platform IP address                                                                                         | Click the System Information link and go to <a href="#">step 3</a> .                                                                                  |
| you want to review Sensor Information                                                                                                                                                         | Go to "Sensor information" in <i>Session Server Trunks Basics</i> , NN10333-111.                                                                      |
| you want to review existing platform alarms                                                                                                                                                   | Go to <a href="#">step 17</a> and go to procedure "View Session Server Trunks alarms" in <i>Session Server Trunks Fault Management</i> , NN10332-911. |
| you want to review node maintenance status                                                                                                                                                    | Click the Node Maintenance link and go to <a href="#">step 5</a> .                                                                                    |
| you want to review the status of system processes, CPU load and memory or related alarm thresholds                                                                                            | Click the System Status link and go to <a href="#">step 7</a> .                                                                                       |
| you want to review the connectivity status of the network links.<br>To perform link management activities, refer to <i>Session Server - Trunks Security and Administration</i> , NN10346-611. | Click the Network Connectivity link and go to <a href="#">step 9</a> .                                                                                |
| you want to review storage related information including array status, disk capacity and disk alarm thresholds                                                                                | Click the Disk Services link and go to <a href="#">step 10</a> .                                                                                      |
| you want to review details about platform services including the network time protocol servers                                                                                                | Click the Services link and go to <a href="#">step 12</a> .                                                                                           |
| you want to review platform version information only                                                                                                                                          | Click the Administration link and go to <a href="#">step 14</a> .                                                                                     |

| If                                                                        | Do                                                                                                                                                |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| you want to review customer logs                                          | Go to <a href="#">step 17</a> and refer to <i>Session Server - Trunks Fault Management</i> , NN10332-911.                                         |
| you want to change root passwords                                         | Go to <a href="#">step 17</a> and refer to <i>Session Server - Trunks Security and Administration</i> , NN10346-611.                              |
| you want to view TLS security information or manage security certificates | Go to <a href="#">step 17</a> and refer to <i>Session Server - Trunks Configuration Management</i> , NN10338-511 to review TLS security settings. |
| you are finished reviewing information and want to log out from the GUI   | <a href="#">step 16</a> .                                                                                                                         |

- 3 Review the system information page and use the following table to review the description of the various fields of the Platform (System) Information page:

**Note:** The Platform (System) Information panel does not update automatically. Click the System Information link again to update it.

| Unit | Activity | Jam | State | Connectivity | Host Name      | Last Update Time |
|------|----------|-----|-------|--------------|----------------|------------------|
| 1    | Active   | no  | .     | .            | rtpsngss1unit1 | 08:55:05         |

The Platform Information panel does not update automatically!  
 Datestamp of last update: Wednesday April 06th 2005 08:55:08 AM EDT

| Platform Information           |                                               |
|--------------------------------|-----------------------------------------------|
| Date:                          | Wednesday April 06th 2005 08:55:08 AM EDT     |
| Time since last reboot:        | 12 days, 20 hours, 23 minutes, 43 seconds     |
| System Power-On Time:          | 1 years 29 days 6 hours                       |
| System booted from:            | Hard disk drive                               |
| Last restart cause:            | Last restart due to soft reset                |
| Last power event cause:        | Last power down caused by loss of power feed. |
| Current version:               | 7.09.1.0.0502281015                           |
| Platform IP Address:           | 172.17.40.216                                 |
| Platform EM Client IP Address: | 47.142.89.70                                  |
| Server Location:               | lab5                                          |
| Host Name:                     | rtpsngss1unit1                                |

| Field    | Description                                                                                                                                                                                     |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit     | unit number in the node that you are logged into                                                                                                                                                |
| Activity | activity of the unit (either active or standby)                                                                                                                                                 |
| Jam      | indicates if the inactive unit is Jammed. The value is YES only if logged in to the inactive unit. From the active unit, the status is NO, but a Jlnact alarm indicates the inactive is Jammed. |

| Field                          | Description                                                                                                                     |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| State                          | indicates if the node is operating in a duplex (fault-tolerant) mode or a simplex mode (the standby unit is off-line)           |
| Connectivity                   | state of the network links on the node                                                                                          |
| Host Name                      | name of the unit (not node)                                                                                                     |
| Date                           | system date as maintained by the network time protocol (NTP) server                                                             |
| Time since last reboot:        | amount of time that has elapsed since the unit was last rebooted for any reason                                                 |
| System Power-On Time:          | recorded system time that the unit has been powered up                                                                          |
| System booted from:            | indicates whether the unit is currently booted from the hard drive or DVD-ROM drive                                             |
| Last restart cause:            | indicates any event that forced a platform reboot (manual or system generated)                                                  |
| Last power event cause:        | indicates any event that affected the power supply subsystem of the unit chassis                                                |
| Current version:               | installed version of the NCGL platform software                                                                                 |
| Platform IP Address:           | unit IP address                                                                                                                 |
| Platform EM Client IP Address: | IP address of the client web browser. When a web proxy is used, the IP address of the machine performing the proxy is displayed |
| Server Location:               | physical location of the unit                                                                                                   |
| Host Name:                     | name of the unit                                                                                                                |

- 4 When you have completed reviewing System Information page, return to [step 2](#).

- 5 Review the Node Maintenance page and use the following table to review the description of the various fields of the Node Maintenance page:

The Node Maintenance panel updates every 45 seconds  
Datestamp of last update: Wednesday April 06th 2005 09:19:40 AM EDT

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | no        |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Jam"/> <input type="checkbox"/> Force |

**Note:** The Node Maintenance panel is refreshed every 45 seconds.

| Field                                  | Description                                                                                                                                                                        |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operation State                        | indicates the operational state of the NCGL software                                                                                                                               |
| Activity                               | indicates the activity state of the platform software                                                                                                                              |
| Jam State                              | indicates if the inactive unit is Jammed                                                                                                                                           |
| Maintenance Actions (active unit only) | maintenance panel for performing SwAct and to Jam. Refer to <i>Session Server - Trunks Security and Administration</i> , NN10346-611, for procedures on performing a SwAct or Jam. |

- 6 When you have completed reviewing the Node Maintenance page, return to [step 2](#).

- 7 Review the System Status page and use the following table to review the descriptions of the various fields of the System Status page.

| Chassis Information |  |  |                        |  |  |
|---------------------|--|--|------------------------|--|--|
| Self Test           |  |  | Chassis Subsystems     |  |  |
| Self tests passed.  |  |  | Chassis subsystems OK. |  |  |

| CPU Load            |                      |                       |                              |                              |                                 |
|---------------------|----------------------|-----------------------|------------------------------|------------------------------|---------------------------------|
| 1 min. load average | 5 mins. load average | 15 mins. load average | Minor alarm threshold 1 min. | Major alarm threshold 1 min. | Critical alarm threshold 1 min. |
| 0.10                | 0.05                 | 0.01                  | 10.00                        | 20.00                        | 40.00                           |

| CPU Utilization             |                              |                              |                              |                               |                                  |
|-----------------------------|------------------------------|------------------------------|------------------------------|-------------------------------|----------------------------------|
| 5 mins. Utilization average | 20 mins. Utilization average | 30 mins. Utilization average | Minor alarm threshold 5 min. | Major alarm threshold 20 min. | Critical alarm threshold 30 min. |
| 2.20                        | 1.99                         | 1.86                         | 95.00%                       | 99.00%                        | 99.00%                           |

| Process Information |                              |                             |                             |                                |
|---------------------|------------------------------|-----------------------------|-----------------------------|--------------------------------|
| Number of processes | Number of zombie process(es) | Zombie                      |                             |                                |
|                     |                              | Minor alarm threshold value | Major alarm threshold value | Critical alarm threshold value |
| 192                 | 1                            | 5                           | 10                          | 15                             |

| Memory Information |                  |                       |                                  |                                  |                                     |
|--------------------|------------------|-----------------------|----------------------------------|----------------------------------|-------------------------------------|
| Total memory (MB)  | Free memory (MB) | Available memory (MB) | Minor alarm threshold value (MB) | Major alarm threshold value (MB) | Critical alarm threshold value (MB) |
| 3,790.29           | 2,945.21         | 3,294.78              | 500.00                           | 250.00                           | 100.00                              |

**Note:** The Chassis Information panel is not automatically refreshed.

| Field                                                   | Description                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chassis information: Self Test                          | status of the self test performed on the platform at boot up                                                                                                                                                                                                                                                                                                                         |
| Chassis information: Chassis Subsystems                 | status of the platform hardware subsystems including the memory, CPU, all drives, network connection, power supplies, cooling and other I/O connections                                                                                                                                                                                                                              |
| CPU Information: load average                           | indicates the 1, 5 and 15 minute load averages for the CPU utilization                                                                                                                                                                                                                                                                                                               |
| CPU information: load average threshold values          | indicates the 1 minute CPU load average utilization threshold value. When the set threshold value is exceeded, the appropriate minor, major or critical alarm is raised.                                                                                                                                                                                                             |
| Chassis Utilization: Utilization average                | indicates the 5, 20 and 30 minute CPU utilization average. When the threshold value is exceeded, an alarm is raised.                                                                                                                                                                                                                                                                 |
| Chassis Utilization: alarm threshold values             | indicates the 5, 20 and 30 minute CPU utilization average threshold value. When the set threshold value is exceeded, an alarm is raised.                                                                                                                                                                                                                                             |
| Process Information: Number of Processes                | total number of processes (non-threaded) that are running on the Session Server - Trunks Platform                                                                                                                                                                                                                                                                                    |
| Process Information: Number of zombie processes         | number of defunct or terminated NCGL zombie processes<br><br><b>Note:</b> A zombie process is a process that has terminated either because it has been killed by a signal or because it has called an exit() and whose parent process has not yet received notification of its termination. A zombie process exists solely as a process table entry and consumes no other resources. |
| Process Information-zombie: minor alarm threshold value | maximum number of zombie processes allowed to be run by the CPU before a minor alarm is raised indicating that the set threshold has been exceeded                                                                                                                                                                                                                                   |



| Field                                                      | Description                                                                                                                                           |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process Information-zombie: major alarm threshold value    | maximum number of zombie processes allowed to be run by the CPU before a major alarm is raised indicating that the set threshold has been exceeded    |
| Process Information-zombie: critical alarm threshold value | maximum number of zombie processes allowed to be run by the CPU before a critical alarm is raised indicating that the set threshold has been exceeded |
| Memory Information: Total Memory (MB)                      | total amount of RAM installed on the motherboard of each Session Server - Trunks unit. Both units must have the same amount.                          |
| Memory Information: Free Memory (MB)                       | amount of memory available unallocated for use                                                                                                        |
| Memory Information: Available memory (MB)                  | amount of memory available for programs                                                                                                               |
| Memory Information: minor alarm threshold value            | indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a minor alarm is raised                         |
| Memory Information: major alarm threshold value            | indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a major alarm is raised                         |
| Memory Information: critical alarm threshold value         | indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a critical alarm is raised                      |

- 8 When you have completed reviewing the System Status, return to [step 2](#).

- 9 Review the Network Connectivity page and use the following table to review the description of the various fields of the Network Connectivity page:

**Note:** The Network Connectivity panel is refreshed every 45 seconds.

| Unit 0 Links  |               |               |               |             |
|---------------|---------------|---------------|---------------|-------------|
| Unit IP       | Inactive IP   | Port 0 IP     | Port 1 IP     | PTP IP      |
| 172.17.40.211 | 172.17.40.215 | 172.17.40.209 | 172.17.40.210 | 192.168.1.1 |
| Links         |               | Status        | Activity      |             |
| Link 0        |               | .             | Active        |             |
| Link 1        |               | .             | Inactive      |             |
| PTP Links     |               | .             |               |             |

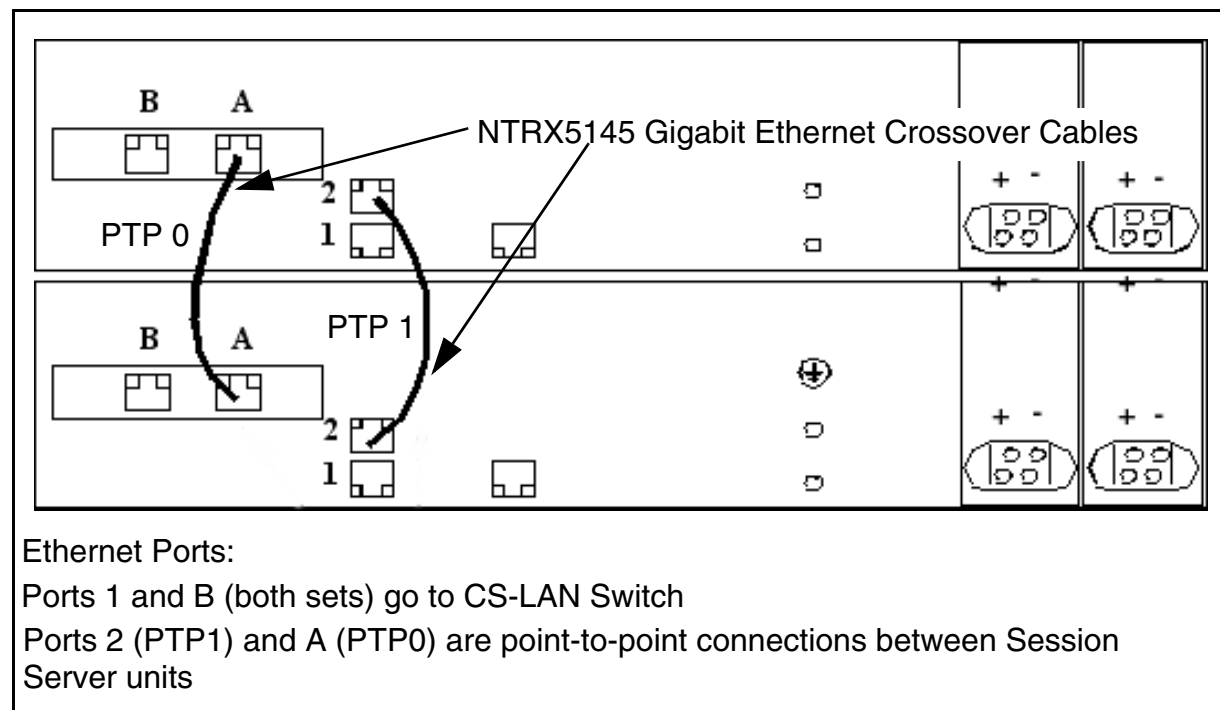
  

| Unit 1 Links  |               |               |               |             |
|---------------|---------------|---------------|---------------|-------------|
| Unit IP       | Active IP     | Port 0 IP     | Port 1 IP     | PTP IP      |
| 172.17.40.214 | 172.17.40.216 | 172.17.40.212 | 172.17.40.213 | 192.168.1.2 |
| Links         | Status        | Activity      | Maintenance   |             |
| Link 0        | .             | Active        | Lock 0        | Swlink      |
| Link 1        | .             | Inactive      | Lock 1        |             |
| PTP Links     | .             |               |               |             |

| Field                     | Description                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------------------|
| Unit 0,1 Links            | indicates which Ethernet IP links are installed on the units (each unit has two links)                       |
| Unit 0,1 Status           | status of the Ethernet links                                                                                 |
| Unit 0,1 Activity         | activity status of the Ethernet links, either active or inactive                                             |
| Unit 0,1 Maintenance      | indicates the maintenance actions that can be performed on the Ethernet links, either Lock, Unlock or Swlink |
| Unit 0,1 PTP Links status | status of the PTP links between both units in the node                                                       |

| Field       | Description                                                    |
|-------------|----------------------------------------------------------------|
| Unit IP     | network IP address of the Session Server - Trunks unit         |
| Active IP   | IP address of the local (active) Session Server - Trunks unit  |
| Inactive IP | IP address of the mate (inactive) Session Server - Trunks unit |
| Port 0 IP   | IP address of the active or inactive Ethernet port 0           |
| Port 1 IP   | IP address of the active or inactive Ethernet port 1           |
| PTP IP      | IP address of the active or inactive PTP link                  |

### Crossover and LAN Ethernet cable connections for Session Server - Trunks units



- 10 Review the Disk Services page and use the following table to review the description of the various fields of the Disk Storage page:

**Note 1:** The Disk Services panel does not update automatically. Click the Disk Services link again to update it.

**Note 2:** To create and remove file systems, refer to applicable procedures in *Session Server - Trunks Configuration Management*, NN10338-511.

| RAID Array Status |           |       |        |        |                             |  |  |  |  |  |
|-------------------|-----------|-------|--------|--------|-----------------------------|--|--|--|--|--|
| Name              | Size (GB) | State | Disk 0 | Disk 1 | Status                      |  |  |  |  |  |
| /boot             | 0.10      | .     | .      | .      | Array is operating normally |  |  |  |  |  |
| ntvg              | 68.26     | .     | .      | .      | Array is operating normally |  |  |  |  |  |

| Disk Maintenance |                |            |                        |
|------------------|----------------|------------|------------------------|
| Disk Number      | Disk Size (GB) | Disk State | Disk Action            |
| 0                | 68.37          | .          | <a href="#">Remove</a> |
| 1                | 68.37          | .          | <a href="#">Remove</a> |

| Filesystem Information |                       |              |                  |                       |                      |                            |                           |                           |                           |                              |
|------------------------|-----------------------|--------------|------------------|-----------------------|----------------------|----------------------------|---------------------------|---------------------------|---------------------------|------------------------------|
| Monitored              | Filesystem Name       | Test Results | Total Space (MB) | Total Space Used (MB) | Total Space Used (%) | Total Space Available (MB) | Total Space Available (%) | Minor Alarm Threshold (%) | Major Alarm Threshold (%) | Critical Alarm Threshold (%) |
|                        | /                     | .            | 61.47            | 58.29                 | 100.00               | 0.00                       | 0.00                      | 85.00                     | 90.00                     | 95.00                        |
| No                     | /boot                 | .            | 98.65            | 19.08                 | 21.00                | 74.48                      | 79.00                     | -                         | -                         | -                            |
| Yes                    | /opt/base             | .            | 699.31           | 0.46                  | 1.00                 | 698.85                     | 99.00                     | 85.00                     | 90.00                     | 95.00                        |
| No                     | /opt/apps             | .            | 507.31           | 314.31                | 62.00                | 193.00                     | 38.00                     | -                         | -                         | -                            |
| Yes                    | /tmp                  | .            | 123.31           | 0.31                  | 1.00                 | 123.00                     | 99.00                     | 85.00                     | 90.00                     | 95.00                        |
| Yes                    | /var/log              | .            | 507.31           | 9.61                  | 2.00                 | 497.71                     | 98.00                     | 85.00                     | 90.00                     | 95.00                        |
| No                     | /opt/swd              | .            | 507.31           | 0.25                  | 1.00                 | 507.06                     | 99.00                     | -                         | -                         | -                            |
| No                     | /opt/apps/webint      | .            | 1,494.00         | 209.78                | 15.00                | 1,284.22                   | 85.00                     | -                         | -                         | -                            |
| No                     | /opt/apps/database    | .            | 10,006.00        | 48.19                 | 1.00                 | 9,957.81                   | 99.00                     | -                         | -                         | -                            |
| No                     | /opt/apps/logs        | .            | 507.31           | 206.34                | 41.00                | 300.98                     | 59.00                     | -                         | -                         | -                            |
| No                     | /opt/apps/ngssbilling | .            | 10,006.00        | 2.50                  | 1.00                 | 10,003.50                  | 99.00                     | -                         | -                         | -                            |

| Create/Remove Filesystem              |                      |                                   |
|---------------------------------------|----------------------|-----------------------------------|
| <a href="#">Create New Filesystem</a> | <input type="text"/> | <a href="#">Remove Filesystem</a> |

| Volume Group Information |                        |                            |                           |                            |                           |
|--------------------------|------------------------|----------------------------|---------------------------|----------------------------|---------------------------|
| Volume Group Name        | Volume Group Size (GB) | Total Space Allocated (GB) | Total Space Allocated (%) | Total Space Available (GB) | Total Space Available (%) |
| ntvg                     | 68.22                  | 23.84                      | 34.95                     | 44.38                      | 65.05                     |

| Field                        | Description                                           |
|------------------------------|-------------------------------------------------------|
| RAID Array Status: Name      | indicates the name of each RAID-1 array in the system |
| RAID Array Status: Size (GB) | indicates the size of the partition in gigabytes      |

| Field                                         | Description                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RAID Array Status: State                      | Indicates a high level state for the array: <ul style="list-style-type: none"> <li>- “.”: indicates the array is functioning normally.</li> <li>- Missing: a disk was removed from the array.</li> <li>- Failed: a disk in the array has failed and needs to be replaced.</li> <li>- Rebuilding: the array is in the process of rebuilding to a fault-tolerant mode.</li> </ul> |
| RAID Array Status: Disk 0                     | service status of disk 0                                                                                                                                                                                                                                                                                                                                                        |
| RAID Array Status: Disk 1                     | service status of disk 1                                                                                                                                                                                                                                                                                                                                                        |
| RAID Array Status: Status                     | Indicates the status of the array. Values are: <ul style="list-style-type: none"> <li>- The array is operating normally</li> <li>- Missing</li> <li>- Failed</li> <li>- Rebuild</li> </ul>                                                                                                                                                                                      |
| Disk Maintenance: Disk Number                 | indicates the disk number in the array, 0 or 1                                                                                                                                                                                                                                                                                                                                  |
| Disk Maintenance: Disk Size (GB)              | total capacity of the disk drive in gigabytes                                                                                                                                                                                                                                                                                                                                   |
| Disk Maintenance: Disk State                  | installation state of the disk                                                                                                                                                                                                                                                                                                                                                  |
| Disk Maintenance: Disk Action                 | indicates whether a hard disk can be inserted into the RAID array                                                                                                                                                                                                                                                                                                               |
| Filesystem Information: Monitor               | indicates the status of individual filesystems on the disk array                                                                                                                                                                                                                                                                                                                |
| Filesystem Information: Filesystem Name       | indicates the name of the filesystem on the disk array. Some filesystem names are reserved.                                                                                                                                                                                                                                                                                     |
| Filesystem Information: Test Results          | indicates the results of any tests run on the filesystems. Tests are run approximately every 10 minutes to verify that all of the basic filesystem operations are working on each of the filesystems.                                                                                                                                                                           |
| Filesystem Information: Total Space (MB)      | total amount of disk space (in MB) allocated for this filesystem                                                                                                                                                                                                                                                                                                                |
| Filesystem Information: Total Space Used (MB) | total amount of disk space (in MB) in use on this file system                                                                                                                                                                                                                                                                                                                   |
| Filesystem Information: Total Space Used (%)  | total amount of disk space (in %) in use on this file system                                                                                                                                                                                                                                                                                                                    |

| Field                                                | Description                                                                                                                                |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Filesystem Information: Total Space Available (MB)   | percentage of total disk space (in MB) free for use on this filesystem                                                                     |
| Filesystem Information: Total Space Available (%)    | amount of disk space (in %) available for use by platform processes and applications                                                       |
| Filesystem Information: Minor Alarm Threshold (%)    | maximum amount of disk space (in %) that can be used before a minor alarm is raised indicating that the set threshold has been exceeded    |
| Filesystem Information: Major Alarm Threshold (%)    | maximum amount of disk space (in %) that can be used before a major alarm is raised indicating that the set threshold has been exceeded    |
| Filesystem Information: Critical Alarm Threshold (%) | maximum amount of disk space (in %) that can be used before a critical alarm is raised indicating that the set threshold has been exceeded |
| Volume Group Information: Volume Group Name          | name of the volume group in the array                                                                                                      |
| Volume Group Information: Volume Group Size (GB)     | total size of the volume group in the array                                                                                                |
| Volume Group Information: Total Space Allocated (GB) | amount of volume group space, in gigabytes, currently allocated to filesystems                                                             |
| Volume Group Information: Total Space Allocated (%)  | amount of volume group space (in %) currently allocated to filesystems                                                                     |
| Volume Group Information: Total Space Available (GB) | amount of unallocated volume group space, in gigabytes, available for filesystems                                                          |
| Volume Group Information: Total Space Available (%)  | amount of unallocated volume group space (in %) available for filesystems                                                                  |

- 11 When you have completed reviewing the Disk Services page, return to [step 2](#).
- 12 Review the Services page and use the following table to review the description of the various fields of the Platform Services page:

**Note:** The Services panel does not update automatically. Click the Services link again to update it.

| Network Services                       |  |  |                                            |  |  |
|----------------------------------------|--|--|--------------------------------------------|--|--|
| Number of Active Command Line Sessions |  |  | Number of Clients with Active Web Sessions |  |  |
| 1                                      |  |  | 1                                          |  |  |

| NTP Information          |                          |           |                         |                    |                      |
|--------------------------|--------------------------|-----------|-------------------------|--------------------|----------------------|
| Server 1                 | Server 2                 | Server 3  | Total Number of Servers | Accessible Servers | Synchronized Servers |
| 47.140.207.50<br>in sync | 47.140.206.50<br>in sync | undefined | 2                       | 2                  | 2                    |

| Field                                                           | Description                                                                                                       |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Network Services:<br>Number of Active Command Line Sessions     | number of command line interface (CLI) sessions (both remote and local) on the unit                               |
| Network Services:<br>Number of Clients with Active Web Sessions | number of clients running one or more web GUI sessions                                                            |
| NTP Information:<br>Server1 - Server 3                          | IP address of up to 3 Network Time Protocol (NTP) servers in the network, along with the status of the connection |
| NTP Information:<br>Total Number of Servers                     | number of NTP servers registered with the CS-LAN network                                                          |
| NTP Information:<br>Accessible Servers                          | number of NTP servers accessible to the Session Server - Trunks                                                   |
| NTP Information:<br>Synchronized Servers                        | number of NTP servers to which the unit is synchronized                                                           |

- 13 When you have completed reviewing Platform Services status, return to [step 2](#).
- 14 Review the Administration page and use the following table to review the description of the various fields of the Administration page:

**Note:** The Administration panel does not update automatically. Click the link again to update it.

| Bootload Management |                                                                                  |
|---------------------|----------------------------------------------------------------------------------|
| Bootload            | Maintenance                                                                      |
| 8.08.1.0.0502231439 | Default Bootload                                                                 |
| 7.09.1.0.0502281015 | <input type="button" value="Set default"/> <input type="button" value="Delete"/> |
| 5.36.2.1.0411021023 | <input type="button" value="Set default"/> <input type="button" value="Delete"/> |

| Software Upgrade     |                      |                      |                      |                      |
|----------------------|----------------------|----------------------|----------------------|----------------------|
| Protocol             | Login ID             | Password             | IP address           |                      |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

| Server Maintenance                                                       |                                                                        |
|--------------------------------------------------------------------------|------------------------------------------------------------------------|
| <b>Unit 0 - Inactive</b>                                                 |                                                                        |
| <input type="button" value="RebootMate"/> <input type="checkbox"/> Force | <input type="button" value="HaltMate"/> <input type="checkbox"/> Force |
| <b>Unit 1 - Active</b>                                                   |                                                                        |
| <input type="button" value="Reboot"/> <input type="checkbox"/> Force     | <input type="button" value="Halt"/> <input type="checkbox"/> Force     |

| Field                            | Description                                                                                                                                                                                  |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bootload Management: Bootload    | load ID for the NCGL platform software load                                                                                                                                                  |
| Bootload Management: Maintenance | indicates whether the Bootload is the default. Can also allow choosing a new default bootload if there is more than one load available. Additional loads can come from maintenance releases. |
| Software Upgrade: Protocol       | file transfer protocol or source location for the platform software upgrade: FTP, Anonymous FTP, HTTP, HTTPS, Local File, Local CDROM                                                        |
| Software Upgrade: Login ID       | If a login ID is required to access the upgrade platform load from another server in the network, a login ID can be entered here.                                                            |



| Field                                          | Description                                                                                                                       |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Software Upgrade: Password                     | If a password is required to access the upgrade platform load from another server in the network, a password can be entered here. |
| Software Upgrade: IP Address                   | If it is required to access the upgrade platform load from another server in the network, an IP address can be entered here.      |
| Software Upgrade: File                         | The target upgrade load path and filename is entered here.                                                                        |
| Software Upgrade: Action Upgrade button        | The Upgrade button initiates a platform NCGL upgrade.                                                                             |
| Server Maintenance (active and inactive units) | used to execute the Reboot, Halt, Rebootmate, and Haltmate functions. These are service affecting commands.                       |

- 15** When you have completed reviewing the Administration page, return to [step 2](#), or continue with [step 16](#).
- 16** If you want to logout from CS 2000 NCGL Platform Manager, click the Logout button.  
*You are returned to the login page*
- 17** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Acquire patch files

### Purpose of this procedure

Use this procedure to identify patch files from a CD/DVD disk or ESD archive file and copy them to an appropriate directory on each unit.

### Limitations and Restrictions

This is not a service impacting procedure and can be performed on either the active or inactive unit.

### Prerequisites

If locating patch files from a CD/DVD disk, ensure that the upgrade, maintenance release or patching CD/DVD disk is inserted into the unit DVD-ROM drive.

If locating patch files from an ESD delivered ISO archive file, refer to [Extract an ISO image from an Electronic Software Delivery \(ESD\) on page 1134](#) for assistance with using an ESD image.

## Action

### *At the Session Server CLI or IEMS client*

- 1 The first action is determined by software delivery method:

| If media is delivered by | Do                                                                                                                                                |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| ESD                      | Perform <a href="#">Extract an ISO image from an Electronic Software Delivery (ESD) on page 1134</a> .<br><br>Then go to <a href="#">step 6</a> . |
| CD/DVD disk              | Continue to <a href="#">step 2</a> .                                                                                                              |

- 2 Log on to either unit and change to the root user.
- 3 Insert the CD/DVD disk into the disk drive.
- 4 At the prompt, type  

```
$ cd /
```
- 5 Mount the DVD-ROM drive by typing  

```
$ mount /cdrom
```
- 6 Change directories to the mounted DVD-ROM filesystem by typing  

```
$ cd /cdrom
```

- 7 Locate the patch files by typing  
**\$ ls**  
*The system responds by displaying a list of files. Locate the patch files with the following filename format:*  
*ncgl\_samxts\_patch\_<rel#>.<wk#>.<major#>.<minor#>*  
**Example**  
*ncgl\_samxts\_patch\_7.31.1.1*  
*ncgl\_samxts\_patch\_7.31.1.2*
- 8 Copy the patch files by typing  
**\$ cp <patchfilename> /patching/patchholding**  
where  
**patchfilename**  
is the file name for the patch file
- 9 Change directories to root by typing  
**\$ cd /**
- 10 Unmount the DVD-ROM drive by typing  
**\$ umount /cdrom**
- 11 Repeat this procedure on the mate unit.
- 12 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Apply and commit an NCGL patch

---

### Purpose of this procedure

Use this procedure to apply patch files to the inactive unit.

### Restrictions and Limitations

**ATTENTION**

Apply NCGL patch files to the inactive unit only.

Patching activities must be completed on both units in the node.

### Prerequisites

The patch files must have already been put into the /patching/patchholding directory on the unit hard drive.

Use the patching or upgrade release notes to verify if any NCGL patches must first be removed before applying new patches.

### Action

#### *At the NCGL CLI or IEMS client*

- 1 Log on to the inactive unit and change to the root user.
- 2 Change directory to the patchholding directory by typing  
**cd /patching/patchholding**
- 3 Retrieve and untar the patch files from the patch archive to the /patching/<patch\_version>/ directory, and fill the patching subsystem's database with the patch information. At the prompt, type:  
**patch\_ha -f <patch\_file\_name> -o Fetch**  
where  
**patch\_file\_name**  
is the name of the patch archive you want to extract patch files from.
- 4 Validate the patch file to verify that the patch file is sane, and the patch is ready to be applied. At the prompt type:  
**patch\_ha -v <patch\_version> -o Validate**  
where

**patch\_version**

is the name of the patch file to be applied

- 5 Apply the patch file:

```
patch_ha -v <patch_version> -o Apply
```

**ATTENTION**

NCGL patches are not automatically committed when applied. In order for a patch to reapply the next time the unit is rebooted, it must first be committed.

- 6 Commit the patch so it is auto-applied at each reboot of the unit:

```
patch_ha -v <patch_version> -o Commit
```

- 7 If necessary, allow the unit to reboot or if requested, perform a reboot using procedure [Reboot a unit on page 1151](#). Otherwise go to the next step.

- 8 Monitor logs and alarms. If errors occur that are related to the patching activity, contact your next level of support.

**Note:** Checking unit status entail different activities depending on the what type of software item has been patched and any special patch application requirements. For example, some software subsystem processes require a reboot before a patch can become active, whereas other subsystem processes restart with the new patched version once patch application is complete.

- 9 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## View web proxy settings in SPFS for Session Server - Trunks

---

### Purpose of this procedure

Use the following activity to view the configuration of existing node web proxy services on the SPFS server (part of the CS 2000 Management Tools server).

### Limitations and restrictions

If the web proxy entry for a particular node requires changing, you must configure a new proxy entry with the modified values, then remove the obsolete proxy entry. Do not use this procedure to add a new node to the proxy service configuration. To perform this activity, refer to procedure "Add a Session Server - Trunks node to the SPFS server web proxy" in *Session Server - Trunks Configuration Management*, NN10338-511.

### Prerequisites

Ensure that the account you use to log into the CS 2000 Management Tools server has root privileges.

Observe all limitations and prerequisites applicable to other procedures referenced in this activity.

Refer to section "Understanding Session Server - Trunks IP addressing" in *Session Server - Trunks Configuration Management*, NN10338-511, for more information about IP addressing and naming schemes needed to complete this activity. The following IP addresses are referenced in this activity:

- Unit 0 (the IP address of physical unit0)
- Unit 1 (the IP address of physical unit 1)
- Active unit (the IP address of the logically active unit, also used for accessing the CS 2000 Session Server Manager)

## Action

### *At the NCGL CLI or IEMS client*

- 1 Verify that a security certificate has been installed on the CS 2000 Management Tools Server SPFS platform. For assistance use procedure "Installing an HTTPS certificate on a Sun server" in *Carrier Voice over IP Network Upgrade Overview*, NN10440-450.
- 2 Log in to the CS 2000 Management Tools server.
- 3 Change to the root user by typing  
**su - root**
- 4 Enter the root password and press Enter.
- 5 Start the command line interface application:  
**cli**
- 6 Enter the number next to the Configuration menu option.
- 7 Enter the number next to the Apache Proxy Configuration menu option.
- 8 Enter the number next to the List the Apache Proxy Module Configuration menu option.
- 9 Locate the proxy entry for the active unit used by the CS 2000 Session Server Manager. Refer to the following figure for assistance in locating this entry.

|                                                                |                           |
|----------------------------------------------------------------|---------------------------|
| <i>ProxyPass /10.65.99.67/ https://10.65.99.67:443/</i>        | Entry for physical unit 0 |
| <i>ProxyPassReverse /10.65.99.67/ https://10.65.99.67:443/</i> |                           |
| <i>ProxyPass /10.65.99.70/ https://10.65.99.70:443/</i>        | Entry for physical Unit 1 |
| <i>ProxyPassReverse /10.65.99.70/ https://10.65.99.70:443/</i> |                           |
| <i>ProxyPass /10.65.99.72/ https://10.65.99.72:443/</i>        | Entry for active unit     |
| <i>ProxyPassReverse /10.65.99.72/ https://10.65.99.72:443/</i> |                           |
| <i>ProxyPass /prov/ https://10.67.99.72:8443/prov/</i>         | Entry for active unit GUI |
| <i>ProxyPassReverse /prov/ https://10.67.99.72:8443/prov/</i>  |                           |

- 10 If necessary, record the label for the remote hostname/tag associated with the active unit.

**ATTENTION**

If necessary, refer to section [Selecting and using tag names in SN08 and newer on page 1195](#) for more information about using remote tag names. The tag name shown must match the tag name used by the SIP Gateway application for the same node when you installed or upgraded it.

- 11 Exit the Apache Proxy Configuration level:  
x
- 12 Exit the Configuration level:  
x
- 13 Exit the CLI:  
x
- 14 If applicable, logout from the server.
- 15 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Selecting and using tag names in SN08 and newer

Tag names for the active unit web proxy entries, must match the tag name entered when installing or upgrading the SIP Gateway application. Failure to use the same tag name will prevent access to the CS 2000 Session Server Manager after the SPFS web proxy services restart.

If the remote tag name for a node does not match that used during installation or upgrade of the SIP Gateway application, you must configure a new proxy entry using the correct remote tag name, then remove the obsolete proxy entry.



## Upgrade/rollback/reinstall a Session Server - Trunks application

### Purpose of this procedure

Use the following procedure to:

- reinstall a current version of the SIP Gateway Application
- upgrade to a newer version of the SIP Gateway Application
- rollback to a previous version of the SIP Gateway Application

#### ATTENTION

It is recommended that this procedure only be used as part of the high level activity [Preparing to upgrade the Session Server Trunks on page 1114](#).

### Limitations and restrictions

If the node is in operation and performing call processing activities, only perform this procedure on the standby unit.

This procedure must be performed on both units based on the upgrade or rollback activity being performed.

### Prerequisites



#### CAUTION

##### Possible loss of customer data

Use care when using this procedure. This procedure can cause the loss of customer data. Ensure that you have backed up the SIP Gateway application database before executing this procedure.

## Action

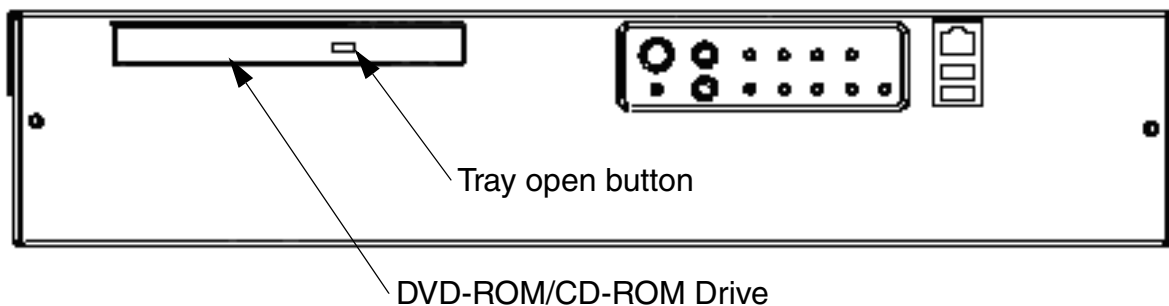
### *At the NCGL CLI or IEMS client*

- 1 If both units are at SN09U, and autopatching is enabled, turn off autopatching using procedure [Enabling/disabling autopatching on Session Server - Trunks application on page 1211](#).
- 2 The first action is determined by software delivery method:

| If media is delivered by | Do                                                                                                                                                                                                                                    |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESD                      | Perform only <a href="#">step 7</a> in procedure <a href="#">Extract an ISO image from an Electronic Software Delivery (ESD)</a> on page <a href="#">1136</a> and return here.<br><br>Go to <a href="#">step 7</a> in this procedure. |
| CD/DVD disk              | Continue to <a href="#">step 3</a> .                                                                                                                                                                                                  |

- 3 Log on to the inactive unit using a secure shell (ssh) and change to root user.
- 4 Ensure that the CD/DVD disk containing the SIP Gateway Application is inserted before continuing.

### *Front Panel*



- 5 To verify the upgrade is being performed from the inactive unit, type

**mtcccli status**

and press the Enter key,

```
$ mtcccli status
Unit 0 Status:
 Jam: Link0: Link1: PTPLink: OperationState:
Unit0 Inact no . Inact . Act . Enabled
Unit1 Act no . Inact . Act . Enabled
```

**Note:** The field after 'Unit0' or 'Unit1' identifies the status of the unit as it relates to being either active or inactive. In this example, 'Unit0 Inact' indicates that this is the inactive unit.

- 6 Mount the CD/DVD disk:

**mount /cdrom**

*The operating system can respond with the following warning:*

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

- 7 Install the SIP Gateway application:

**cd /**

**/cdrom/InstallApps SIPGW**

*The operating system responds:*

```
The NGSS Application layer is currently
installed. Do you wish to uninstall the previous
application and install the newer version? (yes,
no)
```

- 8 Confirm the prompt:

**yes**

```
Do you wish to change the tag name? (yes, no)
```

- 9 The operating system responds:

```

Get Session Server tag name to allow Multiple
HTTPS connection through SSPFS

```

```
Current Tag name: RTPNSST0
Do you wish to change the tag name (yes, no)
```

If it is desired to keep the default tag, enter no, and if not, enter yes and enter a new tag name.

**Note 1:** If the tag name is changed, ensure that an entry for the new tag name is added to the SPFS server web proxy.

**Note 2:** The following labels cannot be used for a remote tag name:

- spc
- ROOT
- webdav
- admin.xml
- manager.xml

**Note 3:** The database being used for restoration must match the software load on which the database is being restored. The database from a previous release may not work properly after upgrading the Session Server Trunks to a higher release resulting in malfunctions on the Provisioning page and performing Maintenance activities.

Starting in SN08, multiple Session Server - Trunks nodes, made up of two units per node, can be installed in the CS-LAN network. Therefore, each node installed on the CS-LAN must have its own unique remote tag name (used on both units in the node). Failure to follow this rule will prevent you from accessing a node's user interfaces properly. Refer to section "Using multiple tag names for multiple Session Server - Trunks nodes", part of procedure "Add a Session Server - Trunks node to the SPFS server web proxy," in *Session Server - Trunks Configuration Management*, NN10338-511, for more information about using multiple remote tag names.

*After pressing Enter, the software installation begins and messages scroll on the screen. No action is needed, and ignore any No such file or directory messages.*

- 10** After the installation completes, change directory:

```
cd /
```

---

**If**

the upgrade is successful and the following message displays,

InstallApps is complete.

WARNING!! A reboot of this unit is recommended in order to properly cleanup all resources from any previous installation. Refer to Nortel Networks Session Server - Trunking documentation for instructions on rebooting a unit.

the upgrade is not successful and the following error displays,

```
rm: Cannot remove directory
"/opt/apps/<dir name>" device or
resource busy
```

```
!!! UnInstallation Failed !!!
```

Please manually remove the affected files and perform Installation again

---

**Do**

continue with [step 11](#)

perform the substeps [step a](#) through [step c](#) below

- 
- a** Remove the file mount of the affected directory.

```
remove_fs -m /opt/apps/<dir name>
```

- b** Remove the directory.

```
rm -rf /opt/apps/<dir name>
```

- c** Repeat this procedure beginning at [step 7](#) to complete the SIP Gateway application installation.

- 11** Ensure file permissions are set correctly for patching

```
chmod 775 /opt/apps/bin/rsync
```

- 12** Unmount the CD/DVD disk or ISO image:

```
umount /cdrom
```

- 13** If both units are at SN09.1, and autopatching must be enabled, perform procedure [Enabling/disabling autopatching on Session Server - Trunks application on page 1211](#).

- 14** Perform procedure [Reboot a unit on page 1151](#) to perform a reboot of this unit. Monitor the reboot progress from the active unit of the CS 2000 NCGL Platform Manager.

- 15** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Acquiring Session Server Trunks patch files

---

### Purpose of this procedure

Use this procedure to identify and download Session Server Trunks (SIP Gateway application) patches from RPS.

### Limitations and restrictions

This is not a service impacting procedure.

### Prerequisites

Access to Regional Patch Selector (RPS) is required to acquire Session Server Trunks patches.

Customers who subscribe to automatic RPS patch delivery need to supply a Session Server Trunks userid to be used for transferring patches to the Session Server Trunks. The mtc userid may be used for this purpose, or if desired, a new userid can be defined using the following commands

```
useradd -g succssn -G succssn <ftpaccount>
```

```
passwd <ftpaccount>
```

where

**ftpaccount**

is the name of the userid to be added

This userid and password must be set up on all Session Server Trunks units that require automated RPS patch downloading.

### Action

#### Checking for the latest patches

##### *At a web browser*

- 1 Go to <http://www.nortel.com>.
- 2 Select Support & Training->Technical Support.
- 3 Select Software Downloads.
- 4 Select Browse Product Support.
- 5 Under Product Category, select Voice & IP Communications->Carrier VoIP Core.

- 6 From Choose a product, select Communication Server 2000 Session Server Trunks.
- 7 From Content, select Software. Then click on Go.
- 8 Select Filter and Sort.
- 9 Select the following:
  - Software type - Patches
  - Release - NGSS0xx  
where  
**NGSS0xx**  
is the software release associated with the patches being downloaded, such as NGSS091
  - Status - Released
- 10 Select Go for a list of all applicable Session Server patches.
- 11 This procedure is complete.



## Downloading the latest patches

### *At a web browser*

- 1 Perform procedure [Checking for the latest patches on page 1202](#) to create a list of applicable Session Server patches.
- 2 Click on the patch to download.
- 3 Click the link next to File Download to download the patch to a designated folder on the workstation.
- 4 Download any additional patches as required and exit the web browser application.
- 5 Using an SFTP application, FTP the patch files from the workstation to the /opt/swd/incoming directory on the active unit of the Session Server Trunks.
- 6 List the contents of the /opt/swd/incoming directory and verify all patch files have been moved to the directory by typing  
**ls**
- 7 This procedure is complete.

---

## Applying a Session Server Trunks patch

---

### Purpose of this procedure

Use these procedures to apply patch files to the Session Server Trunks (SIP Gateway application) active and inactive units.

The following describes two scenarios for applying Session Server Trunks patches:

1. Patching during an upgrade, where the inactive unit has been upgraded to the new load and one SwAct has been performed. The newly inactive unit is now running an old load and the newly active unit must be patched. When this is the case,
  - a. Acquire the patch on the active unit (the unit with the new load), move the patch to the /opt/swd/incoming directory of the active unit.
  - b. Apply only emergency patches (if any) plus dependency patches to the active unit using procedure [Applying a Session Server Trunks patch to the active unit on page 1206](#).
  - c. After a soak period, upgrade the inactive unit and perform the inactive unit reboot.
  - d. Apply the rest of the patches using the ALL option to the active unit using the procedure [Applying a Session Server Trunks patch to the active unit on page 1206](#).
  - e. From the active unit, apply all patches using the ALL option to the inactive unit using procedure [Applying a Session Server Trunks patch to the inactive unit on page 1209](#).
2. Patching not involved with an upgrade, where both units are at the same software release. When this is the case,
  - a. Acquire the patches on the active unit, move the patch to the /opt/swd/incoming directory of the active unit.
  - b. Apply the patches to both units using procedure [Applying a Session Server Trunks patch to the active unit on page 1206](#) and [Applying a Session Server Trunks patch to the inactive unit on page 1209](#). Patching directories are mirrored automatically by swchecker and there is no need to deliver the patches to both units.

### Limitations and restrictions

Patching activities must be completed on both units in the node.  
Patches must be applied in numerical order.

When patches are applied to the inactive unit, the inactive unit creates a log report. Since the log is on the inactive unit only, the Session Server GUI locally will not display it on the active unit's Session Server Customer Logs page, however this log is detected and reported by the IEMS. Patching logs are generated on the unit where the event occurs. Customers only looking at logs from the active unit will not see related logs in response to patching actions performed on the inactive unit.

## Prerequisites

The patch files must have already been put into the /opt/swd/incoming directory on the active unit through RPS.

## Action

Before Session Server Trunks patches can be applied or removed manually, the patches in the /opt/swd/incoming directory must pass security and validation checks and be moved to the /opt/swd/storage directory.

### Applying a Session Server Trunks patch to the active unit

#### *At the NGSS CLI*

- 1 Log on to the **active** unit and change to the root user.
- 2 Move the patches to the /opt/swd/storage directory by running the software checker command by typing  
**/opt/swd/bin/swchecker**
- 3 If a V status patch needs to be applied, use the -V option with the software checker command by typing  
**/opt/swd/bin/swchecker -V**
- 4 Change directory to the /opt/swd/bin directory by typing  
**cd /opt/swd/bin/**
- 5 Apply the Session Server patch to the **active** unit using the following command  
**./ngsspatch apply active <patchid-i386>**  
or when applying a list of patches use  
**./ngsspatch apply active ALL**

#### **Example**

```
./ngsspatch apply active
session_server_NGSS09MC2_i686-91.25.00-001.i386
```

The format of a Session Server patch id is as follows:  
session\_server\_<loadname>\_i686-<release>.<week>

#>.<sub-release>-<patch #>.i386. Session Server patches must be applied in ascending numerical order, that is, 001, 002, 003 and so forth or

./ngsspatch apply active ALL

- 6 If desired, the admin information and status of a validated patch can be displayed by typing the following command

**./ngsspatch display <patchid-i386>**

The following fields are displayed for the patch:

- Title - Title of the patch
- Description - Description of the issues addressed by the patch
- Software Type - NGSS\_PATCH
- RPS Product Component - RPS Product Component (NGSS09.1MC2)
- Product Component Version - RPS Product Component Version (NGSS\_09.1\_25\_mc2)
- Status - RPS patch status (V, R)
- CR - CRs included in the patch
- Installation Instructions - Any special instructions on patch installation
- Test Instructions - Instructions on how to test the patch
- Warning - Any warnings about the patch
- Category - RPS patch category (GEN, EMG, DBG)
- Auto Apply - Safe to auto apply the patch (Y or N)
- Activation Required - Patch requires activation (Y or N)
- Reboot Required - Reboot required after patch application (Y or N)

- 7 If desired, a list of all patches applied on the Session Server unit can be displayed by typing the following command

**./ngsspatch display ALL**

- 8 If desired, the status of all the Session Server Trunks patches can be displayed by typing the following command

**./ngsspatch inform list**

The following fields are displayed for each patch:

- ProdComp - RPS Product Component (NGSS09.1MC2)
- Patch ID - Patch Identifier  
(session\_server\_NGSS09MC2\_i686-91.25.00-001.i386)
- Status Date - Timestamp of the last status change that occurred for the patch
- USM - Indicates the patch utilizes the USM framework
- Category - RPS patch category (GEN, EMG, DBG)
- AutoApp - Safe to Auto Apply (Y or N)
- Warnings - Any warning about the patch (Y or N)
- RebootReq - Reboot required after patch application (Y or N)
- State - USM state of the patch
  - A - Applied to both units (duplex) or one unit (simplex),
  - P - Partial applied to one unit (duplex),
  - V - Passed swchecker aVailable
- NGSS (Y)

**9** This procedure is complete.

## Applying a Session Server Trunks patch to the inactive unit

### At the NGSS CLI

- 1 Log on to the **active** unit and change to the root user.
- 2 Change directory to the /opt/swd/bin directory by typing  
**cd /opt/swd/bin/**
- 3 Execute swchecker, if it has not already been done, by typing  
**/opt/swd/bin/swchecker**
- 4 Apply the Session Server patch to the **inactive** unit using the following command

```
./ngsspatch apply inactive <patchid-i386>
```

or when applying a list of patches use

```
./ngsspatch apply inactive ALL
```

#### Example

```
./ngsspatch apply inactive
session_server_NGSS09MC2_i686-91.25.00-001.i386
```

The format of a Session Server patch id is as follows:  
session\_server\_<loadname>\_i686-<release>.<week #>.<sub-release>-<patch #>.i386. Session Server patches must be applied in ascending numerical order, that is, 001, 002, 003 and so forth.

- 5 If desired, the admin information and status of a validated patch can be displayed by typing the following command

```
./ngsspatch display <patchid-i386>
```

The following fields are displayed for the patch:

- Title - Title of the patch
- Description - Description of the issues addressed by the patch
- Software Type - NGSS\_PATCH
- RPS Product Component - RPS Product Component (NGSS09.1MC2)
- Product Component Version - RPS Product Component Version (NGSS\_09.1\_25\_mc2)
- Status - RPS patch status (V, R)
- CR - CRs included in the patch
- Installation Instructions - Any special instructions on patch installation

- Test Instructions - Instructions on how to test the patch
  - Warning - Any warnings about the patch
  - Category - RPS patch category (GEN, EMG, DBG)
  - Auto Apply - Safe to auto apply the patch (Y or N)
  - Activation Required - Patch requires activation (Y or N)
  - Reboot Required - Reboot required after patch application (Y or N)
- 6** If desired, a list of all patches applied on the Session Server unit can be displayed by typing the following command
- `./ngsspatch display ALL`**
- 7** If desired, the status of all the Session Server Trunks patches can be displayed by typing the following command
- `./ngsspatch inform list`**
- The following fields are displayed for each patch:
- ProdComp - RPS Product Component (NGSS09.1MC2)
  - Patch ID - Patch Identifier  
(session\_server\_NGSS09MC2\_i686-91.25.00-001.i386)
  - Status Date - Timestamp of the last status change that occurred for the patch
  - USM - Indicates the patch utilizes the USM framework
  - Category - RPS patch category (GEN, EMG, DBG)
  - AutoApp - Safe to Auto Apply (Y or N)
  - Warnings - Any warning about the patch (Y or N)
  - RebootReq - Reboot required after patch application (Y or N)
  - State - USM state of the patch
    - A - Applied to both units (duplex) or one unit (simplex),
    - P - Partial applied to one unit (duplex),
    - V - Passed swchecker aVailable
  - NGSS (Y)
- 8** This procedure is complete.

---

## Enabling/disabling autopatching on Session Server - Trunks application

---

### Purpose of this procedure

This procedure is used to enable or disable autopatching on Session Server - Trunks application.

When autopatch is enabled, swchecker is invoked at the specified time to validate all R status patches in the /opt/swd/incoming/ directory. Autopatch then invokes the 'ngsspatch apply inactive/active ALL' command to apply all patches in the /opt/swd/storage directory. Session Server Trunks patches are applied in ascending numerical order to both units. Please note, if swchecker is invoked manually to validate any V status patches, these patches will be applied during the next scheduled autopatch cycle.

If any patches have been manually removed, they must be deleted from the database to prevent autopatch from re-applying these patches. To delete a patch, enter the following command:

```
/opt/swd/bin/ngssdeletepatch <patchid-i386.parcel>
```

Applying patches to the Session Server - Trunks application can be a manual or an automatic process. Manual patch application is the default, but the automatic patch (autopatch) application may be chosen. The autopatch command specifies the time and day(s) of the week that swchecker will automatically run. Once swchecker runs, 30 minutes later ngsspatch automatically runs to apply the patches.

The autopatch command schedules the swchecker and ngsspatch necessary for automatic patch application on the NGSS. If the OFF parameter is specified, the ngsspatch schedule is removed. If specified, the starting\_hour determines when the swchecker is scheduled to run. If not specified, the starting\_hour defaults to 3:00 am. The syntax of the autopatch command is as follows:

```
autopatch <off | on> [starting_hour] [day_of_the_weeks]
{0..23} {daily,sun,mon,tue,wed,thu,fri,sat}
```

Check customer logs in the Session Server Platform Manager GUI for an indication of the success or failure of the autopatch process.



When beginning an upgrade/rollback/reinstall:

- turn autopatching off if either unit has an SN09.1 load or greater and autopatching is set to on
- upgrade/rollback/reinstall both units
- after both units have been upgraded/rolled back/reinstalled (to an SN09.1 load or greater), apply any patches manually as needed/desired to both units
- execute the autopatch command on both units to the desired setting, if necessary

## Limitations and restrictions

After an upgrade/rollback/reinstall, the autopatch application is set to off by default.

## Prerequisites

The autopatch command must be run identically on both Session Server - Trunk units to ensure consistent behavior in the event of a SWACT.

## Action

### Enabling/disabling autopatching on Session Server - Trunks

#### *At the NCGL CLI*

- 1 Log in to either unit and change to the root user.
- 2 Execute autopatch from the /opt/swd/bin directory and type  
**./autopatch <parms>**  
or from the current directory type  
**/opt/swd/bin/autopatch <parms>**

Executing autopatch without any parms gives the current settings of when swchecker/ngsspatch are scheduled to run, whether it is turned on or off, and time and day of the week schedule as shown in the following example:

```
autopatch is currently on
swchecker is scheduled to run at 3:00
ngsspatch is scheduled to run at 3:30
This is scheduled to occur on these days of the
week: daily
```

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

| <b>If autopatching is to be</b> | <b>Do</b>              |
|---------------------------------|------------------------|
| enabled                         | Step <a href="#">4</a> |
| disabled                        | Step <a href="#">5</a> |

- 4** If the ON parameter is specified, the ngsspatch is scheduled to run 30 minutes after swchecker is scheduled to run.  
If specified, the day\_of\_the\_weeks parameter(s) identify which days of the week to run swchecker and ngsspatch.

If `day_of_the_weeks` not specified, this parameter defaults to daily, which means it will run 7 days a week. Multiple occurrences of this parameter are allowed. To enter a `day_of_the_weeks` parameter, the user must first specify both the `off/on` and the `starting_hour` parameter.

**Note:** This command must be executed identically on both NGSS units to ensure consistent behavior in the event of a swact.

**Example**  
**autopatch on 3**

This example shows that `swchecker` is scheduled to run daily at 3:00 am, and that `ngsspatch` is scheduled to run daily at 3:30 am.

**Example**  
**autopatch on 2 mon tue wed thu fri**

This example shows that `swchecker` is scheduled to run at 2:00am, and that `ngsspatch` is scheduled to run at 2:30am, but both will only run on week days.

Go to step [6](#).

- 5 To disable autopatching, type

**autopatch off**

If specified, the `starting_hour` and/or the `day_of_the_weeks` parameter(s) can be used to identify the hour and days of the week `ngsspatch` is to run. If no hour is specified, the default is 3:00 am. If no day of the week is specified, `ngsspatch` runs daily.

**Note:** This command must be executed identically on both NGSS units to ensure consistent behavior in the event of a swact.

- 6 Execute the same action on the other unit as was initiated in step [3](#).
- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Verify synchronization status

### Purpose of this procedure

Use this procedure to determine the synchronization status of the two units.

### Limitations and restrictions

There are no restrictions for performing this procedure.

### Prerequisites

There are no prerequisites for performing this procedure.

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

- 1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu:



- 3 At the bottom of the SIP Gateway Maintenance panel, locate and click the QueryInfo button.

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |
| <div>Refresh</div> <div>QueryInfo</div>                |                                         |

- 4 The synchronization status of the units is displayed at the bottom of the query results panel.

If the units are not in sync, check for alarm conditions.

|                                                 |
|-------------------------------------------------|
| Last Performed Operation: Query Number of Calls |
| Result: Passed                                  |
| Number Of Active Calls: 0                       |
| SIP Gateway is: In Sync                         |
| SIP Gateway Cold SwAct                          |

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Enable a system SwAct (Unjam)

---

### Purpose of this procedure

The Unjam command is used to manually enable a SwAct (switch of activity) of the active and stand-by units by allowing the two units to toggle their operational states.

### Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as replacing a faulty standby unit or upgrading a standby unit.

#### ATTENTION

This procedure can only be performed from the active unit.

### Prerequisites

There are no prerequisites for performing this procedure.

### Action

#### ***At the CS 2000 NCGL Platform Manager or IEMS client***

- 1 Select Succession Communication Server NCGL Platform Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Click the Node Maintenance link.  
*The Node Maintenance page opens in the right side frame.*

- 3 Determine if the Jam State of the standby unit is Yes or No. If it is No, then the unit is already unjammed and you are done with this procedure. If it is Yes, then continue with [step 4](#).

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | yes       |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                      |
|---------------------------------------------------------------------|--------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Unjam"/> |

- 4 Click the Unjam button.
- 5 Click OK to close the dialog box.
- The system responds with a dialog window:*
- Info: Unjam - Command passed.
- Then the Jam State becomes no and the Jlnact alarm clears.*
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Invoke a maintenance SWACT of the Session Server Trunks platform

### Purpose of this procedure

This procedure manually performs a maintenance SWACT (switch of activity). A SWACT gracefully transitions call processing activity from the active unit to the standby unit without first reloading and reinitializing the SIP Gateway application on the standby unit.

Use this procedure as a standalone task or as part of a maintenance or fault clearing activity like replacing a faulty standby unit or a high-level activity such as upgrading a standby unit.

**Note:** An automatic failover SWACT can be initiated by the platform NCGL in cases of critical faults on the active unit. For more information about conditions required for a SWACT, refer to “Understanding conditions for a SWACT” in the *Session Server Trunks Security and Administration*, NN10346-611.

### Limits and Restrictions

#### ATTENTION

Perform a maintenance SWACT only when both the active and standby units are operationally enabled and their databases are synchronized.

You cannot perform a SWACT if the inactive unit is jammed. If the unit Jam state is jammed, refer to procedure [Enable a system SwAct \(Unjam\) on page 1217](#) to unjam the unit.

#### ATTENTION

Logins to the Session Server Trunks do not survive a platform SWACT.

During an unforced maintenance SWACT, new calls are set up on the standby unit, while existing calls continue to be processed on the active unit until they are terminated. SIP-T calls in the process of setup during a SWACT can be lost. Over SIP-T trunks, the far end continues to receive the setup alert (ringing) until one of the following events occur:

- The end user answers and terminates the call.
- A GWC system audit runs and clears the trunks (once every 10 minutes).



## Prerequisites

If you are executing a Forced SWACT, confirm that there are no alarm conditions.

## Action

### ***At the Session Server Manager or IEMS client of the active unit***

- 1 Select Succession Communication Server NCGL Platform Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Click the Node Maintenance link.  
*The Node Maintenance page is displayed.*
- 3 Refer to the table in section [Additional status information on page 1222](#) to review the description of the various fields of the Node Maintenance page.

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                    |
|---------------------------------------------------------------------|------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Jam"/> |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | no        |

- 4 To SWACT the units, click the SWACT button.

or

To override any pre-SWACT queries, first click the Force checkbox, then click the SWACT button.

**CAUTION**

Possible service interruption

Due to the risk for loss of data and service outage, it is recommended that the Forced SWACT option not be used except when instructed by your Nortel customer support representative.

A forced SWACT overrides any SWACT pre-checks and is not recommended. SWACT prechecks monitor the inactive unit for critical faults on the platform, which will prevent a SWACT. In addition, the precheck ensures that the SIP Gateway application is in-sync. A SWACT force can result in a full service outage on the node if the inactive unit is not in-sync. There is potential for loss of provisioned data if a SWACT to an unstable unit is completed.

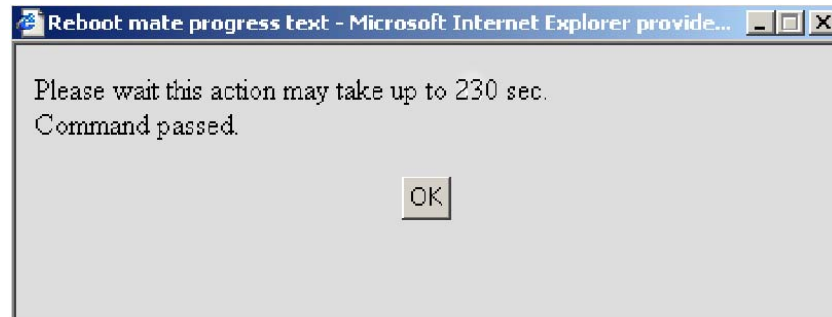
|                                                                     |        |                                    |
|---------------------------------------------------------------------|--------|------------------------------------|
| Enabled                                                             | Active | no                                 |
| <b>Maintenance Actions</b>                                          |        |                                    |
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force |        | <input type="button" value="Jam"/> |

*The system responds:*

Are you sure you wish to swact? This may cause a service interruption to applications running on this server. Click OK to confirm server swact or cancel to abort.

- 5 Click Yes to confirm either the SWACT or forced SWACT.

*The system responds with the following message box:*



- 6 Click OK to close the dialog box.
- 7 Observe the Activity field for each unit. Each unit's activity status (whether Active or Inactive) swaps.
- 8 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Additional status information

The following table describes the various fields of the Node Maintenance panel.

| Field                                  | Description                                                                                                                                                                                                                                                   |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operation State (unit 0 or 1)          | operational state of the platform software, either enabled or disabled                                                                                                                                                                                        |
| Activity (unit 0 or 1)                 | activity state of the platform software, either active or inactive                                                                                                                                                                                            |
| Jam State (active unit only)           | indicates whether or not the unit has been "jammed", preventing the standby unit from being able to become active, regardless of any failures on the active unit. States are either jammed, where a SWACT is disabled, or unjammed, where a SWACT is enabled. |
| Maintenance Actions (active unit only) | maintenance panel for performing node SWACT activity and to jam or unjam node activity switches.                                                                                                                                                              |

---

## Copy security certificates to the mate unit

---

### Purpose of this procedure

The following procedure is used to copy security certificates from one unit to the mate unit.

Use this procedure any time new security certificates are created, or when the system is changed from using self-signed certificates to CA-signed certificates.

### Limitations and Restrictions

There are no restrictions for performing this procedure.

### Prerequisites

New certificates, either self-signed or CA-signed must be installed on the inactive unit.

### Action

Perform the following steps to complete this procedure.

#### ***At the NCGL CLI or IEMS client***

- 1 Log in to the active unit and change to the root user.
- 2 Change directories to the security certificates level:  
`cd /opt/base/share/ssl`
- 3 Copy the security related files to the mate unit:  
`scp server.key mtc@mateblade:/users/mtc`  
`scp certificate.keystore mtc@mateblade:/users/mtc`  
`scp server.crt mtc@mateblade:/users/mtc`  
`scp trusted.crt mtc@mateblade:/users/mtc`

**Note:** For initial connections to the mate unit, confirm that you want to continue connecting by entering yes. Each instance of the scp command requires entering the password for the mtc account.

#### ***At your workstation CLI or IEMS client***

- 4 Log in to the mate unit and change to the root user.
- 5 Change directories to /users/mtc:  
`cd /users/mtc`

**6** Determine the next action:

| <b>If the software version is</b> | <b>Do</b>                                                                                                                                                                                             |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SN08                              | Continue to <a href="#">step 7</a>                                                                                                                                                                    |
| SN09 or newer                     | Enter the <b>cert_mgnt</b> command and select option 3. Performing this action will copy the files to the correct location and set the correct ownership and permissions. This procedure is complete. |

**7** Move the files from the /users/mtc directory to the /opt/base/share/ssl directory:

```
mv server.key /opt/base/share/ssl
mv certificate.keystore /opt/base/share/ssl
mv server.crt /opt/base/share/ssl
mv trusted.crt /opt/base/share/ssl
```

**Note:** If necessary, confirm overwriting any existing files by typing y and pressing Enter.

**8** Change directories to the security certificates level:

```
cd /opt/base/share/ssl
```

**9** Change the owner and group to root for all files:

```
chown root:root *
```

**10** Set the file permissions:

```
chmod 600 server.key
chmod 600 certificate.keystore
chmod 644 server.crt
chmod 644 trusted.crt
```

**11** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

If you did not complete this procedure as part of an upgrade, you must complete procedure “Apply security certificates” in the *Session Server - Trunks Security and Administration*, NN10346-611.



## Policy Controller upgrade

The Policy Controller provides facilities for general application maintenance and network topology provisioning. The management function provides tools and interfaces to monitor network resource usage, as well as to define the relationship between subscriber needs and network resource availability.

Policy-based call admission control decisions take into account the requester's resource reservation request and available capacity to determine whether or not to accept the request. The request for policy control may contain one or more policy elements. Policy control functions include:

- Bandwidth Management
- Call Admission Control

In the event you need or want to downgrade the Policy Controller, refer to [Performing an emergency maintenance release rollback on page 1244](#).

### What's new in Policy Controller Upgrades in (I)SN09U

#### Feature changes

In SN09U, there are no feature changes that affect the Policy Controller upgrade.

#### Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U

## Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

### Time to complete an upgrade

The following table lists the tasks to upgrade Policy Controller software and the estimated time to complete each task.

#### Estimated time to complete a software upgrade

| Task                         | Time       |
|------------------------------|------------|
| Preparing for the upgrade    | 30 minutes |
| Upgrading the software       | 2 hours    |
| Completing the upgrade       | 30 minutes |
| Total estimated upgrade time | 3 hours    |
| Performing a rollback        | 2 hours    |

### Service impacts

The upgrade of Policy Controllers software does not impact service.

### Additional information

The following additional information applies to performing a maintenance release upgrade or rollback of an MR upgrade.

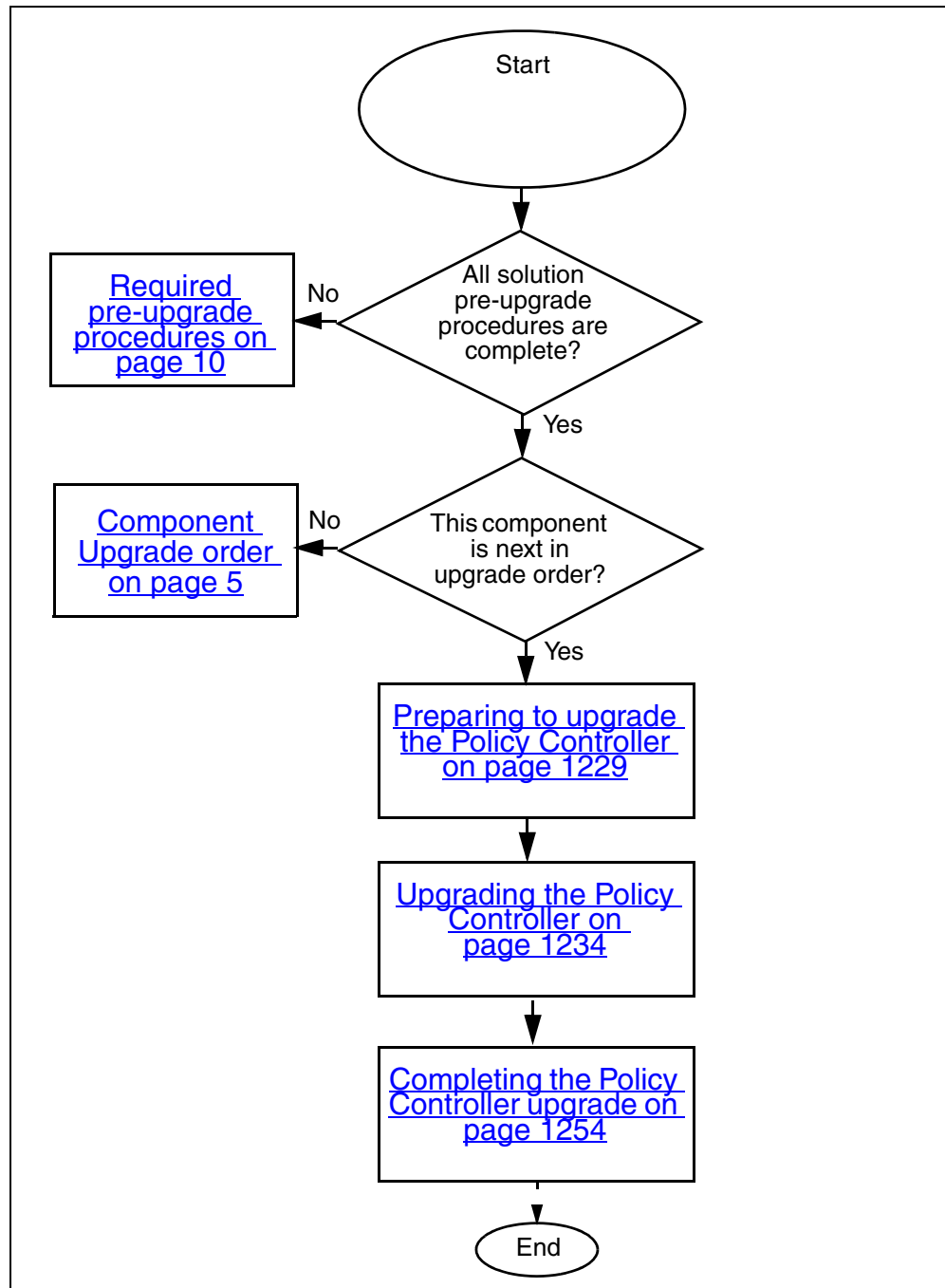
- While an MR upgrade is an in-service upgrade, performing an emergency rollback of a maintenance release is an out-of-service activity. During an out-of-service upgrade, the Policy Controller will stop functioning as a Network Virtual Call Admissions Control (NVCAC) device. All Network VCAC processes will be affected and calls on the CS 2000 will continue without the Virtual Call Admission Control function.
- Only NCGL Platform patching is supported for maintenance releases. Policy Controller application patches are not supported.
- Patches can only be applied using the CLI (command line interface).
- If there have been changes to the Policy Controller database since you last backed it up, do not use the backup copy that contains the

old database to restore it. The result can be file corruption, partially imported data, or a complete failure of the restore.

### **Policy Controller upgrade tasks**

This taskflow shows you the sequence of tasks you perform to upgrade this component.



**Policy Controller upgrade tasks**

---

## Preparing to upgrade the Policy Controller

---

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

Perform the previous required upgrade according to the order listed in the table [Component Upgrade Order on page 6](#). The required upgrade is the previous component in the list according to your network configuration.

### Applying a maintenance release upgrade

This section describes how to perform:

- an in-service maintenance release (MR) upgrade of the Policy Controller units
- a rollback of a partial or complete MR upgrade in cases where a maintenance release fails or causes problems with the system.

#### Maintenance release upgrade strategy

There are two types of Maintenance releases for the Policy Controller: An MR type for the NCGL platform and another MR type for the Policy Controller application.

- **An NCGL platform MR** consists of release notes, CS 2000 NCGL Platform Manager software, NCGL software and optional CS 2000 NCGL Platform Manager patches.

Using the CS 2000 NCGL Platform Manager GUI you can select an MR image to upgrade from. You can upgrade the Policy Controller load from the local DVD-ROM drive, from an ISO image located on a remote system, or from a local file on the Policy Controller disk drive. Space is available on the local hard drive to maintain approximately 2 loads in case fallback to a previous load is necessary. Partial and complete rollbacks of a failed upgrade can be performed.

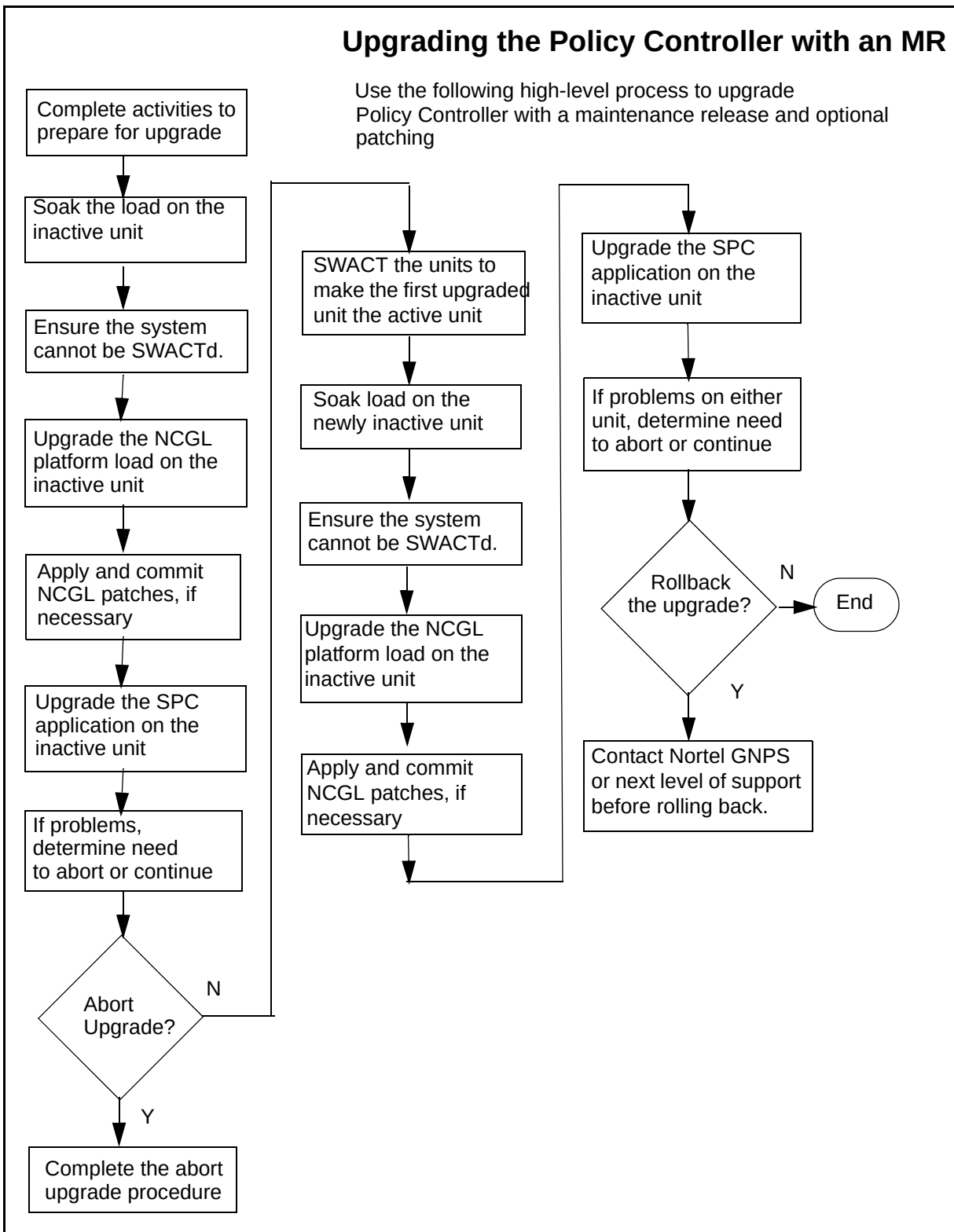
- **A Policy Controller MR** consists of release notes, CS 2000 NCGL Platform Manager software, Policy Controller application software and optional CS 2000 NCGL Platform Manager patches.

Using both the CS 2000 NCGL Platform Manager GUI and the Policy Controller command line interface (CLI), you can upgrade the Policy Controller application.

Refer to the following diagram for a high-level view of the upgrade process for the Policy Controller units.

## Upgrading the Policy Controller with an MR

Use the following high-level process to upgrade Policy Controller with a maintenance release and optional patching



## Software installation methods for maintenance releases

You can upgrade the Policy Controller NCGL load from the local DVD-ROM drive, or from an ISO image located on a remote system, or copied to a local directory. The following upgrade protocols (methods) are selectable from the Policy Controller Manager GUI:

- Local CDROM - the local DVD-ROM drive (labelled as the local CD-ROM).
- Local file - an iso image, or load.tgz file copied from the local DVD-ROM drive copied to the hard drive using the secure copy program, **scp**, to transfer the data.
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP service. If the workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in clear text format across the network. This is not a recommended method.
- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service. This is not a recommended method.

You can upgrade the Policy Controller application from the local DVD-ROM drive, or from an ISO image copied to a local directory. Most of the time the MR for the Policy Controller application is on the same DVD-ROM disk or copied ISO image as the NCGL platform load; however, some customers may receive a separate maintenance release load that contains an MR only for the Policy Controller application. Consult your release notes for details.

## Removing older NCGL bootload versions

By default, the Policy Controller units retain previous bootloads. Older bootloader versions may be manually removed by clicking the **Remove** button using the Web GUI (see graphic below). You cannot delete the bootloader that is set to be the default bootloader, nor can you delete the currently running bootloader.

If a bootloader image upgrade is requested and insufficient disk space is available in the `/boot` directory, the NCGL software deletes the oldest bootloader from the `/boot` directory and performs the requested bootloader image upgrade. The system cannot delete a bootloader that is set to be the default bootloader.

| Bootload Management |                  |        |
|---------------------|------------------|--------|
| Bootload            | Maintenance      |        |
| 4.0.0.0303171003    | Default Bootload |        |
| 4.0.0.0303101433    | Set default      | Remove |
| 4.0.0.0303051030    | Set default      | Remove |
| 4.0.0.0303051012    | Set default      | Remove |

## Action

Complete the steps in the following procedure.

### Preparing to upgrade the Policy Controller

#### *At your workstation*

- 1 If you have purchased security certificates from a Certificate Authority, then ensure that you have made a backup copy of the following security certificate files: server.key, server.crt and certificate.keystore. These files are located in directory /opt/base/share/ssl.  
  
Otherwise, transfer a copy of the default security certificate files (same names and location as above) to a secure location on a remote server. For more information on Policy Controller security certificates, refer to *Policy Controller Security and Administration*, NN10434-611.
- 2 Backup the Policy Controller application database on the active unit using procedure [Perform a manual backup of the Policy Controller database on page 1366](#).
- 3 Acquire the appropriate maintenance release software from Nortel either using ESD delivery to a customer dropbox/repository server or from a maintenance release DVD-ROM disk.
- 4 If performing a maintenance release upgrade with an ISO image acquired using ESD, complete procedure [Extract an ISO image from an Electronic Software Delivery \(ESD\) on page 1255](#) to copy ISO files to hard drive of each unit.

- 5 Use procedure [View release notes for a maintenance release on page 1258](#) to check release notes for the applicability of the MR.
- 6 Locate and have available the original Policy Controller software DVD-ROM along with a copy of the existing version of the Policy Controller application installed on your system. The existing version may be from the last maintenance release image installed from a DVD-ROM or an ESD downloaded image file.
- 7 Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
- 8 You have completed this high-level procedure. Proceed to [Upgrading the Policy Controller on page 1234](#).

## Upgrading the Policy Controller

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

You have completed procedure [Preparing to upgrade the Policy Controller on page 1229](#).

### Upgrade paths

This procedure provides the high-level steps to perform a maintenance release upgrade.

#### Upgrade strategy

The current release of the NCGL platform software can be patched or upgraded by way of a maintenance release upgrade, while the current release of the Policy Controller application software can be upgraded only by way of a maintenance release upgrade.

Activities and procedures are available in this document for performing patching and maintenance release upgrade activities as well as activities for aborting an upgrade. Release notes that are provided with the patch files or maintenance release images offer additional information about performing these activities.

#### Document References

You need the following documents for this upgrade procedure.

| Document name                                 | Document number |
|-----------------------------------------------|-----------------|
| Policy Controller Security and Administration | NN10434-611     |
| Policy Controller Configuration Management    | NN10432-511     |
| Policy Controller Fault Management            | NN10438-911     |

### Tools and utilities for maintenance release upgrades

You upgrade the Policy Controller by using different interfaces depending on the procedure required. The interface required is described at the beginning of each procedure. Use the following interfaces to perform the procedures in this NTP and are accessed

through network workstations or the Integrated Element Management System (IEMS):

- The Policy Controller Manager GUI, a client web browser application, launched from the IEMS client.
- The CS 2000 NCGL Platform Manager GUI, a client web browser application, launched from the IEMS client.
- The NCGL command line interface (CLI).

### **Interfaces used to apply maintenance releases**

The following interfaces are used in applying maintenance releases:

- The Policy Controller Manager GUI, a client web browser application, launched from the IEMS client.
- The CS 2000 NCGL Platform Manager GUI, a client web browser application, launched from the IEMS client.
- The NCGL command line interface (CLI)

### **Interfaces used to apply patches to the NCGL platform**

The NCGL Platform Patching is performed manually using the NCGL command line interface (CLI) available on each NCGL node to be patched.

## **Troubleshooting maintenance release upgrades**

If the system becomes unstable after an upgrade or after aborting an upgrade, contact GNPS for assistance.

## **Action**

Complete the following step-by-step procedure, in the order listed, to perform an in-service maintenance release upgrade and optional patching of the NCGL platform and to perform a maintenance release upgrade of the Policy Controller application.

### **Perform a maintenance release upgrade**

#### ***Upgrade the NCGL platform load on first unit***

- 1 Determine what version of the NCGL platform load is currently installed on your Policy Controller node by going to the **System Info** page of the CS 2000 NCGL Platform manager and using procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#).

Determine what version of the Policy Controller application software (listed as Policy Controller load info) is currently



installed on your Policy Controller node using procedure [Determine the current version of software loads on page 1285](#).

- 2 Compare the current version of the NCGL Platform Load installed with the MR release notes to determine if you must upgrade the NCGL platform load with a newer maintenance release. Also use to determine if you need to upgrade to a previously released MR first.

If the MR contains a newer version of the NCGL platform load than what is currently installed, then proceed with this upgrade. If not then you do not need a maintenance release upgrade. Skip to [step 8](#) to determine if there are any NCGL patches that need to be applied and committed on the inactive unit.

- 3 If applying an MR upgrade using a DVD-ROM, insert the disk into the disk drive of the inactive unit.
- 4 Log onto the active unit and use procedure [Prevent a system SwAct \(Jam\) on page 1262](#) to jam the units.
- 5 Log onto the inactive unit and upgrade the NCGL platform software using procedure [Upgrade Policy Controller NCGL platform software on page 1287](#).
- 6 Log into the active Policy Controller unit, use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure [Reboot a Policy Controller unit on page 1294](#) for assistance.
- 7 After the inactive unit completes rebooting, log into the inactive unit, use the CS 2000 NCGL Platform Manager and go to the **System Info** page to verify that the Current version of the NCGL software matches the expected new version. Use procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#) for assistance with this task.

#### ***Apply and commit NCGL patches to the first unit***

- 8 Use procedure [Patching the NCGL platform on page 1248](#) to apply and commit NCGL patches to the inactive unit.

#### ***Upgrade the Policy Controller application software on the first unit***

- 9 On the inactive unit, upgrade the Policy Controller application software using procedure [Upgrade/rollback/reinstall the Policy Controller application on page 1312](#).

- 10 Log into the inactive unit's CLI and verify that the current version of the Policy Controller application matches the expected new version by executing the following command:

```
$ cat /opt/apps/webint/version_info.txt
```

***Activate and soak the new load on the first unit***

- 11 From the active unit, verify that the Policy Controller application databases on both units have synchronized using procedure [Verify synchronization status of Policy Controller units on page 1324](#)
- 12 Use procedure [Enable a system SwAct \(Unjam\) on page 1327](#) to unjam the units.
- 13 As applicable to your site, test new software on the inactive unit. Testing may include:
- placing test calls per your site upgrade guidelines
  - applying a minimum live traffic soak time for the unit per your site upgrade guidelines
  - Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing
- Only go forward to SwAct when all the tests have passed.
- 14 From the active unit perform a SwAct of the units using procedure [Invoke a maintenance SwAct of the Policy Controller platform on page 1320](#).
- 15 As applicable to your site, test new software on upgraded unit, now active. Testing may include:
- placing test calls per your site upgrade guidelines
  - applying a minimum live traffic soak time for the unit per your site upgrade guidelines
  - Refer to the *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.

**Note:** Perform a check to ensure the system has not SwActed automatically after the software upgrade. An automatic system SwAct could be initiated if a fault is detected

by the system. This will be indicated in the alarms and logs. However, it is still advisable to use the procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#) to confirm the active units software load is as expected before proceeding to upgrade the second Policy Controller unit.

- 16** If all software tests are successful, continue with the next step in this procedure to upgrade the second (mate) Policy Controller unit (now inactive).

Otherwise, if the active unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure and complete procedure [Aborting a maintenance release upgrade on page 1242](#) and contact your next level of support or Nortel GNTS.

### ***Upgrade the NCGL platform load on second unit***

- 17** Verify that all applicable activities in Section [Preparing to upgrade the Policy Controller on page 1229](#) have been completed for the second unit.
- 18** Determine what version of the NCGL platform load is currently installed on the second unit using procedure by going to the **System Info** page of the CS 2000 NCGL Platform manager, using procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#).

Determine what version of the Policy Controller application software (listed as Policy Controller load info) is currently installed on the second unit using procedure [Determine the current version of software loads on page 1285](#).

- 19** Compare the current version of the NCGL Platform Load installed with the MR release notes to determine if you must upgrade the NCGL platform load on the second unit with a newer maintenance release.

If the MR contains a newer version of the NCGL platform load than what is currently installed, then proceed with this upgrade. If not then you do not need to apply a maintenance release upgrade, skip to [step 22](#) to perform any necessary patching of this unit.

- 20** If applying an MR upgrade using a DVD-ROM, insert the disk into the disk drive of the inactive unit.
- 21** Log onto the active unit and use procedure [Prevent a system SwAct \(Jam\) on page 1262](#) to verify that the units are still jammed. If they are not, then jam the units.

- 22 Log onto the inactive unit and upgrade the NCGL platform software using procedure [Upgrade Policy Controller NCGL platform software on page 1287](#).
- 23 Log into the active Policy Controller unit, use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure [Reboot a Policy Controller unit on page 1294](#) for assistance.
- 24 After the inactive unit completes rebooting, log into the inactive unit, use the CS 2000 NCGL Platform Manager and go to the **System Info** page to verify that the Current version of the NCGL software matches the expected new version. Use procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#) for assistance with this task.

***Apply and commit NCGL patches to the second unit***

- 25 Use procedure [Patching the NCGL platform on page 1248](#) to apply and commit NCGL patches to the inactive unit.

***Upgrade the Policy Controller application software on the second unit***

- 26 On the inactive unit, upgrade the Policy Controller application software using procedure [Upgrade/rollback/reinstall the Policy Controller application on page 1312](#).
- 27 Log into the inactive unit's CLI and verify that the current version of the Policy Controller application matches the expected new version by executing the following command:

```
$ cat /opt/apps/webint/version_info.txt
```

***Activate and soak the new load on the second unit***

- 28 From the active unit, verify that the Policy Controller application databases on both units have synchronized using procedure [Verify synchronization status of Policy Controller units on page 1324](#)
- 29 Use procedure [Enable a system SwAct \(Unjam\) on page 1327](#) to unjam the units.

- 30** As applicable to your site, test new software on the inactive unit. Testing may include:
- placing test calls per your site upgrade guidelines
  - applying a minimum live traffic soak time for the unit per your site upgrade guidelines
  - Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing
- Note:** Only go forward to SwAct when all the tests have passed.
- 31** From the active unit perform a SwAct of the units using procedure [Invoke a maintenance SwAct of the Policy Controller platform on page 1320](#).
- 32** As applicable to your site, test new software on the upgraded unit, now active. Testing may include:
- placing test calls per your site upgrade guidelines
  - applying a minimum live traffic soak time for the unit per your site upgrade guidelines
  - Refer to the *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
- Note:** Perform a check to ensure the system has not SwActed automatically after the software upgrade. An automatic system SwAct could be initiated if a fault is detected by the system. This will be indicated in the alarms and logs. However, it is still advisable to use the procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#) to confirm the active units software load is as expected before proceeding to upgrade the second Policy Controller unit.
- 33** If all software tests are successful, continue with the next step in this procedure.
- Otherwise, if the active unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure. Go to and complete the steps in procedure [Emergency maintenance release rollback on page 1244](#) and

- contact your next level of support, Nortel GNPS, or Nortel's emergency response.
- 34** From the active unit, verify that the Policy Controller application databases on both units have synchronized using procedure [Verify synchronization status of Policy Controller units on page 1324](#)
  - 35** Monitor the system for an appropriate period per your site guidelines before declaring this maintenance release complete.
  - 36** Refer to procedure "Viewing managed object details" in *IEMS Configuration Management*, NN10330-511. Locate the Policy Controller element associated with the node you upgraded and select the correct major version number for the Device Version field
  - 37** You have completed the maintenance release upgrade procedure. Proceed to [Completing the Policy Controller upgrade on page 1254](#).

## Aborting a maintenance release upgrade

### ATTENTION

This procedure assumes that you have not upgraded the second Policy Controller unit in the node with the maintenance release. If you have already upgraded both units with the maintenance release, then contact your next level of support or Nortel GNPS.

Complete the following steps, in the order indicated, to abort a maintenance release upgrade procedure in progress.

### Aborting a maintenance release upgrade

- 1 If necessary, use procedure [Enable a system SwAct \(Unjam\) on page 1327](#) to unjam the units.
- 2 If necessary, complete procedure [Invoke a maintenance SwAct of the Policy Controller platform on page 1320](#) to revert call processing to the un-upgraded unit (the unit that is operating with the pre-maintenance release load).
- 3 Use procedure [Prevent a system SwAct \(Jam\) on page 1262](#) to verify that the units are jammed. If they are not, then jam the units.
- 4 Log onto the inactive unit and use procedure [Rollback a Policy Controller NCGL platform software upgrade on page 1330](#) to set the default NCGL bootfile to the pre-MR load (the load the unit operated on prior to the maintenance release upgrade).
- 5 Log into the active Policy Controller unit, use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a FORCED reboot (RebootMate) of the inactive (mate) unit. Refer to procedure [Reboot a Policy Controller unit on page 1294](#) for assistance.  
  
**Note:** All committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying patches is not required.
- 6 On the inactive unit CLI use the pre-MR DVD-ROM or pre-MR Policy Controller application ISO image to downgrade the Policy Controller application software using procedure [Upgrade/rollback/reinstall the Policy Controller application on page 1312](#).
- 7 From the active unit, verify that the Policy Controller application databases on both units have synchronized using procedure

[Verify synchronization status of Policy Controller units on page 1324.](#)

- 8 Once the databases are in sync, release the JAM on the units using procedure [Enable a system SwAct \(Unjam\) on page 1327](#).
- 9 Complete procedure [Invoke a maintenance SwAct of the Policy Controller platform on page 1320](#) to make the downgraded unit active.
- 10 As applicable to your site, test the software on the downgraded unit, now active. Testing may include:
  - placing test calls per your site upgrade guidelines
  - applying a minimum live traffic soak time for the unit per your site upgrade guidelines
  - Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
- 11 Monitor the system for an appropriate period per your site guidelines before declaring this maintenance release complete.

If all software tests are successful, continue with the next step.

Otherwise, if the active unit (with downgraded load) experiences problems with call processing, perform the following tasks in order:

- complete procedure [Invoke a maintenance SwAct of the Policy Controller platform on page 1320](#)
  - complete procedure [Prevent a system SwAct \(Jam\) on page 1262](#)
  - contact your next level of support or Nortel GNPS.
- 12 You have completed this high-level abort procedure.



## Emergency maintenance release rollback



### CAUTION

This is a service affecting procedure. Performing an emergency maintenance release rollback causes approximately a one hour service interruption.

Complete the following steps, in the order indicated, to roll back a maintenance release upgrade that has been performed on both Policy Controller units in the node.

### Performing an emergency maintenance release rollback

- 1 Locate and have available the previous Policy Controller software DVD-ROM or an ESD downloaded image file of the previous maintenance release.

Ensure that you have available a recent backup copy of the Policy Controller application database, for the downgraded software version.

**Note:** There is a potential for database corruption if the database backup is from a different software load to the load being restored.

- 2 If performing a maintenance release rollback using an ISO image acquired using ESD, verify that the applicable ISO files are copied to the hard drive of each unit. If necessary, use procedure [Extract an ISO image from an Electronic Software Delivery \(ESD\) on page 1255](#).
- 3 Log onto the active unit CLI and complete procedure [Drop database synchronization for the Policy Controller application on page 1334](#) executed from the current release of the Policy Controller software DVD-ROM or from the currently installed ISO image.

**Note:** Once executed, this script drops call processing and application database synchronization between the active and inactive units. The Policy Controller application maintains this non-synchronized state until a manual SwAct is performed, later in the procedure.

- 4 Log onto the inactive unit and use procedure [Rollback a Policy Controller NCGL platform software upgrade on page 1330](#) to set the default NCGL bootfile to the pre-MR load (the load the unit operated on prior to the maintenance release upgrade).  
**Note:** All committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying patches is not required.
- 5 Using the CS 2000 NCGL Platform Manager, go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure [Reboot a Policy Controller unit on page 1294](#) for assistance.
- 6 On the inactive unit, rollback the Policy Controller application software. Complete procedures [Upgrade/rollback/reinstall the Policy Controller application on page 1312](#).
- 7 On the inactive unit, prepare to restore a backup copy of the Policy Controller application database using procedure [Prepare for a database restore on a Policy Controller unit on page 1357](#).
- 8 On the inactive unit (the rolled back unit), install the backup copy of the Policy Controller application database using procedure [Perform a database restore to a Policy Controller unit on page 1369](#).
- 9 Perform a SwAct (Force) of the units by completing procedure [Invoke a maintenance SwAct of the Policy Controller platform on page 1320](#) to make the downgraded unit active.
- 10 As applicable to your site, test the software on the downgraded unit, now active. Testing may include:
  - placing test calls per your site upgrade guidelines
  - applying a minimum live traffic soak time for the unit per your site upgrade guidelines
  - Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” and to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
- 11 Monitor the system for an appropriate period per your site guidelines before declaring this rollback complete.  
If all software tests are successful, continue with the next step.

Otherwise, if the active unit (with rolled back load) experiences problems with call processing, STOP executing the procedure and contact your next level of support or Nortel GNPS.

- 12 Use procedure [Prevent a system SwAct \(Jam\) on page 1262](#) to jam the units.
- 13 Log onto the inactive unit and use procedure [Rollback a Policy Controller NCGL platform software upgrade on page 1330](#) to set the default NCGL bootfile to the pre-MR load (the load the unit operated on prior to the maintenance release upgrade).

**Note:** All committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying patches is not required.

- 14 Use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure [Reboot a Policy Controller unit on page 1294](#) for assistance.
- 15 On the inactive unit, rollback the Policy Controller application software using procedure [Upgrade/rollback/reinstall the Policy Controller application on page 1312](#).
- 16 From the active unit, verify that the Policy Controller application databases are synchronizing using procedure [Verify synchronization status of Policy Controller units on page 1324](#).

If they are synchronizing then go to [step 18](#).

If they are not synchronizing then go to the next step.

- 17 Use procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#) to check the status of the inactive unit to determine why database synchronization is not taking place by reviewing existing faults and logs.

Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.

- 18 Once the databases are in sync, release the JAM on the units using procedure [Enable a system SwAct \(Unjam\) on page 1327](#).
- 19 Perform a SwAct of the units by completing procedure [Invoke a maintenance SwAct of the Policy Controller platform on page 1320](#) to make the downgraded unit active.
- 20 Monitor the system for an appropriate period per your site guidelines before declaring this maintenance release rollback complete.

If all software tests are successful, continue with the next step.

Otherwise, if you continue to experience problems with call processing, contact your next level of support or Nortel GNPS.

**21** You have completed this emergency rollback procedure.

**Troubleshooting maintenance upgrades**

If the system becomes unstable after an upgrade or after aborting an upgrade, contact GNPS for assistance.

## Patching the NCGL platform

Only the NCGL platform is patchable.

Platform patching activities occur when new patches become available that must be installed. They also occur when an older patch becomes obsolete and must be removed. Installing some patches may be optional.

### Patching strategy

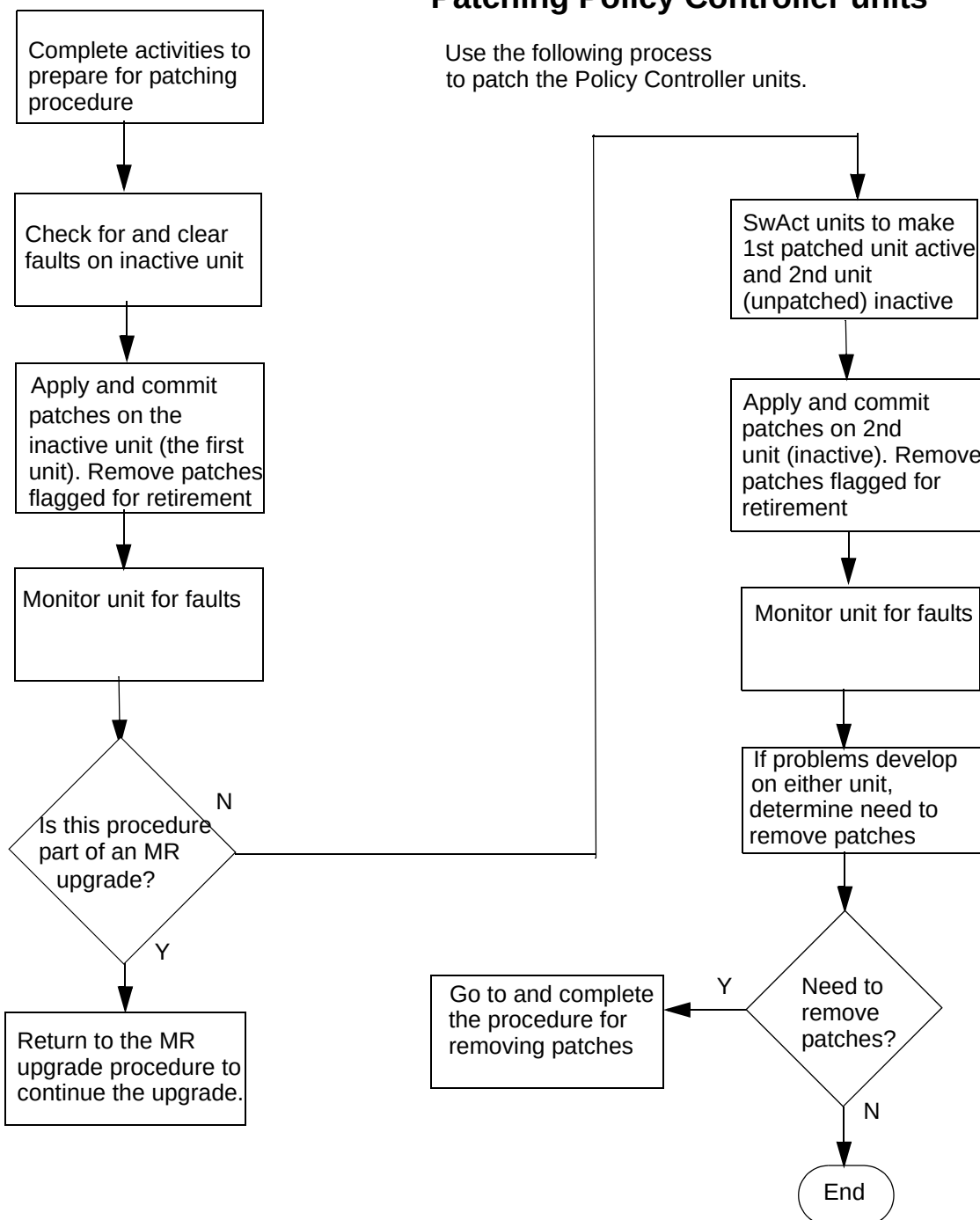
Although most patch files apply to any Nortel customer site, some patch files are created for a particular customer's site-specific installation. Not all patches made available apply to all customer sites. Contact Nortel GNPS customer support if you are concerned about which patches are applicable to your site.

Both units in the Policy Controller node must be patched. Each unit is patched separately while it is operating in standby mode. When patching the units, apply and commit the patch to the inactive unit first, then check logs and system status before SwActing the units. Check the logs and status for some period of time to ensure there are no patch-related events. After a time designated by your site guidelines, apply and commit the patch the newly inactive (unpatched) unit and check for logs and system status again.

Refer to the following diagram for a high-level view of the patching process for the Policy Controller units.

## Patching Policy Controller units

Use the following process to patch the Policy Controller units.



**Patching limitations**

Only NCGL Platform patching is supported. Policy Controller application patches are not supported.

Patches can only be applied using the CLI (command line interface).

**Delivery methods for patch files**

Nortel can release NCGL HA patch files at any time. The patch files can also be made available with a major upgrade or during a maintenance release.

You can locate NCGL HA patch files using the following methods:

- From the <http://www.nortel.com> Web site. Access the Technical Support portal and select Software Downloads. Search under the Carrier VoIP product family for Next Generation Policy Controller.
- From the DVD-ROM software disk, sent to the customer site, that contains the installation software or maintenance release software.
- From a patching CD-ROM sent to the customer site.
- From a customer dropbox service where Nortel delivers patches to a customer-based interface server that is accessible from the internet. The patch files are transferred from the customer-based interface server to the Policy Controller units by the customer network administrator or other trained personnel.

**Locating existing patch files on the Policy Controller units**

Patch files are stored in the /patching/patchholding directory on each unit that is to be patched.

**Prepare for patching activities**

Ensure that any critical data such as security certificates and the Policy Controller application database has been backed up to a safe location.

Complete the following steps, in the order indicated, to prepare for patching activities:

**Patching preparation**

- 1 If you are applying patches while performing a maintenance release upgrade, go to [step 4](#).
  - If you have purchased security certificates from a Certificate Authority then ensure that you have made a backup copy of the following security certificate files: server.crt, server.crt

and certificate.key. These are located in directory /opt/base/share/ssl.

- Otherwise, transfer a copy of the default security certificate files (same names and location as above) to a secure location on a remote server. For more information on security certificates for Session Server refer to *Policy Controller and Administration*, NN10434-611.
- 2 Backup the Policy Controller application database on active unit using procedure “Performing a backup of the Policy Controller database” in *Policy Controller Security and Administration*, NN10434-611.
  - 3 Acquire patch files from Nortel either using ESD delivery or from a patch or maintenance release DVD-ROM disk.
  - 4 Use procedure [View release notes for a maintenance release on page 1258](#) to check release notes to identify the required NCGL patches for your load. Also note any patches that are retired and must be removed.
  - 5 Use procedure [Acquire patch files on page 1300](#) to copy the patch files from a DVD to the /patching/patchholding directory.  
or  
Use procedure [Acquire patch files on page 1300](#) to install patches from a downloaded ISO image, and copy all required patches files from directory /opt/swd/<ESD\_ISO\_directory>/ to the /patching/patchholding directory.
  - 6 Complete procedure [Query status of NCGL patches on page 1304](#)
  - 7 Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
  - 8 You have completed this high-level procedure.



## Applying and committing patches

Complete the following steps, in the order indicated, to patch both of the Policy Controller units:

**Note:** This high-level procedure can be part of a high-level maintenance release upgrade procedure.

### Applying patches

- 1 Complete section [Prepare for patching activities on page 1250](#)
- 2 Use procedure [Prevent a system SwAct \(Jam\) on page 1262](#) to jam the units.
- 3 Complete procedure [Apply and commit an NCGL patch on page 1307](#) on the inactive unit.
- 4 Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
- 5 If you were directed to this patching from procedure [Perform a maintenance release upgrade on page 1235](#), return to that procedure now.  
Otherwise continue with the next step.
- 6 Release the JAM on the units using procedure [Enable a system SwAct \(Unjam\) on page 1327](#).
- 7 Complete procedure [Invoke a maintenance SwAct of the Policy Controller platform on page 1320](#).
- 8 Use procedure [Prevent a system SwAct \(Jam\) on page 1262](#) to jam the units.
- 9 Repeat procedure [Apply and commit an NCGL patch on page 1307](#) for the second (mate) Policy Controller unit, now the new standby unit.
- 10 Release the JAM on the units using procedure [Enable a system SwAct \(Unjam\) on page 1327](#).
- 11 Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
- 12 You have completed this high-level procedure.

## Remove patches

### ATTENTION

Under normal operating conditions patches must be removed from both units. Exceptions to this case may be when a patch is being tested on a single unit before being committed and installed on the second unit.

Complete the following steps, in the order indicated, to remove patches from one or both Policy Controller units:

### Removing patches

- 1 Use procedure [Prevent a system SwAct \(Jam\) on page 1262](#) to jam the units.
- 2 Complete procedure [Remove an NCGL patch on page 1310](#) on the inactive unit.
- 3 Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
- 4 Use procedure [Enable a system SwAct \(Unjam\) on page 1327](#) to unjam the units.
- 5 Complete procedure [Invoke a maintenance SwAct of the Policy Controller platform on page 1320](#).
- 6 Repeat procedure [Remove an NCGL patch on page 1310](#) for the second (mate) Policy Controller unit, now the new standby unit.
- 7 Refer to *Policy Controller Fault Management*, NN10438-911, and use procedures “View Policy Controller alarms” and “View Policy Controller logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
- 8 You have completed this high-level procedure.

---

## Completing the Policy Controller upgrade

---

Perform the next required upgrade according to the order listed in the table [Component Upgrade Order on page 6](#). The required upgrade is the next component in the list according to your network configuration.

---

## Extract an ISO image from an Electronic Software Delivery (ESD)

---

### Purpose of this procedure

Use this procedure to extract an ISO image, patch files and release notes for a maintenance release archive file retrieved from an electronic software delivery dropbox. This procedure may be used as a standalone task or as part of higher level procedure [Perform a maintenance release upgrade on page 1235](#).

### Prerequisites

Ensure that the ESD software archive file has been transferred from the dropbox on the repository server. The repository server is the machine owned by the operating company that was selected to be the destination for the ESD software files

Your existing Regional Customer Service Team has knowledge of your ESD implementation methodology. You can also contact the technical assistance support (TAS) hotline after hours for any urgent issues related to ESD.

For more information about how your site's ESD is implemented, contact your site network administrator. Also, refer to the document Electronic Software Delivery Customer Implementation Guide, found on your solution CD.

### Restrictions and Limitations

This procedure must be completed on both the active and inactive units.

### Action

#### *At a client workstation on the CS-LAN or IEMS client*

- 1 Log onto a Policy Controller unit using a secure shell by typing  
> **ssh -l <userid> <SS\_IP\_address>**  
and pressing the Enter key.

where

**userid**

is a valid userid (like mtc) on the

**SS\_IP\_address**

is the IP address of the Policy Controller unit

**Example**

ssh -l mtc 45.128.54.12

- 2 When prompted, enter your password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directory to the location of the ESD software archive file by typing  

```
$ cd /opt/swd
```

and pressing the Enter key.
- 6 Ensure that enough disk space is available for the extracted ISO image by typing  

```
$ df -k /opt/swd
```

and pressing the Enter key.  
*The free space on the device is printed. The value for “avail” is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes.*
- 7 Uncompress the ESD software load from the ESD archive file by typing  

```
$ gzip -d <esd_ISOfilename>.tar.gz
```

and pressing the Enter key.  
where  
**esd\_ISOfilename**  
is a the file name of the ESD delivered MR file  
**Example**  

```
$ gzip -d NGSS0070.70.P.NCL.NAP.VAULT.6.D.tar.gz
```

*The ESD software load is uncompressed.*
- 8 List the uncompressed file:  

```
$ ls *.tar
```
- 9 Unpack the file:  

```
$ tar -xvf <esd_ISOfilename>.tar
```

where  
**esd\_ISOfilename**  
is the file name of the ESD delivered MR file

The ESD software load is unarchived, and a new directory named after the ESD software filename is created. The directory name is the name of the ESD filename without the .tar.gz suffix. The contents of the ESD software load are placed in this new directory.

- 10** Change directory to the newly created directory by typing

```
$ cd <esd_ISO_directory>
```

and pressing the Enter key.

where

```
<esd_ISO_directory>
```

is a the file name of the ESD delivered MR file

**Example**

```
$ cd NGSS0090.90.P.NCL.NAP.VAULT.6.D
```

- 11** Verify that the image file exists in the directory by typing

```
$ ls -l
```

and pressing the Enter key.

*The system responds by listing the ISO image in the directory.*

- 12** Mount the image file to mount point /cdrom by typing

```
mount -t iso9660 -o loop <iso image> /cdrom
```

where

**iso image**

is the image file name such as NGSS09\_NCL.iso

**Example**

```
mount -t iso9660 -o loop NGSS09_NCL.iso /cdrom
```

*The command prompt returns upon success and the contents of the image are available from the /cdrom mount point.*

- 13** List the contents of the ISO by typing

```
cd /cdrom
```

```
ls -l
```

*The system responds with a list of files in the ISO image including any applicable patch files and the release notes file.*

- 14** This procedure is complete.

---

## View release notes for a maintenance release

---

### Purpose of this procedure

Use this procedure to view the release notes for a maintenance release or patching release. This procedure may be used as a standalone task or as part of a higher level activity.

### Limitations and Restrictions

There are no restrictions for performing this procedure.

### Prerequisites

If reading release notes from a DVD disk, ensure that the maintenance release DVD-ROM disk is inserted into the inactive unit DVD-ROM drive.

If reading release notes from an ESD delivered ISO archive file, ensure that the software archive file has been extracted and put into the /opt/swd directory on both units using procedure [Extract an ISO image from an Electronic Software Delivery \(ESD\) on page 1255](#).

### Action

If reading release notes from a DVD disk, proceed with procedure [View release notes from a DVD-ROM disk on page 1258](#).

If reading release notes from an ESD delivered ISO archive file, then go to [View release notes from an ESD delivered ISO image on page 1260](#).

#### View release notes from a DVD-ROM disk

##### *At a client workstation on the CS-LAN or IEMS client*

- 1 Log onto the Policy Controller unit using a secure shell by typing  
> **ssh -l <userid> <SS\_IP\_address>**  
and pressing the Enter key.

where

##### **userid**

is a valid userid (like mtc) on the Policy Controller

##### **SS\_IP\_address**

is the IP address of the Policy Controller unit

##### **Example**

ssh -l mtc 45.128.54.12

- 2 When prompted, enter your password.
- 3 Change to the root user by typing  
`$ su - root`  
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Verify that the CD/DVD-ROM disk has been inserted into the DVD-ROM disk drive.
- 6 Mount the DVD-ROM drive by typing  
`$ mount /cdrom`  
and pressing the Enter key.
- 7 Change directories to the mounted DVD-ROM file system by typing  
`$ cd /cdrom`  
and pressing the Enter key.
- 8 Locate the release notes file by typing  
`$ ls`  
and pressing the Enter key.
- 9 Read the contents of the release notes file by typing  
`$ cat <release_notes_filename> | more`  
and pressing the Enter key.  
where  
`<release_notes_filename>`  
is a file name for the release notes file
- 10 If necessary use the space bar to page through the contents of the release notes file. If necessary, repeat the previous step to view the contents of the file again.
- 11 When you are done reviewing the release notes file, change directories out of the mounted DVD-ROM file system by typing  
`$ cd /`  
and pressing the Enter key.
- 12 Unmount the DVD-ROM drive by typing  
`$ umount /cdrom`  
and pressing the Enter key.



- 13** You have completed this procedure. Return to [step 6](#) in procedure [Preparing to upgrade the Policy Controller on page 1232](#).

### **View release notes from an ESD delivered ISO image**

#### ***At a client workstation on the CS-LAN or IEMS client***

- 1** Log onto the Policy Controller unit using a secure shell by typing  
> **ssh -l <userid> <SS\_IP\_address>**  
and pressing the Enter key.

where

**userid**

is a valid userid (like mtc) on the Policy Controller

**SS\_IP\_address**

is the IP address of the Policy Controller unit

**Example**

ssh -l mtc 45.128.54.12

- 2** When prompted, enter your password.
- 3** Change to the root user by typing  
\$ **su - root**  
and pressing the Enter key.
- 4** When prompted, enter the root password.
- 5** Change directories to the software directory where the ESD archive file is stored by typing

\$ **cd /opt/swd/<ESD\_ISO\_directory>**

and pressing the Enter key.

where

**<ESD\_ISO\_directory>**

is the directory containing the version of the ISO image and release notes that you want to view.

**Note:** There may be multiple directories containing different versions of ISO images.

- 6** Locate the release notes file by typing  
\$ **ls**  
and pressing the Enter key.

- 7 Read the contents of the release notes file by typing  

```
$ cat <release_notes_filename> | more
```

and pressing the Enter key.  
where  

```
<release_notes_filename>
```

is a file name for the release notes file
- 8 If necessary, use the space bar to page through the contents of the release notes file. If necessary, repeat the previous step to view the contents of the file again.
- 9 You have completed this procedure.

---

## Prevent a system SwAct (Jam)

---

### Purpose of this procedure

The jam command is used to manually prevent a SwAct (switch of activity) of the active and stand-by units by inhibiting the toggling of operational states of both units, thereby preventing the stand-by unit from going active.

### Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as in cases of a replacing a faulty standby unit or upgrading the software for a standby unit.

#### **ATTENTION**

You cannot Jam a Policy Controller unit if the inactive unit is out of service.



#### **CAUTION**

This procedure prevents the Policy Controller node from operating in a duplex, fault-tolerant mode and prevents the Policy Controller application from being able to SwAct between Policy Controller units as needed. Keep a jam in effect only as long as is necessary.

### Prerequisites

There are no prerequisites for performing this procedure.

## Action

### Prevent a system SwAct (Unjam)

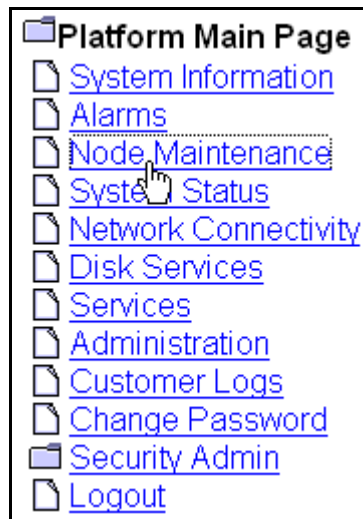
#### *At the CS 2000 Session Server Launch Point*

- 1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Click the **Node Maintenance** link.



The **Node Maintenance** panel displays.

- 3 Determine if the Jam State of the standby unit is **Yes** or **No**. If it is **Yes**, then the unit is already jammed and you have completed this procedure. If it is **No**, then continue with [step 4](#).

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | no        |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Jam"/> <input type="checkbox"/> Force |

- 4 Click the **Jam** button.

or

If you want to override any pre-Jam queries, first click the **Force** check box, then click the **Jam** button.

**Note:** To Jam or Force Jam? The Jam action does not work if critical faults exist on the active unit. Using the Jam command with the Force option overrides any pre-checks. A Forced Jam forces a Jam of the inactive Policy Controller unit even if critical faults exist on the active unit, in which case, a full service outage could occur on the Policy Controller node if the active unit fails.

*The system responds*

Are you sure you wish to perform jam action?

This will prevent the switch of activity to the inactive node.

Click OK to confirm node jam or cancel to abort.

- 5 Click **OK** to proceed with the jam activity.

*The system responds:*

Info: Jam - Command passed.

- 6 Observe the Jam state for the standby Policy Controller unit transitions from **No** to **Yes**.

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | yes       |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                      |
|---------------------------------------------------------------------|--------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Unjam"/> |

- 7 You have completed this procedure. If applicable, return to [Perform a maintenance release upgrade on page 1235](#).

**Note:** To unjam a standby Policy Controller unit, refer to procedure [Enable a system SwAct \(Unjam\) on page 1327](#).

---

## View the operational status of a Policy Controller NCGL platform

---

### Purpose of this procedure

Use the following procedure to view the service status of the Policy Controller platform hardware and NCGL operating system using the CS 2000 NCGL Platform Manager. Use this procedure as a standalone task or as part of a high-level procedure.

### Limitations and restrictions

This procedure provides instructions for determining the service status of the Policy Controller platform only. For instructions on determining the status of the Policy Controller application, refer to procedure [View the operational status of the Policy Controller application on page 1347](#).

Although some activities described in this procedure can be accomplished using the CS 2000 Policy Controller Manager, they are described instead using the more complete CS 2000 NCGL Platform Manager.

This procedure does not describe how to change platform or NCGL settings such as changing BIOS settings or platform provisioning.

This procedure does not describe how to view customer logs, alarms or how to change the root password. For detailed instructions on viewing customer logs or alarms, refer to procedures in *Policy Controller Fault Management*, NN10438-911. For instructions on how to change the platform root password, refer to *Policy Controller Security and Administration*, NN10434-611.

### Prerequisites

There are no prerequisites for using this procedure.

## Action

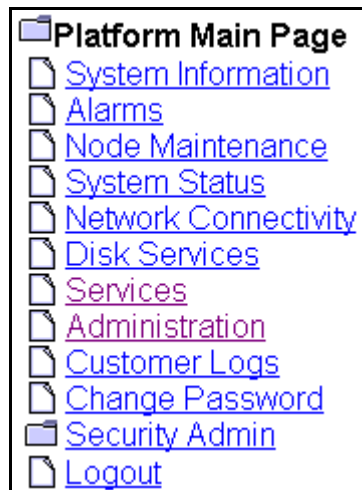
### *At the CS 2000 Session Server Launch Point*

- 1 Select **Succession Communication Server 2000 NCGL Platform Manager** from the launch point menu.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

The **Platform Main Page** menu displays.





**2** From the **Platform Main Page** menu, use the following table to determine your next step.

| If                                                                                                                                                                                     | Do                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| you want to review the version of the platform software load, boot statistics and platform IP address                                                                                  | Click the <b>System Information</b> link and go to <a href="#">step 3</a> .                                                                    |
| you want to review existing platform alarms                                                                                                                                            | Go to procedure "View Policy Controller alarms" in <i>Policy Controller Fault Management</i> , NN10438-911.                                    |
| you want to review node maintenance status                                                                                                                                             | Click the <b>Node Maintenance</b> link and go to <a href="#">step 5</a> .                                                                      |
| you want to review the status of system processes, CPU load and memory or related alarm thresholds                                                                                     | Click the <b>System Status</b> link and go to <a href="#">step 7</a> .                                                                         |
| you want to review the connectivity status of the network links.<br>To perform link management activities, refer to <i>Policy Controller Security and Administration</i> , NN10434-611 | Click the <b>Network Connectivity</b> link and go to <a href="#">step 9</a> .                                                                  |
| you want to review storage related information including array status, disk capacity and disk alarm thresholds                                                                         | Click the <b>Disk Services</b> link and go to <a href="#">step 11</a> .                                                                        |
| you want to review details about platform services including the network time protocol servers                                                                                         | Click the <b>Services</b> link and go to <a href="#">step 13</a> .                                                                             |
| you want to review platform version information only                                                                                                                                   | Click the <b>Administration</b> link and go to <a href="#">step 15</a> .                                                                       |
| you want to review customer logs                                                                                                                                                       | Go to procedure "View Policy Controller logs" in <i>Policy Controller Fault Management</i> , NN10438-911 .                                     |
| you want to change root passwords                                                                                                                                                      | Go to procedure "Manage user passwords with the Policy Controller GUI" in <i>Policy Controller Security and Administration</i> , NN10434-611 . |
| You want to view the security certificate                                                                                                                                              | Go to procedure "View Security Administration information" in <i>Policy Controller Security and Administration</i> , NN10434-611               |
| you are done reviewing information and want to logout from the GUI                                                                                                                     | <a href="#">step 17</a> .                                                                                                                      |

**3** Review the system information page and use the following table to review the description of the various fields of the Platform (System) Information page.

**Note:** The Platform (System) Information panel does not update automatically. Click the **System Information** link again to update it.

| Unit | Activity | Jam | State         | Connectivity | Host Name | Last Update Time |
|------|----------|-----|---------------|--------------|-----------|------------------|
| 0    | Active   | no  | simplex<br>5M | MatCon<br>M  | SPC2      | 03:41:07         |

The Platform Information panel does not update automatically!  
 Datestamp of last update: Sunday January 30th 2005 03:36:01 AM CST

| Platform Information           |                                               |
|--------------------------------|-----------------------------------------------|
| Date:                          | Sunday January 30th 2005 03:36:01 AM CST      |
| Time since last reboot:        | 3 days, 16 hours, 52 minutes, 8 seconds       |
| System Power-On Time:          | 0 years 176 days 21 hours                     |
| System booted from:            | Hard disk drive                               |
| Last restart cause:            | Last restart due to soft reset                |
| Last power event cause:        | Last power down caused by loss of power feed. |
| Current version:               | 7.03.1.0.0501190225                           |
| Platform IP Address:           | 47.153.178.176                                |
| Platform EM Client IP Address: | 47.130.16.56                                  |
| Server Location:               | SUPLAB                                        |
| Host Name:                     | SPC2                                          |

| Field        | Description                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit         | The Unit number of the Policy Controller in the node that is active. This is the unit you are logged into using your GUI.                                                           |
| Activity     | Indicates the activity of the unit (either active or standby).                                                                                                                      |
| Jam          | Indicates if an activity Jam has occurred on the active Policy Controller unit. This prevents the standby unit from becoming active, regardless of any failures on the active unit. |
| State        | Indicates if the Policy Controller node is operating in a duplex (fault-tolerant) mode or a simplex mode (the standby unit is off-line).                                            |
| Connectivity | Indicates the state of the network links on the node.                                                                                                                               |
| Host Name    | Indicates the name of the Policy Controller unit (not node).                                                                                                                        |

| Field                          | Description                                                                                                                                                                                                                                                           |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Last Update Time               | Indicates the last time in hours, minutes and seconds that the Policy Controller unit was updated.                                                                                                                                                                    |
| Date                           | Indicates the system date as maintained by the network time protocol (NTP) server.                                                                                                                                                                                    |
| Time since last reboot:        | Indicates the amount of time that has elapsed since the Policy Controller was last rebooted for any reason.                                                                                                                                                           |
| System Power-On Time:          | Indicates the recorded system time that the Policy Controller was powered up.                                                                                                                                                                                         |
| System booted from:            | Indicates whether the Policy Controller is currently booted from the hard drive, or DVD-ROM drive.                                                                                                                                                                    |
| Last restart cause:            | Indicates any event that forced a platform reboot (manual or system generated).                                                                                                                                                                                       |
| Last power event cause:        | Indicates any event that affected the power supply subsystem of the unit chassis.                                                                                                                                                                                     |
| Current version:               | Indicates the installed version of the Policy Controller platform software. (Does not include the Policy Controller application or other co-resident applications.) Refer to procedure <a href="#">Determine the current version of software loads on page 1285</a> . |
| Platform IP Address:           | Indicates the IP address of the Policy Controller platform.                                                                                                                                                                                                           |
| Platform EM Client IP Address: | Indicates the IP address of the Policy Controller client web interface. This is the IP address of the PC or Unix client from which the GUI was launched. When a web proxy is used, IP address is prefixed with the SPFS proxy IP address.                             |
| Server Location:               | Indicates the physical location of the Policy Controller.                                                                                                                                                                                                             |
| Host Name:                     | Indicates the hostname of the Policy Controller node.                                                                                                                                                                                                                 |

- 4 When you have completed reviewing **System Information** window, return to [step 2](#).
- 5 Review the **Node Maintenance** window and use the following table to review the description of the various fields of the Node Maintenance window:  

**Note:** The Node Maintenance panel is refreshed every 45 seconds.

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | no        |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Jam"/> <input type="checkbox"/> Force |

| Field                                  | Description                                                                                                                                                                                                                        |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operation State (unit 0 or 1)          | Indicates the operational state of the platform software.                                                                                                                                                                          |
| Activity (unit 0 or 1)                 | Indicates the activity state of the platform software.                                                                                                                                                                             |
| Jam State (active unit only)           | Indicates whether or not an activity jam has been requested.                                                                                                                                                                       |
| Maintenance Actions (active unit only) | Maintenance panel for performing node SwAct activity and to unjam node activity. Refer to <i>Policy Controller Security and Administration</i> , NN10434-611 for procedures on performing a SwAct or Jam/unJam of the active unit. |

- 6 When you have completed reviewing the **Node Maintenance** window, return to [step 2](#).
- 7 Review the **System Status** window and use the following table to review the descriptions of the various fields of the System Status page:
 

**Note:** The Chassis Information panel is not automatically refreshed.

| Chassis Information |  |  |                        |  |  |
|---------------------|--|--|------------------------|--|--|
| Self Test           |  |  | Chassis Subsystems     |  |  |
| Self tests passed.  |  |  | Chassis subsystems OK. |  |  |

| CPU Load                  |                            |                             |                                    |                                    |                                          |
|---------------------------|----------------------------|-----------------------------|------------------------------------|------------------------------------|------------------------------------------|
| 1 min.<br>load<br>average | 5 mins.<br>load<br>average | 15 mins.<br>load<br>average | Minor alarm<br>threshold<br>1 min. | Major alarm<br>threshold<br>1 min. | Critical<br>alarm<br>threshold<br>1 min. |
| 0.02                      | 0.01                       | 0.00                        | 10.00                              | 20.00                              | 40.00                                    |

| CPU Utilization                   |                                    |                                    |                                    |                                     |                                           |
|-----------------------------------|------------------------------------|------------------------------------|------------------------------------|-------------------------------------|-------------------------------------------|
| 5 mins.<br>Utilization<br>average | 20 mins.<br>Utilization<br>average | 30 mins.<br>Utilization<br>average | Minor alarm<br>threshold<br>5 min. | Major alarm<br>threshold<br>20 min. | Critical<br>alarm<br>threshold<br>30 min. |
| 0.77                              | 0.62                               | 0.62                               | 95.00%                             | 99.00%                              | 99.00%                                    |

| Process Information    |                                    |                                   |                                   |                                      |
|------------------------|------------------------------------|-----------------------------------|-----------------------------------|--------------------------------------|
| Number of<br>processes | Number of<br>zombie<br>process(es) | Zombie                            |                                   |                                      |
|                        |                                    | Minor alarm<br>threshold<br>value | Major alarm<br>threshold<br>value | Critical alarm<br>threshold<br>value |
| 165                    | 0                                  | 5                                 | 10                                | 15                                   |

| Memory Information      |                        |                             |                                        |                                        |                                              |
|-------------------------|------------------------|-----------------------------|----------------------------------------|----------------------------------------|----------------------------------------------|
| Total<br>memory<br>(MB) | Free<br>memory<br>(MB) | Available<br>memory<br>(MB) | Minor alarm<br>threshold<br>value (MB) | Major alarm<br>threshold<br>value (MB) | Critical<br>alarm<br>threshold<br>value (MB) |
| 3,787.31                | 2,951.86               | 3,539.29                    | 500.00                                 | 250.00                                 | 100.00                                       |

| Field                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chassis information: Self Test                          | Indicates the status of the self test performed on the platform at boot up.                                                                                                                                                                                                                                                                                                                                      |
| Chassis information: Chassis Subsystems                 | Indicates the status of the platform hardware subsystems including the memory, CPU, all drives, network connection, power supplies, cooling and other I/O connections.                                                                                                                                                                                                                                           |
| CPU Information: load average                           | Indicates the 1, 5 and 15 minute load averages for the CPU utilization.                                                                                                                                                                                                                                                                                                                                          |
| CPU information: load average threshold values          | Indicates the 1 minute CPU load average utilization threshold value. When the set threshold value is exceeded, the appropriate minor, major or critical alarm is raised.                                                                                                                                                                                                                                         |
| Chassis Utilization: Utilization average                | Indicates the 5, 20 and 30 minute CPU utilization average. When the threshold value is exceeded, an alarm is raised.                                                                                                                                                                                                                                                                                             |
| Chassis Utilization: alarm threshold values             | Indicates the 5, 20 and 30 minute CPU utilization average threshold value. When the set threshold value is exceeded, an alarm is raised.                                                                                                                                                                                                                                                                         |
| Process Information: Number of Processes                | Indicates the total number of processes (non-threaded) that are running on the Policy Controller Platform.                                                                                                                                                                                                                                                                                                       |
| Process Information: Number of zombie processes         | Indicates the number of defunct or terminated NCGL zombie processes.<br><br><b>Note:</b> A zombie process is a process that has terminated either because it has been killed by a signal or because it has called an <code>exit()</code> and whose parent process has not yet received notification of its termination. A zombie process exists solely as a process table entry and consumes no other resources. |
| Process Information-zombie: minor alarm threshold value | Indicates the maximum number of zombie processes allowed to be run by the CPU before a minor alarm is raised indicating that the set threshold has been exceeded.                                                                                                                                                                                                                                                |

| Field                                                      | Description                                                                                                                                                          |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process Information-zombie: major alarm threshold value    | Indicates the maximum number of zombie processes allowed to be run by the CPU before a major alarm is raised indicating that the set threshold has been exceeded.    |
| Process Information-zombie: critical alarm threshold value | Indicates the maximum number of zombie processes allowed to be run by the CPU before a critical alarm is raised indicating that the set threshold has been exceeded. |
| Memory Information: Total Memory (MB)                      | The total amount of RAM installed on the motherboard of each Policy Controller unit. Both units must have the same amount.                                           |
| Memory Information: Free Memory (MB)                       | The amount of memory available unallocated for use.                                                                                                                  |
| Memory Information: Available memory (MB)                  | The amount of memory available for programs.                                                                                                                         |
| Memory Information: minor alarm threshold value            | Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a minor alarm is raised.                                       |
| Memory Information: major alarm threshold value            | Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a major alarm is raised.                                       |
| Memory Information: critical alarm threshold value         | Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a critical alarm is raised.                                    |

- 8 When you have completed reviewing the System Status, return to [step 2](#).

## 9

**ATTENTION**

Do not perform link management activities such as Lock, Suspend or Swlink using this procedure. Refer to *Policy Controller Security and Administration*, NN10434-611 to perform these activities.

Review the **Network Connectivity** window and use the following table to review the description of the various fields of the Network Connectivity page:

**Note:** The Network Connectivity panel is refreshed every 45 seconds.

| Unit 0 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Active IP   | Port 0 IP   | Port 1 IP   | PTP IP      |
| 10.67.99.67  | 10.67.99.72 | 10.67.99.65 | 10.67.99.66 | 192.168.1.1 |
| Links        | Status      | Activity    | Maintenance |             |
| Link 0       | .           | Active      | Lock 0      | Swlink      |
| Link 1       | .           | Inactive    | Lock 1      |             |
| PTP Links    | .           |             |             |             |

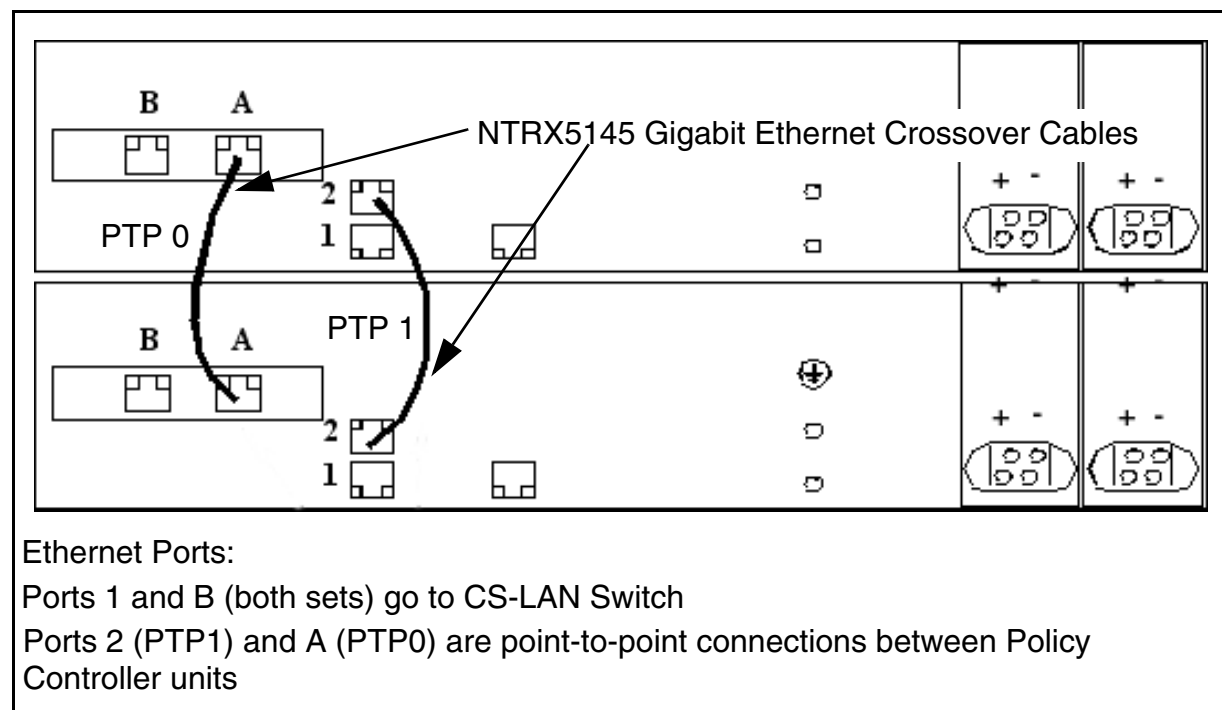
| Unit 1 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Inactive IP | Port 0 IP   | Port 1 IP   | PTP IP      |
| 10.67.99.70  | 10.67.99.71 | 10.67.99.68 | 10.67.99.69 | 192.168.1.2 |
| Links        | Status      | Activity    |             |             |
| Link 0       | .           | Active      |             |             |
| Link 1       | .           | Inactive    |             |             |
| PTP Links    | .           |             |             |             |

| Field           | Description                                                                                               |
|-----------------|-----------------------------------------------------------------------------------------------------------|
| Unit 0,1 Links  | Indicates which ethernet IP links are installed on the Policy Controller units (each unit has two links). |
| Unit 0,1 Status | Indicates the status of the ethernet links.                                                               |



| Field                     | Description                                                                                                                                                                                                           |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit 0,1 Activity         | Indicates the activity status of the ethernet links; either active or inactive.                                                                                                                                       |
| Unit 0,1 Maintenance      | Indicates the maintenance actions that can be performed on the ethernet links; either Lock, Unlock or Swlink. Refer to <i>Policy Controller Security and Administration</i> , NN10434-611 to perform link management. |
| Unit 0,1 PTP Links status | Indicates the status of the PTP links between both units in the node.                                                                                                                                                 |
| Unit IP                   | The network IP address of the Policy Controller unit.                                                                                                                                                                 |
| Active IP                 | The IP address of the local (active) Policy Controller unit.                                                                                                                                                          |
| Inactive IP               | The IP address of the mate (inactive) Policy Controller unit.                                                                                                                                                         |
| Port 0 IP                 | The IP address of the active or inactive ethernet port 0.                                                                                                                                                             |
| Port 1 IP                 | The IP address of the active or inactive ethernet port 1.                                                                                                                                                             |
| PTP IP                    | The IP address of the active or inactive PTP link.                                                                                                                                                                    |

### Crossover and LAN ethernet cable connections for Policy Controller units



- 10 When you have completed reviewing the Network Connectivity files, return to [step 2](#).
- 11 Review the **Disk Services** window and use the following table to review the description of the various fields of the Disk Storage page:

**Note 1:** The Disk Services panel does not update automatically. Click the **Disk Services** link again to update it.

**Note 2:** To create and remove file systems, refer to applicable procedures in *Policy Controller Configuration Management*, NN10432-511.

| RAID Array Status |           |       |        |        |                             |  |  |  |  |  |
|-------------------|-----------|-------|--------|--------|-----------------------------|--|--|--|--|--|
| Name              | Size (GB) | State | Disk 0 | Disk 1 | Status                      |  |  |  |  |  |
| /boot             | 0.10      | .     | .      | .      | Array is operating normally |  |  |  |  |  |
| ntvg              | 68.26     | .     | .      | .      | Array is operating normally |  |  |  |  |  |

| Disk Maintenance |                |            |                        |
|------------------|----------------|------------|------------------------|
| Disk Number      | Disk Size (GB) | Disk State | Disk Action            |
| 0                | 68.37          | .          | <a href="#">Remove</a> |
| 1                | 68.37          | .          | <a href="#">Remove</a> |

| Filesystem Information |                       |              |                  |                       |                      |                            |                           |                           |                           |                              |
|------------------------|-----------------------|--------------|------------------|-----------------------|----------------------|----------------------------|---------------------------|---------------------------|---------------------------|------------------------------|
| Monitored              | Filesystem Name       | Test Results | Total Space (MB) | Total Space Used (MB) | Total Space Used (%) | Total Space Available (MB) | Total Space Available (%) | Minor Alarm Threshold (%) | Major Alarm Threshold (%) | Critical Alarm Threshold (%) |
|                        | /                     | .            | 61.47            | 58.29                 | 100.00               | 0.00                       | 0.00                      | 85.00                     | 90.00                     | 95.00                        |
| No                     | /boot                 | .            | 98.65            | 19.08                 | 21.00                | 74.48                      | 79.00                     | -                         | -                         | -                            |
| Yes                    | /opt/base             | .            | 699.31           | 0.46                  | 1.00                 | 698.85                     | 99.00                     | 85.00                     | 90.00                     | 95.00                        |
| No                     | /opt/apps             | .            | 507.31           | 314.31                | 62.00                | 193.00                     | 38.00                     | -                         | -                         | -                            |
| Yes                    | /tmp                  | .            | 123.31           | 0.31                  | 1.00                 | 123.00                     | 99.00                     | 85.00                     | 90.00                     | 95.00                        |
| Yes                    | /var/log              | .            | 507.31           | 9.61                  | 2.00                 | 497.71                     | 98.00                     | 85.00                     | 90.00                     | 95.00                        |
| No                     | /opt/swd              | .            | 507.31           | 0.25                  | 1.00                 | 507.06                     | 99.00                     | -                         | -                         | -                            |
| No                     | /opt/apps/webint      | .            | 1,494.00         | 209.78                | 15.00                | 1,284.22                   | 85.00                     | -                         | -                         | -                            |
| No                     | /opt/apps/database    | .            | 10,006.00        | 48.19                 | 1.00                 | 9,957.81                   | 99.00                     | -                         | -                         | -                            |
| No                     | /opt/apps/logs        | .            | 507.31           | 206.34                | 41.00                | 300.98                     | 59.00                     | -                         | -                         | -                            |
| No                     | /opt/apps/ngssbilling | .            | 10,006.00        | 2.50                  | 1.00                 | 10,003.50                  | 99.00                     | -                         | -                         | -                            |

| Create/Remove Filesystem              |                      |                                   |
|---------------------------------------|----------------------|-----------------------------------|
| <a href="#">Create New Filesystem</a> | <input type="text"/> | <a href="#">Remove Filesystem</a> |

| Volume Group Information |                        |                            |                           |                            |                           |
|--------------------------|------------------------|----------------------------|---------------------------|----------------------------|---------------------------|
| Volume Group Name        | Volume Group Size (GB) | Total Space Allocated (GB) | Total Space Allocated (%) | Total Space Available (GB) | Total Space Available (%) |
| ntvg                     | 68.22                  | 23.84                      | 34.95                     | 44.38                      | 65.05                     |

| Field                        | Description                                            |
|------------------------------|--------------------------------------------------------|
| RAID Array Status: Name      | Indicates the name of each RAID-1 array in the system. |
| RAID Array Status: Size (GB) | Indicates the size of the partition in gigabytes.      |

| Field                                         | Description                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RAID Array Status: State                      | Indicates a high level state for the array:<br><ul style="list-style-type: none"> <li>- “.”: indicates the array is functioning normally.</li> <li>- Missing: a disk was removed from the array.</li> <li>- Failed: a disk in the array has failed and needs to be replaced.</li> <li>-Rebuilding: the array is in the process of rebuilding to a fault-tolerant mode.</li> </ul> |
| RAID Array Status: Disk 0                     | Indicates the service status of disk 0.                                                                                                                                                                                                                                                                                                                                           |
| RAID Array Status: Disk 1                     | Indicates the service status of disk 1.                                                                                                                                                                                                                                                                                                                                           |
| RAID Array Status: Status                     | Indicates the status of the array. Values are:<br><ul style="list-style-type: none"> <li>- The array is operating normally</li> <li>- Missing</li> <li>- Failed</li> <li>- Rebuild.</li> </ul>                                                                                                                                                                                    |
| Disk Maintenance: Disk Number                 | Indicates the disk number in the array; 0 or 1.                                                                                                                                                                                                                                                                                                                                   |
| Disk Maintenance: Disk Size (GB)              | Indicates the total capacity of the disk drive in gigabytes.                                                                                                                                                                                                                                                                                                                      |
| Disk Maintenance: Disk State                  | Indicates the installation state of the disk.                                                                                                                                                                                                                                                                                                                                     |
| Disk Maintenance: Disk Action                 | Indicates whether a hard disk can be inserted into the operating system.                                                                                                                                                                                                                                                                                                          |
| Filesystem Information: Monitor               | Indicates the status of individual file systems on the disk array.                                                                                                                                                                                                                                                                                                                |
| Filesystem Information: Filesystem Name       | Indicates the name of the filesystem on the disk array. Some filesystem names are reserved.                                                                                                                                                                                                                                                                                       |
| Filesystem Information: Test Results          | Indicates the results of any tests run on the filesystems. Tests are run approximately every 10 minutes to verify that all of the basic filesystem operations are working on each of the filesystems.                                                                                                                                                                             |
| Filesystem Information: Total Space (MB)      | Indicates the total amount of disk space (in MB) allocated for this filesystem.                                                                                                                                                                                                                                                                                                   |
| Filesystem Information: Total Space Used (MB) | Indicates the total amount of disk space (in MB) in use on this file system.                                                                                                                                                                                                                                                                                                      |
| Filesystem Information: Total Space Used (%)  | Indicates the total amount of disk space (in %) in use on this file system.                                                                                                                                                                                                                                                                                                       |

| Field                                                | Description                                                                                                                                                         |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filesystem Information: Total Space Available (MB)   | Indicates the percent of total disk space (in MB) free for use on this filesystem.                                                                                  |
| Filesystem Information: Total Space Available (%)    | Indicates the amount of disk space (in %) available for use by platform processes and applications.                                                                 |
| Filesystem Information: Minor Alarm Threshold (%)    | Indicates the maximum amount of disk space (in percent) that can be utilized before a minor alarm is raised indicating that the set threshold has been exceeded.    |
| Filesystem Information: Major Alarm Threshold (%)    | Indicates the maximum amount of disk space (in percent) that can be utilized before a major alarm is raised indicating that the set threshold has been exceeded.    |
| Filesystem Information: Critical Alarm Threshold (%) | Indicates the maximum amount of disk space (in percent) that can be utilized before a critical alarm is raised indicating that the set threshold has been exceeded. |
| Volume Group Information: Volume Group Name          | Indicates the name of the volume group in the array.                                                                                                                |
| Volume Group Information: Volume Group Size (GB)     | Indicates the total size of the volume group in the array.                                                                                                          |
| Volume Group Information: Total Space Allocated (GB) | Indicates the amount of volume group space, in gigabytes, currently allocated to filesystems.                                                                       |
| Volume Group Information: Total Space Allocated (%)  | Indicates the amount of volume group space (in %) currently allocated to file systems.                                                                              |
| Volume Group Information: Total Space Available (GB) | Indicates the amount of unallocated volume group space, in gigabytes, available for filesystems.                                                                    |
| Volume Group Information: Total Space Available (%)  | Indicates the amount of unallocated volume group space (in %) available for file systems.                                                                           |

**12** When you have completed reviewing the Disk Services page, return to [step 2](#).

**13** Review the Services page and use the following table to review the description of the various fields of the Platform Services page:

**Note:** The Services panel does not update automatically. Click the **Services** link again to update it.

| Network Services                       |  |  |                                            |  |  |
|----------------------------------------|--|--|--------------------------------------------|--|--|
| Number of Active Command Line Sessions |  |  | Number of Clients with Active Web Sessions |  |  |
| 3                                      |  |  | 2                                          |  |  |

| NTP Information          |           |           |                         |                    |                      |
|--------------------------|-----------|-----------|-------------------------|--------------------|----------------------|
| Server 1                 | Server 2  | Server 3  | Total Number of Servers | Accessible Servers | Synchronized Servers |
| 47.140.162.68<br>in sync | undefined | undefined | 1                       | 1                  | 1                    |

| Field                                                           | Description                                                                                                                      |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Network Services:<br>Number of Active Command Line Sessions     | Indicates the number of command line interface (CLI) sessions (both remote and local) on the Policy Controller.                  |
| Network Services:<br>Number of Clients with Active Web Sessions | Indicates the number of clients running one or more web GUI sessions.                                                            |
| NTP Information:<br>Server1 - Server 3                          | Indicates the IP address of up to 3 Network Time Protocol (NTP) servers in the network, along with the status of the connection. |
| NTP Information:<br>Total Number of Servers                     | Indicates the number of NTP servers registered with the CS-LAN network.                                                          |
| NTP Information:<br>Accessible Servers                          | Indicates the number of NTP servers accessible to the Policy Controller.                                                         |
| NTP Information:<br>Synchronized Servers                        | Indicates the number of NTP servers to which the Policy Controller is synchronized.                                              |

- 14** When you have completed reviewing Platform Services status, return to [step 2](#).

- 15** Review the Administration page and use the following table to review the description of the various fields of the Platform Admin page:

**Note:** The Administration panel does not update automatically. Click the link again to update it.

| Bootload Management |  |  |                  |  |  |
|---------------------|--|--|------------------|--|--|
| Bootload            |  |  | Maintenance      |  |  |
| 5.20.1.0.0405122209 |  |  | Default Bootload |  |  |

| Software Upgrade     |                      |                      |                      |                      |                                        |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------------------------|
| Protocol             | Login ID             | Password             | IP address           | File                 | Action                                 |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="button" value="Upgrade"/> |

| Server Maintenance                                                       |                                                                        |
|--------------------------------------------------------------------------|------------------------------------------------------------------------|
| Unit 0 - Active                                                          |                                                                        |
| <input type="button" value="Reboot"/> <input type="checkbox"/> Force     | <input type="button" value="Halt"/> <input type="checkbox"/> Force     |
| Unit 1 - Inactive                                                        |                                                                        |
| <input type="button" value="RebootMate"/> <input type="checkbox"/> Force | <input type="button" value="HaltMate"/> <input type="checkbox"/> Force |

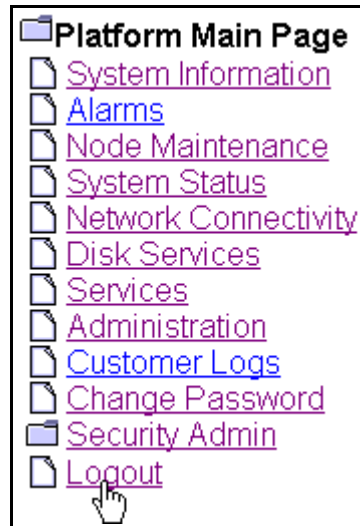
| Field                         | Description                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bootload Setting: Bootload    | Indicates the load ID for the NCGL platform software load.                                                                                                                                   |
| Bootload Setting: Maintenance | Indicates whether the Bootload is the default. May also allow choosing a new default bootload if there is more than one load available. Additional loads can come from maintenance releases. |
| Software Upgrade: Protocol    | Indicates the file transfer protocol or source location for the platform software upgrade: FTP, Anonymous FTP, HTTP, HTTPS, Local File, Local CDROM.                                         |
| Software Upgrade: Login ID    | If a login ID is required to access the upgrade platform load from another server in the network, a login ID can be entered here.                                                            |

| Field                                          | Description                                                                                                                                                                                             |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Software Upgrade: Password                     | If a password is required to access the upgrade platform load from another server in the network, a password can be entered here.                                                                       |
| Software Upgrade: IP Address                   | If it is required to access the upgrade platform load from another server in the network, an IP address can be entered here.                                                                            |
| Software Upgrade: File                         | The target upgrade load path and filename is entered here.                                                                                                                                              |
| Software Upgrade: Action Upgrade button        | The <b>Upgrade</b> button initiates a platform NCGL upgrade.                                                                                                                                            |
| Server Maintenance (active and inactive units) | To execute the <b>Reboot</b> , <b>Halt</b> , <b>Rebootmate</b> and <b>Haltmate</b> functions, refer to the applicable procedures in <i>Policy Controller Security and Administration</i> , NN10434-611. |

- 16** When you have completed reviewing Platform Admin page, return to [step 2](#), or continue with [step 17](#).



- 17 If you want to logout from platform GUI, click the **Logout** link.  
You are returned to the login page.



- 18 You have completed this procedure. If applicable, return to [Perform a maintenance release upgrade on page 1235](#).

---

## Determine the current version of software loads

---

### Purpose of this procedure

Use this procedure to do the following tasks:

- Determine the version of the software for the Policy Controller application on the Active unit.
- Determine the version of the software for the NGGL platform on the Active unit only if a maintenance release has not been applied.
- Use it as a standalone task or as part of a higher level activity.

### Limitations and Restrictions

Applying a maintenance release to the NGGL platform load causes inaccurate NGGL platform version information to show in the **Version Information** window. Use this procedure to view the NGGL platform version only if a maintenance release has not been applied to the NGGL platform load.

If a maintenance release has been applied to the NCGL platform load, determine the NCGL platform load version by using procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#) and go to the **System Info** window.

### Prerequisites

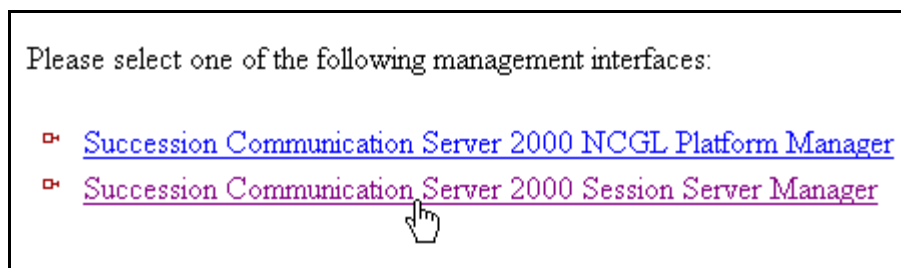
This procedure has no prerequisites.

### Action

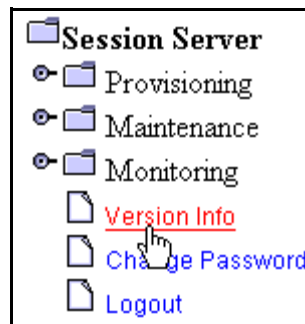
#### Determine the current version of the software load

##### *At an Integrated EMS or client workstation*

- 1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



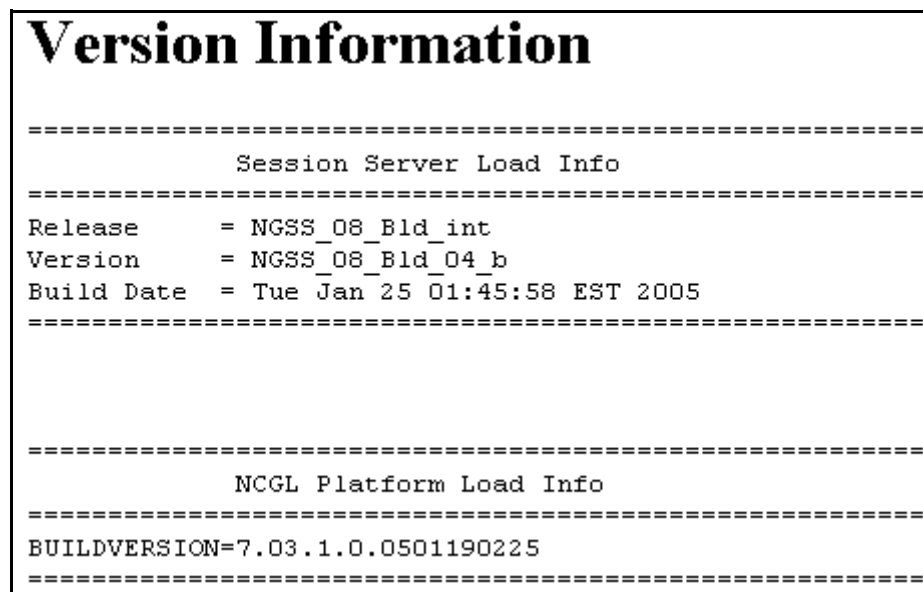
- 2 At the **Session Server** folder, click the **Version Info** link.



The **Version Information** window displays.

- 3 Review and record the load version information for the Policy Controller application or the NGGL platform.

**Note:** The version information for the NCGL platform load is only accurate if a maintenance release has not been applied to the load. If a maintenance release has been applied to the NCGL platform load, the version information is not accurately reflected in this window.



- 4 You have completed this procedure.

---

## Upgrade Policy Controller NCGL platform software

---

### Purpose of this procedure

This procedure describes how to use the CS 2000 NCGL Platform Manager GUI to apply (upgrade) a maintenance release to an NCGL platform load.

#### ATTENTION

This procedure should only be used as part of the high level activity [Perform a maintenance release upgrade on page 1235](#).

### Limitations and Restrictions

You can upgrade the NCGL platform load from the local DVD-ROM drive, from an ISO image located on the system disk drive, or from a Policy Controller DVD data disk mounted elsewhere in the network (via FTP). The following upgrade protocols (methods) are selectable from the CS 2000 NCGL Platform Manager GUI:

- Local CDROM - the local DVD-ROM drive (labelled as the local CD-ROM)
- Local file - an iso image, or load.tgz file copied from the local DVD-ROM drive copied to the hard drive using the secure copy program, **scp**, to transfer the data
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the FTP service. If the workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in clear text format across the network.
- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service.

### Prerequisites

When upgrading, first refer to [Preparing to upgrade the Policy Controller on page 1232](#) for the prerequisites of performing a maintenance release.

## Action

### *At the CS 2000 Session Server Launch Point*

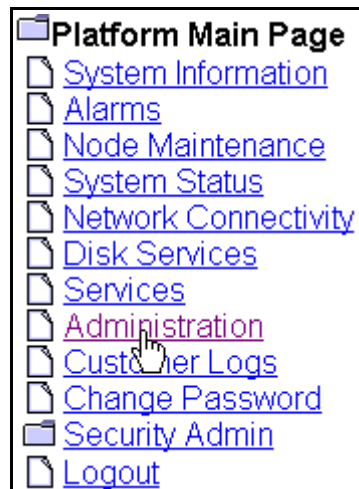
- 1 Select **Succession Communication Server 2000 NCGL Platform Manager** from the launch point menu.

Please select one of the following management interfaces:

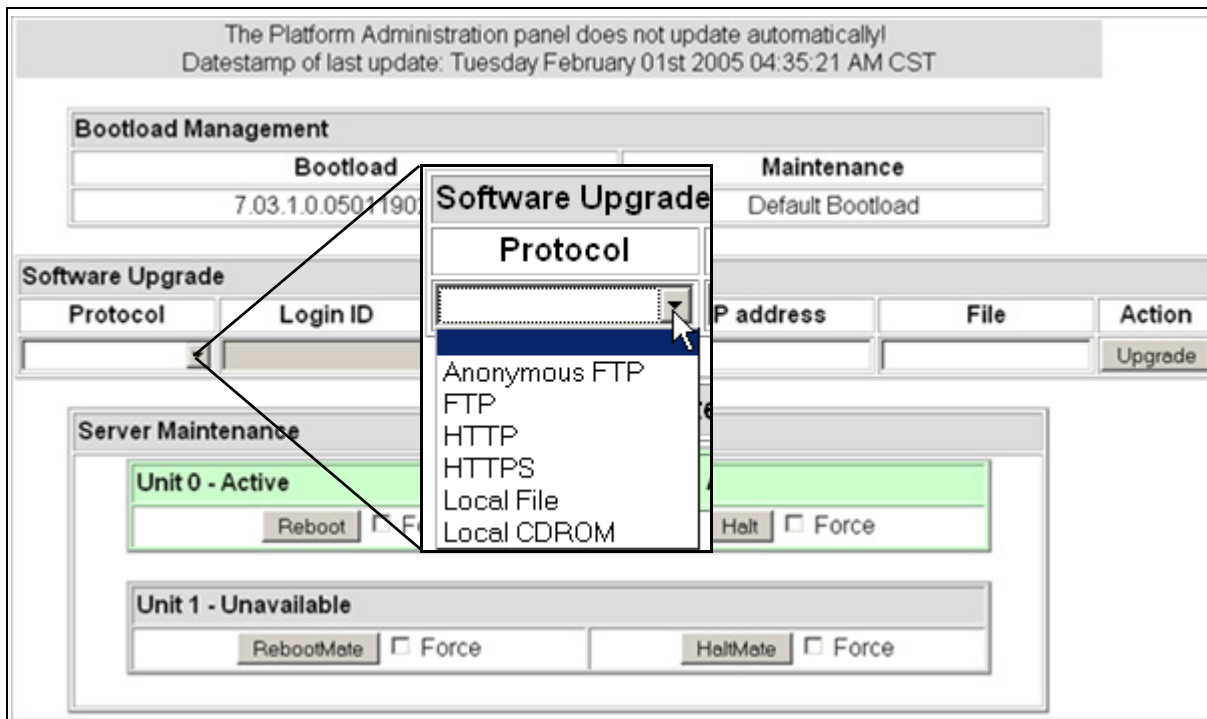
- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

The **Platform Main Page** menu displays.

- 2 Click the **Administration** link.



- 3 Click the **Protocol** drop down menu and select an upgrade protocol. Refer to the following table to help you determine the appropriate protocol:



| If the Protocol is | Do                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anonymous FTP      | <p>Enter the IP address of the remote server which has the bootload image in the IP address text box.</p> <p>Enter the location (as a relative path on the remote server) of the bootload image file <code>load.tgz</code> in the File text box. For example, <code>/opt/swd/load.tgz</code>.</p> <p>then continue with <a href="#">step 4</a></p> |

| If the Protocol is | Do                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FTP                | <p>Enter your username in the Login ID text box.</p> <p>Enter your password in the Password text box.</p> <p>Enter the IP address of the remote server which has the bootloader image in the IP address text box.</p> <p>Enter the location (as a relative path) of the bootloader image file <code>load.tgz</code> in the File text box. For example, <code>/opt/swd/load.tgz</code>.</p> <p>then continue with <a href="#">step 4</a></p> |
| HTTP or HTTPS      | <p>Enter the IP address of the remote server which has the bootloader image in the IP address text box.</p> <p>Enter the location (as a relative path on the remote server) of the bootloader image file <code>load.tgz</code> in the File text box. For example, <code>/opt/swd/load.tgz</code>.</p> <p>then continue with <a href="#">step 4</a></p>                                                                                      |
| Local File         | <p>Enter the location (as a relative path of the Policy Controller unit) of the bootloader image file <code>load.tgz</code> in the File text box. For example, <code>/opt/swd/load.tgz</code>.</p> <p>then continue with <a href="#">step 4</a></p>                                                                                                                                                                                         |
| Local CDROM        | <p>Ensure that the DVD-ROM disk is inserted into the drive</p> <p>then continue with <a href="#">step 4</a></p>                                                                                                                                                                                                                                                                                                                             |

---

**4** Click the **Upgrade** button.

|         |            |      |         |
|---------|------------|------|---------|
| assword | IP address | File | Action  |
|         |            |      | Upgrade |

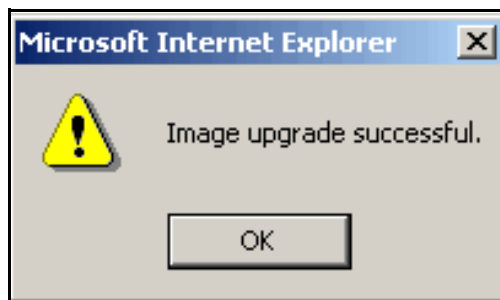
A popup window appears indicating the success of the upgrade.

5

#### ATTENTION

Click OK on the popup window to continue. Once complete, you will be able to verify the files were successfully copied. Refer to the [Troubleshooting on page 1292](#) section if you encounter problems.

Verify that the load files were successfully copied by clicking **OK** on the popup window.



6 When the selected NCGL load has been successfully copied to the unit, look for the load name to appear in the Bootload Management panel.

| Bootload Management |                    |
|---------------------|--------------------|
| <b>Bootload</b>     | <b>Maintenance</b> |
| 7.46.1.0.0411100433 | <b>Set default</b> |
| 5.36.1.0.0409032059 | <b>Delete</b>      |
| Default Bootload    |                    |

| Software Upgrade     |                      |                      |                      |                      |
|----------------------|----------------------|----------------------|----------------------|----------------------|
| Protocol             | Login ID             | Password             | IP address           | File                 |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

7 Click the **Set Default** button to the right of the new (upgraded) bootload.



| Bootload Management |                                                                                  |
|---------------------|----------------------------------------------------------------------------------|
| Bootload            | Maintenance                                                                      |
| 7.46.1.0.0411100433 | <input type="button" value="Set default"/> <input type="button" value="Delete"/> |
| 5.36.1.0.0409032059 | Default Bootload                                                                 |

*The system responds by setting the newly installed load as the default load, as shown below.*

| Bootload Management |                                                                                  |
|---------------------|----------------------------------------------------------------------------------|
| Bootload            | Maintenance                                                                      |
| 7.46.1.0.0411100433 | Default Bootload                                                                 |
| 5.36.1.0.0409032059 | <input type="button" value="Set default"/> <input type="button" value="Delete"/> |

- 8 Verify that you have set the correct bootload to be the default.
- 9 If you upgraded using the Local CD-ROM protocol, remove the DVD-ROM disk from the drive.
- 10 You have completed this procedure. If you were forwarded to this procedure from another procedure, return to that procedure and continue with the steps.

## Troubleshooting

For [step 5](#) of this procedure, review the message in the popup window. The following possible error messages and their meaning are described:

- Error: Failed to update image /usr/bin/copy\_boot\_image -f /opt/swd/load.tgz Invalid load file content. Exiting  
Indication: If the bootload file is corrupt, the system software indicates that the bootload contains invalid content.
- Error: Failed to update image /usr/bin/copy\_boot\_image -u https://10.40.5.62/tmp/load.tgz: Failed to retrieve file from the network.  
Indication: The user has attempted to perform software upgrade where the file path or the IP address used is not correct. You need

to validated that the IP address is correct, also, make sure the file path is correct.

- Error: Failed to update image /usr/bin/copy\_boot\_image -u ftp://mtc:mtc@10.40.5.59//usr/load.tgz: Failed to retrieve file from the network.

Indication: The user has attempted to perform software upgrade where the file path or the user ID or password used is not correct. You need to validated that the file path is correct and make sure to check the user ID and password.

- Error: Failed to update image /usr/bin/copy\_boot\_image -u ftp://mtc:mtc@10.40.5.59//usr/load.tgz: 10.40.5.59 IP address is not responding.

Indication: The user has attempted to perform software upgrade from a host that is not responding. You need to check that the host IP address is available and try again.

- Error: Failed to update image /usr/bin/copy\_boot\_image -f load.tgz: Could not find load.tgz

Indication: The user has attempted to perform software upgrade where the file path is not correct. Validate that the file path is correct.

- Error: Failed to update image /usr/bin/copy\_boot\_image -c: Failed to mount the cdrom RC=32

Indication: If the CDROM is not placed in the CDROM drive and an attempt is made to upgrade software with the "Local CDROM" option, the following message window appears. Verify that the CDROM is in the drive. If the CDROM is inserted, verify that the drive is functioning properly.

or

The user has attempted to perform a software upgrade where there is a problem with mounting the CD-ROM drive. Mount or remount the CD-ROM drive before attempting another software upgrade process.

- Error: Failed to update image /usr/bin/copy\_boot\_image -u https://10.40.5.62/load.tgz: Unable to decompress /opt/base/upgrade/29335/load.tgz Exiting

Indication: The user has attempted to perform software upgrade, which uses filesystem (/opt/base) that is full. You need to remove unwanted files and make sure there is enough space in the targeted filesystem.

---

## Reboot a Policy Controller unit

---

### Purpose of this procedure

Use this procedure to perform a graceful shut down and reboot of the NCGL operating system running on a Policy Controller unit. Use this procedure only as part of a high-level activity such as part of maintenance or fault clearing activities or part of a software upgrade activity.

#### ATTENTION

This procedure causes a 3-4 minute service interruption of the affected unit and should only be used when recommended by Nortel support personnel.

### Limitations and restrictions

#### ATTENTION

Nortel Networks recommends performing this procedure only on the standby unit.



#### CAUTION

If both the active and inactive units are rebooted, the reboot procedure prevents the Policy Controller from performing Virtual Call Admission Control processing. If the inactive unit alone is rebooted, then this prevents the Policy Controller node from operating in a fault-tolerant state.

**Note:** The CS 2000 will still process calls without VCAC if it determines the Policy Controller is unreachable.

You cannot reboot an active unit in duplex mode. A rebootmate is the only command that will work in duplex mode.

## Prerequisites

Use procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#) to verify any disk array rebuilds in progress, by checking the Alarms on the Policy Controller. Wait for the rebuild to complete before executing this procedure.

Ensure that you have your bootable software installation DVD disk available, in case you have trouble rebooting the unit.

## Action

### Reboot a Policy Controller Unit

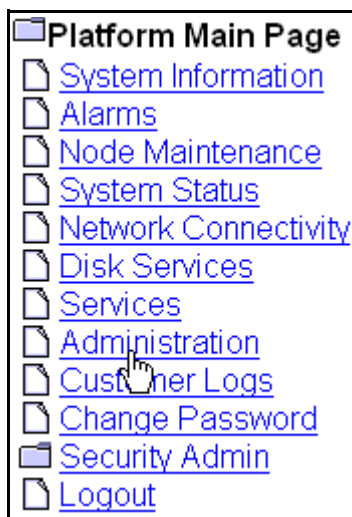
#### *At the CS 2000 Session Server Launch Point*

- 1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Click the **Administration** link.



### 3 Review the status of the unit you want to reboot.

| Bootload Management |  |  |                  |  |
|---------------------|--|--|------------------|--|
| Bootload            |  |  | Maintenance      |  |
| 5.20.1.0.0405122209 |  |  | Default Bootload |  |

| Software Upgrade     |                      |                      |                      |                      |
|----------------------|----------------------|----------------------|----------------------|----------------------|
| Protocol             | Login ID             | Password             | IP address           | File                 |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

| Server Maintenance                                                       |                                                                        |
|--------------------------------------------------------------------------|------------------------------------------------------------------------|
| Unit 0 - Active                                                          |                                                                        |
| <input type="button" value="Reboot"/> <input type="checkbox"/> Force     | <input type="button" value="Halt"/> <input type="checkbox"/> Force     |
| Unit 1 - Inactive                                                        |                                                                        |
| <input type="button" value="RebootMate"/> <input type="checkbox"/> Force | <input type="button" value="HaltMate"/> <input type="checkbox"/> Force |

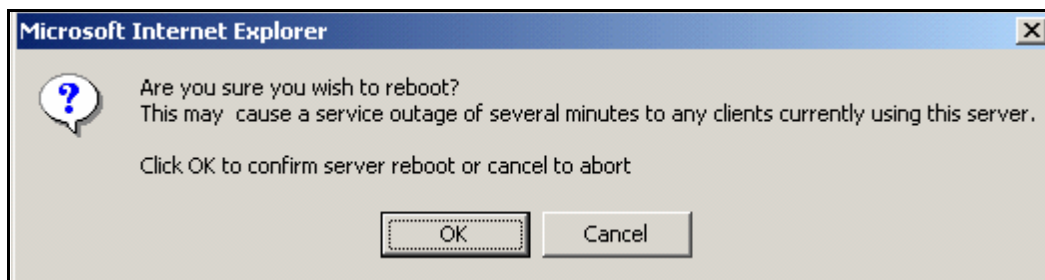
### 4 Click the **Reboot** button (for the active unit) or **RebootMate** button (for the inactive unit) for the Policy Controller unit you want to reboot.

**Note 1:** If you want to override any pre-reboot queries including a pre-checked by applications running on the unit, click the **Force** check box before clicking the **Reboot** or **RebootMate** button.

**Note 2:** In a system operating in fault-tolerant (duplex) mode, only the inactive unit can be rebooted using RebootMate or a Forced RebootMate. A Reboot or Forced Reboot can only be performed if the system is operating in simplex mode.

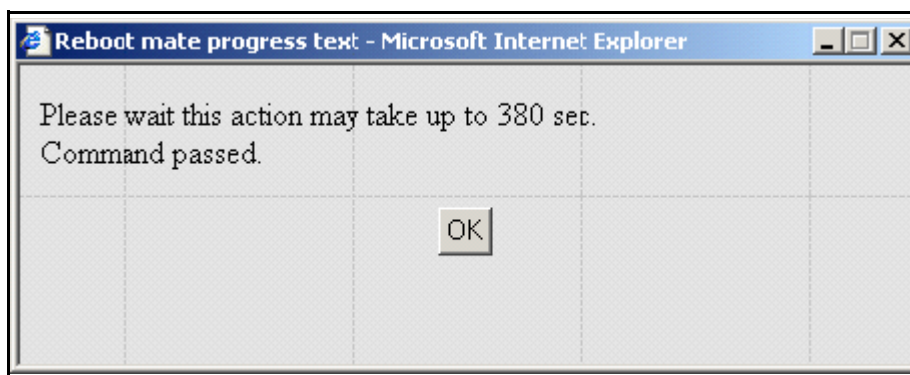
|                                                                          |                                                                        |
|--------------------------------------------------------------------------|------------------------------------------------------------------------|
| <input type="button" value="Reboot"/> <input type="checkbox"/> Force     | <input type="button" value="Halt"/> <input type="checkbox"/> Force     |
| Unit 1 - Inactive                                                        |                                                                        |
| <input type="button" value="RebootMate"/> <input type="checkbox"/> Force | <input type="button" value="HaltMate"/> <input type="checkbox"/> Force |

*The system responds with the following message:*



- 5 Click **OK** to confirm the reboot operation.

*The NGCL and all call activity on the affected unit is shutdown and the unit begins to reboot. The system responds with the following message box:*



- 6 Click **OK** to close the dialog box.

*The NGCL and all call activity on the affected unit is shutdown.*

**Note 1:** If you receive the following message, you must reboot the unit using the [Alternate command line interface \(CLI\) method on page 1298](#) otherwise consult section [Troubleshooting reboots on page 1298](#).

Error: Command failed. Reason: Mate not available.

**Note 2:** If you try to reboot an active unit in duplex mode, you will receive the following message:

Error: Reboot - Command rejected. Reason: Request only supported on INACTIVE unit when system is in DUPLEX mode.

- 7 Use procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#) to confirm the recovery of the unit after reboot.

- 8 This procedure is complete. If you were sent to this procedure by another procedure, return to that procedure and continue with the steps.

## Troubleshooting reboots

The following possible error messages received during a reboot attempt and their meaning are described:

**Error: Reboot - Command rejected. Reason: Mate is available.**

The user has attempted to reboot the active server when the inactive server is available.

**Error: Halt - Command rejected. Reason: Mate is available.**

The user has attempted to halt the active server when the inactive server is available.

**Error: Command failed. Reason: PRECHECK FAILED: application rejected request.**

The user has attempted to rebootmate or haltmate command and the application rejected the request. The user should check /var/log/designlog to determine the name of the application that rejected the maintenance command.

Actions:

- Using the Force option overcomes a pre-check failure by any application running on the unit.
- Try the operation again later. If the problem persists, then contact Nortel Networks support personnel for assistance.

## Alternate command line interface (CLI) method

**ATTENTION**

All prerequisites and limitations and restrictions shown on page [1295](#) apply for this procedure.

### *At the Policy Controller console interface*

- 1 Log onto the active Session Policy Controller unit and change to the root user.
- 2 Reboot the selected Session Policy Controller unit by typing  
**# mtcli rebootmate** (to reboot the inactive unit)  
or  
**# mtcli reboot** (to reboot the active unit operating in simplex mode)

and pressing the **Enter** key.

- 3** Use procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#) to confirm the recovery of the unit after reboot.
- 4** You have completed this procedure.



---

## Acquire patch files

---

### Purpose of this procedure

Use this procedure to identify patch files from a DVD-ROM or ESD archive file and copy them to the patch holding directory on each Policy Controller unit. This procedure may be used as a standalone task or as part of a higher level activity found in section [Patching the NCGL platform on page 1248](#) or [Perform a maintenance release upgrade on page 1235](#).

### Limitations and Restrictions

As this is not a service impacting procedure, it can be performed on either the active or inactive units.

### Prerequisites

If locating patch files from a DVD disk, ensure that the maintenance release or patching DVD-ROM disk is inserted into the unit DVD-ROM drive.

If reading release notes from an ESD delivered ISO archive file, ensure that the software archive file has been extracted and put into the /opt/swd directory on both units using procedure [Extract an ISO image from an Electronic Software Delivery \(ESD\) on page 1255](#).

### Action

If locating patch files from a DVD disk, proceed with procedure [Procedure: Acquire patch files from a DVD-ROM disk](#).

If locating patch files from an ESD delivered ISO maintenance release image file, then go to [Procedure: Acquire patch files from an ESD delivered ISO image on page 1302](#).

#### Procedure: Acquire patch files from a DVD-ROM disk

##### *At a client workstation on the CS-LAN or IEMS client*

- 1 Log onto the inactive Policy Controller unit using a secure shell by typing

```
> ssh -l <userid> <inactive_SS_IP_address>
```

and pressing the Enter key.

where

**userid**

is a valid userid (like mtc) on the Policy Controller

**inactive\_SS\_IP\_address**

is the IP address of the inactive Policy Controller unit

**Example**

```
ssh -l mtc 45.128.54.12
```

- 2 When prompted, enter your password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Insert the CD/DVD-ROM disk into the disk drive.
- 6 Mount the DVD-ROM drive by typing  

```
$ mount /cdrom
```

and pressing the Enter key.
- 7 Change directories to the mounted DVD-ROM file system by typing  

```
$ cd /cdrom
```

and pressing the Enter key.
- 8 Locate the patch files by typing  

```
$ ls
```

and pressing the Enter key.

*The system responds by displaying a list of files. Locate the patch files with the following filename format:*

```
ncgl_samxts_patch_<rel#>.<wk#>.<major#>.<minor#>
```

**Example**

```
ncgl_samxts_patch_5.31.1.1
```

```
ncgl_samxts_patch_5.31.1.2
```

- 9 Copy the patch files from the CD/DVD-ROM disk to the patch holding directory on the Policy Controller unit by typing  

```
$ cp <patchfilename> /patch/patchholding
```

and pressing the Enter key.  
where

**patchfilename**

list the file name for the patch file

- 10 Change directories to root by typing  
`$ cd /`  
and pressing the Enter key.
- 11 Unmount the DVD-ROM drive by typing  
`$ umount /cdrom`  
and pressing the Enter key.
- 12 Repeat this procedure on the mate Policy Controller unit.
- 13 You have completed this procedure.

### **Procedure: Acquire patch files from an ESD delivered ISO image**

#### ***At a client workstation on the CS-LAN or IEMS client***

- 1 Log onto the inactive Policy Controller unit using a secure shell by typing  
`> ssh -l <userid> <inactive_SS_IP_address>`  
and pressing the Enter key.  
where

#### **userid**

is a valid userid (like mtc) on the Policy Controller

#### **inactive\_SS\_IP\_address**

is the IP address of the inactive Policy Controller unit

#### **Example**

`ssh -l mtc 45.128.54.12`

- 2 When prompted, enter your password.
- 3 Change to the root user by typing  
`$ su - root`  
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directories to the directory where the maintenance release ISO image (and associated patch files) is located by typing  
`$ cd /opt/swd/<ESD_ISO_directory>`  
and pressing the Enter key.  
where

**<ESD\_ISO\_directory>**

is the directory containing the version of the ISO image and associated patch files.

**Note:** There may be multiple directories containing different versions of ISO images.

- 6 Locate the patch files by typing

```
$ ls
```

and pressing the Enter key.

*The system responds by displaying a list of files. Locate patch files with the following filename format:*

ncgl\_samxts\_patch\_<rel#>.<wk#>.<major#>.<minor#>

**Example**

ncgl\_samxts\_patch\_5.31.1.1

ncgl\_samxts\_patch\_5.31.1.2

- 7 Copy the patch files from the /opt/swd/<ESD\_ISO\_directory> to the patch holding directory by typing

```
$ cp <patchfilename> /patch/patchholding
```

and pressing the Enter key.

where

**patchfilename**

list the file name for the patch file

- 8 Repeat the previous step for additional patch files you need to install.
- 9 Repeat this procedure on the mate Policy Controller unit.
- 10 You have completed this procedure.

---

## Query status of NCGL patches

---

### Application

Use this procedure to review the status of patch files on a Policy Controller unit and to ensure that a patching file has been installed on both units in the node. This procedure may be used as a standalone task or as part of a higher level activity.

Two patch query methods are available:

- [Displaying patch status information for all patches on page 1304](#)
- [Displaying detailed information for a specific patch on page 1305](#)

### Prerequisites

Patch files must first be copied to the Policy Controller unit.

### Action

#### Displaying patch status information for all patches

##### *At a client workstation on the CS-LAN or IEMS client*

- 1 Open a secure shell to a Policy Controller unit by typing  

```
> ssh -l <userid> <SS_IP_address>
```

and pressing the Enter key.  
where  
**userid**  
is a valid userid (like mtc) on the Policy Controller  
**SS\_IP\_address**  
is the IP address of the selected Policy Controller unit

##### **Example**

```
ssh -l mtc 45.128.54.12
```

- 2 When prompted, enter your password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

- 5 To display patch status information for all patches type:  
**# patch\_ha -o QueryAll**  
and press the Enter key.
- 6 To compare this patch information to that on the mate unit, repeat this procedure for the second (mate) Policy Controller unit.
- 7 You have completed this procedure.

### Displaying detailed information for a specific patch

#### *At a client workstation on the CS-LAN or IEMS client*

- 1 Open a secure shell to a Policy Controller unit by typing  
**> ssh -l <userid> <SS\_IP\_address>**  
and pressing the Enter key.  
where  
**userid**  
is a valid userid (like mtc) on the Policy Controller  
**SS\_IP\_address**  
is the IP address of the Policy Controller unit  
**Example**  
ssh -l mtc 45.128.54.12
- 2 When prompted, enter your password.
- 3 Change to the root user by typing  
**\$ su - root**  
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 To display detailed patch status information for a a specific patch on a unit, at the prompt type:  
**# patch\_ha -v <patch\_version> -o QueryPatch**  
and press the Enter key.  
where  
**patch\_version**  
is the name of the patch file to be queried in the format:  
<NCGL\_release\_number>.<week\_number>.<major\_version\_number>.<minor\_version\_number>

- 6** To compare this patch information to that on the mate unit, repeat this procedure for the second (mate) Policy Controller unit.
- 7** You have completed this procedure.

---

## Apply and commit an NCGL patch

---

### Purpose of this procedure

Use this procedure to apply patch files to the inactive Policy Controller unit. This procedure should only be used as part of the high level activity [Applying patches on page 1252](#).

### Restrictions and Limitations

|                                                     |
|-----------------------------------------------------|
| <p style="text-align: center;"><b>ATTENTION</b></p> |
|-----------------------------------------------------|

NCGL patch files should only be applied the inactive unit.

Patching activities must be completed on both units in the node.

### Prerequisites

The patch files must have already been put into the **/patching/patchholding** directory on the Policy Controller hard drive. Contact your network administrator to determine if this has already been done. Refer to [Patching the NCGL platform on page 1248](#) to copy patch file to the hard drives.

### Action

#### *At a client workstation on the CS-LAN or IEMS client*

- 1 Log onto the inactive Policy Controller unit using a secure shell by typing  

```
> ssh -l <userid> <inactive_SS_IP_address>
```

and pressing the Enter key.  
where  
**userid**  
is a valid userid (like mtc) on the Policy Controller  
**inactive\_SS\_IP\_address**  
is the IP address of the Policy Controller unit  
**Example**  

```
ssh -l mtc 45.128.54.12
```
- 2 When prompted, enter your password.
- 3 Change to the root user by typing  

```
$ su - root
```



and pressing the Enter key.

- 4 When prompted, enter the root password.

- 5 Change directory to the patchholding directory by typing

```
$ cd /patching/patchholding
```

and pressing the Enter key.

- 6 Retrieve and untar the patch files from the patch archive to the /patching/<patch\_version>/ directory, and fill the patching subsystem's database with the patch information. At the prompt, type:

```
patch_ha -f <patch_file_name> -o FetchPatch
```

and press the Enter key.

*where*

**patch\_file\_name**

is the name of the patch archive you want to extract patch files from

- 7 Validate the patch file to verify that the patch file is sane, and the patch is ready to be applied. At the prompt type:

```
patch_ha -v <patch_version> -o Validate
```

and press the Enter key.

*where*

**patch\_version**

is the name of the patch file to be applied

- 8 Apply the patch file. Type:

```
patch_ha -v <patch_version> -o Apply
```

and press the Enter key.

*where*

**patch\_version**

is the name of the patch file to be applied

#### **ATTENTION**

NCGL patches are not automatically committed when applied. In order for a patch to reapply the next time the unit is rebooted, it must first be committed.

- 9 Commit the patch so it is auto-applied at each reboot of the unit.  
Type:  
**patch\_ha -v <patch\_version> -o Commit**  
and press the Enter key.  
*where*  
**patch\_version**  
is the name of the patch file to be committed
- 10 If necessary, allow the unit to reboot or if requested, perform a reboot using procedure [Reboot a Policy Controller unit on page 1294](#). Otherwise skip to the next step.
- 11 Perform a status check of the unit including checking for newly generated logs and alarms, to ensure the inactive unit is operating without error. Refer to *Policy Controller Fault Management*, NN10438-911, for applicable procedures. If errors occur that are related to the patching activity, contact your next level of support.  
  
**Note:** Checking unit status can entail different activities depending on what type of software item has been patched and any special patch application requirements. For example, some software subsystem processes may require a reboot before a patch can become active, while other subsystem processes restart with the new patched version once the patch application is complete.
- 12 You have completed this procedure. If you were forwarded to this procedure from another procedure, return to that procedure now and continue with the steps.

---

## Remove an NCGL patch

---

### Purpose of this procedure

Use this procedure to perform the following tasks:

- Remove patches from the inactive Policy Controller unit.
- Use this procedure only as part of the procedure [Removing patches on page 1253](#).

### Restrictions and Limitations

|                  |
|------------------|
| <b>ATTENTION</b> |
|------------------|

|                                                      |
|------------------------------------------------------|
| Remove NCGL patch files only from the inactive unit. |
|------------------------------------------------------|

Patching activities must be completed on both units in the node.

### Prerequisites

Verify which patches should be removed by referring to the patching or maintenance release notes.

### Action

#### Remove an NCGL patch

##### *At a client workstation on the CS-LAN or IEMS client*

- 1 Log onto the inactive Policy Controller unit using a secure shell by typing

> **ssh -l <userid> <SS\_IP\_address>**

and pressing the Enter key.

where

**userid**

is a valid userid (like mtc) on the Policy Controller

**SS\_IP\_address**

is the IP address or host name of the Policy Controller unit

**Example**

ssh -l mtc 45.128.54.12

- 2 When prompted, enter your password.
- 3 Change to the root user by typing

\$ **su - root**

and pressing the Enter key.

- 4 When prompted, enter the root password.

- 5 Uncommit the patch by typing:

**# patch\_ha -v <patch\_version> -o Uncommit**

and pressing the Enter key.

*where*

**patch\_version**

is the name of the patch file to be uncommitted

- 6 Remove the patch files and replace them with the files that existed prior to the patch. At the prompt type:

**# patch\_ha -v <patch\_version> -o Remove**

and press the Enter key.

*where*

**patch\_version**

is the name of the patch file to be removed

- 7 Delete the patch file. Type:

**# patch\_ha -v <patch\_version> -o Delete**

and press the Enter key.

*where*

**patch\_version**

is the name of the patch file to be deleted

- 8 If necessary, allow the unit to reboot or if requested, perform a reboot using procedure [Reboot a Policy Controller unit on page 1294](#).

- 9 This procedure is complete. Return to procedure [Removing patches on page 1253](#).

## Upgrade/rollback/reinstall the Policy Controller application

### Purpose of this procedure

Use this procedure to install the Policy Controller application onto a Policy Controller unit using one of the following methods:

- Reinstall a current version of the Policy Controller Application.
- Upgrade to a newer version of the Policy Controller Application (Maintenance Release).
- Rollback to a previous version of the Policy Controller Application.

#### ATTENTION

It is recommended that this procedure only be used as part of the high level activity [Perform a maintenance release upgrade on page 1235](#).

### Limitations and restrictions

If the Policy Controller node is in operation and performing call processing activities, only perform this procedure on the standby unit.

### Prerequisites



#### CAUTION

Use care when you perform this procedure. This procedure may cause the loss of customer data. Ensure that you have backed up the Policy Controller application database before performing this procedure by using procedure [Perform a manual backup of the Policy Controller database on page 1366](#).

## Action

If reinstalling, upgrading or rolling back the Policy Controller application from an ESD delivered ISO image file, then go to [Reinstall, upgrade or rollback the Policy Controller application from an ISO image file on page 1316](#). Otherwise, continue with this procedure.

### Reinstall, upgrade or rollback the Policy Controller application from a DVD-ROM disk

#### *At the Policy Controller Serial Console*

- 1 Log onto the inactive Policy Controller unit using a secure shell by typing

```
> ssh -l <userid> <inactive_SS_IP_address>
```

and press **Enter**.

where

**userid**

is a valid userid (like mtc) on the Policy Controller

**inactive\_SS\_IP\_address**

is the IP address of the Policy Controller unit

**Example**

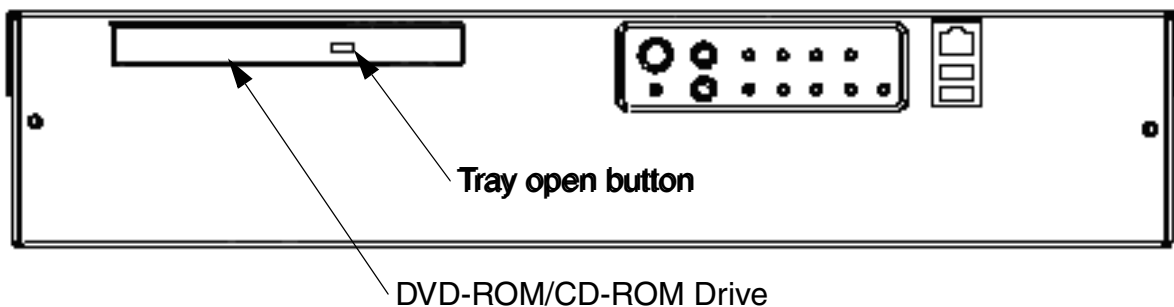
```
ssh -l mtc 45.128.54.12
```

- 2 When prompted, enter your password.

- 3 Change to the root user by typing  
`$ su - root`  
and press **Enter**.
- 4 When prompted, enter the root password.
- 5 Ensure that the DVD-ROM disk containing the Policy Controller Application is inserted before continuing.

**Note:** In some cases the Policy Controller Application may be on its own disk or it may be on the NCGL DVD data disk.

#### ***Policy Controller Front Panel***



- 6 At the prompt, type: `mount /cdrom`  
and press **Enter**.

#### **Example**

```
mount -t iso9660 -o loop
/opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS_07
_MNCL.ISO /cdrom
```

*The operating system may respond with the following warning:*

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

- 7 From the root level, at the prompt, type  
`/cdrom/Tools/InstallApps <app>`

**Note:** For `<app>`, type **spc** or **SPC**  
and press **Enter**.

*The operating system responds:*

```
The Policy Controller Application layer is
currently installed. Do you wish to uninstall
the previous application and install the newer
version? (yes, no)
```

**8** Type**yes**and press **Enter**.*The inactive unit begins installing the application. You will see messages scrolling on the screen.**After confirming the installation, the operating system responds and asks you for a tagname. For an upgrade, the tagname is already installed, but it can be changed.*

-----  
- Get a tag name to allow Multiple HTTPS  
connection through SSPFS -  
-----

Current tag name: SS00

Do you wish to change the tag name (yes, no)

*You will be prompted to change the SPC tagname also.*

-----  
- Get SPC tag name to allow Multiple HTTPS  
connection through SSPFS -  
-----

Current tag name: PC00

Do you wish to change the tag name (yes, no)

*If you do not want to change the tag name, type **no** and press **Enter**. If you want to change the tag name, type **yes**, enter the new tag name (The tag name cannot be **spc**), and press **Enter**.***9** After the application has completed installation, at the prompt, type**cd /**

and press Enter.

**10** Unmount the disk drive by typing**umount /cdrom**

and pressing the Enter key.

**11** Press the tray open button and remove the DVD-ROM disk from the drive.**12** You have completed this procedure. If applicable, return to [Perform a maintenance release upgrade on page 1235](#).



## Reinstall, upgrade or rollback the Policy Controller application from an ISO image file

### *At the Policy Controller Serial Console*

- 1 Log onto the inactive Policy Controller unit using a secure shell by typing

```
> ssh -l <userid> <inactive_SS_IP_address>
```

and pressing the Enter key.

where

**userid**

is a valid userid (like mtc) on the Policy Controller

**inactive\_SS\_IP\_address**

is the IP address or host name of the Policy Controller unit

**Example**

```
ssh -l mtc 45.128.54.12
```

- 2 When prompted, enter your password.

- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

- 5 Verify that the CD/DVD-ROM drive is not currently mounted to the /cdrom directory by typing

```
umount /cdrom
```

and pressing the Enter key.

- 6 At the prompt, type  
**mount -o loop**  
**/opt/swd/<ESD\_ISO\_directory>/<ESD\_file\_ISO> /cdrom**  
and press **Enter**.

where

**ESD\_file\_ISO**

is the name of the maintenance release ISO file

**Example**

```
mount -o loop
/opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_
MNCL.ISO. /cdrom
```

*The operating system responds with the following warning:*

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

- 7 From the root level, at the prompt, type  
**/cdrom/Tools/InstallApps <app>**

**Note:** For <app>, type **spc** or **SPC**  
and press **Enter**.

*The operating system responds:*

```
The Policy Controller Application layer is
currently installed. Do you wish to uninstall
the previous application and install the newer
version? (yes, no)
```

**8** Type**yes**and press **Enter**.*The inactive unit begins installing the application. You will see messages scrolling on the screen.**After confirming the installation, the operating system responds and asks you for a tagname. For an upgrade, the tagname is already installed, but it can be changed.*

```

- Get a tag name to allow Multiple HTTPS
connection through SSPFS -

```

```
Current tag name: SS00
```

```
Do you wish to change the tag name (yes, no)
```

*You will be prompted to change the SPC tagname also.*

```

- Get SPC tag name to allow Multiple HTTPS
connection through SSPFS -

```

```
Current tag name: PC00
```

```
Do you wish to change the tag name (yes, no)
```

*If you do not want to change the tag name, type **no** and press **Enter**. If you want to change the tag name, type **yes**, enter the new tag name (The tag name cannot be **spc**), and press **Enter**.***9** After the application has completed installation, at the prompt, type**cd /**

and press Enter.

**10** Unmount the ISO image by typing**umount -f /opt/swd/<ESD\_ISO\_directory>/<ESD\_file\_ISO>**

and pressing Enter.

**Example**

```
umount -f
/opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_
MNCL.ISO
```

- 11 You have completed this procedure. If applicable, return to the high-level activity [Perform a maintenance release upgrade on page 1235](#).

---

## Invoke a maintenance SwAct of the Policy Controller platform

---

### Purpose of this procedure

This procedure manually performs a maintenance SwAct (switch of activity) of the Policy Controller platform. A SwAct gracefully transitions call processing activity from the active Policy Controller unit to the standby unit without first reloading and reinitializing the Policy Controller application on the standby unit. All call data and Bandwidth resource usage counters for the Policy Application will be maintained during SwAct.

Use this procedure as a standalone task or as part of a maintenance or fault clearing activity like replacing a faulty standby unit or a high-level activity such as upgrading a standby unit.

**Note:** An automatic failover SwAct can be initiated by the platform NCGL in cases of critical faults on the active unit. For more information about conditions required for a SwAct, refer to section "Understanding conditions for a SWACT" found in *Policy Controller Security and Administration*, NN10434-611.

### Limitations and Restrictions

#### ATTENTION

A maintenance SwAct should only be performed when both the active and standby units are operationally enabled and their databases are synchronized.

You cannot SwAct Policy Controller units if the inactive unit Jam state is *jammed*. If the unit Jam state is jammed, refer to procedure [Enable a system SwAct \(Unjam\) on page 1327](#) to unjam the unit.

#### ATTENTION

Logins to the Policy Controller do not survive a platform SwAct.

### Prerequisites

If you are executing a Forced SwAct, confirm that there are no alarm conditions.

## Action

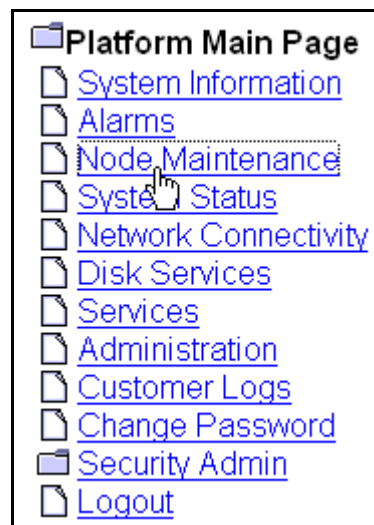
### *At the CS 2000 Session Server Launch Point*

- 1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Click the **Node Maintenance** link.



- 3 Refer to the table in section [Additional status information on page 1323](#) to review the description of the various fields of the Node Maintenance page.

| Unit 0                                                              |                 |                                    |
|---------------------------------------------------------------------|-----------------|------------------------------------|
| <b>Operation State</b>                                              | <b>Activity</b> | <b>Jam State</b>                   |
| Enabled                                                             | Active          | no                                 |
| <b>Maintenance Actions</b>                                          |                 |                                    |
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force |                 | <input type="button" value="Jam"/> |
| <b>Unit 1</b>                                                       |                 |                                    |
| <b>Operation State</b>                                              | <b>Activity</b> | <b>Jam State</b>                   |
| Enabled                                                             | Inactive        | no                                 |

4

**CAUTION**

Due to the risk for loss of data and service outage, it is recommended that the Forced SWACT option not be used except when instructed by your Nortel customer support representative.

To SwAct the Policy Controller units, click the **SWACT** button.

OR

To override any pre-SwAct queries, first click the **Force** check box, then click the **SWACT** button.

**Note:** A forced SWACT overrides any SWACT pre-checks and is not recommended. SWACT pre-checks monitor the inactive unit for critical faults on the platform that should prevent a SWACT. In addition, the pre-check ensures that the Policy Controller application is in-sync. A SWACT force may result in a full service outage on the Policy Controller node if the inactive unit is not in-sync. There are also potential for

losses of provisioned data if a SWACT to an unstable unit is completed.

|                                                                     |        |                                    |
|---------------------------------------------------------------------|--------|------------------------------------|
| Enabled                                                             | Active | no                                 |
| <b>Maintenance Actions</b>                                          |        |                                    |
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force |        | <input type="button" value="Jam"/> |

*The system responds:*

Are you sure you wish to swact? This may cause a service interruption to applications running on this server. Click OK to confirm server swact or cancel to abort.

- 5 Click **Yes** to confirm either the SwAct or forced SwAct.
- 6 Observe the *Activity* field for each unit. Each unit's activity status (whether Active or Inactive) swaps.
- 7 The procedure is complete. If applicable, return to procedure [Perform a maintenance release upgrade on page 1235](#).

### Additional status information

The following table describes the various fields of the Node Maintenance panel.

| Field                                  | Description                                                                                                                                                                                                                                                   |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operation State (unit 0 or 1)          | The operational state of the platform software, either enabled or disabled.                                                                                                                                                                                   |
| Activity (unit 0 or 1)                 | The activity state of the platform software, either active or inactive.                                                                                                                                                                                       |
| Jam State (active unit only)           | Indicates whether or not the unit has been "jammed", preventing the standby unit from being able to become active, regardless of any failures on the active unit. States are either jammed, where a SwAct is disabled, or unjammed, where a SwAct is enabled. |
| Maintenance Actions (active unit only) | Maintenance panel for performing node SWACT activity and to jam or unjam node activity switches.                                                                                                                                                              |



## Verify synchronization status of Policy Controller units

### Purpose of this procedure

Use this procedure to determine the synchronization status of the Policy Controller units. Use this procedure as a standalone task or as part of a higher level activity.

### Limitations and restrictions

There are no limitations or restrictions for this procedure.

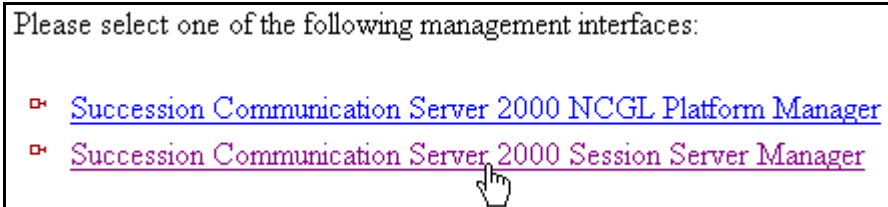
### Prerequisites

There are no prerequisites for this procedure.

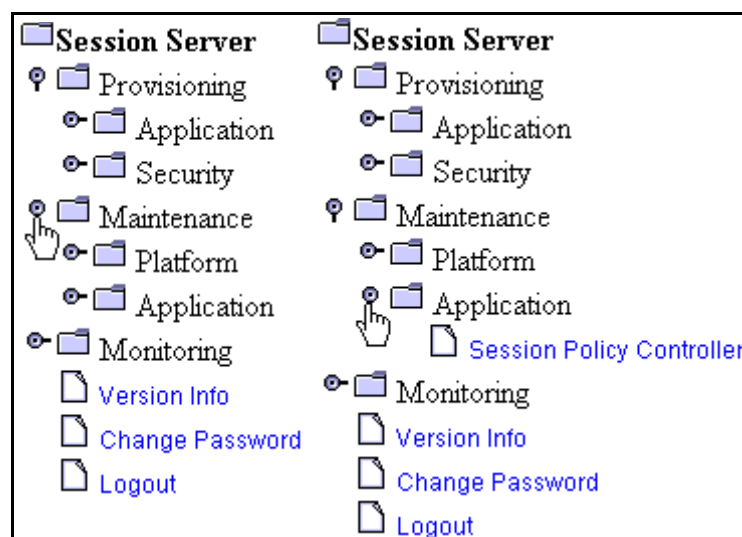
### Action

#### At the CS 2000 Session Server Launch Point

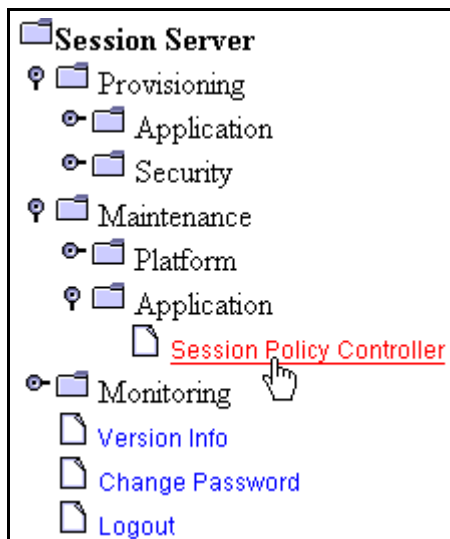
- 1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



- 2 At the **Session Server** folder, click the **Maintenance** folder, then click the **Application** folder.



- 3 Click on the Session **Policy Controller** link.



The **Policy Controller Maintenance** panel opens.

- 4 At the bottom of the **Policy Controller Maintenance** panel, locate and click the **QueryInfo** button.

| Session Policy Controller Status |                   |                   |                |
|----------------------------------|-------------------|-------------------|----------------|
| Administrative State             | Operational State | Procedural Status | Control Status |
| UnLocked                         | Enabled           | -                 | -              |

| Session Policy Controller Maintenance                  |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |
| <div>Refresh</div> <div>QueryInfo</div>                |                                         |

- 5 The synchronization status of the Policy Controller units displays at the bottom of the query results panel.

If the units are not in sync, execute procedure *View Policy Controller alarms*, found in *Policy Controller Fault Management*, NN10438-911 and check for alarm conditions.

|                                                 |           |
|-------------------------------------------------|-----------|
| Refresh                                         | QueryInfo |
| Last Performed Operation: Query Number of Calls |           |
| Result: Passed                                  |           |
| Number Of Active Calls: 0                       |           |
| Session Policy Controller is: Not InSync        |           |

- 6 You have completed this procedure. If you were forwarded to this procedure by another procedure, return to that procedure and continue.

---

## Enable a system SwAct (Unjam)

---

### Purpose of this procedure

Use the Unjam command to manually enable a SwAct (switch of activity) of the active and stand-by units by allowing the two units to toggle their operational states.

### Limitations and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as replacing a faulty standby unit or upgrading a standby unit.

### Prerequisites

There are no prerequisites for performing this procedure.

### Action

#### Enable a system SwAct (Unjam)

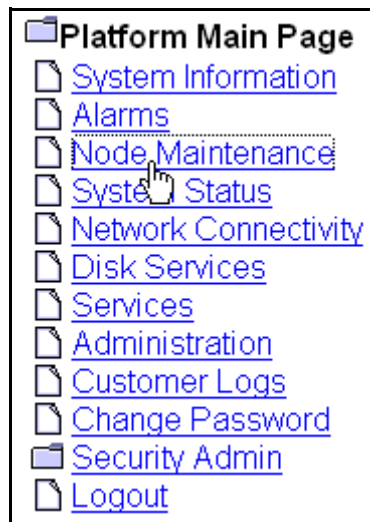
##### *At the CS 2000 Session Server Launch Point*

- 1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Click the **Node Maintenance** link.



- 3 Determine if the Jam State of the standby unit is **Yes** or **No**. If it is **No**, then the unit is already unjammed and you are done with this procedure. If it is **Yes**, then continue with [step 4](#).

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | yes       |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                      |
|---------------------------------------------------------------------|--------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Unjam"/> |

- 4 Click the **UnJam** button.

*The system responds:*

Info: Unjam - Command passed.

- 5 Observe the Jam state for the standby Policy Controller unit transitions from **Yes** to **No**.

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | no        |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Jam"/> <input type="checkbox"/> Force |

- 6 You have completed this procedure. If applicable, return to [Perform a maintenance release upgrade on page 1235](#).

---

## Rollback a Policy Controller NCGL platform software upgrade

---

### Purpose of this procedure

This procedure describes how to use the NCGL Platform Manager software to rollback a maintenance release NCGL platform.

#### ATTENTION

Only use this procedure as part of the high level activities [Aborting a maintenance release upgrade on page 1242](#) or [Performing an emergency maintenance release rollback on page 1244](#).

### Limitations and Restrictions

You can only rollback to a previous load if it exists on the Policy Controller unit disk drive. If not, you must reinstall the load onto the disk drive from DVD-ROM disk or ESD ISO image. Refer to section [Preparing to upgrade the Policy Controller on page 1232](#) for instructions to perform this activity.

### Prerequisites

#### ATTENTION

This procedure assumes that you are experiencing problems with a maintenance release upgrade on a single Policy Controller unit and that you have not upgraded the second unit in the node with the maintenance release. If you have already upgraded both units with the maintenance release and are having problems, then refer first to section [Performing an emergency maintenance release rollback on page 1244](#) for the complete prerequisite steps.

## Action

### *At the CS 2000 Session Server Launch Point*

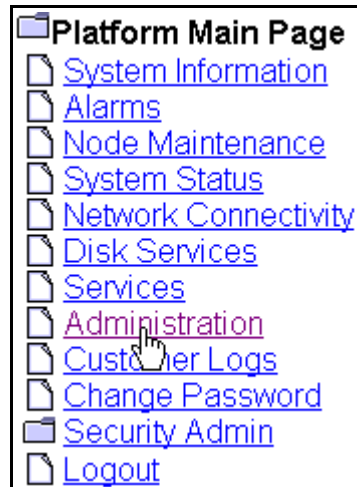
- 1 Select **Succession Communication Server 2000 NCGL Platform Manager** from the launch point menu.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

*The Platform Main Page menu is displayed.*

- 2 Click the **Administration** link.





- 3 Select the bootloader version that you want to roll the NCGL platform back to and click the **Set default** button.

The Platform Administration panel does not update automatically!  
Datestamp of last update: Tuesday September 21st 2004 02:59:18 PM EDT

| Bootload Management |                                                                                  |
|---------------------|----------------------------------------------------------------------------------|
| Bootload            | Maintenance                                                                      |
| 5.36.1.0.0409032059 | Default Bootload                                                                 |
| 5.26.1.0.0406231534 | <input type="button" value="Set default"/> <input type="button" value="Delete"/> |

- 4 Verify that the default bootloader has been set to the version previous to the maintenance release upgrade.

| Bootload Management |                                                                                  |
|---------------------|----------------------------------------------------------------------------------|
| Bootload            | Maintenance                                                                      |
| 5.36.1.0.0409032059 | <input type="button" value="Set default"/> <input type="button" value="Delete"/> |
| 5.26.1.0.0406231534 | Default Bootload                                                                 |

| Software Upgrade |          |          |            |      |
|------------------|----------|----------|------------|------|
| Protocol         | Login ID | Password | IP address | File |
|                  |          |          |            |      |

| Server Maintenance                                                   |                                                                    |
|----------------------------------------------------------------------|--------------------------------------------------------------------|
| Unit 0 - Active                                                      |                                                                    |
| <input type="button" value="Reboot"/> <input type="checkbox"/> Force | <input type="button" value="Halt"/> <input type="checkbox"/> Force |

- 5 You have completed this procedure. Return to your applicable high-level activity: [Aborting a maintenance release upgrade on page 1242](#) or [Performing an emergency maintenance release rollback on page 1244](#).

## Additional information

By default, the Policy Controller units retain previous bootloads. For housekeeping purposes, older bootloader versions may be manually removed by clicking the **Remove** button.

**Note:** You cannot delete the bootloader that is set to be the default bootloader, nor can you delete the currently running bootloader.

If a bootloader image upgrade is requested and insufficient disk space is available in the `/boot` directory, the NCGL software deletes the oldest bootloader from the `/boot` directory and performs the requested bootloader image upgrade. The system can not delete a bootloader that is set to be the default bootloader.

| Bootload Management |                                            |                                       |
|---------------------|--------------------------------------------|---------------------------------------|
| Bootload            | Maintenance                                |                                       |
| 4.0.0.0303171003    | Default Bootload                           |                                       |
| 4.0.0.0303101433    | <input type="button" value="Set default"/> | <input type="button" value="Remove"/> |
| 4.0.0.0303051030    | <input type="button" value="Set default"/> | <input type="button" value="Remove"/> |
| 4.0.0.0303051012    | <input type="button" value="Set default"/> | <input type="button" value="Remove"/> |

## Drop database synchronization for the Policy Controller application

### Purpose of this procedure

Use this procedure to drop call processing application and application database synchronization between the active and inactive Policy Controller units.

#### ATTENTION

Only use this procedure as part of the high level activity [Performing an emergency maintenance release rollback on page 1244](#).

### Limitations and restrictions

Perform this procedure only on the active Policy Controller unit.

After this procedure has executed, the Policy Controller application database continues in a non-synchronized state until a SwAct is performed.



#### CAUTION

Use care when you use this procedure as this procedure may cause the loss of customer data. Ensure that you have backed up the Policy Controller application database on the active unit before executing this procedure.

### Prerequisites

There are no prerequisites for performing this procedure.

### Action

| If                                                                     | Then                                                                                      |
|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| you are performing this procedure from a DVD-ROM disk                  | go to procedure <a href="#">Run dropSync script from a DVD-ROM disk on page 1335</a> .    |
| you are performing this procedure from an ESD delivered ISO image file | go to procedure <a href="#">Run dropSync script from an ISO image file on page 1336</a> . |

## Run dropSync script from a DVD-ROM disk

### *At the Policy Controller Serial Console*

- 1 Log onto the active Policy Controller unit using a secure shell by typing  

```
> ssh -l <userid> <active_SS_IP_address>
```

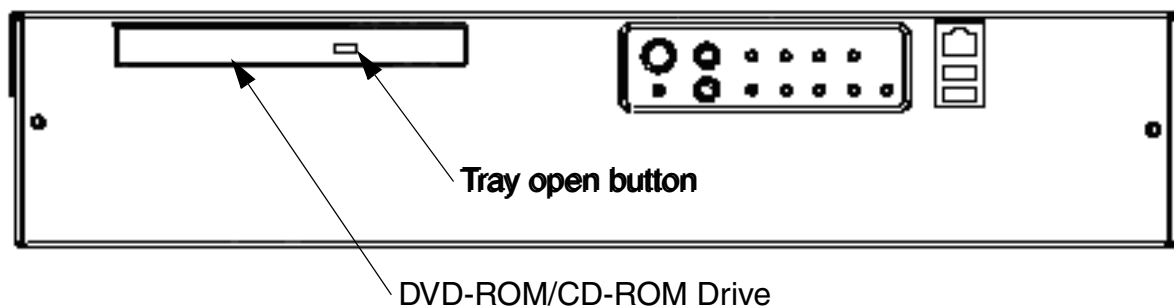
and pressing the Enter key.  
where  
**userid**  
is a valid userid (like mtc) on the Policy Controller  
**active\_SS\_IP\_address**  
is the IP address of the active Policy Controller unit  
**Example**  

```
ssh -l mtc 45.128.54.12
```
- 2 When prompted, enter your password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Ensure that the latest version of the software installation DVD-ROM disk is inserted into the active unit before continuing.

### *Policy Controller Front Panel*



- 6 At the prompt, type  
**mount /cdrom**  
and press Enter.

*The operating system responds with the following warning:*

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

- 7 From the root level, at the prompt, type  
**./cdrom/Tools/dropSync**  
and press Enter.
- 8 After you are returned to the prompt, type  
**cd /**  
and press Enter.
- 9 Unmount the disk drive by typing  
**umount /cdrom**  
and pressing the Enter key.
- 10 If desired, press the tray open button and remove the DVD-ROM disk from the drive.
- 11 You have completed this procedure. Return to the high-level activity [Performing an emergency maintenance release rollback on page 1244](#).

## Run dropSync script from an ISO image file

### *At the Policy Controller Serial Console*

- 1 Log onto the active Policy Controller unit using a secure shell by typing  
**> ssh -l <userid> <active\_SS\_IP\_address>**  
and pressing the Enter key.  
where

#### **userid**

is a valid userid (like mtc) on the Policy Controller

#### **active\_SS\_IP\_address**

is the IP address of the active Policy Controller unit

#### **Example**

```
ssh -l mtc 45.128.54.12
```

- 2 When prompted, enter your password.
- 3 Change to the root user by typing  
**\$ su - root**  
and pressing the Enter key.

- 4 When prompted, enter the root password.
- 5 Verify that the CD/DVD-ROM drive on the active unit is not currently mounted to the /cdrom directory by typing  
**umount /cdrom**  
and pressing the Enter key.
- 6 At the prompt, type  
**mount -t iso9660 -o loop**  
**/opt/swd/<ESD\_ISO\_directory>/<ESD\_file\_ISO> /cdrom**  
and press **Enter**.  
where  
**ESD\_file\_ISO**  
is the name of the maintenance release ISO file  
**Example**  
mount -t iso9660 -o loop  
/opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07\_  
MNCL.ISO /cdrom  
*The operating system responds with the following warning:*  
mount: block device /dev/hda is  
write-protected, mounting read-only
- 7 From the root level, at the prompt, type  
**./cdrom/Tools/dropSync**  
and press **Enter**.
- 8 After the application has completed installation, at the prompt, type  
**cd /**  
and press Enter.
- 9 Umount the ISO image by typing  
**umount -f /opt/swd/<ESD\_ISO\_directory>/<ESD\_file\_ISO>**  
and pressing Enter.  
**Example**  
umount -f  
/opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07\_  
MNCL.ISO
- 10 You have completed this procedure. Return to the high-level activity [Performing an emergency maintenance release rollback on page 1244](#).

---

## Suspend the Policy Controller application

---

### Purpose of this procedure

Use this procedure to temporarily take the Policy Controller application out of service.

**Note:** For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section of *Policy Controller Security and Administration*, NN10434-611.

### Limitations and restrictions

This procedure can only be performed when the Policy Controller application is in the following service states:

- the Operational State is **Enabled**
- the Administrative State is **Locked**

### Prerequisites

The Policy Controller application must have previously been locked. If it is not locked or you are uncertain of the state of the application, refer to procedure [Lock the Policy Controller application on page 1342](#).

### Action



#### CAUTION

This procedure is used to temporarily take the Policy Controller out of service. Suspending the Policy Controller Application means the lines or gateways configured for Network Virtual Call Admission Control will be processed by the CS 2000 without the Virtual Call Admission Control function. When the Policy Controller is suspended, it is equivalent to being unreachable by the CS2000, but the Lines or Gateways will be able to continue to make or receive calls without the Policy Controller.

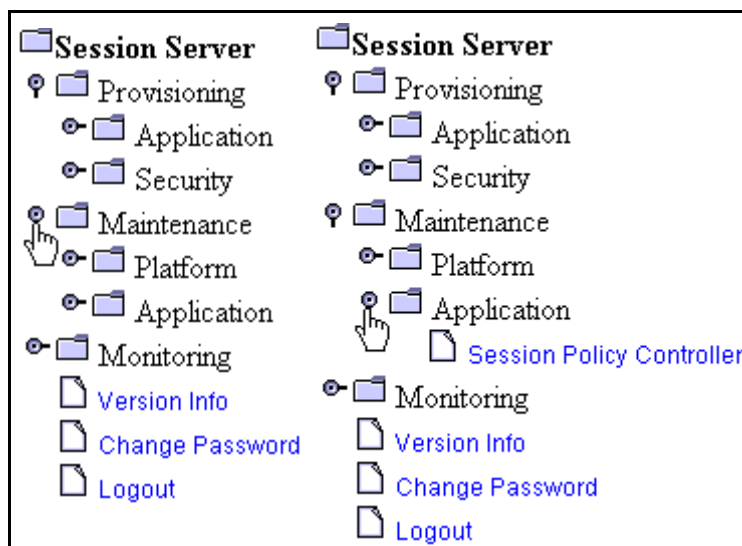
#### *At the CS 2000 Session Server Launch Point*

- 1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

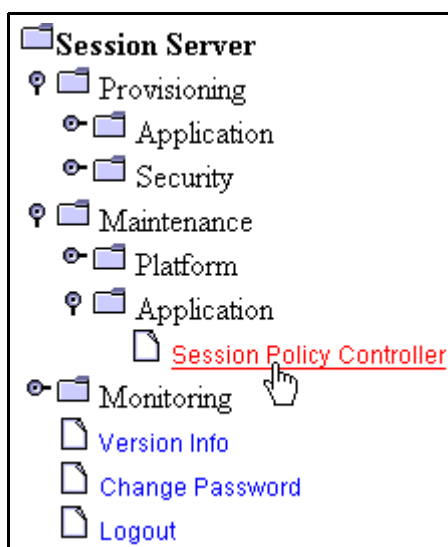
Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 At the Session Server folder, click the **Maintenance folder**, then click the **Application** folder.



- 3 Click the **Session Policy Controller** link to open it.



- 4 In the Policy Controller Maintenance panel click **Suspend**.



| Session Server Status - Connected to Unit #0 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Active         | Enabled           |
| 1                                            | unknown        | Disabled          |

| Session Policy Controller Status |                   |                   |                |
|----------------------------------|-------------------|-------------------|----------------|
| Administrative State             | Operational State | Procedural Status | Control Status |
| Locked                           | Enabled           | -                 | -              |

| Session Policy Controller Maintenance                  |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh QueryInfo

- 5 Monitor the status of the Policy Controller application in the Policy Controller Status box:
- the Operational State changes to **Disabled**
  - the Control Status changes to **Suspended**

| Session Server Status - Connected to Unit #0 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Active         | Enabled           |
| 1                                            | unknown        | Disabled          |

| Session Policy Controller Status |                   |                   |                |
|----------------------------------|-------------------|-------------------|----------------|
| Administrative State             | Operational State | Procedural Status | Control Status |
| Locked                           | Disabled          | -                 | Suspended      |

| Session Policy Controller Maintenance                  |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh

QueryInfo

- 6 If applicable, restart the Policy Controller application by executing procedure [Unlock the Policy Controller application on page 1362](#).
- 7 The procedure is complete.

## Lock the Policy Controller application

### Purpose of this procedure

Use the following procedure to change the administrative status of the Policy Controller application to Locked. This will cause all call data to be reset, and will also automatically reset Bandwidth resource usage counters to zero for the Policy Controller.

**Note:** For more detailed information about Policy Controller application services states and administrative functions, refer to *Policy Controller Security and Administration*, NN10434-611.

### Limitations and restrictions



#### CAUTION

This is a service affecting procedure. Locking the Policy Controller application prevents any lines configured for Virtual Call Admission Control via the Policy Controller to make or receive calls. Existing calls regardless of call state will not be released by this procedure. However, once locked, the Policy Controller application will not be able to process any new VCAC requests.

**Note:** The CS 2000 will still process calls without Network VCAC if it determines the Policy Controller is in Locked State.

This procedure provides instructions for changing the service status of the Policy Controller application software only. For instructions on determining the status of the Policy Controller platform, refer to procedure [View the operational status of a Policy Controller NCG platform on page 1266](#)

### Prerequisites

There are no prerequisites for this procedure.

### Action

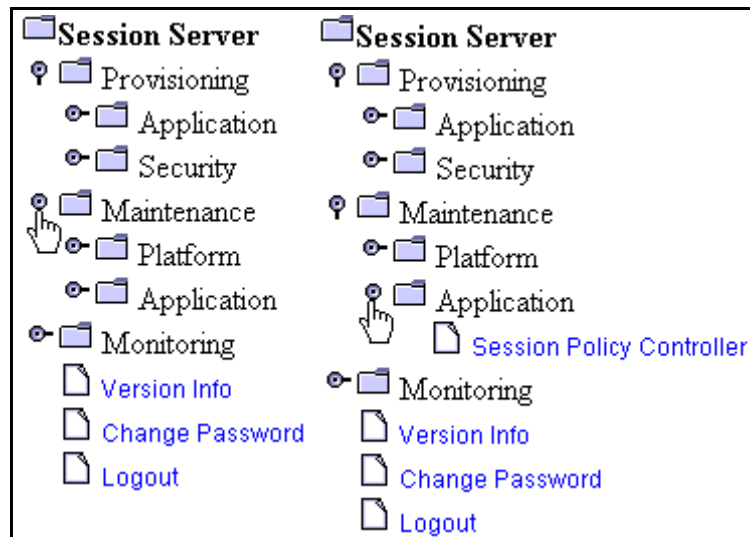
#### ***At the CS 2000 Session Server Launch Point***

- 1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

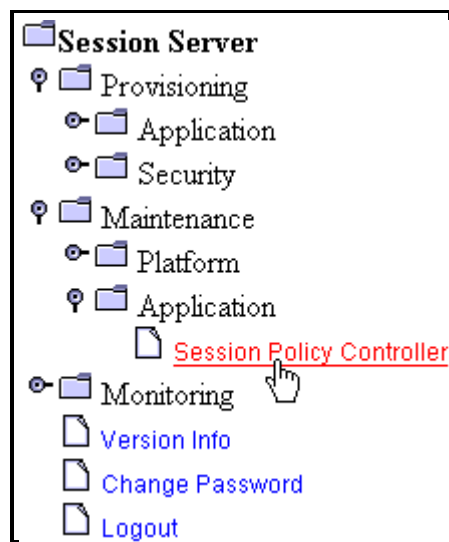
Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 At the Session Server folder, click the **Maintenance** folder, then click the **Application** folder.



- 3 Click on the **Session Policy Controller** link to open it.



- 4 In the Policy Controller Maintenance panel click the **Lock** button.

| Session Server Status - Connected to Unit #0 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Active         | Enabled           |
| 1                                            | unknown        | Disabled          |

| Session Policy Controller Status |                   |                   |                |
|----------------------------------|-------------------|-------------------|----------------|
| Administrative State             | Operational State | Procedural Status | Control Status |
| UnLocked                         | Enabled           | -                 | -              |

| Session Policy Controller Maintenance                  |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh QueryInfo

The system responds with the following message box:

This action will release all existing Session Policy Controller calls and will cause a SERVICE OUTAGE on this Session Server. There are x active calls. Do you wish to continue?

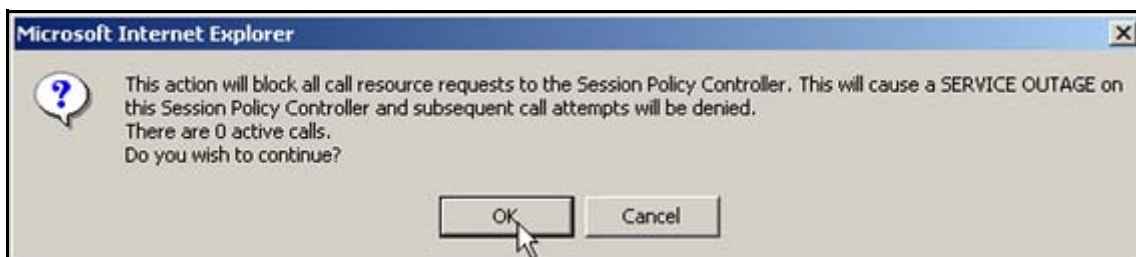
## 5

**CAUTION**

This is a service affecting procedure. Locking the Policy Controller application prevents any lines configured for Virtual Call Admission Control via the Policy Controller to make or receive calls. Existing calls regardless of call state will not be released by this procedure. However, once locked, the Policy Controller application will not be able to process any new VCAC requests.

**Note:** The CS 2000 will still process calls without Network VCAC if it determines the Policy Controller is in Locked State.

Click **OK** to confirm locking the Policy Controller application or click **Cancel** to cancel the action and close the message box.



- 6 Monitor the status of the Policy Controller application in the Policy Controller Status box:
- the Administrative State changes to **Locked**

| Session Server Status - Connected to Unit #0 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Active         | Enabled           |
| 1                                            | unknown        | Disabled          |

| Session Policy Controller Status |                   |                   |                |
|----------------------------------|-------------------|-------------------|----------------|
| Administrative State             | Operational State | Procedural Status | Control Status |
| Locked                           | Enabled           | -                 | -              |

| Session Policy Controller Maintenance                  |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |
| <div>Refresh</div> <div>QueryInfo</div>                |                                         |

The status panel refreshes automatically according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the **Refresh Rate** button. Otherwise, manually refresh the panel by clicking on the **Refresh** button on the **Session Policy Controller Maintenance** panel.

This page updates automatically every 60 seconds!  
 Last update: Mon Jan 31 03:39:52 CST 2005

1 min

▼

Refresh Rate

- 7 You have completed this procedure.

---

## View the operational status of the Policy Controller application

---

### Purpose of this procedure

Use the following procedure to view the service status of the Policy Controller application. This procedure may be used as a standalone task or as part of a high-level activity.

### Limitations and restrictions

This procedure provides instructions for determining the service status of the Policy Controller application software only. For instructions on determining the status of the Policy Controller platform, refer to procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#).

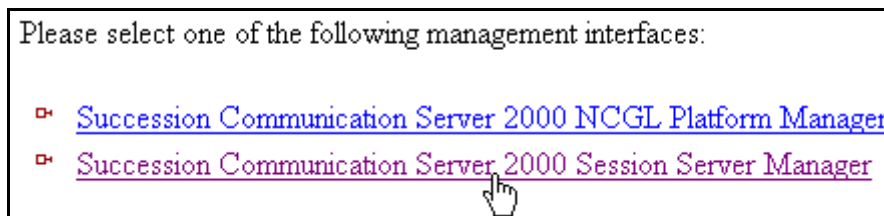
### Prerequisites

There are no prerequisites for this procedure.

### Action

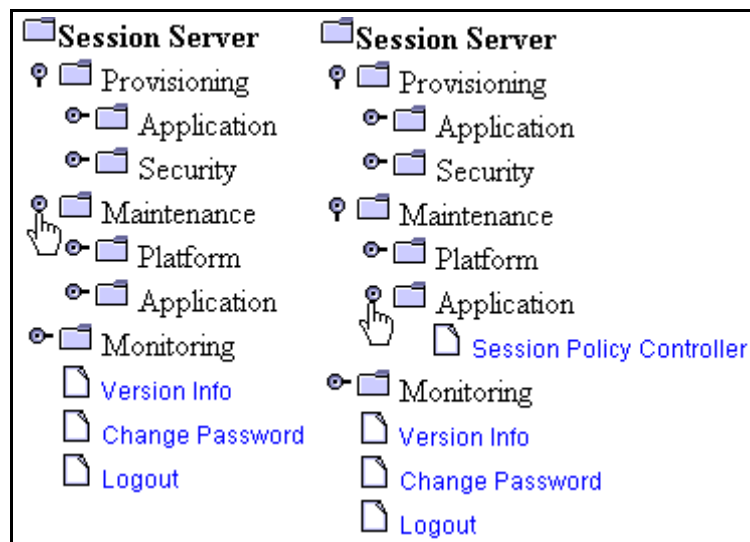
#### ***At the CS 2000 Session Server Launch Point***

- 1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

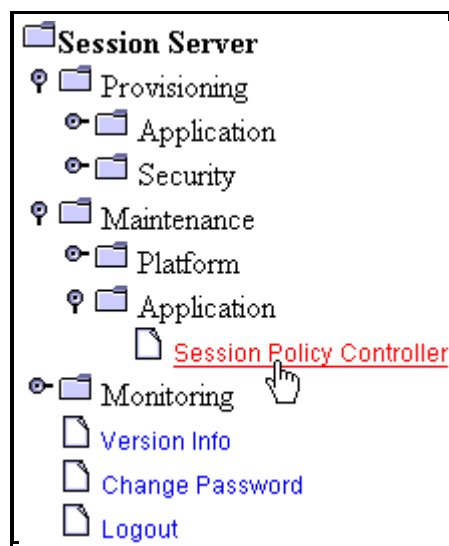


- 2 At the **Session Server** folder, click the **Maintenance** folder, then click the **Application** folder.





- 3 Click on the **Policy Controller** folder to open it.



- 4 Monitor the status of the Policy Controller application on the active Policy Controller node from this view.

| Session Server Status - Connected to Unit #1 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Inactive       | Enabled           |
| 1                                            | Active         | Enabled           |

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh QueryInfo

Last Performed Operation: Refresh

Result: Passed

SIP Cold SwAct

This page updates automatically every 10 seconds!  
Last update: Thu Jun 10 13:04:20 EDT 2004

10 sec Refresh Rate

**Note:** This view is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the **Refresh Rate** button or manually refresh the page by clicking the **Refresh** button.

- 5 Refer to section [Interpreting Policy Controller application status and maintenance fields on page 1351](#) to review the description of the various fields of this view.

**Note:** For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section "Interpreting Policy Controller application states" in *Policy Controller Security and Administration*, NN10434-611.

- 6 To perform available Policy Controller application maintenance activities, refer to the following procedures in *Policy Controller Security and Administration*, NN10434-611:
- Lock the Policy Controller application
  - Unlock the Policy Controller application
  - Suspend the Policy Controller application
  - Unsuspend the Policy Controller application
  - Shutdown the Policy Controller application
  - Cold SwAct the Policy Controller application
- 7 To view the number of active calls currently being handled by the application and the sync status of the Policy Controller units, click the **QueryInfo** button.

|                                                 |           |
|-------------------------------------------------|-----------|
| Refresh                                         | QueryInfo |
| Last Performed Operation: Query Number of Calls |           |
| Result: Passed                                  |           |
| Number Of Active Calls: 0                       |           |
| Units #0 and #1 are: In Sync                    |           |

- 8 You have completed this procedure.

## Interpreting Policy Controller application status and maintenance fields

Use the following table to assist you in interpreting the Policy Controller Status area.

### Policy Controller node status field descriptions

| Field                      | Description                                                                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit Connection Status Bar | Indicates which Policy Controller unit in the node the CS 2000 Policy Controller Manager is connected to.                                                 |
| Unit Number                | indicates the units in the Policy Controller node, (labelled 0 and 1) and a maximum of one node on the Call Server-LAN                                    |
| Activity State             | indicates which unit is Active and which is Inactive (standby), also an indirect indicator of fault-tolerant status, assuming both units are operational. |
| Operational State          | indicates the service status of each Policy Controller unit (either Enabled or Disabled).                                                                 |

Use the following table to assist you in interpreting the Policy Controller status area.

### Policy Controller application Status field descriptions

| Field                | indication                     |
|----------------------|--------------------------------|
| Administrative State | Locked, Unlocked, ShuttingDown |
| Operational State    | Enabled or Disabled            |
| Procedural Status    | Terminating or -               |
| Control Status       | Suspended or -                 |

Use the following table to assist you in interpreting the Policy Controller area's CCITT X.731-style and related DMS-style status indicators:

**Policy Controller Maintenance field descriptions and interpretation of service states**

| Administrative State                              | Operational State | Procedural Status | Control Status | DMS style Service States          |
|---------------------------------------------------|-------------------|-------------------|----------------|-----------------------------------|
| Locked                                            | Disabled          | -                 | Suspended      | Offline (OFFL)                    |
| Locked                                            | Enabled           | -                 | -              | Manual Busy (MANB)                |
| Locked                                            | Enabled           | Terminating       | -              | Manual Busy Transitioning (MANBP) |
| Unlocked                                          | Enabled           | -                 | -              | In Service (INSV)                 |
| Unlocked                                          | Disabled          | -                 | -              | System Busy (SYSB)                |
| Shutting Down                                     | Enabled           | -                 | -              | Going out of service (INSVD)      |
| <b>Note:</b> (-) indicates a status of in-service |                   |                   |                |                                   |

---

## Unsuspend the Policy Controller application

---

### Purpose of this procedure

Use the following procedure to bring the Policy Controller application back into service without restarting the Policy Controller application.

**Note:** For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section "Interpreting Policy Controller application states" in *Policy Controller Security and Administration*, NN10434-611.

### Limitations and restrictions

This procedure can only be performed when the Policy Controller application is in the following service states:

- the Operational State is **Disabled**
- the Administrative State is **Locked**
- the Control Status is **Suspended**

### Prerequisites

The Policy Controller application must previously have been suspended. If it is not suspended or you are uncertain of the state of the application, refer to procedure [Suspend the Policy Controller application on page 1338](#).

### Action

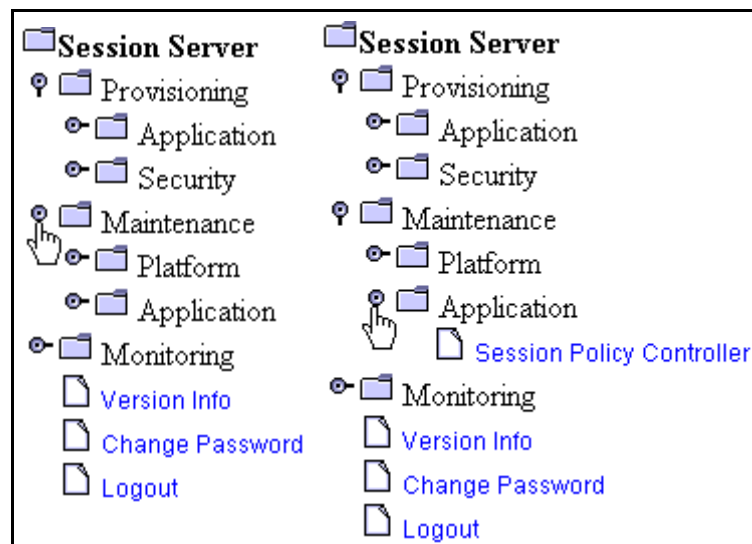
#### ***At the CS 2000 Session Server Launch Point***

- 1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

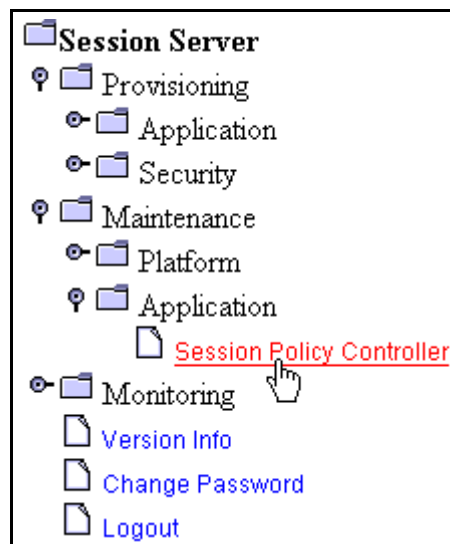
Please select one of the following management interfaces:

- ❑ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ❑ [Succession Communication Server 2000 Session Server Manager](#)

- 2 At the **Session Server** folder, click the **Maintenance** folder, then click the **Application** folder.



- 3 Click on the **Policy Controller** folder to open it.



- 4 In the Policy Controller panel click **Unsuspend**.

| Session Server Status - Connected to Unit #0 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Active         | Enabled           |
| 1                                            | unknown        | Disabled          |

| Session Policy Controller Status |                   |                   |                |
|----------------------------------|-------------------|-------------------|----------------|
| Administrative State             | Operational State | Procedural Status | Control Status |
| Locked                           | Disabled          | -                 | Suspended      |

| Session Policy Controller Maintenance                  |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh QueryInfo



- 5 Monitor the status of the Policy Controller application in the Policy Controller Status box:
- the Operational State changes to **Enabled**
  - the Control status changes to -

| Session Server Status - Connected to Unit #0 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Active         | Enabled           |
| 1                                            | unknown        | Disabled          |

| Session Policy Controller Status |                   |                   |                |
|----------------------------------|-------------------|-------------------|----------------|
| Administrative State             | Operational State | Procedural Status | Control Status |
| Locked                           | Enabled           | -                 | -              |

| Session Policy Controller Maintenance                  |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh

QueryInfo

- 6 If necessary, bring the Policy Controller application back into service by executing procedure [Unlock the Policy Controller application on page 1362](#).
- 7 You have completed the procedure.

---

## Prepare for a database restore on a Policy Controller unit

---

### Purpose of this procedure

Use this procedure to prepare for a restoration of the Policy Controller application database from a backup copy.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of procedure [Performing an emergency maintenance release rollback on page 1244](#).

### Limitations and Restrictions



#### CAUTION

Performing a restore of the Policy Controller application database is a service affecting activity and can cause data mismatches at the Communication Server 2000.

#### ATTENTION

For security reasons, you can only copy the database file from a remote server to the /users/mtc directory on the unit and you must use the secure copy command **scp** to perform this activity.

Automatic backup of the Policy Controller application database occurs at 1:00 AM each day on both Policy Controller units. This configuration setting cannot be modified and does not impact the use of this procedure.

The name of the backup database file is *solid.db*. Do not modify this name.

### Prerequisites

You must have secure copy (scp) access to the Policy Controller unit from the remote system or other server location from where the database backup file *solid.db* is copied.

## Action

### ***From the remote server where the backup database file is located***

- 1 Log onto the remote server, locate and navigate to the directory where the backup copy of the database file is stored.
- 2 Secure copy the database file to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
$ scp solid.db mtc@<SS_IP_address>:
```

and pressing the Enter key.

where

#### **SS\_IP\_address**

is the IP address of the Policy Controller unit

*The database file is copied to the /user/mtc directory on the target Policy Controller unit. This is the only Policy Controller directory that files can be copied into from an external server.*

### ***At a Policy Controller command line interface***

- 3 Open a secure shell to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
> ssh -l <userid> <SS_IP_address>
```

and pressing the Enter key.

where

#### **userid**

is a valid userid (like mtc) on the Policy Controller

#### **SS\_IP\_address**

is the IP address of the Policy Controller

#### **Example**

```
ssh -l mtc 45.128.54.12
```

- 4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 5 When prompted, enter the root password.

- 6 Move the solid.db file you copied in [step 2](#) from the /user/mtc directory to the /opt/apps/database/solid/backup directory by typing  

```
$ mv /users/mtc/solid.db
/opt/apps/database/solid/backup
```

and pressing the Enter key.
- 7 Change directory to the backup database directory by typing  

```
$ cd/opt/apps/database/solid/backup
```

and pressing the Enter key.
- 8 Verify that the correct version (based on the file date) of the solid.db database file that you want to restore is located in the directory by typing  

```
$ ls -l /opt/apps/database/solid/backup
```

and pressing the Enter key.
- 9 Verify that the presence of files *solid.ini* and *solmsg.out* files are also in the /opt/apps/database/solid/backup directory.

**ATTENTION**

The restorebackup.sh script does not run if you do not have the solid.ini and solmsg.out files located in the correct directory.

- 10 If the solid.ini file is not present, copy it into the backup directory by typing  

```
$ cp /opt/apps/database/solid/dbfiles/solid.ini
/opt/apps/database/solid/backup/solid.ini
```

and pressing the Enter key
- 11 If the solmsg.out file is not present, copy it into the backup directory by typing  

```
$ cp
/opt/apps/database/solid/dbfiles/solmsg.out
/opt/apps/database/solid/backup/solmsg.out
```

and pressing the Enter key
- 12 Change the ownership of all files in the backup directory by typing  

```
$ chown soliddb *
```

and pressing the Enter key.

- 13 Change the group of all files in the backup directory by typing  
`$ chgrp adm *`  
and pressing the Enter key.
- 14 Change the access permissions for all files in the backup directory by typing  
`$ chmod 600 *`  
and pressing the Enter key.
- 15 The database is now ready to be restored. You have completed this procedure. Return to the high-level activity.

## Additional information

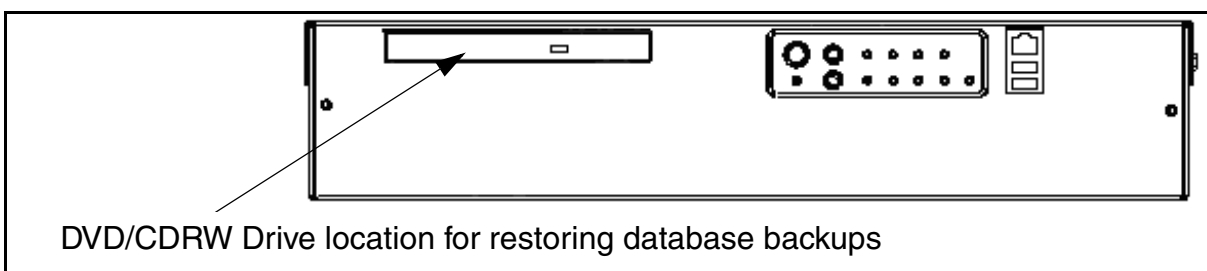
This section provides additional information regarding database restore activities.

### To restore a backup database saved to a CD.

If you must restore a database backup that has been saved to a CD, you must first copy the database file from the CD to the default backup directory on the active Policy Controller unit. The selected backup database file must be restored to the following location:

*/opt/apps/database/solid/backup/solid.db*

To restore a backup of the database file to the backup directory, you must use a Policy Controller command line interface to copy the database file from a CD or CD-RW disk containing a copy of the backup database file to the `opt/apps/database/solid/backup` directory.



Ensure that you remove the CD disk from the DVD/CDRW drive, and store it in a safe place when you are done.

### To restore a database backup save to another system

If you must restore a database backup that has been saved to another system, you must first copy the database file from the remote system back to the default backup directory on the active Policy Controller unit.

The selected backup database file must be restored to the following location:

*/opt/apps/database/solid/backup*

To restore a backup of the database to the backup directory you must use a Policy Controller command line interface to copy the database file `solid.db` from the remote system to the `opt/apps/database/solid/backup` directory. You may also be able to remote copy the backup database file from the remote system to the Policy Controller `opt/apps/database/solid/backup` directory. However, for security reasons, you may need to consult your site network administrator for instructions and permission to perform a remote copy.

---

## Unlock the Policy Controller application

---

### Purpose of this procedure

Use the following procedure to change the administrative status of the Policy Controller application to Unlocked, bringing the application into service.

**Note:** For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section of *Policy Controller Security and Administration*, NN10434-611.

### Limitations and restrictions

This procedure provides instructions for changing the service status of the Policy Controller application software only. For instructions on determining the status of the Policy Controller platform, refer to procedure [View the operational status of a Policy Controller NCGL platform on page 1266](#)

### Prerequisites

The active Policy Controller unit must be in a locked Administrative state. If it is not locked or you are uncertain of the state of the application, refer to procedure [Lock the Policy Controller application on page 1342](#).

### Action

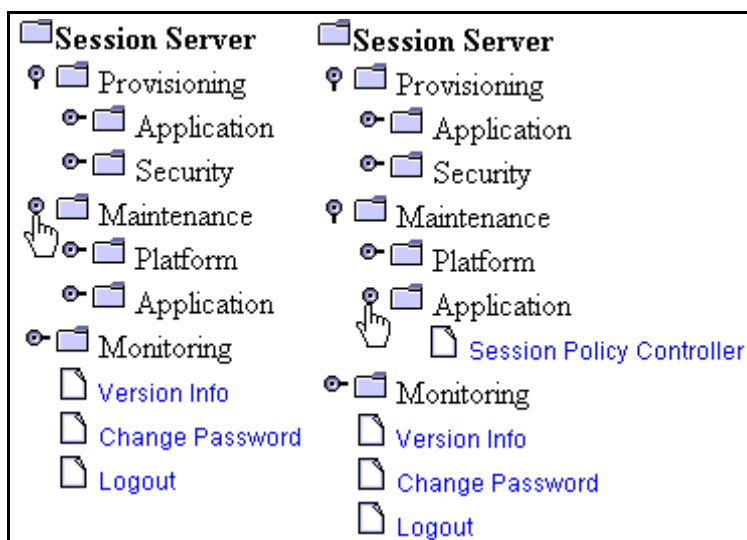
#### ***At the CS 2000 Session Server Launch Point***

- 1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

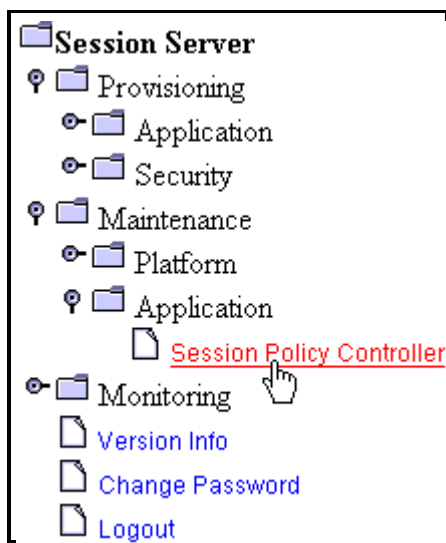
Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 At the Session Server folder, click the **Maintenance** folder, then click the **Application** folder.



- 3 Click on the **Policy Controller** folder to open it.



- 4 In the Policy Controller panel, click the **Unlock** button.



| Session Server Status - Connected to Unit #0 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Active         | Enabled           |
| 1                                            | unknown        | Disabled          |

| Session Policy Controller Status |                   |                   |                |
|----------------------------------|-------------------|-------------------|----------------|
| Administrative State             | Operational State | Procedural Status | Control Status |
| Locked                           | Enabled           | -                 | -              |

| Session Policy Controller Maintenance                  |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh

QueryInfo

- 5 Monitor the status of the Policy Controller application in the Session Policy Controller Status box:
- the Administrative State changes to **Unlocked**

| Session Server Status - Connected to Unit #0 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Active         | Enabled           |
| 1                                            | unknown        | Disabled          |

| Session Policy Controller Status |                   |                   |                |
|----------------------------------|-------------------|-------------------|----------------|
| Administrative State             | Operational State | Procedural Status | Control Status |
| UnLocked                         | Enabled           | -                 | -              |

| Session Policy Controller Maintenance                  |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

The status panel refreshes automatically according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the **Refresh Rate** button. Otherwise, manually refresh the panel by clicking on the **Refresh** button on the **Session Policy Controller Maintenance** panel.

|                                                                                                |                                             |
|------------------------------------------------------------------------------------------------|---------------------------------------------|
| This page updates automatically every 60 seconds!<br>Last update: Mon Jan 31 03:39:52 CST 2005 |                                             |
| <div>1 min</div>                                                                               | <input type="button" value="Refresh Rate"/> |

- 6 You have completed this procedure.

---

## Perform a manual backup of the Policy Controller database

---

### Purpose of this procedure

Use this procedure to do the following tasks:

- Perform a backup of the Policy Controller application database of the active Policy Controller unit.
- Create regular backup copies of the database or as a precautionary activity before starting a maintenance release upgrade of the Policy Controller application.
- Perform as a standalone task or as part of a higher level upgrade activity



#### CAUTION

If you perform provisioning changes during this procedure, it can lead to database corruption and possible system outages. To ensure that you create an accurate and complete copy of the active unit database, verify that all provisioning changes are stopped before continuing this procedure.

### Prerequisites

#### ATTENTION

The Policy Controller database and the CS 2000 database must always be in sync. CS 2000 core images, CS 2000 GWC Manager Oracle database backups, and the Policy Controller application backups must always be maintained in sync for emergency recovery. To ensure they are in sync, perform images and backups at the same time.

## Action

### *At a client workstation on the CS-LAN or IEMS client*

- 1 Log into the active Policy Controller unit using a secure shell by typing

```
> ssh -l <userid> <active_SS_IP_address>
```

and pressing the Enter key.

where

**userid**

is a valid userid (like mtc) on the Policy Controller

**active\_SS\_IP\_address**

is the IP address of the active Policy Controller

**Example**

```
ssh -l mtc 45.128.54.12
```

- 2 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 3 When prompted, enter the root password.

- 4 Change to the database directory by typing

```
cd /opt/apps/database/solid/dbfiles
```

and pressing the Enter key.

- 5 Put a copy of the database for the active unit in the backup directory by typing

```
cp solid.db /opt/apps/database/solid/backup
```

and pressing the Enter key.

**Note:** If other backup copies of the database exist with the same filename, you have the option of deleting those files or putting the backup copy into the backup directory under a new file name.

**Example**

```
cp solid.db
/opt/apps/database/solid/backup/solid.db.backup1
```

- 6 For security purposes, ensure that you transfer a backup copy of the database file to a secure location.

Use the **scp** command to make a secure copy of the backup database file to a secure and remote server on your network. This server is contiguously available in case a restoration of the

Policy Controller application database is necessary, such as during an upgrade rollback.

- 7 You have completed this procedure. Return to [step 3](#) in procedure [Preparing to upgrade the Policy Controller on page 1232](#).

---

## Perform a database restore to a Policy Controller unit

---

### Purpose of this procedure

Use this service impacting procedure to restore a Policy Controller application database from a backup copy to either the active or inactive Policy Controller units.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of procedure [Performing an emergency maintenance release rollback on page 1244](#).

### Limitations and Restrictions



#### CAUTION

Performing a restore of the Policy Controller application database is a service affecting activity and can cause data mismatches at the Communication Server 2000.

### Prerequisites

You must first have completed procedure [Prepare for a database restore on a Policy Controller unit on page 1357](#).

### Action

#### *At a Session Server command line interface*

- 1 Open a secure shell to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
> ssh -l <userid> <SS_IP_address>
```

and pressing the Enter key.

where

**userid**

is a valid userid (like mtc) on the Policy Controller

**SS\_IP\_address**

is the IP address of either Policy Controller unit

**Example**

```
ssh -l mtc 45.128.54.12
```

- 2 Change to the root user by typing  
**\$ su - root**  
and pressing the Enter key.
- 3 When prompted, enter the root password.
- 4 Change directories by typing  
**\$ /opt/apps/database/solid\_install**  
and pressing the Enter key.
- 5 Run the database restore script by typing  
**\$ ./restorebackup.sh**  
and pressing the Enter key.
- 6 You have completed this procedure. Return to the high-level activity.



# Nortel SAM21 Shelf Controller Upgrades

Use the following procedures to upgrade software on the Services Application Module 21 Shelf Controller (SAM21 SC).

The SAM21 SC resides in a Services Application Module 21 (SAM21) shelf. Each SAM21 shelf includes two SAM21 SC blades.

## New in this release

This section describes the changes to SAM21 SC upgrades in this release.

### Feature changes

There are no feature changes in the SAM21 SC upgrade.

#### **ATTENTION**

An upgrade to SN09U is only required from the SN08 release. No upgrade is required from the SN09 release.

### Other changes

The following additional changes affect upgrades of this component:

- New high-level procedures to guide you through the upgrade process
- New requirement and procedure to test each SAM21 SC blade before the upgrade

## Upgrade paths

The following procedures support the following upgrade paths:

- (I)SN08 to (I)SN09U
- (I)SN09 to (I)SN09U



## Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

### Time to complete an upgrade

The following table lists the tasks to upgrade SAM21 Shelf Controller software and the estimated time to complete each task.

**Table 1 Estimated time to complete a software upgrade**

| Task                      | Time              |
|---------------------------|-------------------|
| Preparing for the upgrade | 60 minutes        |
| Upgrading the software    | 35 minutes        |
| Completing the upgrade    | 15 minutes        |
| Total estimated time      | 1 hour 40 minutes |
| Performing a rollback     | 25 minutes        |

### Service impacts

None

### Notes

The following additional information applies to the upgrade of SAM21 Shelf Controller software:

- Make sure all ATM connections are established before performing the upgrade switch of activity (SWACT).

## System capacity

The software upgrade procedure can impact the system capacity. This means that additional disk space on the OAMP workstation is required for converting existing databases.

## System performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade

## System limitations during upgrade

During a software upgrade, the system prohibits the following actions:

- System administration
  - adding, deleting, or modifying users
  - setting the time of day
  - changing passwords
- System management
  - modifying the system name
  - adding or deleting system nodes
  - modifying the IP addresses

## Shelf Controller Upgrade Tool

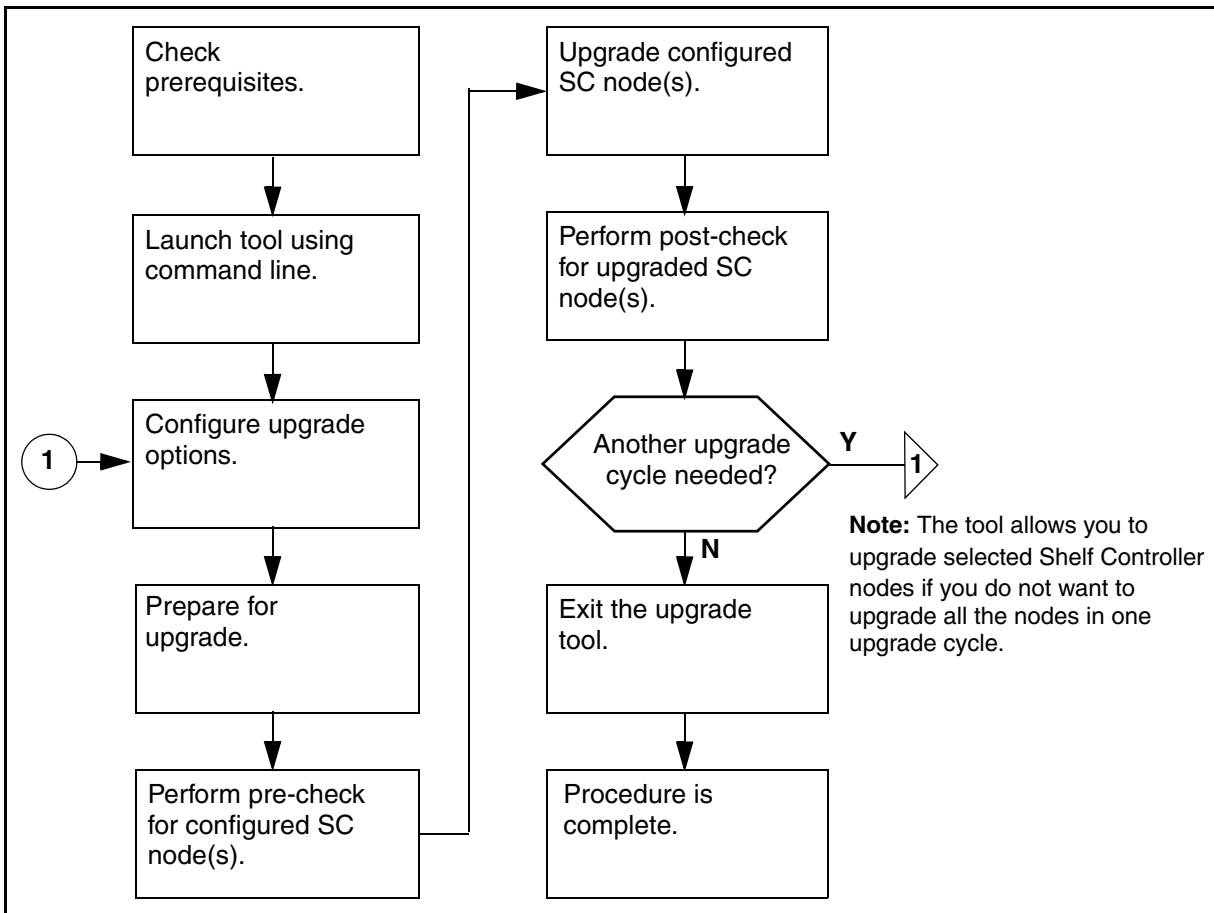
The Shelf Controller Upgrade Tool supports software upgrades through the command line user interface (CLUI). The tool automatically performs the following tasks:

- locks and unlocks the inactive unit
- swacts the inactive unit
- locks and unlocks a newly inactive unit

The automated Shelf Controller Upgrade tool supports the following upgrade modes:

- single, which allows you to upgrade one or more configured Shelf Controller nodes one at a time
- bulk, which allows you to upgrade all configured Shelf Controller nodes simultaneously

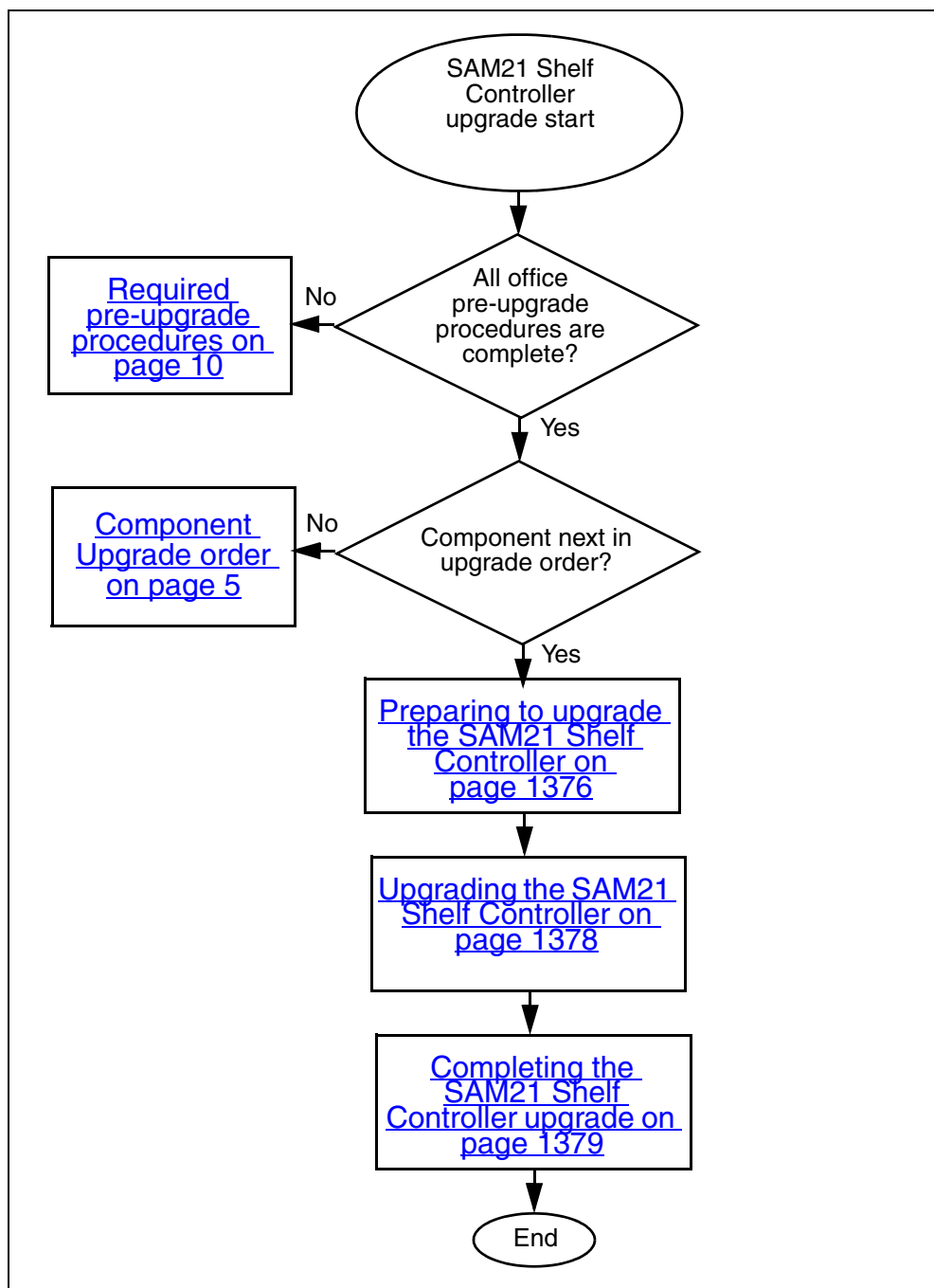
The following figure shows the high-level steps to upgrade Shelf Controller nodes using the Shelf Controller Upgrade Tool.

**Figure 1 Automated upgrade overview**

If you want to manually upgrade the software on the SAM21 Shelf Controller, refer to the manual upgrade procedures in *Upgrading the SAM21 Shelf Controller*, NN10067-461.

## **SAM21 Shelf Controller upgrade tasks**

This taskflow shows you the sequence of tasks you perform to upgrade this component.

**Figure 2 SAM21 Shelf Controller upgrade tasks**

### Aborting an upgrade

If failure occurs and you need to abort the upgrade, perform [Aborting a SAM21 Shelf Controller software upgrade on page 1441](#).

---

## Preparing to upgrade the SAM21 Shelf Controller

---

**CAUTION****Possible upgrade failure if blade not tested**

Test each Shelf Controller no more than 24 hours before the software upgrade. An unhealthy Shelf Controller blade can cause the software upgrade to fail.

The following procedure provides the steps you need to execute prior to upgrading the SAM21 Shelf Controller. When applicable, a reference to the procedure that contains the detailed steps is provided.

### Prerequisites

You have completed the following tasks:

- Complete all tasks listed in [Preparing to upgrade the Carrier Voice over IP Network on page 9](#).
- Complete the upgrade of all components that precede the component, as listed in [Component Upgrade order on page 5](#).
- Know the load server for the SAM21 Shelf Controller. The load server can be any of the following devices:
  - CS 2000 Core Manager
  - CBM
- Know the amount of available disk space on the CS 2000 Core Manager or CBM. Nortel recommends a minimum of 25 megabytes of disk space in the /swd/sam21 volume for an upgrade of the SAM21 Shelf Controller.

## Action

Perform the following procedures:

1. Test each Shelf Controller blade. Perform [Testing the inactive Shelf Controller blade before an upgrade on page 1399](#).
2. If necessary, remove old filesets.
  - If old filesets are stored on the CS 2000 Core Manager, perform [Removing old SAM21 SC filesets on the CS 2000 Core Manager on page 1380](#).
  - If old filesets are stored on the CBM, perform [Removing old SAM21 SC filesets on the core manager on page 1391](#).
3. Load the new software.
  - If you receive Shelf Controller software through Electronic Software Delivery (ESD), perform the following procedures:
    - [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
    - [Loading the Shelf Controller software delivered through ESD on page 1382](#).
  - If you receive Shelf Controller software on compact disk (CD), perform [Loading the Shelf Controller software from CD on page 1386](#).

When you have finished preparing the SAM21 Shelf Controller for an upgrade, go to [Upgrading the SAM21 Shelf Controller on page 1378](#).

---

## Upgrading the SAM21 Shelf Controller

---

The following procedure provides the steps you need to execute to upgrade the SAM21 Shelf Controller. When applicable, a reference to the procedure that contains the detailed steps is provided.

### Prerequisites

You have completed procedure [Preparing to upgrade the SAM21 Shelf Controller on page 1376](#).

### Action

Perform the following procedures:

- Make sure the Shelf Controller meets the prerequisites. Perform [Checking the Shelf Controller upgrade prerequisites on page 1396](#)
- [Upgrade the Shelf Controller using the Shelf Controller Upgrade Tool on page 1406](#)

When you finish these procedures, go to [Completing the SAM21 Shelf Controller upgrade on page 1379](#).

---

## Completing the SAM21 Shelf Controller upgrade

---

Perform the procedures listed below to complete the software upgrade of a SAM21 Shelf Controller. The SAM21 Shelf Controller Upgrade tool performs most completion tasks. These procedures verify the upgrade was successful.

### Prerequisites

All procedures listed in [Upgrading the SAM21 Shelf Controller on page 1378](#)

### Action

Perform the following steps to complete this procedure.

#### Completing the SAM21 Shelf Controller upgrade

##### *From the Application Launch Point*

- 1 Launch the CS 2000 SAM21 Manager.

*Response*

*The main window of the CS 2000 SAM21 Manager appears.*

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

| If the GUI      | Do                                  |
|-----------------|-------------------------------------|
| launches        | <a href="#">step 3</a>              |
| does not launch | Contact your next level of support. |

- 3 Make sure each SAM21 SC you upgraded is unlocked. If the SAM21 Shelf Controller remains locked, the SAM21SC failed to reboot.

Perform [Check a Shelf Controller that does not unlock on page 1432](#) to determine if a SAM21SC is unlocked or troubleshoot a locked SAM21 SC.

- 4 Make sure the SAM21 Manager displays the correct software load for each SAM21 SC you upgraded. Check the software load running on each SAM21 Shelf Controller you upgraded. Perform [Confirming SAM21 Shelf Controller loads after an upgrade on page 1439](#).
- 5 Upgrade the next component in the end-to-end upgrade. Refer back to [Component Upgrade order on page 5](#).



---

## Removing old SAM21SC filesets on the CS 2000 Core Manager

---

### Purpose of this procedure

This procedure removes old SAM21 Shelf Controller filesets on the CS 2000 Core Manager before an upgrade of SAM21 Shelf Controller software.

### When to use this procedure

Perform this procedure only if you need additional disk space in the /swd/sam21 volume of the CS 2000 Core Manager for a SAM21 Shelf Controller upgrade. Nortel recommends a minimum of 25 megabytes of disk space.

### Prerequisites

This procedure has no prerequisites.

### Action

#### *At the console or terminal window*

- 1 Change directory to /var/adm/sam21:  
**# cd /var/adm/sam21**
- 2 Copy the custlog, designlog, and statlog configuration files to a backup version in the /var/adm directory:  
**# cp custlog ../custlog.bak**  
**# cp designlog ../designlog.bak**  
**# cp statlog ../statlog.bak**
- 3 List the existing filesets:  
**# sdmmtc details**
- 4 Find the SAM21 Shelf Controller fileset to be removed by using the filter command:  
**> filter sam21**

**Filter command example**

|          |                                  |                          |             |              |                |
|----------|----------------------------------|--------------------------|-------------|--------------|----------------|
| SDM      | CON                              | NET                      | APPL        | SYS          | CLLI: clliname |
| .        | .                                | .                        | .           | .            | Host: hostname |
| Details  |                                  |                          |             |              |                |
| 0 Quit   | Filter: SAM21 (Description View) |                          |             |              |                |
| 2        | #                                | Fileset                  | Description | Version      | Status         |
| 3        | 1                                | SAM21 Platform           | v10         | 10.0.117.0   | APPLIED        |
| 4        | 2                                | SAM21 Platform           | v7          | 7.0.558.4    | APPLIED        |
| 5        | 3                                |                          |             | >> 7.0.558.0 | ARCHIVED       |
| 6        | 4                                | SAM21 Platform           | v8          | 8.0.24.9     | APPLIED        |
| 7 Select | 5                                |                          |             | >> 8.0.24.0  | ARCHIVED       |
| 8 Remove | 6                                | SAM21 Platform           | v9          | 9.0.66.5     | APPLIED        |
| 9        | 7                                |                          |             | >> 9.0.66.0  | ARCHIVED       |
| 10       | 8                                | Succession SAM21 Manager |             | 8.0.24.2     | APPLIED        |
| 11       | Filesets: 1 to 8 of 8            |                          |             |              |                |

**5 Remove the old SAM21 Shelf Controller fileset:**

```
> remove <#>
```

```
#
```

is the number for the SAM21 Platform fileset to remove.  
For example, remove 3 to remove version 7.0.558.0.

**6 Make the /var/adm/sam21 directory:**

```
mkdir -p /var/adm/sam21
```

**7 Change directory to /var/adm, the location of the backup configuration files:**

```
cd /var/adm
```

**8 Move the backup configuration files into the /var/adm/sam21 directory, and remove the backup suffix:**

```
mv custlog.bak sam21/custlog
mv designlog.bak sam21/designlog
mv statlog.bak sam21/statlog
```

**9 You have completed this procedure. Return to [Preparing to upgrade the SAM21 Shelf Controller on page 1376](#)**

---

## Loading the Shelf Controller software delivered through ESD

---

Use this procedure to prepare SAM21 Shelf Controller software delivered through Electronic Software Delivery (ESD) for an upgrade of the SAM21 Shelf Controller.

### Prerequisites

Use this procedure after you have performed the procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

Do not remove old SAM21 Shelf Controller filesets (NCL and MNCL filesets of the same release) from the CS 2000 Core Manager or CBM unless you need additional space on the device to apply the new releases. It is recommended to have a minimum of 25 Megabytes of available disk space. If required, follow one of the following procedures

- [Removing old SAM21SC filesets on the CS 2000 Core Manager on page 1380](#)
- [Removing old SAM21 SC filesets on the core manager on page 1391](#)

## Action

### *At the CS 2000 Management Tools server terminal*

- 1 Log in to the CS 2000 Management Tools server using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 List the contents of the `/tmpmnt/noarch` directory.

```
ls /tmpmnt/noarch
```

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

| If you want to install the software | Do                     |
|-------------------------------------|------------------------|
| later                               | <a href="#">step 4</a> |
| now                                 | <a href="#">step 6</a> |

- 4 Copy the contents to a location of your choice on the CS 2000 Management tools server.
- 5 When you are ready to install the software, list the contents of the directory from [step 4](#).
- 6 Record the name of the .rpm file.
- 7 Launch the installation tool.  

```
/opt/nortel/sspfs/Scripts/platform_load_install.sh
```
- 8 Enter the number next to `Install RPM from Disk`.
- 9 When prompted, enter the .rpm filename.
- 10 When prompted for the location of the .rpm file, enter `/tmpmnt/noarch`.

**11** When asked if you want to continue, enter **y**.

*Example system response:*

```
Installing RPM package SAM21_PLAT-12.0-45.0
Sun Microsystems Inc. SunOS 5.9 Generic May 2002
aps11: Installed on May 04, 2005 at 05:56:33
SAM21_PLAT_12_0_45_0.rpm 100% 25MB 5.1MB/s 00:05
The authenticity of host '47.142.116.150 (47.142.116.150)' can't be
established.
RSA key fingerprint is cc:5a:42:6a:1e:c2:08:49:c5:c0:b7:65:cb:04:7d:c4.
Are you sure you want to continue connecting (yes/no)?
```

**12** Enter **yes** to continue.

*Example system response:*

```
Warning: Permanently added '47.142.116.150' (RSA) to the list of known
hosts.
Password:
```

**13** Enter the root password of the CBM or CS 2000 Management Tools server.

*The system displays messages telling of its progress through the process of installing the rpm package. The final messages it displays are as follows:*

```
Installation of Platform Load Complete.
```

```
***** Please hit ENTER key to continue *****
```

**14** Press the Enter key.*System response:*

```
Welcome to the Platform Installation Tool Version 3.2
=====
RPM INSTALLATION/REMOVAL
=====
1) Install RPM from CDROM 2) Install RPM from Disk
3) Uninstall RPM 4) Query all RPMs

OTHER
=====
C) Change Rotation Parameters P) View Rotation Parameters
V) SAM21 Platform Version Installed X) Exit

Please choose one of the following:
```

**15** Enter **x** to exit the installation tool.*System response:*

Exiting Installation Tool, GoodBye

**16** Make sure you are not in the /tmpmnt directory.**17** Unmount the ESD file. Perform procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).

**Note:** If you are in the /tmpmnt directory, you can not unmount the ESD file from the /tmpmnt directory. The unmount command will show busy if you are in the directory.

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

---

## Loading the Shelf Controller software from CD

---

Use this procedure to install the SAM21 Shelf Controller software from a compact disk (CD) to the CS 2000 Core Manager or Core and Billing Manager (CBM). The CS 2000 Core Manager or CBM provide the software a SAM21 Shelf Controller on a BOOTP request.

### Prerequisites

Do not remove old SAM21 Shelf Controller filesets (NCL and MNCL filesets of the same release) from the CS 2000 Core Manager or CBM unless you need additional space on the device to apply the new releases. It is recommended to have a minimum of 25 Megabytes of available disk space. If required, follow one of the following procedures

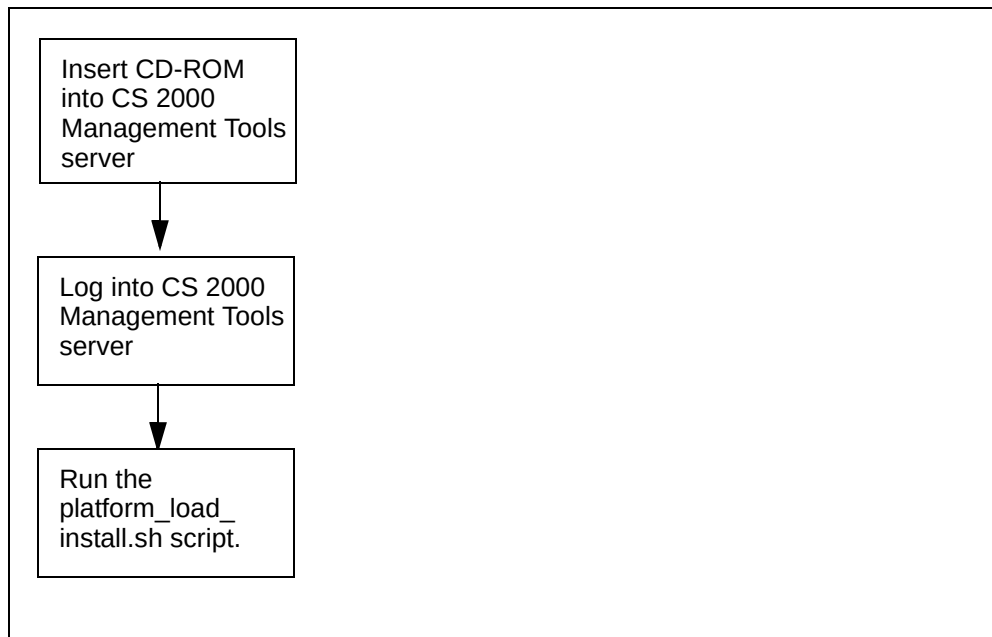
- [Removing old SAM21SC filesets on the CS 2000 Core Manager on page 1380](#)
- [Removing old SAM21 SC filesets on the core manager on page 1391](#)

### Additional information

Do not use file links (hard or soft symbolic links) in the filesystem for bootloads. Links are not supported, they defeat the caching mechanism, and increase the time required to boot a SAM21 Shelf Controller.

### Action

The following figure summarizes the procedure.



***At the CS 2000 Management Tools frame (Sun Microsystems t1400 or Netra 240)***

- 1 Insert the CD-ROM into the CD-ROM tray. If the unit is a Netra 240 in a cluster configuration, use the active Netra 240 unit. The active unit is identified by a lit USER LED on the front of the unit.  
  
The CD-ROM label for the SAM21 Shelf Controller software includes the product code, SAM20008, on the lower half of the label.

***At the CS 2000 Management Tools terminal***

- 2 Log in to the CS 2000 Management Tools server using the root user ID and password.  
  
For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 3 Launch the platform installation tool.  
  
`/opt/nortel/sspfs/Scripts/platform_load_install.sh`



The screen clears and a menu is displayed.

```
Welcome to the Platform Installation Tool Version 3.2
=====
RPM INSTALLATION/REMOVAL
=====
1) Install RPM from CDROM 2) Install RPM from Disk
3) Uninstall RPM 4) Query all RPMs

OTHER
=====
C) Change Rotation Parameters P) View Rotation Parameters
V) SAM21 Platform Version Installed X) Exit

Please choose one of the following: 1
```

**Note:** Options C and P are not available for offices configured with a CS 2000 Core Manager or a CBM.

**4** Enter the number next to Install RPM from CDROM.

The screen clears and the contents of the .rpm package are displayed.

```
Verifying CDROM is mounted
/cdrom/cdrom on /vol/dev/dsk/c0t0d0/cdrom read only/nosuid/mapl-
case/noglobal/rr/traildot/dev=16c0001 on Sat Mar 27 16:34:13 2004
CDROM is mounted.
Listing file names in the rpm on the cd.

/swd/sam21/10.0.0.0401211453
/swd/sam21/10.0.0.0401211453.cksum
/swd/sam21/F695_flash.10.0.0.0401211453
/swd/sam21/F695_flash.10.0.0.0401211453.chksum
/swd/sam21/N765.flash.10.0.0.0401211453
/swd/sam21/N765a.flash.10.0.0.0401211453
/swd/sam21/Sitka.flash.10.0.0.0401211453
/swd/sam21/checkLoad
/swd/sam21/hostsmodify
/swd/sam21/hostsmodify.sh
/swd/sam21/hostsmodify.sspfs
/swd/sam21/logs/logfile
/swd/sam21/logs/slgcleansam
/swd/sam21/sc-atm-tools.rpm
/swd/sam21/sc-ip-tools.rpm
/swd/sam21/sc-mtc-tools.rpm

Do you want to continue (y/n)? Y
```

**Note:** If the message There is no cd in the CDROM drive, please check drive is displayed, ensure that the CD-ROM is inserted in the tray for this unit.

**5** Enter **Y** to proceed with the software installation.

The software is extracted from the .rpm package. The .rpm package is transferred to the CS 2000 Core Manager or CBM.

Extracting files from the rpm archive on the cd.

```
Installing RPM package SAM21_PLAT-10.0-223.0
Sun Microsystems Inc. SunOS 5.8 Generic Patch December 2002
sam21_plat_10_0_223_0.rpm 100% 11MB 750.4KB/s 00:14
root@47.135.214.127's password: <enter root password>
```

**6** Enter the root password for the CS 2000 Core Manager or the CBM.

If you are prompted to accept the RSA key, enter **y**.

The software is installed on the CS 2000 Core Manager or CBM. If a CBM is used, the .rpm package is then copied to the inactive CBM unit and another prompt for the root password appears. If this happens enter the root password and press Return. After the load file is installed on the CS 2000 Core Manager or CBM, the transferred .rpm package is deleted from the CS 2000 Core Manager or CBM.

Extracting files from the rpm archive on the cd.

```
Installing RPM package SAM21_PLAT-10.0-223.0
Sun Microsystems Inc. SunOS 5.8 Generic Patch December 2002
sam21_plat_10_0_223_0.rpm 100% 11MB 750.4KB/s 00:14
root@47.135.214.127's password: <enter root password>
Mate IP is 47.135.214.129
Sun Microsystems Inc. SunOS 5.8 Generic Patch December 2002
root@47.135.214.129's password: <enter root password>
```

Configuring syslog to add designlog, statlog and customerlog files.  
Log files already added to syslog.

Adding log rotation for designlog/statlog/customerlog files.  
Installation of Platform Load Complete.

\*\*\*\*\* Please hit ENTER key to continue \*\*\*\*\*

**Note:** After the first installation, syslog and log rotation will not be reconfigured.

- 7 Enter **x** to exit the installation tool.
- 8 Eject the CD.  
**eject**
- 9 Log out of the CS 2000 Management Tools server.

***At the CS 2000 Management Tools frame***

- 10 Remove the CD from the server.
- 11 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

**Note:** For customers experienced with upgrading the SAM21 Shelf Controllers in earlier releases, no action is required at the CS 2000 Core Manager for software installation.

---

## Removing old SAM21 SC filesets on the core manager

---

### Purpose of this procedure

This procedure removes old SAM21 shelf controller filesets on the core manager, which can be a CS 2000 Core Manager or a Core and Billing Manager (CBM), before an upgrade of SAM21 shelf controller software.

### When to use this procedure

Perform this procedure only if you need additional disk space in the /sam21 volume of the core manager for a SAM21 shelf controller upgrade. Nortel recommends a minimum of 25 megabytes of disk space.

### Prerequisites

None

### Action

#### *At the CS 2000 Management Tools terminal*

- 1 Log in to the CS 2000 Management Tools server using the root user ID and password.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 2 Launch the platform installation tool.

**/opt/nortel/sspfs/Scripts/platform\_load\_install.sh**

The screen clears and a menu is displayed.

```
Welcome to the Platform Installation Tool Version 3.2
=====
RPM INSTALLATION/REMOVAL
=====
1) Install RPM from CDROM 2) Install RPM from Disk
3) Uninstall RPM 4) Query all RPMs

OTHER
=====
C) Change Rotation Parameters P) View Rotation Parameters
V) SAM21 Platform Version Installed X) Exit

Please choose one of the following: 3
```

### 3 Enter the number next to Uninstall RPM.

The application connects to the core manager and displays the installed .rpm packages.

```
Uninstalling RPM Software.
```

```
The Following RPM files are installed
```

```
3PC_MC_SSPFS-7.09-1.0
```

```
SAM21_PLAT-10.0-223.0
```

```
Please enter rpm file you would like to uninstall or q to exit>
```

### 4 Enter the name of the .rpm package to remove. For example, SAM21\_PLAT-10.0-223.0.

**Note:** The .rpm package name is case sensitive.

A confirmation prompt is provided.

```
Please enter rpm file you would like to uninstall or q to exit>
```

```
SAM21_PLAT-10.0-223.0
```

```
Sun Microsystems Inc. SunOS 5.8 Generic Patch December 2002
```

```
Are you sure you want to uninstall SAM21_PLAT-10.0-223.0 (y,n)>? Y
```

### 5 Enter **Y** to confirm the uninstall prompt.

The uninstall begins. When prompted, enter the root password on the core manager. If the office uses a dual CBM configuration, a second prompt for the root password appears for the mate CBM unit.

```
Uninstalling RPM on SDM/CBM, you will be prompted for the sdm/cbm
root passwd.
```

```
root@47.135.214.127's password: <enter root password>
```

```
Mate IP is 47.135.214.129
```

```
root@47.135.214.129's password: <enter root password>
```

```
SAM21_PLAT-10.0-223.0 RPM has been uninstalled
```

```
***** Please hit ENTER key to continue *****
```

**6** Press the Enter key to continue.

The main RPM Installation/Removal menu appears.

```

Welcome to the Platform Installation Tool Version 3.2
=====
RPM INSTALLATION/REMOVAL
=====
1) Install RPM from CDROM 2) Install RPM from Disk
3) Uninstall RPM 4) Query all RPMs

OTHER
=====
C) Change Rotation Parameters P) View Rotation Parameters
V) SAM21 Platform Version Installed X) Exit

Please choose one of the following: x
```

**7** Enter **x** to exit the installation tool.**8** You have completed this procedure. Return to [Preparing to upgrade the SAM21 Shelf Controller on page 1376](#).

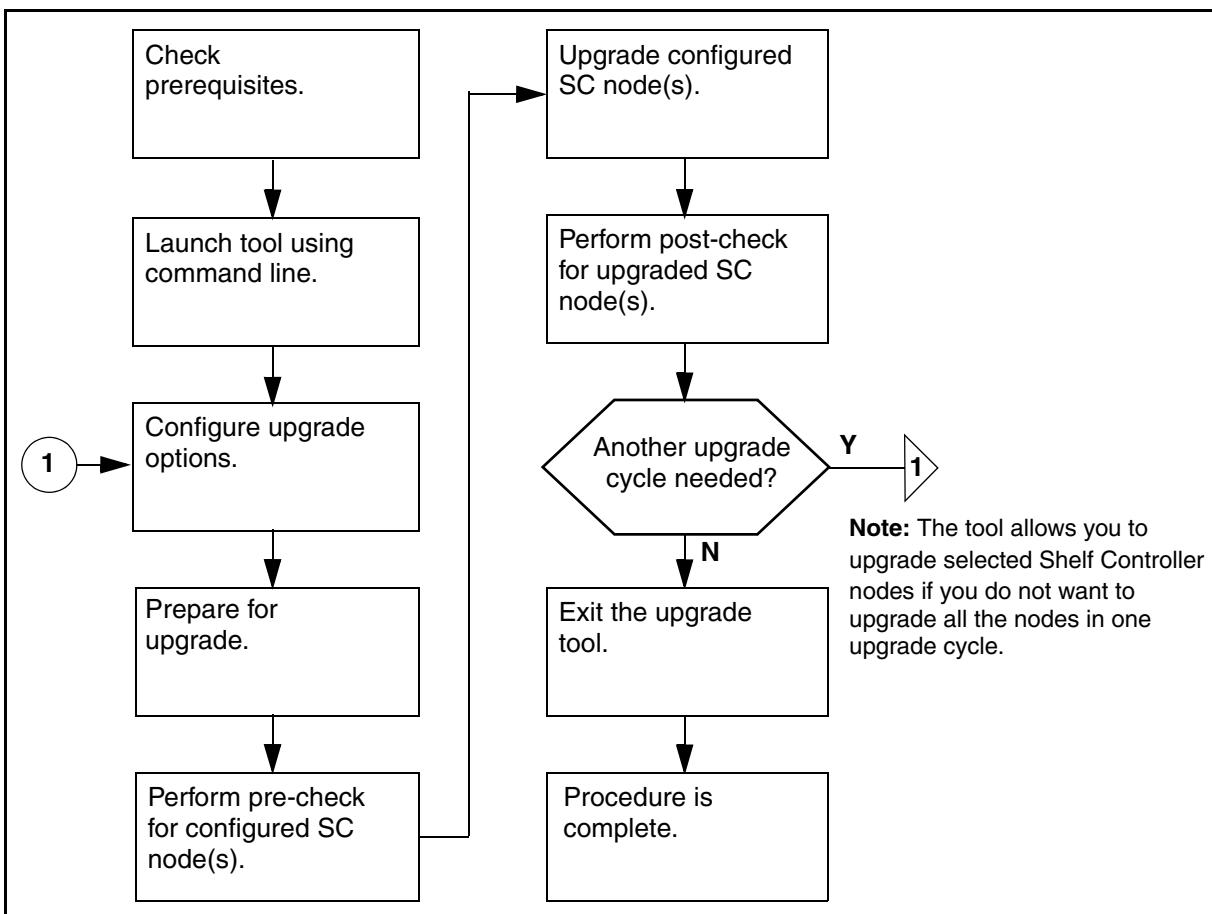
## Overall Shelf Controller upgrade process - automated

The Shelf Controller Upgrade Tool is a subcomponent of the upgrade manager in the Carrier Voice over IP Upgrade Management Architecture. The tool supports Shelf Controller software upgrades through the command line user interface (CLUI). The tool automatically performs the following required manual operations:

- locks and unlocks the inactive unit
- swacts the inactive unit
- locks and unlocks a newly inactive unit

The following figure provides an overview of these steps. The automated upgrade process involves two procedures: [Checking the Shelf Controller upgrade prerequisites on page 1396](#) and [Upgrade the Shelf Controller using the Shelf Controller Upgrade Tool on page 1406](#).

### Automated upgrade overview



The automated Shelf Controller Upgrade tool supports the following upgrade modes:

- single, which allows you to upgrade one or more configured Shelf Controller nodes one at a time
- bulk, which allows you to upgrade all configured Shelf Controller nodes simultaneously

If you want to upgrade a Shelf Controller node using the manual method, refer to procedure “Manual software upgrade procedure” in document *Upgrading the SAM21 Shelf Controller*, NN10067-461.



---

## Checking the Shelf Controller upgrade prerequisites

---

### Purpose of this procedure

This procedure checks that suitable conditions exist for using the automated Shelf Controller Upgrade Tool. This procedure verifies that the user ID that will be used for the upgrade, can launch the upgrade tool, and that the SAM21EM and CORBA server applications are running.

### When to use this procedure

Use this procedure before upgrading the Shelf Controller software using the automated Shelf Controller Upgrade Tool.

### Prerequisites

Complete the [Preparing to upgrade the SAM21 Shelf Controller on page 1376](#).

### Action

#### ***At the CS 2000 Management Tools server***

- 1 Log in to the CS 2000 Management Tools server using the user ID and password that will be used for the upgrade (other than root).
- 2 Determine which groups the user ID belongs to by typing  
`$ id -a`  
and pressing the Enter key.

*Example response:*

```
$ id -a
uid=104(ptm) gid=105(succssn)
groups=105(succssn),1001(trkadm),1006(lnadm),1011
(mgcadm),1016(mgadm),1021(emsadm)
$ _____ Group names _____
```

- 3** Ensure the user ID belongs to one of the following groups: mgcmtc, mgcadm, emsmtc or emsadm.

---

| <b>If</b>                                                     | <b>Do</b>                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| the user ID belongs to group mgcmtc, mgcadm, emsmtc or emsadm | <a href="#">step 4</a>                                                                                                                                                                                                                                                                                            |
| otherwise                                                     | add the required groups to the user ID. (Refer to procedure “Setting up local user accounts on an SPFS-based server” in <i>ATM/IP Solution-level Security and Administration</i> , NN10402-600.) When the groups have been added to the user ID, return to this procedure and proceed to <a href="#">step 4</a> . |

---

- 4** Change to the root user by typing

\$ **su -**

and pressing the Enter key.

- 5 Verify the SAM21EM and CORBA server applications are running by typing

```
servquery -status all
```

and pressing the Enter key.

*Example response:*

```
servquery -status all
APP NAME STATUS
===== =====
DATABASE RUNNING
CINOTIFIER RUNNING
BACKUP_MANAGER Group Started. Current status unavailable
BOOTP RUNNING
WEBSERVER RUNNING
CORBA RUNNING
OMPUSH RUNNING
SESMSERVICE RUNNING
WEBSERVICES RUNNING
DDMSPROXY RUNNING
ORA_AUTO_BACKUP RUNNING
DELEGATE RUNNING
ORA_ARCHIVE_ROTATOR RUNNING
NPM RUNNING
PROP_SRV RUNNING
SAM21EM RUNNING
SNMP_POLLER Group Started. Current status unavailable
QCA RUNNING
```

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

---

## Testing the inactive Shelf Controller blade before an upgrade

---

**CAUTION****Possible upgrade failure**

Make sure the shelf has NOT been provisioned with new software before you begin this procedure. Hardware must take place before the software upgrade.

Perform the following procedure to test the inactive Shelf Controller blade before an upgrade of SAM21 Shelf Controller software. Repeat this procedure as necessary to test each Shelf Controller blade before a software upgrade.

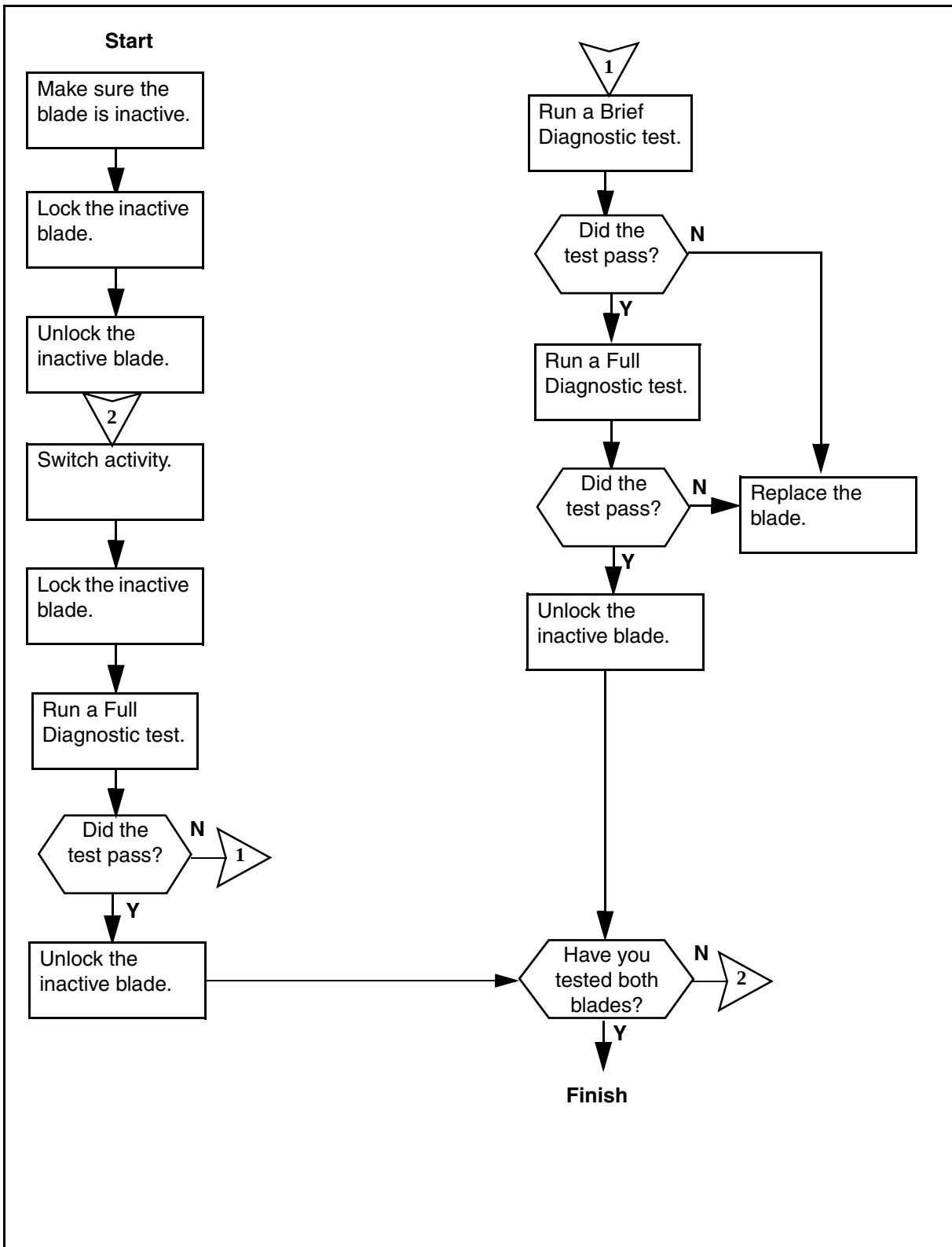
Perform this procedure no more than 24 hours before the upgrade of SAM21 Shelf Controller software.

### Prerequisites

This procedure has no prerequisites.

### Action

The following flowchart shows a high-level summary of the tasks performed during this procedure. Use the step-by-step instructions after the flowchart to perform the procedure.

**Testing the inactive Shelf Controller blade before an upgrade**

## Testing the inactive Shelf Controller blade before an upgrade

### At the CS 2000 SAM21 Manager

- 1 Make sure you are at the Shelf View of the SAM21 shelf with the inactive Shelf Controller blade you want to upgrade.
- 2 Go to the Card View of the inactive Shelf Controller. Right-click the icon of the inactive Shelf Controller blade and select Card View from the list of commands.

#### *Response*

*The Card View window appears.*

- 3 Click the States tab and make sure the Status of the selected Shelf Controller is Inactive.
- 4 Use the following table to determine your next step.

| If the status is | Do |
|------------------|----|
|------------------|----|

|          |                                                          |
|----------|----------------------------------------------------------|
| Active   | Close this window and return to <a href="#">step 1</a> . |
| Inactive | <a href="#">step 5</a>                                   |

- 5 Lock the inactive blade. On the left side of the Card View window, right-click the Shelf Controller icon and select Lock from the list of commands.

#### *Response*

*The CS 2000 SAM21 Manager locks the selected Shelf Controller blade.*

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

| If the lock is | Do |
|----------------|----|
|----------------|----|

|                |                                                                                            |
|----------------|--------------------------------------------------------------------------------------------|
| successful     | <a href="#">step 7</a>                                                                     |
| not successful | Repeat <a href="#">step 5</a> . If the second attempt fails, go to <a href="#">step 28</a> |

- 7 Unlock the inactive blade. On the left side of the Card View window, right-click the Shelf Controller icon and select Unlock from the list of commands.

#### *Response*

*The CS 2000 SAM21 Manager unlocks the selected Shelf Controller blade.*

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

| If the unlock is | Do                                                                                           |
|------------------|----------------------------------------------------------------------------------------------|
| successful       | <a href="#">step 9</a>                                                                       |
| not successful   | Repeat <a href="#">step 7</a> . If the second attempt fails, go to <a href="#">step 28</a> . |

- 9 Close the Card View of the inactive Shelf Controller.

*Response*

*The Shelf View window appears.*

- 10 Go to the card view of the active Shelf Controller. Right-click the icon of the active Shelf Controller blade and select Card View from the list of commands.

*Response*

*The Card View Window appears.*

- 11 Switch activity between the Shelf Controller blades. On the left side of the Card View window, right-click the Shelf Controller icon and select Swact from the list of commands.

*Response*

*The CS 2000 SAM21 Manager switches activity between the Shelf Controller blades.*

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

| If the switch of activity is | Do                                                                                        |
|------------------------------|-------------------------------------------------------------------------------------------|
| successful                   | <a href="#">step 13</a>                                                                   |
| not successful               | Repeat <a href="#">step 11</a> If the second attempt fails, go to <a href="#">step 28</a> |

- 13 Lock the inactive blade. On the left side of the Card View window, right-click the Shelf Controller icon and select Lock from the list of commands.

*Response*

*The CS 2000 SAM21 Manager locks the selected Shelf Controller blade.*

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

| If the lock is | Do                                                                                          |
|----------------|---------------------------------------------------------------------------------------------|
| successful     | <a href="#">step 15</a>                                                                     |
| not successful | Repeat <a href="#">step 13</a> . If the second attempt fails, go to <a href="#">step 28</a> |

- 15 Click the Diags tab.

- 16 Run a Full Diagnostic test on the locked Shelf Controller blade. At Type, select Full from the pull-down menu and click the Start button.

*Response*

*A window asking you to confirm the diagnostic run appears. The window shows the estimated time to complete the test.*

- 17 In the Confirm Diag Run window, click the Yes button.

*Response*

*The CS 2000 SAM21 Manager performs a full diagnostic test on the selected Shelf Controller blade. When the test finishes, the result of the test is indicated under Status.*

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

| If the Full Diagnostic test | Do                      |
|-----------------------------|-------------------------|
| passes                      | <a href="#">step 25</a> |
| fails                       | <a href="#">step 19</a> |

- 19 Run a Brief Diagnostic test. At Type, select Brief from the pull-down menu and click the Start button.

*Response*

*A window asking you to confirm the diagnostic run appears. The window shows the estimated time to complete the test.*

- 20 In the Confirm Diag Run window, click the Yes button.

*Response*

*The CS 2000 SAM21 Manager performs a brief diagnostic test on the selected Shelf Controller blade. When the test finishes, the result of the test is indicated under Status.*



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

| If the Brief Diagnostic test | Do                      |
|------------------------------|-------------------------|
| passes                       | <a href="#">step 22</a> |
| fails                        | <a href="#">step 28</a> |

- 22 Run a second Full Diagnostic test. At Type, select Full from the pull-down menu and click the Start button.

*Response*

*A window asking you to confirm the diagnostic run appears. The window shows the estimated time to complete the test.*

- 23 In the Confirm Diag Run window, click the Yes button.

*Response*

*The CS 2000 SAM21 Manager performs a full diagnostic test on the selected Shelf Controller blade. When the test finishes, the result of the test is indicated under Status.*

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

| If the second Full Diagnostic test | Do                      |
|------------------------------------|-------------------------|
| passes                             | <a href="#">step 25</a> |
| fails                              | <a href="#">step 28</a> |

- 25 Unlock the inactive blade. On the left side of the Card View window, right-click the Shelf Controller icon and select Unlock from the list of commands.

*Response*

*The CS 2000 SAM21 Manager unlocks the selected Shelf Controller blade.*

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

| If the unlock is | Do                                                                                            |
|------------------|-----------------------------------------------------------------------------------------------|
| successful       | <a href="#">step 27</a>                                                                       |
| not successful   | Repeat <a href="#">step 25</a> . If the second attempt fails, go to <a href="#">step 28</a> . |

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

| <b>If you have successfully tested</b> | <b>Do</b>               |
|----------------------------------------|-------------------------|
| one Shelf Controller blade             | <a href="#">step 9</a>  |
| both Shelf Controller blades           | <a href="#">step 29</a> |

- 28** Replace the Shelf controller blade before you continue with this software upgrade. If necessary contact your next step level of support.
- 29** You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

## Upgrade the Shelf Controller using the Shelf Controller Upgrade Tool

### Purpose of this procedure

This procedure upgrades the Shelf Controller software using the automated Shelf Controller Upgrade Tool.

### When to use this procedure

Use this procedure after checking the upgrade prerequisites (see procedure [Checking the Shelf Controller upgrade prerequisites on page 1396](#)).

### Prerequisites

The prerequisites for this procedure are as described in [Checking the Shelf Controller upgrade prerequisites on page 1396](#).

### Aborting an upgrade

If the automated upgrade fails and you need to abort the upgrade, perform [Aborting a SAM21 Shelf Controller software upgrade on page 1441](#).

### Action

**CAUTION****Interruption of upgrade**

Do not exit the automated upgrade tool before the upgrade is complete.

**CAUTION****Termination of automated upgrade tool**

Do not press CTRL+C or close the TERM window. These actions terminate the upgrade tool.

**ATTENTION**

The scuptool does not support rollback for automated upgrades. If problems occur during the upgrade, you can terminate the upgrade and use the manual rollback procedure *Roll back the SAM21 Shelf Controller software* in NN10067-461.

**At the CS 2000 Management Tools server**

- 1 Log in to the CS 2000 Management Tools server using your user ID and password. In a two-server configuration, log in to the active server.

**Note:** The user ID must be assigned to the correct group, determined through the procedure mentioned under [Prerequisites on page 1406](#) of this procedure) to launch the upgrade tool.

- 2 **Launch SC upgrade tool**

Launch the upgrade tool (scuptool) to display the Main Menu for the Shelf Controller upgrade tool:

```
> /opt/nortel/sam21em/bin/scuptool.sh
```

*Example system response:*

```
$ /opt/nortel/sam21em/bin/scuptool.sh
Starting

Main Menu for SC upgrade tool
1 - Display all SC pairs
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

### 3 Display all SC pairs

Select Display all SC pairs from the Main Menu.

Enter:

> 1

*Example system response:*

```
List All SC Units From SAM21EM:
=====
SC2 GTWD-SAM21-2 slot 7 ip: 172.16.0.74
SCUnit Status:
 Card Status : Unlocked
 Operational state : Enabled
 Activity state : Active
 Availability state : None

Total Alarms:
 Critical Alarms : 0
 Major Alarms : 1

Load name : 11.0.0.0503041646

SC2 GTWD-SAM21-2 slot 9 ip: 172.16.0.75
SCUnit Status:
 Card Status : Unlocked
 Operational state : Enabled
 Activity state : Inactive
 Availability state : None

Total Alarms:
 Critical Alarms : 0
 Major Alarms : 1

Load name : 11.0.0.0503041646
```

### 4 Configure upgrade options

Select Configure upgrade-related options from the Main Menu.

Enter:

> 2

*Example system response:*

```
[Step 1 - LOAD SERVER TYPE]
Values:
1 - SDM
2 - CBM

Enter the load server type (1-2), (default 1):
```

- 5** Select the load server type. Enter 1 for CS 2000 Core Manager/SDM (the default load file is under /swd/sam21/) or enter 2 for CBM (the default load file is under /sam21).

*System response (after entering 1):*

```
Load server is SDM, default load directory is /swd/sam21
fetching load file list
```

```
1) 11.0.0.0503041646
2) 12.0.0.0509021118
3) 13.0.0.0511110436
```

*System response (after entering 2):*

```
Load server is CBM, default load directory is /sam21
fetching load file list
```

```
1) 11.0.0.0503041646
2) 12.0.0.0509021118
3) 13.0.0.0511110436
```

*System response:*

```
[Step 2 - LOAD FILE NAME]
Enter the index No. of the new load file (Example: 1):
```

- 6** Enter the index number of the load file name. Ensure that the load file exists in the load server (CBM or CS 2000 Core Manager/SDM).

For instance, enter:

**> 1**

*System response:*

```
[Step 3 - SC LIST]
Input the SCs to be upgraded.
Separate the names with comma, for example: SC1,SC2,SC3,SC4
Enter the SC list (default: all):
```

- 7 Enter the list of Shelf Controllers to be upgraded. The Shelf Controller contains node names to be upgraded in the same upgrade cycle with the same configured options.

**Note:** Enter the node names without spaces between the entries.

*Example list entry:*

**SC1,SC2**

The system displays the current input configuration values.

*Example system response for CBM:*

[Step 4 - INPUT VALUES]

```
NewLoadFileName : 13.0.0.05111110436
SCList : SC1
Default values
LoadDirectory : /sam21
OldLoadName : "(ignored)"
UpgradeMode : bulk
PausePoint : 0 (none)
LoggingLevel : MAJ
MaxTime : 0 (no time limit)
AlarmLevel : MAJ
AlarmNumber : 2
```

Do you want to use these configuration values [Y|N]  
(default: N):

- 8 Review all values displayed in the system response, including the default values, to ensure they are acceptable.

**Note:** By default, no pause points are defined. Pause points allow you to perform manual checks at selected intervals during the upgrade process. At each pause point, you are prompted to continue the upgrade. If you do not specify any pause points, you are not prompted at any point to continue the upgrade unless an error condition occurs. If you want to be prompted at certain points during the upgrade, enter N in the next step to change the default value for PausePoint.

- 9** Refer to the following table to determine your next step

| If                                                                  | Do                      |
|---------------------------------------------------------------------|-------------------------|
| all the values, including the Default values, are acceptable        | <a href="#">step 10</a> |
| one or more of the values are not acceptable and you want to change | <a href="#">step 11</a> |

- 10** Enter **y** and go to [step 21](#).

- 11** Enter **N**.

*System response (after entering **N**):*

Do not use the default values.

[Step 5 - LOAD DIRECTORY]

Enter the load directory : (current value is /swd/sam21/):

- 12** Enter the load file directory in the CBM or CS 2000 Core Manager/SDM. Load file directory formats are different for CBM and SDM.

| If you want to configure for | Do                                                 |
|------------------------------|----------------------------------------------------|
| CBM                          | enter /sam21, and go to <a href="#">step 13</a>    |
| SDM                          | enter /swd/sam21 and go to <a href="#">step 13</a> |

*Example system response:*

[Step 6 - OLD LOAD NAME]

Enter the old load name:



**13** Refer to the following table to determine your next action.

| If                                               | Do                                                                                        |
|--------------------------------------------------|-------------------------------------------------------------------------------------------|
| you want to do the precheck for the current load | enter the name of the current load (referred to as the old load) for the Shelf Controller |
| otherwise                                        | press Enter, and go to <a href="#">step 14</a>                                            |

*Example system response:*

[Step 7 - UPGRADE MODE]

Values:

1 - single 2 - bulk

h - help

Enter the upgrade mode (1-2,h), (default: 2): 1

**14** Refer to the following table to determine your next action.

| If you want to                                                                | Do                                     |
|-------------------------------------------------------------------------------|----------------------------------------|
| upgrade all configured Shelf Controller nodes one at a time ( <i>single</i> ) | enter 1 and review the system response |
| upgrade all configured Shelf Controller nodes simultaneously ( <i>bulk</i> )  | enter 2 and review the system response |

*Example system response:*

[Step 8 - PAUSE POINTS]

Values:

0 - no pause point. If 0 is applied, all other pause points are ignored

(1) For the single mode SC pair.

1 - before lock.

2 - before warm swact.

3 - after upgrade.

4 - pause on all the above conditions.

(2) For bulk upgrade of SC pairs.

5 - before warm swact.

Separate the numbers with comma, for example, 1,3

Enter the pause points (default: 0):

- 15** Enter the pause points for the upgrade. Pause points allow you to perform manual checks at selected intervals during the upgrade process. At each specified pause point, you will be prompted to continue the upgrade. If you do not specify any pause points, you will not be prompted at any point to continue the upgrade unless an error condition occurs.

*Example pause point entry for the single mode SC pair:*

Enter the pause points (default: 0): **1, 3**

*These selections allow pause points for a Shelf Controller pair in single mode to pause before the first upgrade unit of the "seed" pair is locked (**1**) and after the pair is upgraded (**3**).*

*Example pause point entry for bulk upgrade of SC pairs:*

Enter the pause points (default: 0): **5**

*This selection allows a pause point for Shelf Controller pairs in bulk mode to pause before the warm swact.*

*Example system response:*

[Step 9 LOGGING LEVEL]

Values:

- 1 - Verbose (VRB)
- 2 - Minor (MNR)
- 3 - Major (MAJ)
- 4 - Critical (CRT)

Enter the logging level (1-4), (default: 3): 1

- 16** Enter one of the logging levels: VRB, MNR, MAJ or CRT (default: MAJ). Upgrade logs are stored in a file in upgrade.log under /opt/nortel/sam21em/logs/. Use the logs for troubleshooting.

*Example system response:*

[Step 10 - TIME LIMIT]

Note: 0 means no time limit

Enter the time limit in minutes, (default 0):

- 17** Enter a time limit (in minutes) for the upgrade. If the upgrade cannot complete on all Shelf Controller pairs in the specified time, the non-upgraded pairs remain un-upgraded and the process ends. The default value, 0, disables the time limit check.

*Example system response:*

```
[Step 11 - ALARM LEVEL]
Values:
1 - Critical (CRT)
2 - Major (MAJ)

Enter the alarm level, (default: 2):
```

- 18** Enter the alarm level (CRT, MAJ).

*Example system response:*

```
[Step 12 - ALARM NUMBER]

Enter the maximum allowed alarm number, (default: 2):
```

- 19** Enter the maximum alarm level and number allowed during the upgrade. If the current alarm state has a higher priority than is defined in this entry, the upgrade process pauses and the system notifies the end user.

*Command format:*

**-a <alarm\_level> -an <alarm\_number>**

*Example command:*

```
Enter the maximum allowed alarm number, (default: 2): -aMAJ-an2

Alarm level (Major)_____↑
Alarm number_____↑
```

The entries in the example allow a maximum number of two Major (MAJ) alarms during the upgrade process. In this case, if three MAJ alarms occur in the element server for the pair, the upgrade tool pauses. If one MAJ alarm occurs, the upgrade tool ignores it and continues the upgrade process. If one Critical (CRT) alarm occurs, the upgrade tool pauses because CRT alarms have a higher priority than MAJ alarms.

*Example system response:*

```
Configuration values:
NewLoadFileName : 13.0.0.05111110436
SCList : SC1
LoadDirectory : /sam21
OldLoadName :
UpgradeMode : single
PausePoint : 1,3
LoggingLevel : VRB
MaxTime : 0
AlarmLevel : MAJ
AlarmNumber : 2

Is this information correct? [Y|N] (DEFAULT: n): y
```

- 20** Review the values displayed in the system response and refer to the following table to determine your next action.

| If                                                          | Do                                                                                                                                    |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| you want to confirm the selections for configuration        | enter Y. Note the following system response, and go to <a href="#">step 21</a>                                                        |
| you do not want to confirm the selections for configuration | enter N and return to <a href="#">step 5</a> on <a href="#">page 1409</a> , or go to <a href="#">step 39</a> to exit the upgrade tool |

*Example system response:*

**Current configuration values:**

```

New load file name : 13.0.0.05111110436
Old load name :
Load directory name : /sam21
Upgrade mode : single
Check points : 1,3
Log level : VRB
SC lists : SC1
Max Time for Doing upgrade : no time limit
Max parallel number for bulk upgrade : 8
Allowed Highest alarm level : MAJ
Allowed Maximum alarm number : 2
```

- 21** You have completed the procedure for configuring upgrade-related options. Press Enter to return to the Main Menu for the Shelf Controller upgrade tool.

*Example system response:*

```
Main Menu for SC upgrade tool
1 - Display all SC pairs
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

- 22** Enter the Upgrade Menu for the Shelf Controller tool:

**> 4**

*Example system response:*

```
Upgrade Menu for SC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - Exit

Enter selection (1-5,x):
```

**23 Prepare for upgrade**

Select the Prepare option:

> 1

*Example system response:*

```
Upgrade Menu for SC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - Exit

Enter selection (1-5,x): 1
The configured load is available.

=====Upgrade Schedule=====
Group 1 :SC1
Estimated total time :660 seconds
```

- 24** Check whether the load is available in the CBM or CS 2000 Core Manager/SDM (as the example shows). Make an upgrade plan for the Shelf Controller and calculate the estimated time (in seconds) for the upgrade. The example shows an estimated total time of 660 seconds.

| If the load                                                                                        | Do                                                            |
|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| is not available, the system responds:<br>SC load file does not exist. Please check and try later. | return to <a href="#">step 5</a> on <a href="#">page 1409</a> |
| is available                                                                                       | <a href="#">step 25</a>                                       |

**25 Perform pre-check**

At the Upgrade Menu, enter:

**> 2**

*Example system response:*

```
SAM21EM is alive.
Configured load is available.

Checking SC nodes state...
Group 1
 SC1 is ready to upgrade.

Upgrade Status Report:
SC node : SC1
Upgrade status : Upgrade not started
SCUnitUpgrade order : slot7 (inactive), slot9 (active)
Estimated time left : 11 minutes

SC1-0 slot7 ip: 47.142.128.182
SCUnit Status:
 Administrative state : Unlocked
 Operational state : Enabled
 Activity state : Active
 Card status : None

Total Alarms:
 Critical alarms : 0
 Major alarms : 0

Load name : 11.0.0.0503041646

SC1-1 slot9 ip: 47.142.128.183
SCUnit status:
 Administrative state : Unlocked
 Operational state : Enabled
 Activity state : Inactive
 Card status : None

Total Alarms:
 Critical alarms : 0
 Major alarms : 0

Load name : 11.0.0.0503041646
```

Review the information in the system response ([step 26](#) to [step 29](#)).

- 26** Check the status of the SAM21 manager server (SAM21EM). If the manager is not alive, go to procedure [Starting the SAM21 Manager server application on page 461](#).

- 27** Verify that the load is available on the load server. If the load is not available, refer to [Loading the Shelf Controller software from CD on page 1386](#) or [Loading the Shelf Controller software delivered through ESD on page 1382](#).
- 28** Clear any existing alarms.
- 29** Verify that the two physical units of the Shelf Controller pair are in service.

| If                                         | Do                                                                                                 |
|--------------------------------------------|----------------------------------------------------------------------------------------------------|
| any of the pre-check conditions is not met | resolve the conditions and continue at <a href="#">step 30</a> to proceed with the upgrade process |
| all the pre-check conditions are met       | <a href="#">step 30</a>                                                                            |

- 30** You have completed the pre-check procedure. The system automatically returns to the Upgrade Menu for the SC upgrade tool.

*Example system response:*

```
Upgrade Menu for SC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - Exit

Enter selection (1-5,x):
```

**31**

#### **ATTENTION**

The automated upgrade tool does not allow provisioning activity on the system while the upgrade is in progress.

#### **Upgrade SC nodes**

When the upgrade starts, the system performs another pre-check and displays the upgrade status (refer to the example system response shown in [step 25](#)).



If any of the problems or conditions in the following table occur, resolve the problem as indicated.

| If                                                                                                                                                                              | Do                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pause points are enabled by the configuration step ( <a href="#">step 15</a> on <a href="#">page 1413</a> ), when the tool pauses at the specified intervals during the upgrade | enter the desired value(s), and continue with this step                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| the Shelf Controller has an active ATM link                                                                                                                                     | verify that the inactive SAM21 Shelf Controller does not carry the active ATM link. Select Configuration and then IPOA Services from the Subnet View to open the ATM Connections window. If all the connections are in the yellow state, then SWACT the SAM21 Shelf Controller at a period of low activity before proceeding. If some of the connections are in the green state and some are in the yellow state, then check for alarms at the ATM equipment between the SAM21 Shelf Controller and the end node with the yellow connection. Correct the condition, check again that all connections are green. Then return to this procedure and continue with this step. |
| the Communications Server LAN (CS LAN) is provided by Nortel Ethernet Routing Switch (ERS) 8000 series                                                                          | Reprovision the port on the routing switch to auto-negotiate according to procedure <a href="#">Reprovision the Ethernet Routing Switch 8600 port to auto-negotiate on page 1429</a> . (This procedure is required only once.) When the reprovisioning is complete, continue with this step.                                                                                                                                                                                                                                                                                                                                                                               |

| If                                                                                                                                                                                                                                                                                                                                                                                        | Do                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| the Communications Server LAN (CS LAN) is provided by a switch other than Nortel Ethernet Routing Switch (ERS) 8000 series                                                                                                                                                                                                                                                                | Reprovision the port on the routing switch to auto-negotiate according to the appropriate router product documentation. When the reprovisioning is complete, continue with this step. |
| the real alarms on the Shelf Controller card exceed the configured alarm state                                                                                                                                                                                                                                                                                                            | perform the appropriate alarm clearing procedures. When the action is complete, return to this procedure and continue with this step.                                                 |
| the upgrade is in progress, and you want to query the overall status of the upgrade (for example, if the upgrade is taking longer than expected)                                                                                                                                                                                                                                          | launch another telnet or SSH session to the server, and enter:<br><b>&gt;/opt/nortel/sam21em/bin/scuptool.sh<br/>-query</b>                                                           |
| you have an AAL1 solution, and the system displays the following message:<br>SWACT denied. The inactive Shelf Controller does not have a complete set of redundant ATM connections. A SWACT would isolate the affected gateways, resulting in an outage. Resolve any issues with the ATM connections from the gateways before requesting a SWACT. Select from the following: Retry Abort. | wait two minutes and then retry                                                                                                                                                       |

- 32** To begin the upgrade, select the Upgrade option from the Main Menu. Enter:

**> 3**

The upgrade tool

- provisions the software load in the inactive Shelf Controller card
- prompts for confirmation that it can lock the inactive Shelf Controller card if pause points were configured in [step 15](#)

*Example system response:*

**Note:** The entire system response as shown below will not necessarily appear instantaneously. The system will display some output, then pause, then continue. Such pauses are normal.

```

=====Upgrade Schedule=====
Group 1 SC1

Start upgrade at 2004-11-10 02:35:07.152
Upgrading with no time limit.
Group 1
Upgrade Status Report:
SC node : SC1
Upgrade status : Upgrade starting.

SC unit upgrade order: slot7 (inactive), slot9 (active)
Start time : 2004-11-10 02:35:07.542
Estimated time left : 10 minutes

Provision software load on the inactive (first) unit.
Provisioning in progress...

Provisioning completed successfully.

Lock the inactive (first) SC unit started.

Message received from the server:

Locking the inactive SC will cause the SCs to operate
in simplex mode. Do you wish to proceed?

Please select from the following:
Continue

Answer:

```

---

**If the value for pause  
points**
**Do**

was the default value or zero

[step 35](#)

was any other value

[step 33](#)

- 33** At the Answer: prompt, you can enter Continue. To continue the upgrade, type

**Continue**

and press the Enter key.

The upgrade tool

- locks the inactive Shelf Controller card
- unlocks the inactive Shelf Controller card

- swacts the current active Shelf Controller card
- prompts for confirmation that it can lock the second inactive Shelf Controller card

*Example system response:*

**Note:** The entire system response as shown below will not necessarily appear instantaneously. The system will display some output, then pause, then continue. Such pauses are normal.

```
Lock in progress...
Lock completed successfully.
Unlock the inactive (first) unit started.
Unlock in progress...
Unlock completed successfully.
Swact the active (second) unit started.
Swact in progress...
Swact completed successfully.
Lock the inactive (second) unit started.
Locking the inactive SC will cause the SCs to operate
in simplex mode. Do you wish to proceed?

Please select from the following:
Continue

Answer:
```

- 34** At the Answer: prompt, you can enter Continue. To continue the upgrade, type

**Continue**

and press the Enter key.

The upgrade tool

- locks the newly inactive Shelf Controller Card
- unlocks the newly inactive Shelf Controller Card.

*Example system response:*

**Note:** The entire system response as shown in the figure that follows will not necessarily appear instantaneously. The system will display some output, then pause, then continue. Such pauses are normal.

```
Lock in progress...
Lock completed successfully.
Unlock the second unit started.
Unlock in progress...
Unlock completed successfully.

Upgrade Status Report:
SC node : SC1
Upgrade status : Both SC units finished successfully.

SCUnitUpgrade order : slot7 (inactive), slot9 (active)
Start time : 2004-11-10 02:35:07.542
Stop time : 2004-11-10 02:47:25.305
Elapsed time : 12 minutes 17 seconds

SC1-0 slo7 ip: 47.142.114.222
SCUnit status:
Administrative state : Unlocked
Operational state : Enabled
Activity state : Active
Card status : None

Total alarms:
Critical alarms : 0
Major alarms : 1

Load name : 13.0.0.051111104360

SC1-1 slot9 ip: 47.142.114.223
SCUnit status:
Administrative state : Unlocked
Operational state : Enabled
Activity state : Inactive
Card status : None

Total alarms:
Critical Alarms : 0
Major alarms : 1

Load name : 13.0.0.05111110436

Upgrade of both SC units finished successfully.
```

- 35** The upgrade is complete. The system automatically returns to the Upgrade Menu for the SC upgrade tool.

*Example system response:*

```
Upgrade Menu for SC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - Exit

Enter selection (1-5,x):
```

- 36 Perform post-check**  
The post-check ensures that the load, state, and alarm conditions are correct. To display the data, enter:
- > 5

*Example system response:*

```
Upgrade Status Report:
SC node : SC1
Upgrade status : Both SC units finished successfully.

SCUnitUpgrade order : slot7 (inactive), slot9 (active)
Start time : 2004-11-10 02:35:07.542
Stop time : 2004-11-10 02:47:25.305
Elapsed time : 12 minutes 17 seconds

SC1-0 slo7 ip: 47.142.114.222
SCUnit status:
Administrative state : Unlocked
Operational state : Enabled
Activity state : Active
Card status : None

Total alarms:
Critical alarms : 0
Major alarms : 1

Load name : 13.0.0.05111110436

SC1-1 slot9 ip: 47.142.114.223
SCUnit status:
Administrative state : Unlocked
Operational state : Enabled
Activity state : Inactive
Card status : None

Total alarms:
Critical Alarms : 0
Major alarms : 1

Load name : 13.0.0.05111110436
```

Once the post-check is complete, the system automatically returns to the Upgrade menu.

*Example system response:*

```
Upgrade Menu for SC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - Exit

Enter selection (1-5,x):
```



**Note:** If the upgrade fails, contact the next level of support.

### 37 Exit SC upgrade tool

Exit the Upgrade Menu for the Shelf Controller upgrade tool and return to the Main Menu for the Shelf Controller upgrade tool.

Enter:

> **x**

*Example system response:*

```
Main Menu for SC upgrade tool
1 - Display all SC pairs
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

### 38 Refer to the following table to determine your next action.

| If                                                                 | Do                               |
|--------------------------------------------------------------------|----------------------------------|
| you want to continue upgrading other Shelf Controller nodes        | return to <a href="#">step 3</a> |
| you do not want to continue upgrading other Shelf Controller nodes | <a href="#">step 39</a>          |

### 39 Stop the upgrade tool and exit the CLUI. Enter:

> **x**

*Example system response:*

```
SC Upgrade Manager Stopped successfully at 2004-11-09
05:37:25.813
```

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

---

## Reprovision the Ethernet Routing Switch 8600 port to auto-negotiate

---

### Purpose of this procedure

If the Communication Server LAN (CS LAN) is provided by Nortel Ethernet Routing Switch 8600 routers, the port on the CS LAN router must be set to auto-negotiate the Ethernet port speed and duplex state. The port is normally configured that way. However, if the setting is incorrect, the port must be reconfigured before launching the SAM21 Shelf Controller or Gateway Controller upgrade tool.

### When to use this procedure

If the Ethernet port on the CS LAN router is not set to auto-negotiate, use this procedure before launching the Shelf Controller or Gateway Controller upgrade tool.

### Prerequisites

You must use READ/WRITE/ALL (RWA) login and/or password privileges when performing this procedure. For more information about RWA privileges, refer to the Ethernet Routing Switch 8600 configuration documentation.

### Action

At the CLI for the Ethernet Routing Switch 8600

- 1 Determine the slot and port on the router that connects to the device. Type:

```
> show ip arp info <ip_address>
```

and press the Enter key

where <ip\_address>

is the physical IP address of the Shelf Controller, Gateway Controller, or Universal SignalingPoint.

## Example system response:

```
prompt:cpu> show ip arp info 172.30.242.25
```

```
=====
 Ip Arp
=====
 IP_ADDRESS MAC_ADDRESS VLAN PORT TYPE TTL

172.30.242.25 00:90:69:1a:d4:fc 200 1/2 DYNAMIC 272
```

Record the slot and port number; you will need this information in the next step of this procedure.

**Note:** If the response indicates MLT instead of the slot and port, perform this operation from the mate unit. If the response indicates that no arp entry is found, ping the IP address from the CLI, and retry the command.

- 2 Use the values recorded in [step 1](#) to set the slot and port to auto-negotiate. Type:

```
> config ethernet <slot>/<port> auto-negotiate
enable
```

and press the Enter key.

System response:

```
prompt:cpu> config ethernet 1/2 auto-negotiate enable
prompt:cpu>
```

The system configures the slot and port to auto-negotiate, and the prompt returns.

- 3 Verify the port configuration. Type:

```
> show port info config port <slot>/<port>
```

and press the Enter key.

## System response:

```
prompt:cpu> show port info config port 1/2
```

```
=====
 Port Config
=====
```

| PORT<br>NUM | TYPE      | AUTO<br>NEG. | SFFD  | ADMIN<br>DUPLX | SPD | OPERATE<br>DUPLX | SPD | DIFF-SERV<br>EN | QOS<br>TYPE | MLT<br>LVL | ID |
|-------------|-----------|--------------|-------|----------------|-----|------------------|-----|-----------------|-------------|------------|----|
| 1/2         | 100BaseTX | true         | false | half           | 100 | full             | 100 | fals            | core        | 1          | 0  |

The system displays the slot and port configuration.

- 4** Commit the change. Type:

```
> save config
```

and press the Enter key.

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

---

## Check a Shelf Controller that does not unlock

---

### Purpose of this procedure

This procedure enables you to check, and if necessary correct, the condition of a Shelf Controller that does not unlock. The checks include items such as such as physical positioning, port settings, and IP addresses.

### When to use this procedure

Use this procedure if the Shelf Controller does not unlock. This condition is indicated by the lock icon persisting on the SAM21 Shelf View, showing that the Shelf Controller failed to boot.

### Prerequisites

This procedure has no prerequisites.

### Action

#### ***At the CS 2000 SAM21 Manager client***

- 1 Open the Shelf View of the SAM21 Shelf with the SAM21 Shelf Controller.
- 2 Use the following table to determine your next step.

| If a lock icon                  | Do                      |
|---------------------------------|-------------------------|
| appears over a SAM21 SC         | <a href="#">step 3</a>  |
| does not appear over a SAM21 SC | <a href="#">step 21</a> |

- 3 Ensure that the SAM21 Shelf Controller has enough time to boot. A SAM21 Shelf Controller can take up to four minutes to boot on a slow network.  
  
If the SAM21 Shelf Controller has enough time to boot and still has a lock icon and a hashed outline, continue with this procedure.

#### ***At the SAM21 frame***

- 4 Verify that the SAM21 Shelf Controller is fully seated in the slot. Check the latches on the SAM21 Shelf Controller and the Hot Swap Controllers. The latch handles are perpendicular to the faceplate when the card is inserted properly and the latches are latched properly.

**Note:** Do not push on the faceplate to seat the card; use the levers.

- 5 Connect a VT100 terminal or a PC with terminal application software to the serial port labeled COM1 on the rear of the SAM21 shelf. If the SAM21 Shelf Controller in slot 7 does not boot, connect to slot 7. If the SAM21 Shelf Controller in slot 9 does not boot, connect to slot 9.
- 6 To start the HyperTerminal application, click Start menu, click Programs, click Accessories, and click HyperTerminal.
- 7 Double-click the Hyperterm.exe icon to open a new connection. The system displays the Connection Description box.
- 8 Enter SC in the Name field and click OK. The system displays the Phone Number box.
- 9 Select Direct to COM1 from the Connecting using: list. Leave other entries in the box empty. Click OK.
- 10 Open the COM1 Properties box and set the port settings to the following:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Flow control: HardwareClick OK.
- 11 Press the Enter key. The system displays a new Hyperterm window with a login prompt.
- 12 If the console displays the message  
`em respawning too fast`  
the latches are not latched properly.  
  
Press the reset button on the faceplate while the console is connected and verify that the firmware revision is RM12 or the firmware revision indicated in the *SAM21 Platform Base Release Notes*.

*Example system response:*

Copyright Motorola Inc. 1988-2000, All Rights Reserved

PPC1 Debugger/Diagnostics Release Version 4.9 - 07/12/01 HA **RM12**  
COLD Start

Local Memory Found=08000000 (&134217728)

MPU Clock Speed=367Mhz

BUS Clock Speed=67Mhz

WARNING: Keyboard Not Connected

Reset Vector Location : ROM Bank B  
Mezzanine Configuration : Single-MPU  
Current 60X-Bus Master : MPU0  
Idle MPU(s) : none

L2Cache : 1024KB, 147Mhz  
System Memory : 128MB, ECC Enabled (ECC-Memory Detected)

HA Mesquite Abbreviated Self-Tests about to Begin...

ISABRIDGE IRQ: Interrupt Request.....Running---> PASSED

SelfTest/Boots about to Begin... Press <BREAK> at anytime to Abort ALL

NetBoot about to begin... Press <ESC> to Bypass, <SPC> to Continue

Firmware revision RM12

- 13 Press the Esc key to bypass NetBoot and access the PPC-Bug prompt.

- 14 Type **cnfg** at the PPC-Bug prompt and press Enter.

**Note:** The MAC address of the SAM21 Shelf Controller card should be displayed. Verify that this is the address used in the CS 2000 SAM21 Manager client on the Reprovisioning window.

- 15 Type **niot** at the PPC-Bug prompt and press Enter.

- 16 The SAM21 Shelf Controller software provides a series of prompts. Accept the default values, except for the following options in bold. For the options in bold, enter the value indicated in the table.

**Note:** If an error is entered, type . (period) and press Enter to quit. Restart niot by typing **niot** and pressing Enter.

| Prompt                                                                     | Value           |
|----------------------------------------------------------------------------|-----------------|
| Controller LUN                                                             | 00              |
| Device LUN                                                                 | 00              |
| Node Control Memory Address                                                | 07F9E000        |
| <b>Client IP Address</b>                                                   | <b>0.0.0.0</b>  |
| <b>Server IP Address</b>                                                   | <b>0.0.0.0</b>  |
| Subnet IP Address Mask                                                     | 255.255.255.0   |
| Broadcast IP Address                                                       | 255.255.255.255 |
| <b>Gateway IP Address</b>                                                  | <b>0.0.0.0</b>  |
| <b>Boot File Name</b>                                                      | NULL            |
| Argument File Name                                                         | NULL            |
| Boot File Load Address                                                     | 001F0000        |
| Boot File Execution Address                                                | 001F0000        |
| Boot File Execution Delay                                                  | 00000000        |
| Boot File Length                                                           | 00000000        |
| Boot File Byte Offset                                                      | 00000000        |
| <b>BOOTP/RARP Request Retry</b>                                            | <b>00</b>       |
| <b>TFTP/ARP Request Retry</b>                                              | <b>00</b>       |
| <b>Hardware Error Retry Attempts</b>                                       | <b>20</b>       |
| Trace Character Buffer Address                                             | 00000000        |
| <b>BOOTP/RARP Request Control</b>                                          | <b>A</b>        |
| <b>BOOTP/RARP Reply Update Control</b>                                     | <b>N</b>        |
| <b>Update Non-Volatile RAM</b><br>(only appears if a change has been made) | <b>Y</b>        |

17 Type **env** at the PPC-Bug prompt and press Enter.



- 18** The SAM21 Shelf Controller software provides a series of prompts. Accept the default values, except for the following options in bold. For the options in bold, enter the value indicated in the table.

| Prompt                                                   | Value                   |
|----------------------------------------------------------|-------------------------|
| Bug or System Environment                                | B                       |
| Field Service Menu Enable                                | N                       |
| Probe System for Supported I/O Controllers               | Y                       |
| Auto-Initialize of NVRAM Header Enable                   | Y                       |
| <b>Network PReP-Boot Mode Enable</b>                     | <b>Y</b>                |
| SCSI Bus Reset on Debugger Startup                       | N                       |
| Primary SCSI Bus Negotiations Type                       | A                       |
| Primary SCSI Data Bus Width                              | N                       |
| Secondary SCSI Identifier                                | 07                      |
| NVRAM Boot List (GEV.fw-boot-path) Boot Enable           | N                       |
| NVRAM Boot List (GEV.fw-boot-path) Boot at power-up only | N                       |
| NVRAM Boot List (GEV.fw-boot-path) Boot Abort Delay      | 5                       |
| Auto Boot Enable                                         | N                       |
| Auto Boot at power-up only                               | N                       |
| Auto Boot Scan Enable                                    | N                       |
| Auto Boot Scan Device Type List                          | FDISK/CDROM/TAPE/HDISK/ |
| Auto Boot Controller LUN                                 | 00                      |
| Auto Boot Device LUN                                     | 00                      |
| Auto Boot Partition Number                               | 00                      |
| Auto Boot Abort Delay                                    | 7                       |

| Prompt                                                     | Value        |
|------------------------------------------------------------|--------------|
| Auto Boot Default String                                   | NULL         |
| ROM Boot Enable                                            | N            |
| ROM Boot at power-up only                                  | Y            |
| ROM Boot Abort Delay                                       | 5            |
| ROM Boot Direct Starting Address                           | FFF00000     |
| ROM Boot Direct Ending Address                             | FFFFFFFC     |
| <b>Network Auto Boot Enable</b>                            | <b>N</b>     |
| Network Auto Boot at power-up only                         | N            |
| Network Auto Boot Controller LUN                           | 00           |
| Network Auto Boot Device LUN                               | 00           |
| Network Auto Boot Abort Delay                              | 5            |
| Network Auto Boot Configuration Parameters Offset (NVRAM)  | 00001000     |
| <b>Watchdog prior status ignored at autoboot</b>           | <b>Y</b>     |
| <b>Watchdog reset at board reset</b>                       | <b>Y</b>     |
| <b>Reset Ethernet chip after file reception</b>            | <b>Y</b>     |
| Stop Auto Boot After Selftest Failure                      | N            |
| Memory Size Enable                                         | Y            |
| Memory Size Starting Address                               | 00000000     |
| Memory Size Ending Address                                 | 08000000     |
| DRAM Speed in NANO Seconds                                 | 50           |
| ROM First Access Length (0-31)                             | 10           |
| ROM Next Access Length (0-15)                              | 0            |
| DRAM Parity Enable [On-Detection/Always/<br>Never - O/A/N] | O (letter O) |

| Prompt                                                                 | Value                                                                                                                                                                                   |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L2Cache Parity Enable<br>[On-Detection/Always/Never - O/A/N]           | O (letter O)                                                                                                                                                                            |
| PCI Interrupts Route Control Registers<br>(PIRQ0/1/2/3)                | 0A050000                                                                                                                                                                                |
| Serial Startup Code Master Enable                                      | N                                                                                                                                                                                       |
| Serial Startup Code LF Enable                                          | N                                                                                                                                                                                       |
| Claim domain A                                                         | N                                                                                                                                                                                       |
| Claim domain B                                                         | N                                                                                                                                                                                       |
| Slot power control word                                                | 00000000                                                                                                                                                                                |
| Ignore healthy control word                                            | 00000000                                                                                                                                                                                |
| <b>Firmware Command Buffer Enabled</b>                                 | <b>Y</b>                                                                                                                                                                                |
| <b>Firmware Command Buffer Delay</b>                                   | <b>20</b>                                                                                                                                                                               |
| <b>Firmware Command Buffer</b>                                         | <b>ma cboot</b> <Enter key><br><b>pboot 14 0</b> <Enter key><br><b>nbo</b> <Enter key><br><Enter key><br><b>ma ;l</b> <Enter key> (letter L)<br><b>cboot</b> <Enter key><br><b>NULL</b> |
| <b>Update Non-Volatile RAM</b><br>(appears only when a change is made) | <b>Y</b>                                                                                                                                                                                |
| Reset local system (CPU)                                               | Y                                                                                                                                                                                       |

On completion of the entries, the SAM21 Shelf Controller reboots.

- 19** Optionally, verify that calls can originate and complete.
- 20** If the problem persists (that is, the SAM21 Shelf Controller still does not unlock) contact Nortel support personnel.
- 21** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Confirming SAM21 Shelf Controller loads after an upgrade

---

Use this procedure to confirm each SAM21 Shelf Controller has the correct software load after an upgrade. Repeat this procedure for each SAM21 Shelf Controller with upgraded software.

### Prerequisites

Perform this procedure after you complete the upgrade of software on a SAM21 Shelf Controller.

### Action

#### Confirming SAM21 Shelf Controller loads after an upgrade

##### *From the main window of the CS 2000 SAM21 Manager*

- 1 Double-click the icon of a SAM21 shelf with an upgraded SAM21 Shelf Controller.

*Response*

*The Shelf View window appears.*

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

| If the Shelf View window | Do                                                                                            |
|--------------------------|-----------------------------------------------------------------------------------------------|
| appears                  | <a href="#">step 3</a>                                                                        |
| does not appear          | Troubleshoot the problem or contact your next level of support. The upgrade was unsuccessful. |

- 3 Double-click the icon of an upgraded SAM21 Shelf Controller.

*Response*

*The Card View window appears.*

- 4 Click the Provisioning tab. Under Load Info, note the load names identified for Provisioned Load Name and Current Running Version.

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

| If the load names are                                 | Do                                                                                            |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| the new loads for the SAM21 Shelf Controller software | <a href="#">step 6</a>                                                                        |
| anything else                                         | Troubleshoot the problem or contact your next level of support. The upgrade was unsuccessful. |

- 6 Close the Card View window.

*Response*

*The Shelf View window appears.*

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

| If you confirmed the load for                   | Do                     |
|-------------------------------------------------|------------------------|
| one SAM21 Shelf Controller blade in the shelf   | <a href="#">step 3</a> |
| both SAM21 Shelf Controller blades in the shelf | <a href="#">step 8</a> |

- 8 Close the Shelf View window.

*Response*

*The main window of the CS 2000 SAM21 Manager appears.*

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

| If you                                                                      | Do                      |
|-----------------------------------------------------------------------------|-------------------------|
| need to check additional SAM21 shelves for upgraded SAM21 Shelf Controllers | <a href="#">step 1</a>  |
| do not need to check additional SAM21 shelves                               | <a href="#">step 10</a> |

- 10 You have completed this procedure. Return to [Completing the SAM21 Shelf Controller upgrade on page 1379](#).

---

## Aborting a SAM21 Shelf Controller software upgrade

---

Use this procedure to abort an upgrade of SAM21 Shelf Controller software when a failure occurs during the upgrade.

### Prerequisites

Perform this procedure after you receive an error message with a prompt to retry or abort the upgrade step. An error message can indicate a card could not be locked or unlocked, a load could not be changed, or a switch of activity could not be completed.

### Action

#### Aborting a SAM21 Shelf Controller software upgrade

##### *At the CLUI*

- 1      At the prompt to retry or abort, abort the upgrade by typing  
**abort**  
and pressing the Enter key.  
*Response*  
*The Upgrade Menu for the SAM21 Shelf Controller appears.*
- 2      Exit the Upgrade Tool by typing  
**x**  
and pressing the Enter key.  
*Response*  
*The Main Menu for the SAM21 Shelf Controller appears*
- 3      Stop the upgrade and exit the CLUI by typing  
**x**  
and pressing the Enter key.  
*Response*  
*The CLUI exits and a command prompt appears.*

**At the CS 2000 SAM21 Manager**

- 4 Make sure you are at the Shelf View of the SAM21 shelf with the inactive Shelf Controller blade you want to upgrade.
- 5 Go to the Card View of the inactive Shelf Controller. Right-click the icon of the inactive Shelf Controller blade and select Card View from the list of commands.

*Response*

*The Card View window appears.*

- 6 Click the States tab and make sure the Status of the selected Shelf Controller is Inactive
- 7 Use the following table to determine your next step.

| If the status is | Do                     |
|------------------|------------------------|
| Active           | <a href="#">step 4</a> |
| Inactive         | <a href="#">step 8</a> |

- 8 Check the state of the card, as displayed in the following OSI fields:
  - Card Status
  - Operational
  - Availability

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

| If                                                                        | Do                                  |
|---------------------------------------------------------------------------|-------------------------------------|
| Card Status is Locked<br>Operational is Enabled<br>Availability is None   | <a href="#">step 10</a>             |
| Card Status is Unlocked<br>Operational is Enabled<br>Availability is None | <a href="#">step 12</a>             |
| anything else                                                             | Contact your next level of support. |

- 10** Unlock the Shelf Controller Blade. On the left side of the Card View window, right-click the Shelf Controller icon and select Unlock from the list of commands.

*Response*

*The CS 2000 SAM21 Manager unlocks the selected Shelf Controller blade.*

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

| If the unlock is | Do                                                                                                |
|------------------|---------------------------------------------------------------------------------------------------|
| successful       | <a href="#">step 12</a>                                                                           |
| not successful   | Repeat <a href="#">step 10</a> . If the second attempt fails, contact your next level of support. |

- 12** Close the Card View of the inactive Shelf Controller.

*Response*

*The Shelf View window appears.*

- 13** You have aborted the upgrade of the SAM21 Shelf Controller software. Troubleshoot the upgrade failure or contact your next level of support.

To resume the upgrade, go to [Upgrade the Shelf Controller using the Shelf Controller Upgrade Tool on page 1406](#).





# GWC upgrade

---

This chapter describes how to upgrade the software on the Gateway Controller (GWC).

## New in this release

This section describes changes in GWC upgrades in (I)SN09U.

### Feature changes

None

### Other changes

This release introduces the following additional changes to GWC upgrades:

- new high-level procedures to improve usability of detailed GWC upgrade procedures and simplify the GWC upgrade process

## Upgrade paths

Nortel Networks supports the following upgrade paths:

- (I)SN08 to (I)SN09U
- (I)SN09 to (I)SN09U

## Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

**Time to complete an upgrade**

The following table lists the tasks to upgrade the software on a Gateway Controller node and the estimated time to complete each task.

**Table 1 Estimated time to complete a software upgrade**

| Task                         | Time                      |
|------------------------------|---------------------------|
| Preparing for the upgrade    | 45 minutes                |
| Upgrading the software       | 18 to 24 minutes per node |
| Completing the upgrade       | 15 minutes to 1 hour      |
| Total estimated upgrade time | 2 hours 10 minutes        |

**Note:** The condition of the office before the upgrade may require additional traffic analysis and log monitoring after the upgrade.

## Service impacts



### CAUTION

#### Loss of service

Service outages occur during the upgrade of Gateway Controller software.

The upgrade of Gateway Controller software creates the following service impacts:

- Stable two-port calls survive a switch of activity between the GWC nodes. However, calls in setup mode during the SWACT are dropped.
- The following table lists possible call service impacts for the GWC card types during the following scenarios:
  - an upgrade from one release to a newer release
  - an maintenance upgrade to a newer version of the same release
  - a downgrade from one release to a previous release

**Table 2 GWC upgrade call service impacts (Sheet 1 of 2)**

| GWC Type | Upgrade                                                                                               | Maintenance                                       | Downgrade                                                                |
|----------|-------------------------------------------------------------------------------------------------------|---------------------------------------------------|--------------------------------------------------------------------------|
| AUDCNTL  | Stable announcement and conference calls survive.                                                     | Stable announcement and conference calls survive. | Stable announcement and conference calls not using new features survive. |
| VRDN     | All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive. | ALL calls survive.                                | Calls not using new features survive.                                    |
| SIP-T    | All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive. | ALL calls survive.                                | NO calls survive.                                                        |

**Table 2 GWC upgrade call service impacts (Sheet 2 of 2)**

| <b>GWC Type</b> | <b>Upgrade</b>                                                                                                                                                                   | <b>Maintenance</b>                                                                                                                                                               | <b>Downgrade</b>                                                                                                                               |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| MG 15000 trunk  | All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.                                                                            | ALL calls survive.                                                                                                                                                               | NO calls survive.                                                                                                                              |
| Line or H.323   | Stable 2-party calls survive. Possible limited functionality after the swact.<br><br>For unstable dialing, ringing, clearing or multi-party calls the behavior is unpredictable. | Stable 2-party calls survive. Possible limited functionality after the swact.<br><br>For unstable dialing, ringing, clearing or multi-party calls the behavior is unpredictable. | SOME calls may survive.<br><br>Billing records might not be produced when calls go on-hook.<br><br>H.323 gateway-based calls will not survive. |

**Additional information**

Starting in (I)SN08, the Upgrade Automation Tool supports parallel Gateway Controller upgrades.

CS 2000 Management Tools generates new middlebox IDs for network address translator (NAT) devices and policy enforcement point (PEP) servers if these items were provisioned before the upgrade.

**System capacity**

The software upgrade procedure can impact the system capacity. This means that additional disk space on the OAMP workstation is required for converting existing databases.

**System performance**

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade

## System limitations during upgrade

During a software upgrade, the system prohibits the following actions:

- System administration
  - adding, deleting, or modifying users
  - setting the time of day
  - changing passwords
- System management
  - modifying the system name
  - adding or deleting system nodes
  - modifying the IP addresses
- Once ethics 2000 Core Manager or CBM is upgraded, you cannot provision Gateway Controllers until the CS 2000 Management software package is upgraded and configured on the CS 2000 Management Tools server.

## Upgrade order for GWC card types

Upgrade GWC card pairs in order based on the type of GWC card. If you use the GWC Upgrade Tool, the tool automatically upgrades the card types in the correct order. If you do not use the GWC Upgrade Tool, you must identify the GWC card types in your office and schedule the upgrades in the correct order.

All GWC cards of the same type must be upgraded before moving on to the next group. For example, you must all audio controller GWC cards before you upgrade the next GWC card-type present in your system.

The following table lists the upgrade order for all available GWC card types.

**Note:** The table lists all available GWC card types. Your office will not have all the card types listed in the table. Refer to the *Gateway Controller Basics*, NN10189-111, for details on the card types listed in this table and supported in your release.

#### GWC card type upgrade order

| Order | GWC card type                                               |
|-------|-------------------------------------------------------------|
| 1     | AC                                                          |
| 2     | BICC - Long Distance Voice over IP (UA-AAL1) solutions only |
| 3     | VRDN                                                        |
| 4     | Session Server - see <a href="#">Note 1</a>                 |
| 5     | SIP-T                                                       |
| 6     | Trunk                                                       |
| 7     | H.323                                                       |
| 8     | V5.2 trunk                                                  |
| 9     | Lines - includes Centrex IP Client Manager (CICM)           |

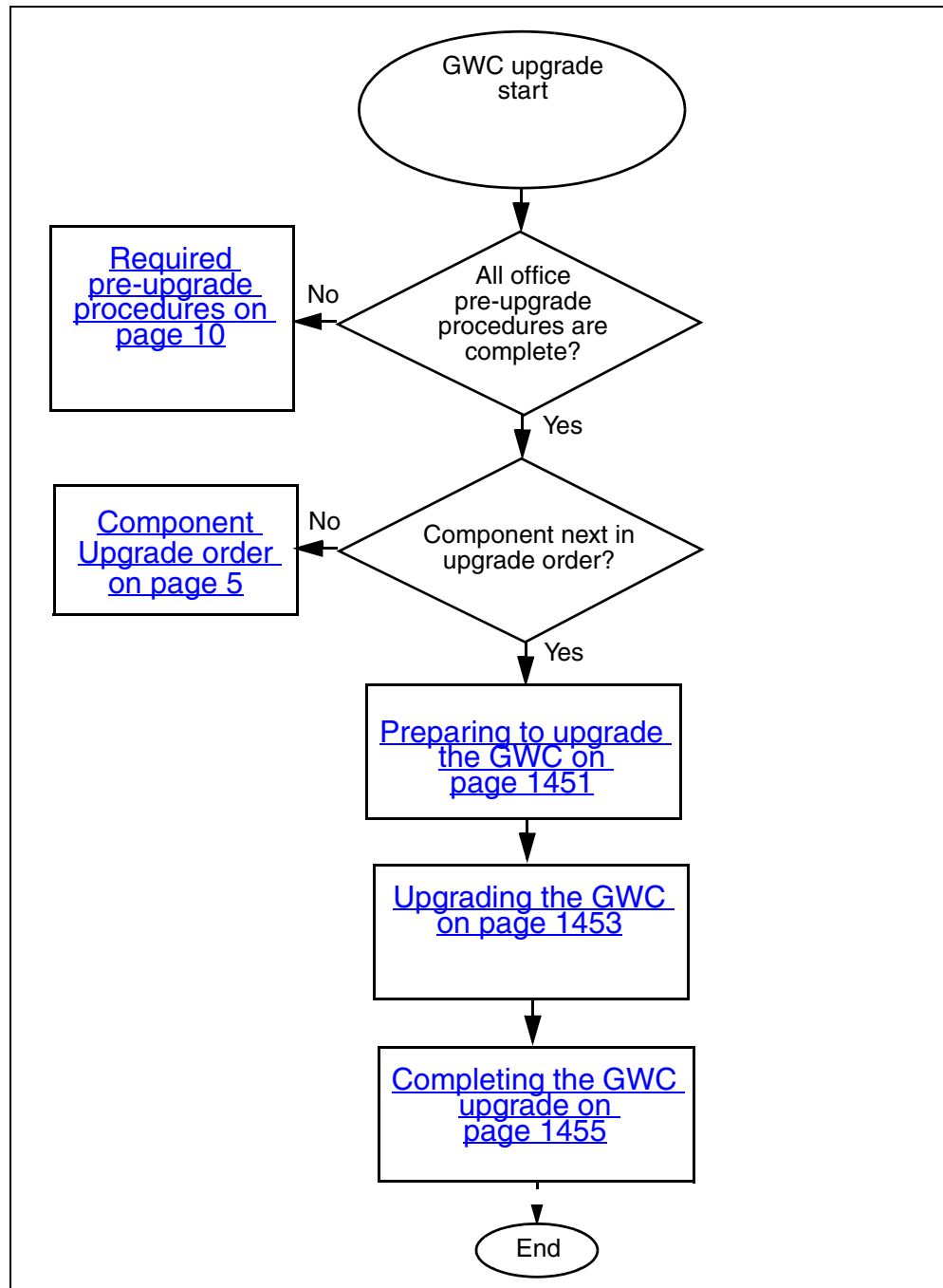
**Note 1:** The Session Server-Trunks (SS-T) can replace the Virtual Routing Destination Node (VRDN) GWC as a SIP-T interface. The following office configurations are supported: SS only, VRDN SIP-T only, or VRDN SIP-T and SS-T co-existing in the same office.

**Note 2:** The manual upgrade process does not support parallel upgrades. While it is possible to save time by loading all GWC card pairs of a given GWC type and performing all the SwActs at the same time, this is not recommended or supported for a live office upgrade as it would cause an out of service condition for all GWC nodes.

## GWC upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

**Figure 1 GWC upgrade tasks**



---

## Preparing to upgrade the GWC

---

The following procedure provides the steps you need to execute prior to upgrading the GWC. When applicable, a reference to the procedure that contains the detailed steps is provided.

### Prerequisites

You have completed the following tasks:

- all [Required pre-upgrade procedures on page 10](#)
- the upgrade of all components that precede the component in the [Component Upgrade order on page 5](#)

### Action

#### *At the CS 2000 Management Tools server*

- 1 Transfer the new software to the boot server for your GWC using one of the following procedures:
  - If you are using a load delivered on CD, perform [Copying GWC software from CD to the boot server on page 1456](#)
  - If you are using a load delivered through Electronic Software Delivery (ESD), perform the following procedures:
    - [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)
    - [Copying GWC software from an SPFS-based server to the boot server on page 1461](#)
- 2 Use the following table to determine your next step.

| If                               | Do                     |
|----------------------------------|------------------------|
| you received patches on CD       | <a href="#">step 3</a> |
| you received patches through ESD | <a href="#">step 4</a> |
| you do not have any patches      | <a href="#">step 6</a> |
- 3 Insert the CD-ROM that contains the patches into the CD-ROM drive of the SPFS-based server where the NPM resides.
- 4 Log in to the SPFS-based server where the NPM resides.



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

| <b>If you are retrieving the patches from</b> | <b>Do</b>                                                                                                              |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| CD                                            | perform procedure <a href="#">Transferring patches delivered on CD to the NPM database on page 2297</a>                |
| ESD                                           | perform procedure <a href="#">Transferring patches delivered as an ISO image file to the NPM database on page 2309</a> |

- 6 You have completed this procedure. Proceed to [Upgrading the GWC on page 1453](#).

---

## Upgrading the GWC

---

The following procedure provides the steps you need to execute to upgrade the GWC. When applicable, a reference to the procedure that contains the detailed steps is provided.

### Prerequisites

This procedure has the following prerequisites:

- You have completed procedure [Preparing to upgrade the GWC on page 1451](#).
- Your office has access to the following patch audit tools:
  - Pre Upgrade Patch Calculator
  - Patch Audit for Inform ListsPatch audit tools are available at [www.nortel.com](http://www.nortel.com).
- Make sure your current GWC software is patch current.

### Action

Perform the following procedures

1. Identify and download any Released (R) and Propagated (P) patches for the new release.
  - Use the Pre Upgrade Patch Calculator Tool, download any patches to your site, and transfer the patches to the NPM database.
    - If your new GWC software is delivered on CD, perform procedure [Transferring patches delivered on CD to the NPM database on page 2297](#).
    - If your new GWC software is delivered through ESD, perform [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#).

|                  |
|------------------|
| <b>ATTENTION</b> |
|------------------|

|                                                             |
|-------------------------------------------------------------|
| Pre-patched GWC loads cannot be used across multiple sites. |
|-------------------------------------------------------------|

2. Backup your existing GWC software. Perform [Create a backup of the GWC load file on page 1465](#).
3. Remove old GWC load files. Perform [Remove old GWC load files on page 1471](#).

4. Determine if the new load image contains any patches. Perform [View the contents of a load file image on page 1467](#). If the new load image contains patches, ensure all the patches contained in the image are in the NPM database. If you are unsure if the patches are in the NPM database, repeat the patch download procedures performed in [step 2](#) of procedure [Preparing to upgrade the GWC on page 1451](#) and step [1](#) on page [1453](#).
5. Upgrade the GWC software. Perform [Upgrade the GWC using the GWC Upgrade Tool on page 1473](#).
6. If you upgraded a VRDN GWC or Session Server GWC, and your office interworks with an MCS gateway, change the GWC settings in the MCS Manager. Perform [GWC provisioning on MCS on page 1515](#).
7. You have upgraded the software on the GWC. Go to [Completing the GWC upgrade on page 1455](#).

---

## Completing the GWC upgrade

---

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

You have completed procedure [Upgrading the GWC on page 1453](#).

GWC node hardware has been upgraded from the MCPN750 to MCPN905. If this has not been completed, contact your next level of support.

### Action

#### ***At the CS 2000 Management Tools server***

- 1 Re-enable the plans you disabled at the beginning of the GWC upgrade. Refer to procedure [Modifying NPM patching plans on page 2409](#).

#### ***At the CS 2000 Management Tools GUI***

- 2 Make sure the correct load name for each Gateway Controller appears in the CS 2000 Management Tools application. Perform [Confirming Gateway Controller loads after an upgrade on page 1522](#).
- 3 If a rollback is required, refer to [Rolling back a software upgrade on a standby GWC node on page 1524](#).
- 4 If you need to upgrade your GWC node hardware from the MCPN750 to MCPN905, contact your next level of support.
- 5 You have completed the upgrade of the Gateway Controller. Continue with the next component to be upgraded.

---

## Copying GWC software from CD to the boot server

---

### Purpose of this procedure

This procedure describes how to copy GWC software from a CD to the boot server. The boot server for the GWC can be any of the following devices:

- CS 2000 Core Manager
- Core and Billing Manager (CBM)

### When to use this procedure

Use this procedure to install a Maintenance Non-Computing Load (MNCL) or a standard software release (NCL) GWC load.

### Prerequisites

This procedure has no prerequisites.

### Action

#### ***At the CS 2000 Management Tools frame***

- 1 Insert the CD-ROM into the CD-ROM tray of the 'active' CS 2000 Management Tools server.

#### ***At the CS 2000 Management Tools terminal***

- 2 Log in and then use the su command to gain root privilege.

```
Trying <hostname>....
Connected to <hostname>.
Escape character is '^'.

Authorized use only, activities logged.
login: username
Password: <password>
Last login: Fri Jan 30 12:48:10 from <otherhost>
prompt:>
prompt:> su - root
Password: <root_password>
#
```

### 3 Execute the installation script by typing

```
/opt/nortel/sspfs/Scripts/platform_load_
install.sh
```

and pressing the Enter key.

*Example response:*

```
Welcome to the Platform Installation Tool Version 3.3
=====
RPM INSTALLATION/REMOVAL
=====
1) Install RPM from CDROM 2) Install RPM from Disk
3) Uninstall RPM 4) Query all RPMs

TAR INSTALLATION/REMOVAL
=====
5) Install SC load from Tape 6) Install SC load from cdrom
7) Install SC load from Disk 8) Remove a SC Load
9) Install 3PC Load from Tape 10) Install 3PC Load from Disk

OTHER
=====
L) Install SOS/MS/PMLOADS D) Install SOS/MS/PMLOADS from disk
C) Change Rotation Parameters P) View Rotation Parameters
V) Platform Version Installed X) Exit

Please choose one of the following: 1
```

### 4 Install the software by typing

```
> 1
```

and pressing the Enter key.

The system displays the contents of the RPM package.

*Example response:*

```
Verifying CDROM is mounted
/cdrom/cdrom on /vol/dev/disk/c0t0d0/cdrom read
only/mosuid/map1-case/noglobal/rr/traildot/dev=16c0001
on Sat Mar 27 16:34:13 2004
 CDROM is mounted.
 Listing file names in the rpm on the cd.
/swd/gwc/gwcConFig.sh
/swd/gwc/gn070be.imag

Do you want to continue (y/n)? Y
```

**Note:** If the system displays the following message: There is no cd in the CDROM drive, please check drive, ensure that the CD-ROM is inserted in the tray for this unit.

- 5 Confirm that you want to proceed with the installation by typing  
> **y**

and pressing the Enter key.

The software is extracted from the RPM package. The RPM package is transferred to the CS 2000 Core Manager or CBM.

Example response:

```
Extracting files from the rpm archive on the cd.

Installing RPM package gn070be_plat-1.0-041304.moarch.rpm
Sun Microsystems Inc. Sun 5.8 Generic Patch December 2002
gn070be_plat-1.0-041304.noarch.rpm 100% 11MB 750.4KB 00:14
root@47.135.214.127's password: <enter root password>
```

- 6 Enter the root password for the CS 2000 Core Manager or the CBM.

The system installs the software on the CS 2000 Core Manager or CBM. If CBM is used, the RPM package is then copied to the inactive CBM unit and another prompt for the root password is displayed. Enter the root password again and press the Enter key.

After the load file is installed on the CS 2000 Core Manager or CBM, the transferred RPM package is deleted from the CS 2000 Core Manager or CBM.

Example response:

```
Extracting files from the rpm archive on the cd.

Installing RPM package gn070be_plat-1.0--41304.moarch.rpm
Sun Microsystem Inc. SunOs 5.8 Generic Patch December 2002
gn070be_plat-1.0-041304.noarch.rpm 100% 11MB 8.2MB/s 00:40
root@47.135.214.127's password: <enter root password>
Mate IP is 47.135.214.129
Sun Microsystem Inc. SunOs 5.8 Generic Patch December 2002
root@47.135.214.129's password: <enter root password>
```

```
*****Please hit ENTER key to continue*****
```

**Note:** An additional confirmation prompt can display requesting acceptance of the RSA key. Confirm the following sample prompt by typing yes.

RSA key fingerprint is 99:09:e2:80:57:95:3e:be:26:08:a0:c6:32:ed:48.  
Are you sure you want to continue connecting (yes/no)?

- 7 Exit the installation program by typing

# **x**

and pressing the Enter key.

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

| If the GWC load is being installed on the |  | Do                            |
|-------------------------------------------|--|-------------------------------|
| CS 2000 Core Manager                      |  | go to <a href="#">step 9</a>  |
| CBM                                       |  | go to <a href="#">step 14</a> |

**At the CS 2000 Core Manager Console**

- 9 Log in to the CS 2000 Core Manager as the root user.

AIX Version 4  
(C) Copyrights by IBM and by others 1982, 1996.  
login: root  
root's Password: <password>

- 10 Access the gwc directory by typing

# **cd /swd/gwc**

and pressing the Enter key.

- 11 Execute the GwcConfig.sh script by typing

# **./GwcConfig.sh**

and pressing the Enter key.

*System response:*

*The script checks whether the appropriate configuration data is present in the /swd/gwc directory.*

- 12 If prompted, enter the hostname of the CS 2000 Management Tools server (where the SAM21 EM server process resides) and press the Enter key. Otherwise, continue with [step 13](#).



- 13 Log out of the CS 2000 Core Manager by typing  
`# exit`  
and pressing the Enter key.

***At the CS 2000 Management Tools terminal***

- 14 Eject the CD-ROM from the CD-ROM tray by typing  
`# eject cdrom`  
and pressing the Enter key.
- 15 Log out of the CS 2000 Management Tools server.
- 16 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure

---

## Copying GWC software from an SPFS-based server to the boot server

---

### Purpose of this procedure

This procedure describes how to copy GWC software loads from an SPFS-based server, such as the CS 2000 Management Tools server to the boot server for the GWC. The boot server can be any of the following devices:

- CS 2000 Core Manager
- Core and Billing Manager (CBM)

### When to use this procedure

Use this procedure to install a Maintenance Non-Computing Load (MNCL) or a standard software release (NCL) GWC load.

### Prerequisites

You must have already performed procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

### Action

#### *At the CS 2000 Management Tools terminal*

- 1 Log in and then use the su command to gain root privilege.
- 2 List the contents of the directory you created in procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#) by typing  

```
$ ls <directory_name>
```

and pressing the Enter key.  
where  
**directory\_name**  
is the directory path specified in [step 2](#) of [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).
- 3 Locate the .rpm file by accessing the following directories.  

```
cd /tmpmnt/noarch
```

**Note:** Record the name of the .rpm file. You will use this filename later.

**4** Execute the installation script by typing

```
/opt/nortel/sspfs/Scripts/platform_load_
install.sh
```

and pressing the Enter key.

*Example response:*

```

Welcome to the Platform Installation Tool Version 3.3
=====
RPM INSTALLATION/REMOVAL
=====
1) Install RPM from CDROM 2) Install RPM from Disk
3) Uninstall RPM 4) Query all RPMs

TAR INSTALLATION/REMOVAL
=====
5) Install SC load from Tape 6) Install SC load from cdrom
7) Install SC load from Disk 8) Remove a SC Load
9) Install 3PC Load from Tape 10) Install 3PC Load from Disk

OTHER
=====
L) Install SOS/MS/PMLOADS D) Install SOS/MS/PMLOADS from disk
C) Change Rotation Parameters P) View Rotation Parameters
V) Platform Version Installed X) Exit

Please choose one of the following: 2
```

**5** Install the software by typing

```
> 2
```

and pressing the Enter key.

**6** When prompted, enter the .rpm filename recorded in [step 3](#) and press the Enter key.**7** When prompted for the location of the .rpm file, enter the directory specified in [step 3](#) of this procedure and press the Enter key.**8** Confirm that you want to proceed with the installation by typing

```
> Y
```

and pressing the Enter key.

**9** When prompted, continue collecting by typing.

```
> yes
```

and pressing the Enter key.

- 10 When prompted for the password, enter the root password of the CS 2000 Core Manager or CBM and press the Enter key.
- 11 The system displays messages telling of its progress through the process of installing the rpm package. The final messages it displays are as follows:
- Installation of Platform Load Complete.  
 \*\*\*\*\*Please hit ENTER key to continue\*\*\*\*\*

- 12 Press the Enter key.

*System response*

```

Welcome to the Platform Installation Tool Version 3.2
=====
RPM INSTALLATION/REMOVAL
=====
1) Install RPM from CDROM 2) Install RPM from Disk
3) Uninstall RPM 4) Query all RPMs

OTHER
=====
C) Change Rotation Parameters P) View Rotation Parameters
V) SAM21 Platform Version Installed X) Exit

Please choose one of the following:

```

- 13 Exit the installation program by typing  
**# x**  
 and pressing the Enter key.
- 14 Change to the root directory by typing  
**# cd /**  
 and pressing the Enter key.
- 15 Unmount the ESD. Reference procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#)
- 16 Use the following table to determine your next step.

| <b>If the GWC load is being installed on the</b> | <b>Do</b>                     |
|--------------------------------------------------|-------------------------------|
| CS 2000 Core Manager                             | go to <a href="#">step 17</a> |
| CBM                                              | go to <a href="#">step 22</a> |

***At the CS 2000 Core Manager console or terminal window***

- 17 Log in to the CS 2000 Core Manager as the root user.

- 18 Access the gwc directory by typing  
**# cd /swd/gwc**  
and pressing the Enter key.
- 19 Execute the GwcConfig.sh script by typing  
**# ./GwcConfig.sh**  
and pressing the Enter key.  
*System response:*  
*The script checks whether the appropriate configuration data is present in the /swd/gwc directory.*
- 20 If prompted, enter the hostname of the CS 2000 Management Tools server (where the SAM21 EM server process resides) and press the Enter key. Otherwise, continue with [step 21](#).
- 21 Log out of the CS 2000 Core Manager by typing  
**# exit**  
and pressing the Enter key.

***At the CS 2000 Management Tools terminal***

- 22 Log out of the CS 2000 Management Tools server.
- 23 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Create a backup of the GWC load file

---

### Purpose of this procedure

This procedure is used to log onto the CS 2000 Core Manager or Core and Billing Manager (CBM) and manually make a backup copy of one or more existing GWC load images stored on the CS 2000 Core Manager or CBM.

### When to use this procedure

Use this procedure prior to saving an image of a GWC load if you wish to save a backup of the original GWC load stored on the CS 2000 Core Manager or CBM.

**CAUTION****Possible rollback failure**

If a backup is not created, the process of taking a GWC load image overwrites the existing image stored on the CS 2000 Core Manager or CBM, preventing a rollback.

### Prerequisites

There are no prerequisites to this procedure.

### Action

***At the CS 2000 Core Manager or CBM console***

- 1 Log in to the CS 2000 Core Manager or CBM as the root user.

```
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password: <password>
```

- 2 Change directory to the GWC software directory by typing  
**# cd /swd/gwc**  
and pressing the Enter key.
- 3 Type **ls** and press the Enter key to list the contents of the directory.
- 4 Locate the load file name that corresponds to the load you wish to back up.  
  
There are likely to be multiple load file names. Ensure that you select the correct load filename. If you are saving the load file of

a specific GWC card or node, refer to procedure “View the operational status of a GWC” in *Gateway Controller Configuration Management*, NN10205-511, to locate the load filename associated with a specific GWC card.

5



#### CAUTION

Be sure to use the command `cp` in this step. Failure to use the `cp` command can cause problems with the general upgrade process.

Make a copy of the existing GWC software load file by typing

**# `cp <load_filename>.imag <load_filename>.imag.bak`**

and pressing the Enter key.

where

**<load\_filename>**

is the GWC load filename that you want to copy.

You can use any name for the backup file name. You can also include the date in this filename, for example:

`<load_filename>.imag.031201`

6

Change the permissions for the image file by typing

**# `chmod 755 <load_filename>.imag.bak`**

and pressing the Enter key.

where

**<load\_filename>**

is the GWC load filename

7

You have completed this procedure. Return to [Upgrading the GWC on page 1453](#).

---

## View the contents of a load file image

---

### Purpose of this procedure

This procedure allows you to view the content of the current load file located on the CS 2000 Core Manager or Core and Billing Manager (CBM). You can view the list of patches that have been applied and activated on the load file image. A load file is created by taking an image of a software load present on a GWC device. You may take an image manually or automatically.

Perform this procedure on the CS 2000 Management Tools server since the gwclinfo command is a SESM application script, and the /swd/gwc load directory is NFS-mounted on the CS 2000 Management Tools server in the /var/opt/nortel/gwc directory.

### When to use this procedure

Use this procedure to confirm the contents of a load file image on the CS 2000 Core Manager or CBM before rebooting GWC devices from the file.

Use this procedure to determine if the delivered load contains patches.

### Prerequisites

This procedure has no prerequisites.

### Action

Use the following table to determine your first step.

| If your office has               | Do                           |
|----------------------------------|------------------------------|
| a CS 2000 Core Manager installed | go to <a href="#">step 1</a> |
| a CBM installed                  | go to <a href="#">step 5</a> |

#### ***At the CS 2000 Management Tools server***

- 1 Access the directory where the GWC load file information is located by typing  

```
cd /var/opt/nortel/gwc
```

and pressing the Enter key.
- 2 List all the GWC load names by typing  

```
ls
```

and pressing the Enter key.



- 3 Select the new GWC software load from the list and display its content by typing

```
/opt/nortel/NTsesm/tools/gwc_tools/
gwclfinfo /var/opt/nortel/gwc/<gwc_load_file>
```

and pressing the Enter key.

where

**<gwc\_load\_file>**

is the name of the selected GWC load image file, for example pgc09bl\_patched\_03\_04.imag

**Note:** In the above command, insert a space after the gwclfinfo character string. Do not insert any other spaces.

*Example response:*

Load information from pgc09bl\_patched\_03\_04.imag

Load name: PGC09BL Image created: Fri Mar 5 7:0:21 2004

| Patch-ID | Status  | Activation |
|----------|---------|------------|
| XBN63GZ9 | Applied | NonAct     |
| XED41GZ9 | Applied | NonAct     |
| XQA89GZ9 | Applied | NonAct     |

.  
.  
.

- 4 Go to [step 14](#)

**At the CS 2000 Management Tools terminal**

- 5 Access the temporary directory by typing

```
cd /tmp
```

and pressing the Enter key.

- 6 Access the CBM server by typing

```
ftp <CBM_IP_address>
```

and pressing the Enter key.

where

**<CBM\_IP\_address>**

is the IP address of the CBM server

- 7 When prompted, enter the user name by typing

```
Name: gwcload
```

and pressing the Enter key.

- 8 When prompted, enter the password by typing  
**Password: gwcload**  
and pressing the Enter key.
- 9 Set up the ftp transfer process to binary by typing  
**ftp> bin**  
and pressing the Enter key.
- 10 Transfer the GWC image load file by typing  
**ftp> get <gwc\_image\_name>**  
and pressing the Enter key.  
where  
**<gwc\_image\_name>**  
is the name of the GWC load image file stored on the CBM server

*Example response:*

```
200 PORT command successful.
150 Opening data connection for pgt93ax.imag (binary mode
 (10294018)).
226 Transfer complete.
local: pgt93ax.imag remote: pgt93ax.imag
10294018 bytes received in 5.3 seconds (1908.92 Kbytes/s)
```

- 11 Return to the /tmp directory on the CS 2000 Management Tools server by typing  
**ftp> quit**  
and pressing the Enter key.
- 12 Display the content of the GWC software load image by typing  
**# /opt/nortel/NTsesm/tools/gwc\_tools/gwclfinfo /tmp/<gwc\_image\_name>**  
and pressing the Enter key.  
where  
**<gwc\_image\_name>**  
is the name of the transferred GWC load image file

*Example response:*

```
Load information from pgt93ax.imag
```

```
Load name: PGT93AX Image created: Fri Mar 5 7:0:21 2004
```

| Patch-ID | Status  | Activation |
|----------|---------|------------|
| XBN63GZ9 | Applied | NonAct     |
| XED41GZ9 | Applied | NonAct     |
| XQA89GZ9 | Applied | NonAct     |
| .        |         |            |
| .        |         |            |
| .        |         |            |

- 13** When you are finished reviewing the content of the file, remove the GWC load image from the /tmp directory by typing

```
rm /tmp/<gwc_image_name>
```

and pressing the Enter key.

where

**<gwc\_image\_name>**

is the name of the transferred GWC load image file

- 14** You have completed this procedure. Return to [Upgrading the GWC on page 1453](#).

---

## Remove old GWC load files

---

### Purpose of this procedure

This procedure is used to log onto the CS 2000 Core Manager or Core and Billing Manager (CBM) and manually remove one or more old GWC load images stored on the CS 2000 Core Manager or CBM.

### When to use this procedure

Use this procedure when you want to free up space on the CS 2000 Core Manager or CBM.

### Prerequisites

There are no prerequisites to this procedure.

### Action

#### ***At the CS 2000 Management Tools GUI***

- 1 Launch the CS 2000 Management Tools GUI, and click on Gateway Controller under Device Types.
- 2 Click on the first GWC in the list on the left-hand side, to display its information.
- 3 Click the Maintenance tab if not already displayed, and note the name of the load next to Loadname for unit 0 or unit 1.
- 4 Repeat [step 2](#) and [step 3](#) for each GWC in the list.

#### ***At the CS 2000 Core Manager or CBM console***

- 5 Log in to the CS 2000 Core Manager or CBM using the root user ID and password.
- 6 Use the following table to determine your next step.

| If you logged in to a | Do                     |
|-----------------------|------------------------|
| CBM                   | <a href="#">step 7</a> |
| CS 2000 Core Manager  | <a href="#">step 9</a> |

- 7 Change directory to the GWC software directory by typing  
# `cd /data/swd/gwc`  
and pressing the Enter key.
- 8 Proceed to [step 10](#).

- 9 Change directory to the GWC software directory by typing  
# **cd /swd/gwc**  
and pressing the Enter key.
- 10 List the contents of the directory by typing  
# **ls**  
and pressing the Enter key.
- 11 Using the list you made of the load files that are in use, as a reference, make note of the load files that are not in use.
- 12 Delete each load file that is not in use by typing  
# **rm <old\_load>.imag**  
and pressing the Enter key.
- 13 You have completed this procedure. Return to [Upgrading the GWC on page 1453](#).

---

## Upgrade the GWC using the GWC Upgrade Tool

---

### Purpose of this procedure

This procedure describes how to upgrade the software load from which the GWC cards boot, located on the CS 2000 Core Manager or Core and Billing Manager (CBM).

### When to use this procedure

Use this procedure after installing a newer version of the GWC software load onto CS 2000 Core Manager or CBM. This procedure upgrades all selected GWC nodes installed in the SAM21 shelf that is being upgraded.

### Prerequisites

The following prerequisites and guidelines apply to this procedure.



#### CAUTION

No provisioning activity can occur on the system while the GWC software upgrade is in progress.

All the necessary patches must be loaded into the Network Patch Manager (NPM) application.

CS 2000 SAM21 Manager must be installed on the same server as the GWC Upgrade Tool. For the GWC Upgrade Tool to be launched, CORBA, SESMSservice, NPM, and CS 2000 SAM21 Manager software packages must be running in this server.

If the NPM server is configured within the same server, it must be configured and running correctly. If NPM server is running with the Integrated EMS server, the PSE package within the same server must be configured and running correctly (and NPM may not appear in the system response below).

The NPM automated processes must be disabled. Refer to [step 34](#) of this procedure for more information.

If the Communication Server LAN (CS LAN) is provided by Nortel Ethernet Routing Switch 8600 routers, the port connecting to the CS 2000 Management Tools server and gateway controllers on the CS LAN router, must be set to auto-negotiate. The port is normally configured that way. However, if the setting is incorrect, the port must be reconfigured before launching the GWC Upgrade Tool. Refer to procedure [Reprovision the Ethernet Routing Switch 8600 port to auto-negotiate on page 1429](#).

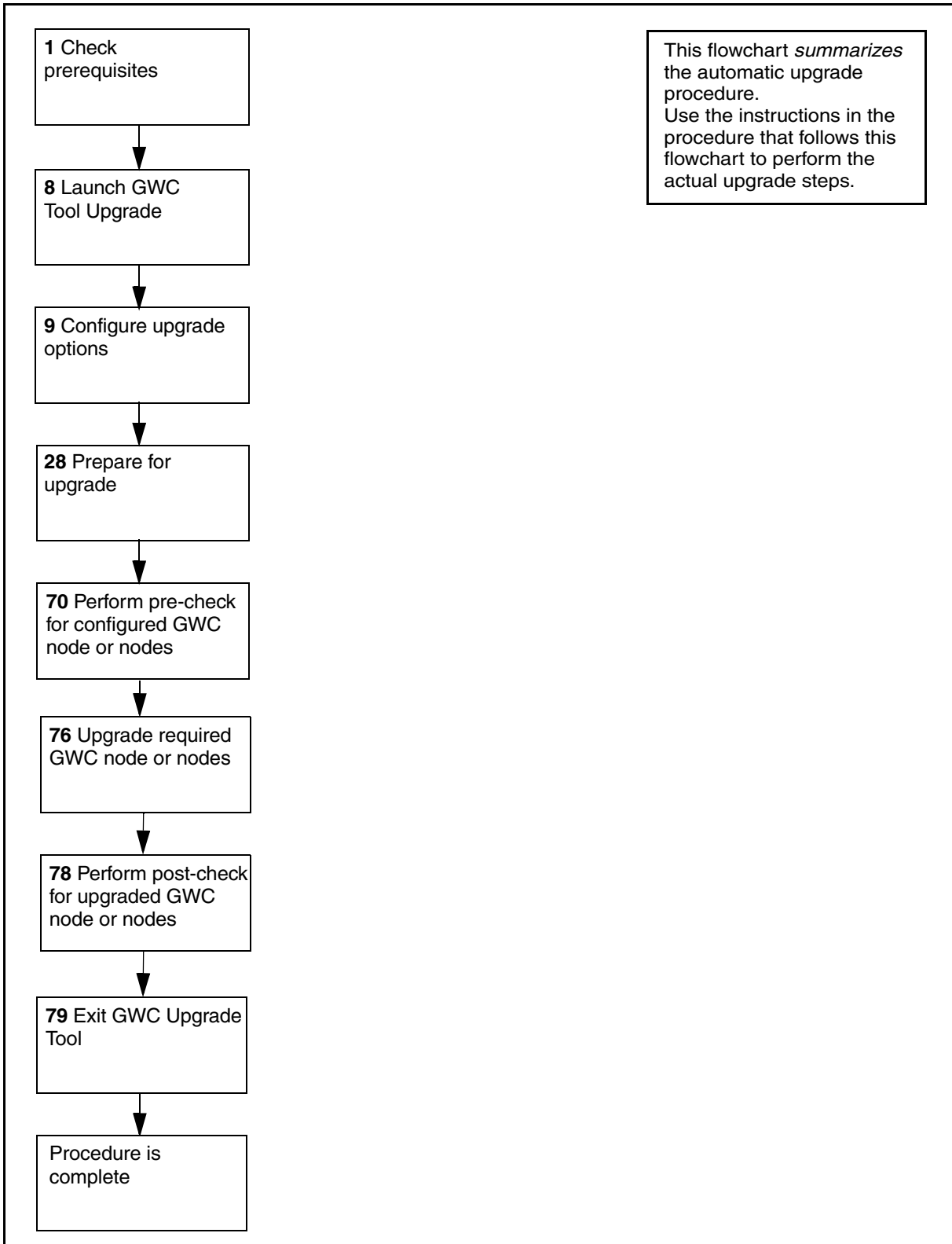
## Overview

The GWC Upgrade Tool is distributed with the CS 2000 Management Tools SESM software package. The tool supports GWC upgrades using the command line user interface (CLUI). The tool automatically performs the following GWC upgrade operations:

- locks the inactive unit of the first selected GWC node (seed node), provisions it with a new load, and unlocks the unit
- busies the upgraded inactive unit, carries out a device audit, applies all available patches, returns the unit to service and swacts the seed node
- locks the newly inactive unit of the seed node, provisions it with the new soaked load, and unlocks the unit
- for all the other selected GWC nodes in turn (non-seed nodes) locks the inactive unit, provisions it with the newly soaked load, unlocks the unit, and swacts the node
- locks the newly inactive unit of the non-seed node, provisions it with the new soaked load, and unlocks the unit

The following flowchart provides an overview of the automated upgrade procedure. The numbers correlate to the steps of [Action: upgrade procedure on page 1480](#), following the flowchart.

## Automatic upgrade overview





## Configurable options

As shown in the following table, the user can configure 11 options in the GWC Upgrade Tool. Two options are mandatory, and one of them must be given a specific value. For the optional items, the user can press the Enter key to accept the default values.

| Option name    | Mandatory (M) or optional (O) | Description                                                                                                                                                                                                                                                                                          | Default value                         |
|----------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| New Load File  | M                             | The name of the new GWC load file.                                                                                                                                                                                                                                                                   |                                       |
| GWC List       | M                             | The GWCs to be upgraded. By default, all GWC nodes managed by the CS 2000 GWC Manager and CS 2000 SAM21 Manager are selected.                                                                                                                                                                        | All                                   |
| Load Directory | O                             | The GWC load directory configured in CS 2000 SAM21 Manager. The default value is /swd/gwc. If the Core and Billing Manager (CBM) was used, the user must change the load directory to /gwc.                                                                                                          | current configured load path          |
| New Load Name  | O                             | The target load name of the given GWC load file. If the file name does not contain the GWC load name, the user must specify a valid GWC load name here. The new load name is used to query the patch list from NPM. By default, the new load file name is LOAD_NAME.imag, for example, gn090ch.imag. | new load file name (excluding .imag') |
| Old Load Name  | O                             | The load upgraded from. The default value is null. If the user ignores this option (the default), the upgrade manager server bypasses old load checking and all selected GWC nodes are upgraded automatically.                                                                                       | old load file name (excluding .imag') |

| Option name  | Mandatory (M) or optional (O) | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Default value |
|--------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Upgrade Mode | O                             | <p>Defines whether GWCs are upgraded singly or together. Three modes are available:</p> <p>single - All GWC nodes are upgraded one by one, ordered by GWC profile type and GWC ID.</p> <p>bulk - All GWC nodes within the same service group (for example, TRUNK, LINE) are upgraded at the same time. If patching is needed, the first selected seed GWC node which is used to create the soak image uses single mode, and the other nodes that do not need patching use bulk mode.</p> <p>mix - In the same GWC profile group (for example, Trunk GWCs, Line GWCs), one GWC node is upgraded first. This enables the user to verify a specific type of GWC. After the first node is upgraded successfully, all the other GWC nodes within the same profile group are upgraded together.</p> | bulk          |

| Option name   | Mandatory (M) or optional (O) | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Default value     |
|---------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Pause Point   | O                             | <p>Specifies the points at which the upgrade process pauses to allow the user to make manual checks.</p> <p>Seven options are available:<br/> 0 - No pause points; if 0 is selected, all other pause points are ignored.<br/> 1 - Pause before locking the first unit of the seed GWC node.<br/> 2 - Pause after patches are applied to the seed node.<br/> 3 - Pause before warm swact of the seed node.<br/> 4 - Pause after warm swact of the seed node.<br/> 5 - Pause after the seed node is upgraded.<br/> 6 - Pause before warm swact of non-seed nodes.</p> <p>Pause points 1 to 5 apply only to the seed GWC node; pause point 6 applies to all other bulk upgrade GWC nodes.</p> | 0                 |
| Logging Level | O                             | Defines the default logging level of the GWC Upgrade Tool.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | VRB               |
| Max Time      | O                             | <p>Defines the time limit (in minutes) for the upgrade.</p> <p>If the upgrade cannot complete all the GWC nodes in the specified time, the non-upgraded GWCs remain un-upgraded and the process ends. The default value <b>0</b> disables the time limit check.</p>                                                                                                                                                                                                                                                                                                                                                                                                                        | 0 (no time limit) |

| Option name  | Mandatory (M) or optional (O) | Description                                                                                                                                                                                                                                                   | Default value |
|--------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Alarm Level  | O                             | Defines the alarm level of the in-service GWC unit that the GWC Upgrade Tool reports to the user. Values are:<br>MAJ - indicating a major alarm<br>CRT - indicating a critical alarm                                                                          | MAJ           |
| Alarm Number | O                             | Defines the acceptable alarm count, that is, the number of in-service GWC alarms of the specified alarm level at which the GWC Upgrade Tool reports to the user (refer to section <a href="#">Alarm checking on page 1479</a> in this procedure for details). | 2             |

## Alarm checking

During the upgrade only the in-service GWC unit is checked for alarms, and only the critical and major alarms are checked. When the actual GWC alarms reach the defined alarm state, the upgrade pauses and the system displays a message to the user.

For example, if the alarm checking is set to the default values MAJ 2, the following table shows how the GWC Upgrade Tool behaves when different numbers of in-service GWC alarms occur:

| In-service GWC alarms | Upgrade pauses? |
|-----------------------|-----------------|
| CRT 0, MAJ 1          | N               |
| CRT 0, MAJ 2          | N               |
| CRT 0, MAJ 3          | Y               |
| CRT 1, MAJ 0          | Y               |
| CRT 1, MAJ 1          | Y               |
| CRT 2, MAJ 0          | Y               |

| In-service GWC alarms | Upgrade pauses? |
|-----------------------|-----------------|
| CRT 2, MAJ 1          | Y               |
| CRT 2, MAJ 2          | Y               |

For an additional example, if the alarm checking is set to the values CRT 2, the following table shows how the tool behaves when different numbers of in-service GWC alarms occur:

| In-service GWC alarms | Upgrade pauses? |
|-----------------------|-----------------|
| CRT 0, MAJ 1          | N               |
| CRT 0, MAJ 2          | N               |
| CRT 0, MAJ 3          | N               |
| CRT 1, MAJ 0          | N               |
| CRT 1, MAJ 1          | N               |
| CRT1, MAJ 2           | N               |
| CRT 2, MAJ 0          | N               |
| CRT 2, MAJ 1          | N               |
| CRT 2, MAJ 2          | N               |
| CRT 3, MAJ 0          | Y               |

## Action: upgrade procedure

### *At the CS 2000 Management Tool interface*

- 1 Check the prerequisites for this procedure as described in section [Prerequisites on page 1473](#).
- 2 Ensure that you have a valid user ID and password to access the GWC Upgrade Tool.
- 3 Log in to the CS 2000 Management Tools server using telnet or SSH. If your CS 2000 Management Tools server is in a

high-availability cluster, make sure you log in to the active server.

Type:

```
> telnet <server>
```

or

```
> ssh -l <user_ID> <server>
```

where <server> is the IP address or host name of the Sun server where CS 2000 Management Tools SESM application resides.

and press the Enter key.

- 4 When prompted, type your user ID and password, and press the Enter key.
- 5 Ensure that the operator belongs to one of the following groups authorized to launch the GWC Upgrade Tool: mgcmtc, mgcadm, emsmtc or emsadm. If necessary, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP Solution-level Security and Administration*, NN10402-600.  
Type:

```
$ id -a
```

and press the Enter key.

System response:

```
$ id -a
uid=104(ptm) gid=105(succssn)
groups=105(succssn),1001(trkadm),1006(lnadm),
1011(mgcadm),1016(mgadm),1021(emsadm)
$
```

\_\_\_\_\_ Group names \_\_\_\_\_

- 6 Change to the root user by typing

```
$ su -
```

and press the Enter key.

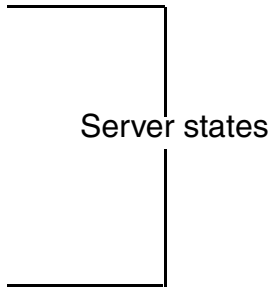
- 7 Check the status of the SAM21EM and CORBA server applications to ensure they are running properly by typing

# **servquery -status all**

and pressing the Enter key.

Example system response:

```
$ servquery -status all
APP NAME STATUS
===== =====
DATABASE RUNNING
CINOTIFIER RUNNING
BACKUP_MANAGER Group Started. Current status unavailable
BOOTP RUNNING
WEBSERVER RUNNING
CORBA RUNNING
OMPUSH RUNNING
SESMSservice RUNNING
WEBSERVICES RUNNING
DDMSPROXY RUNNING
ORA_AUTO_BACKUP RUNNING
DELEGATE RUNNING
ORA_ARCHIVE_ROTATOR RUNNING
NPM RUNNING
PROP_SRV RUNNING
SAM21EM RUNNING
SNMP_POLLER Group Started. Current status unavailable
QCA RUNNING
```



Server states

## 8 Launch GWC Upgrade Tool

Exit from root and start the GWC Upgrade Tool CLUI. Type:

```
> exit
> cd /opt/nortel/NTsesm/gwcuptool/bin
> ./gwcuptool.sh
```

and press the Enter key.

System response:

```
cd /opt/nortel/NTsesm/gwcuptool/bin
./gwcuptool.sh
Starting

Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

**Note:** If the GWC Upgrade Tool fails to start, check the logs. These are in the same directory as the tool, that is, gwcuptool/logs.

Within the GWC Upgrade Tool, after typing a menu option or other input value, press the Enter key. Details of the Main Menu options are as follows:

### 1 - Display all GWC nodes

This option is to query the name and card type for all GWC nodes.

Example system response:



```
Enter selection (1-4,x): 1
```

```

GWC-7 TRUNKNA
GWC-0 SMALL_LINENA
GWC-2 SMALL_LINENA
GWC-3 LARGE_LINENA
GWC-4 SMALL_LINENA
GWC-5 SMALL_LINENA
GWC-6 SMALL_LINENA

```

```
Total: 7
```

## 2 - Configure upgrade-related options

This option is to configure upgrade options manually. The CLUI prompts the user to input the necessary information step by step. These configuration options are then effective throughout the whole upgrade process.

## 3 - List current configuration values

This option lists all the configuration options currently applied.

## 4 - Enter Upgrade Menu

This option is to enter the upgrade submenu.

## x - Stop upgrade tool and exit CLUI

This option stops the GWC Upgrade Tool and exits the CLUI.

## 9 Configure upgrade options

From the Main Menu, enter:

> 2

System response:

```
Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x): 2

GWC upgrade configuration
[Step 1 - LOAD FILE NAME]
Enter the new load file name(Example: gn070bv.imag):
```

- 10** Enter the name of the new GWC load file name. The load file name has a .imag extension. Make sure that the configured load file name exists on the CS 2000 Core Manager or CBM.

Load file name format:

nnnnnnnn.nnnnn

Example file name entry:

gn090bv.imag

System response:

```
Enter the new load file name(Example: gn070bv.imag): gn090bv.imag

[Step 2 - GWC LIST]
Separate GWC names with comma, for example: GWC-1,GWC-2,GWC-3,GWC-5

Enter the GWC list (Default: all):
```

- 11** Enter the GWC nodes to be upgraded. To select all available GWCs, press the Enter key. To select specific GWCs, enter the names of those required (separated with commas and no spaces).

**Note:** If you select all available GWCs, the GWC Upgrade Tool automatically upgrades the card types in the correct order. Refer to section [Upgrade order for GWC card types on page 1448](#).

Example list entry:

GWC-1,GWC-2,GWC-3,GWC-5

The system displays the current input configuration values.

Example system response:

```
Enter the GWC list (Default: all): GWC-2,GWC-4
```

```
[Step 3 - INPUT VALUES]
```

```
New Load File Name : gn090bv.imag
```

```
GWC List : GWC-2,GWC-4
```

```
Default values
```

```
Load Directory : /swd/gwc/
```

```
New Load Name : " " (ignored)
```

```
Old Load Name : " " (ignored)
```

```
Upgrade Mode : bulk
```

```
Pause Point : 0 (none)
```

```
Logging Level : VRB
```

```
Max Time : 0 (no limitation)
```

```
Alarm Level : MAJ
```

```
Alarm Number : 2
```

```
Do you want to use these configuration values? [Y|N] (Default: N):
```

- 12** Review the values displayed in the system response and refer to the following table to determine your next action.

| If                            | Do                                                     |
|-------------------------------|--------------------------------------------------------|
| your office uses a CBM        | enter <b>N</b> and continue at <a href="#">step 13</a> |
| you want to use the values    | enter <b>Y</b> and go to <a href="#">step 28</a>       |
| you want to change the values | enter <b>N</b> and continue at <a href="#">step 13</a> |

**Note:** In the downgrade procedure, you must enter **N** to reject the default values, otherwise you cannot continue with [step 13](#) and the rest of the downgrade steps.

- 13** System response (after entering **N**):

```
Do you want to use these configuration values? [Y|N] (Default: N): n
```

```
[Step 4 - LOAD DIRECTORY]
```

```
Default load directory formats are different for SDM and CBM.
```

```
If SDM is used, it should be "/swd/gwc".
```

```
If CBM is used, it should be "/gwc".
```

```
Enter the load directory (Default: "/swd/gwc"):
```

- 14** Enter the load directory for CS 2000 Core Manager or CBM.

**Note:** The load directory must be as same as the Load Info --> Path value.

---

| If you want to configure for | Do |
|------------------------------|----|
|------------------------------|----|

---

|                      |                       |
|----------------------|-----------------------|
| CS 2000 Core Manager | enter <b>/swd/gwc</b> |
|----------------------|-----------------------|

|     |                   |
|-----|-------------------|
| CBM | enter <b>/gwc</b> |
|-----|-------------------|

---

- 15** System response (after pressing Enter):

```
Enter the load directory (Default: "/swd/gwc"): /swd/gwc
```

```
[Step 5 - NEW LOAD NAME]
```

```
Enter the new load name (Default: ""):
```

- 16** Enter the name of the new GWC load file. The load file name is used to query the patch list from NPM. If the file name does not contain the GWC load name, you must specify a valid GWC load name here, otherwise the GWC Upgrade Tool cannot retrieve the available patch list.

System response (after pressing Enter):

```
Enter the new load name (Default: ""): gn090bv
```

```
[Step 6 - OLD LOAD NAME]
```

```
Enter the old load name (Default: ""):
```

- 17** Optionally, enter the name of the old GWC load file, that is, the file from which the load was upgraded. This is not normally needed; if you ignore this option, the upgrade manager server bypasses old load checking.

---

| If you want to | Do |
|----------------|----|
|----------------|----|

---

|                                                                                 |  |
|---------------------------------------------------------------------------------|--|
| carry out a restricted upgrade, involving only GWCs running with a special load |  |
|---------------------------------------------------------------------------------|--|

|  |                                  |
|--|----------------------------------|
|  | enter the old GWC load file name |
|--|----------------------------------|

|                    |  |
|--------------------|--|
| ignore this option |  |
|--------------------|--|

|  |                     |
|--|---------------------|
|  | press the Enter key |
|--|---------------------|

**Note:** This is the recommended action.

---

**18** System response (after pressing Enter):

Enter the old load name (Default: ""): gn080bv

[Step 7 - UPGRADE MODE]

Values:

1 - single  
2 - bulk  
3 - mix  
h - help

Enter the upgrade mode (1-3,h), (Default: 2):

**19** Enter the upgrade mode (see section [Configurable options on page 1476](#)).

| If                                                                               | Do                  |
|----------------------------------------------------------------------------------|---------------------|
| upgrade all configured GWC nodes one at a time (single)                          | enter <b>1</b>      |
| upgrade all configured GWC nodes in the same service group simultaneously (bulk) | enter <b>2</b>      |
| upgrade all configured GWC nodes in the same profile group simultaneously (mix)  | enter <b>3</b>      |
| accept the default (bulk)                                                        | press the Enter key |

**20** System response (after pressing Enter):

Enter the upgrade mode (1-3,h), (Default: 2):

[Step 8 - PAUSE POINTS]

Values:

0 - no pause points.

(1) For the first GWC node within the same GWC group.

1 - before locking first upgrade unit of "seed" node.

2 - after patch applied to "seed" unit.

3 - before warm-swact.

4 - after warm-swact.

5 - after "seed" node upgraded.

(2) For bulk upgrade GWC nodes with same GWC service type.

6 - before warm-swact.

Separate numbers with comma, for example: 1,3,4

Enter the pause points (Default: 0):

- 21** Enter the pause points for the upgrade (see section [Configurable options on page 1476](#)). Pause points allow you to carry out manual checks at selected intervals during the upgrade process. Pause points 1 to 5 (refer to the previous screen) apply only to the patched seed GWC node; pause point 6 applies to all other bulk upgrade GWC nodes.

To accept the default value (0), press the Enter key.

Example pause point entry for a single GWC node:

Enter the pause points (Default: 0): 1, 3

These entries allow two pause points:  
before the first upgrade unit of the seed pair is locked (1)  
and before a warm SwAct (3).

*Example pause point entry for bulk upgrade GWC nodes:*

Enter the pause points (default: 0): 5

This entry allows a pause point for GWC nodes in bulk mode to pause before the warm swact.

System response (after pressing Enter):

Enter the pause points (Default: 0):

[Step 9 - LOGGING LEVEL]

Values:

- 1 - Verbose
- 2 - Minor
- 3 - Major
- 4 - Critical

Enter the logging level (1-4), (Default: 1):

- 22** Enter the required logging level: VRB, MNR, MAJ or CRT (default: VRB). Upgrade logs are stored in a file in upgrade.log

under /opt/nortel/sam21em/logs/. Use the logs for troubleshooting.

To accept the default value (VRB), press the Enter key.

System response (after pressing Enter):

```
Enter the logging level (1-4), (Default: 1):
```

```
[Step 10 - TIME LIMIT]
```

```
Note: 0 means no time limit.
```

```
Enter the time limit in minutes (Default: 0):
```

- 23** Enter a time limit (in minutes) for the upgrade. If the upgrade cannot complete all the GWC nodes in the specified time, the non-upgraded GWCs remain un-upgraded and the process ends.

The default value (0) disables the time limit check. To accept the default value, press the Enter key.

In the Prepare step (see [step 28](#)), this value is compared with the estimated time for the upgrade. If the upgrade cannot be completed within the given time limit, the Prepare step fails.

System response (after pressing Enter):

```
Enter the time limit in minutes (Default: 0):
```

```
[Step 11 - ALARM LEVEL]
```

```
Values:
```

```
1 - Critical
```

```
2 - Major
```

```
Enter the alarm level (Default: 2):
```

- 24** Enter the required alarm level: CRT or MAJ. For details, refer to section [Alarm checking on page 1479](#).

To accept the default value (MAJ), press the Enter key.

System response (after pressing Enter):

```
Enter the alarm level (Default: 2):
```

```
[Step 12 - ALARM NUMBER]
```

```
Enter the maximum allowed alarm number (Default: 2)
```

- 25** Enter the maximum number of alarms allowed during the upgrade. For details, refer to section [Alarm checking on page 1479](#). If the current alarm state has a higher priority than the alarm number defined in this entry, the upgrade process pauses and the system notifies the user.

To accept the default value (2), press the Enter key.

The entries in the example allow a maximum of two Major alarms during the upgrade process. In this case, if three Major alarms occur during the upgrade, the GWC Upgrade Tool pauses. If one Major alarm occurs, the tool ignores it and continues the upgrade process. If one Critical alarm occurs, the tool also pauses, because Critical alarms have a higher priority than Major alarms.

System response (after pressing Enter):

```
Enter the maximum allowed alarm number (Default: 2)
```

```
Configuration values:
```

```
New Load File Name : gn090bv.imag
GWC List : GWC-2,GWC-4
Load Directory : /swd/gwc
New Load Name : gn090bv
Old Load Name : gn080bm
Upgrade Mode : bulk
Pause Point : 0
Logging Level : VRB
Max Time : 0
Alarm Level : MAJ
Alarm Number : 2
```

```
Is this information correct? [Y|N] (Default: N):
```

- 26** Check the upgrade configuration options. Review the values displayed in the system response (shown in the previous screen) and decide whether or not to proceed with the upgrade.

| If                                                           | Do                                                                                                                                             |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| you want to confirm the upgrade configuration options        | enter <b>Y</b> ; note the following system response, and go to <a href="#">step 28</a>                                                         |
| you do not want to confirm the upgrade configuration options | enter <b>N</b> , then go back to <a href="#">step 9</a> to re-enter the options, or go to <a href="#">step 69</a> to exit the GWC Upgrade Tool |

- 27** System response:



```
Is this information correct? [Y|N] (Default: N): y
```

```
Current configuration values:
```

```
GWC load file: gn090bv.imag
New load name: GN090BV
Load directory: /swd/gwc
Working mode: bulk
Selcted nodes: GWC-2,GWC-4
Pause points: 0
Max time: unlimited
Ignored alarms: MAJ 2
Logging level: VRB
```

```
Main Menu for GWC upgrade tool
```

```
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu
```

```
x - Stop upgrade tool and exit CLUI
```

```
Enter selection (1-4,x):
```

**Note:** After confirming the configuration, you can display the current configuration settings at any time by selecting option 3 from the Main Menu.

Example system response:

```
Enter selection (1-4,x): 3
```

```
Current configuration values:
```

```
GWC load file: gn090bv.imag
New load name: GN090BV
Load directory: /swd/gwc
Working mode: bulk
Selcted nodes: GWC-2,GWC-4
Pause points: 0
Max time: unlimited
Ignored alarms: MAJ 2
Logging level: VRB
```

```
Main Menu for GWC upgrade tool
```

```
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu
```

```
x - Stop upgrade tool and exit CLUI
```

```
Enter selection (1-4,x):
```

**28 Prepare for upgrade**

On completion of the configuration steps, you must select the Upgrade Menu to carry out the actual upgrade. From the Main Menu, enter:

**> 4**

System response:

```
Enter selection (1-4,x): 4

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x):
```

**29 Select the Prepare option from the Upgrade Menu. Enter:**

**> 1**

Example system response:

```
Enter selection (1-5,x): 1

[1 Prepare step]

The following patches are available in NPM:
1, NBF00G09
2, NBF01G09
3, NBF02G09
4, NBF03G09
5, NBF04G09
6, NBF05G09
7, NBF06G09
8, NBF07G09
9, NBF08G09
10, NBF09G09
11, NBF11G09
12, NBF12G09
13, NBF13G09
14, NBF14G09
15, NBF15G09
16, NBF17G09

Please disable the NPM automated processes.
```

- 30** Refer to the following table to determine your next action.

| <b>If</b>                | <b>Do</b>                                                                                                       |
|--------------------------|-----------------------------------------------------------------------------------------------------------------|
| upgrading using a CD-ROM | insert the upgrade CD-ROM into the 'active' CS 2000 Management Tools server, then go to <a href="#">step 32</a> |
| upgrading using ESD      | <a href="#">step 31</a>                                                                                         |

- 31** Check that the load is available in CS 2000 Core Manager or CBM. At the CS 2000 Manager server, type:

```
> cd /swd/gwc
> ls
```

and press the Enter key.

The system displays the loads in the GWC directory.

- 32** Refer to the following table to determine your next action.

| <b>If the load</b>                                                                                                                                                                     | <b>Do</b>                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| is not available, the system displays the following message:<br>GWC load file doesn't exist. Please check and try later.<br>(see <a href="#">GWC load not available on page 1509</a> ) | go back to <a href="#">step 10</a>  |
| is available                                                                                                                                                                           | continue at <a href="#">step 33</a> |

- 33** Refer to the following table to determine your next step.

| <b>If the NPM automated processes</b> | <b>Do</b>               |
|---------------------------------------|-------------------------|
| have already been disabled            | <a href="#">step 49</a> |
| have not been disabled                | <a href="#">step 34</a> |

- 34** Disable the NPM automated processes.

| <b>If you want to log in to the</b> | <b>Do</b>                           |
|-------------------------------------|-------------------------------------|
| NPM GUI                             | continue at <a href="#">step 35</a> |
| NPM CLUI                            | go to <a href="#">step 41</a>       |

**At your workstation**

- 35 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

**At the NPM GUI**

- 36 Select System from the tool bar.
- 37 Select Plans from the menu.
- 38 Click on the Plan List tab.
- 39 If any of the plans in the list are Enabled, as indicated by the check mark, they must be disabled. For each plan that is enabled, highlight the plan in the menu and click on the Disable button at the bottom.
- 40 Go to [step 48](#).

**At your workstation**

- 41 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

**A the NPM CLUI**

- 42 Display all the plans defined on the system by typing  
`npm> viewplan all`  
and pressing the Enter key.
- 43 List the details of each plan on the list, one at a time, to determine if the plan is enabled by typing  
`npm> viewplan <plan_name>`  
and pressing the Enter key.
- 44 Use the following table to determine your next step.

| If the plan is | Do                      |
|----------------|-------------------------|
| Enabled = Y    | <a href="#">step 45</a> |
| Enabled = N    | <a href="#">step 46</a> |

- 45 Disable the plan by typing  
`npm> disableplan <plan_name>`  
and pressing the Enter key.

**Note:** To use the NPM for patching activities, your user account must be assigned to both the primary user group

succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in ATM/IP Security and Administration, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in IEMS Security and Administration, NN10336-611, for centrally-managed user accounts.

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

| If                                                   | Do                      |
|------------------------------------------------------|-------------------------|
| you need to verify the enable status of another plan | <a href="#">step 43</a> |
| otherwise                                            | <a href="#">step 48</a> |

- 47** Exit the NPM CLUI by typing

`npm> quit`

and pressing the Enter key.

- 48** Keep a record of the plans that were disabled. These plans must be re-enabled at the end of the upgrade process.

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

| If                       | Do                      |
|--------------------------|-------------------------|
| upgrading using a CD-ROM | <a href="#">step 50</a> |
| upgrading using ESD      | <a href="#">step 52</a> |

***At the CS 2000 Management Tool interface***

- 50** Change directory by typing

`cd`

and pressing the Enter key.

**Note:** You must change directory from the cdrom directory for the next command (eject cdrom) to execute successfully.

**51** Eject the CD-ROM from the drive by typing**eject cdrom**

and pressing the Enter key.

Example system response:

```
--{ Group-1 }-----
GWC-2 SMALL_LINENA

--{ Group-2 }-----
GWC-4 SMALL_LINENA

Estimated time: 1 hour 5 minutes 30 seconds

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x):
```

The system displays the GWC upgrade plan and estimated upgrade time, then returns to the Upgrade Menu.

**52** **Perform pre-check**

In the Upgrade Menu, select the Pre-check option. Enter:

**> 2**

Example system response:

```

Enter selection (1-5,x): 2

[2 Pre-check step]

--{ Group-1 }-----
 GWC-2 SMALL_LINENA ... passed

--{ Group-2 }-----
 GWC-4 SMALL_LINENA ... passed

Estimated time: 1 hour 5 minutes 30 seconds

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x):

```

**53** Check the pre-check conditions. Review the information in the system response (refer to the previous screen) as described in [step 54](#) to [step 64](#).

**54** Open a new window and log in to the CS 2000 Management Tools server.  
For detailed steps, refer to [Logging in to an SPFS-based server on page 323](#).

**55** Verify the CS 2000 SAM21 Manager is running by typing  
**# servman query -status -group SAM21EM**

**56** Use the following table to determine your next step.

| <b>If the CS 2000 SAM21 Manager is</b> | <b>Do</b>               |
|----------------------------------------|-------------------------|
| running                                | <a href="#">step 58</a> |
| not running                            | <a href="#">step 57</a> |

**57** Start the CS 2000 SAM21 Manager by typing  
**# servstart SAM21EM**

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

| If the NPM is   | Do                      |
|-----------------|-------------------------|
| located on CMT  | <a href="#">step 60</a> |
| located on IEMS | <a href="#">step 59</a> |

- 59 Telnet to IEMS.

**Note:** Please exit the telnet session after verifying that the NPM is running

- 60 Verify the NPM server is running by typing  
**# servman query -status -group NPM**  
and pressing the Enter key.

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

| If the NPM application is | Do                      |
|---------------------------|-------------------------|
| running                   | <a href="#">step 63</a> |
| not running               | <a href="#">step 62</a> |

- 62 Start the NPM server application by typing

**# servstart NPM**

and pressing the Enter key.

**Note:** If the NPM is located on IEMS, please exit the telnet session after completing this step.

- 63 Check that neither GWC card has a hardware alarm.

For detailed steps, refer to *GWC Fault Management*, NN10202-911.

- 64 Verify that one GWC card is in service, and the other card is hot-standby.

For detailed steps, refer to *Gateway Controller Security and Administration*, NN10213-611.



**65** Refer to the following table to determine your next action.

| If                                                                                                  | Do                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| any of the pre-check conditions is not met<br>(see <a href="#">Pre-check failure on page 1509</a> ) | resolve the error conditions (go to <a href="#">step 7</a> to activate the servers, clear any hardware alarms, correct the status of the GWC cards), then continue the upgrade process at <a href="#">step 66</a> |
| all the pre-check conditions are met<br>(screen displays <code>passed</code> )                      | continue the upgrade process at <a href="#">step 66</a>                                                                                                                                                           |

**66 Upgrade GWC nodes**

In the Upgrade Menu, select the Upgrade option. Enter:

> 3

**Internal procedures**

At the start of the upgrade, the GWC Upgrade Tool performs the pre-check again. During the upgrade, the system displays a continuous log of the upgrade status (the log freezing may indicate a problem with one of the internal upgrade procedures).

You can also use the query option (refer to section Query upgrade status on [page 1504](#)) to display the upgrade status. If any unexpected problems occur, the system normally prompts you for a response or confirmation before continuing.

If pause points were enabled during configuration (see [step 21](#)), the tool pauses at the specified points and waits for you to carry out the required manual checks. When you have finished, enter Continue to continue the upgrade.

During the upgrade, the GWC firmware flash is enabled automatically.

There are two different internal upgrade procedures:

- For the seed GWC node there are 16 steps. The seed node is based on the upgrade order of the GWC card types, and GWC node ID. The GWC Upgrade Tool automatically selects the seed node from the GWC list entered by the user (see [step 11](#)).
- For all other (non-seed) nodes there are 11 steps. The tool automatically upgrades the other nodes when the seed is upgraded successfully.

## Example system response from the seed node:

```
Enter selection (1-5,x): 3

[3 Upgrade step]

--{ Group-1 }-----
GWC-2 SMALL_LINENA ... passed

--{ Group-2 }-----
GWC-4 SMALL_LINENA ... passed

Estimated time: 1 hour 5 minutes 30 seconds

Group-1 started
GWC-2: Upgrade task started.
GWC-2 [1/16] Busy the hot-standby first unit.(GWC-2-UNIT-1)
GWC-2 [2/16] Lock the inactive first unit. (GWC-2-UNIT-1)
GWC-2 [3/16] Change the load of the locked first unit. (GWC-2-UNIT-1)
GWC-2 [4/16] Unlock the first unit. (GWC-2-UNIT-1)
GWC-2 [5/16] Wait for the first unit to become hot-standby. (GWC-2-UNIT-1)
GWC-2 [6/16] Upgraded first unit is hot-standby. (GWC-2-UNIT-1)
GWC-2 [7/16] Apply patch to the upgraded first unit. (GWC-2-UNIT-1)
Apply request was attempted by the NPM server.
GWC-2 [8/16] Patches are applied to the upgraded first unit (GWC-2-UNIT-1)
GWC-2 [9/16] Wait for the patched unit to become hot-standby (GWC-2-UNIT-1)
GWC-2 [10/16] Patched unit is hot-standby, load imaging starts (GWC-2-UNIT-1)
GWC-2 [11/16] GWC load imaging is finished, perform the warm swact(GWC-2-UNIT-0)
GWC-2 [12/16] Warm swact is finished, busy the second unit. (GWC-2-UNIT-0)
GWC-2 [13/16] Lock the second unit. (GWC-2-UNIT-0)
GWC-2 [14/16] Second unit is locked. (GWC-2-UNIT-0)
GWC-2 [15/16] Change the load of the locked second unit. (GWC-2-UNIT-0)
GWC-2 [16/16] Second unit is booted up with the soaked load. (GWC-2-UNIT-0)
GWC-2 Upgrade finished successfully.
Group-1 finished
Elapsed time: 16 minutes 25 seconds
```

**Note:** If during the upgrade process, the upgrade tool displays patches requiring special attention and prompts to Continue Retry or Abort, apply the patches to the GWC unit shown using procedure [Applying patches using the NPM on page 2319](#), and then type Continue.

**Upgrade steps for the seed GWC node**

This section assumes that GWC-2 is the seed node, GWC-2 UNIT-0 is in service, GWC-2 UNIT-1 is hot-standby, the new load file name is gn090bv.imag, and the load version is GN090BV.

The GWC Upgrade Tool automatically performs the following actions in the order listed:

1. Busies the inactive unit GWC-2 UNIT-1 in the GWC EM.
2. Locks the inactive unit GWC-2 UNIT-1 in the SAM21 EM.
3. Provisions GWC-2 UNIT-1 with the new load gn090bv.imag in the SAM21 EM.
4. Unlocks GWC-2 UNIT-1 in the SAM21 EM.
5. Waits for the inactive/upgraded GWC-2 UNIT-1 to become hot-standby.
6. Busies the upgraded GWC-2 UNIT-1 in the GWC EM.
7. Carries out a device audit against GWC-2 UNIT-1 in NPM.
8. Applies all available patches to GWC-2 UNIT-1 in NPM. (see Note on page [1501](#)).
9. Returns To Service the patched GWC-2 UNIT-1 in the GWC EM.
10. Waits for GWC-2 UNIT-1 to become hot-standby.
11. Saves the soaked GWC image to the CS 2000 Core Manager or CBM.

**Note:** The gn090bv.imag is now a soaked load which contains all applicable patches for the GN090BV load.

12. Warm swacts the GWC-2 nodes: GWC-2 UNIT-1 provides service, and GWC-2 UNIT-0 is hot-standby.
13. Locks the inactive second unit GWC-2 UNIT-0 in the SAM21 EM.
14. Provisions GWC-2 UNIT-0 with the new soaked load gn090bv.imag in the SAM21 EM.
15. Unlocks GWC-2 UNIT-0 in the SAM21 EM.
16. Waits for the inactive/upgraded GWC-2 UNIT-0 to become hot-standby.

### Example system response - non-seed nodes:

```
Group-2 started
GWC-4: Upgrade task started.
GWC-4 [1/11] Busy the hot-standby first unit. (GWC-4-UNIT-0)
GWC-4 [2/11] Lock the inactive first unit. (GWC-4-UNIT-0)
GWC-4 [3/11] Change the load of the locked first unit. (GWC-4-UNIT-0)
GWC-4 [4/11] Unlock the first unit. (GWC-4-UNIT-0)
GWC-4 [5/11] Wait for the first unit to become hot-standby. (GWC-4-UNIT-0)
GWC-4 [6/11] First unit is hot-standby, perform the warm-swact. (GWC-4-UNIT-1)
GWC-4 [7/11] Warm swact is finished, busy the second unit. (GWC-4-UNIT-1)
GWC-4 [8/11] Lock the second unit. (GWC-4-UNIT-1)
GWC-4 [9/11] Second unit is locked. (GWC-4-UNIT-1)
GWC-4 [10/11] Change the load of the locked second unit. (GWC-4-UNIT-1)
GWC-4 [11/11] Second unit is booted up with the soaked load. (GWC-4-UNIT-1)
GWC-4 Upgrade finished successfully.
Group-2 finished
Elapsed Time: 26 minutes 2 seconds
```

### Upgrade steps for the non-seed GWC nodes

This section assumes that GWC-4 is a non-seed node, GWC-4 UNIT-1 is in service, GWC-4 UNIT-0 is hot-standby, the new load file name is gn090bv.imag, and it is a soaked load which contains all applicable patches for the GN090BV load.

The GWC Upgrade Tool automatically performs the following actions in the order listed:

1. Busies the inactive unit GWC-4 UNIT-0 in the GWC EM.
2. Locks the inactive unit GWC-4 UNIT-0 in the SAM21 EM.
3. Provisions GWC-4 UNIT-0 with the newly soaked load gn090bv.imag in the SAM21 EM.
4. Unlocks GWC-4 UNIT-0 in the SAM21 EM.
5. Waits for the inactive/upgraded GWC-4 UNIT-0 to become hot-standby.
6. Warm swacts the GWC-4 nodes: GWC-4 UNIT-0 provides service, and GWC-4 UNIT-1 is hot-standby.
7. Busies the hot-standby GWC-4 UNIT-1 in the GWC EM.
8. Locks the inactive second unit GWC-4 UNIT-1 in the SAM21 EM.
9. Provisions GWC-4 UNIT-1 with the new soaked load gn090bv.imag in the SAM21 EM.
10. Unlocks GWC-4 UNIT-1 in the SAM21 EM.
11. Waits for the inactive/upgraded GWC-4 UNIT-1 to become hot-standby.

### Pause conditions

During upgrade, the system may pause, because manual actions are needed, or an operation has failed. The table below shows the various pause conditions and the user action required:

| If                                                                                                                                                                                            | Do                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| the current upgrade state is a pause point that you configured (see <a href="#">step 21</a> ) (see <a href="#">Pause point on page 1511</a> )                                                 | carry out the required manual check, then enter Continue to continue the upgrade                                                           |
| NPM requires manual actions to be taken during the patching step (see <a href="#">Patch problem on page 1512</a> )                                                                            | launch the NPM GUI or CLUI to perform the required actions, then return to the GWC Upgrade Tool and enter Continue to continue the upgrade |
| the GWC alarms (on the in-service unit) exceed the configured alarm level (see <a href="#">step 24</a> and <a href="#">step 25</a> ) (see <a href="#">Alarm level exceeded on page 1512</a> ) | refer to section <a href="#">Alarm checking on page 1479</a>                                                                               |
| an operation failed when the tool invoked the GWC EM, SAM21 EM or NPM functions (e.g. the GWC EM cannot save the GWC load image to CS 2000 Core Manager or CBM)                               | check and rectify the failed operation manually, then enter Retry to continue the upgrade                                                  |
| an operation timeout occurs (refer to the following screen), for example, the upgraded inactive unit is not hot-standby; refer to section <a href="#">Operation timeout on page 1513</a>      | carry out the timed-out operation manually, then enter Retry to continue the upgrade                                                       |

#### **Note: Query upgrade status**

While the upgrade in progress, you can launch another telnet or SSH session to the server and type the following command to query the overall status of the upgrade:

```
/opt/nortel/NTsesm/gwcuptool/bin/gwcuptool.sh -query
```

- 67** When the upgrade completes, the system reports the final service status of the upgraded GWC nodes and returns to the Upgrade Menu.

System response:

```
--{ Group-1 }-----
 GWC Node: GWC-2
 Profile: SMALL_LINENA
 Status: Upgrade finished successfully.
.
.
.
--{ Group-2 }-----
 GWC Node: GWC-4
 Profile: SMALL_LINENA
 Status: Upgrade finished successfully.
.
.
.
States from SAM21EM:
 Card status: Unlocked
 Operational state: Enabled
 Availability state: None
 Total Alarms: 0
 - Critical: 0
 - Major: 0

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x):
```

**68 Perform post-check**

In the Upgrade Menu, select the Post-check option. Enter:

> 5

Example system response:

```
Enter selection (1-5,x): 5
```

```
[5 Post-check step]
```

```
--{ Group-1 }-----
```

```
GWC-2 SMALL_LINENA ... passed
```

```
 GWC Node: GWC-2
```

```
 Profile: SMALL_LINENA
```

```
 Status: Upgrade finished successfully.
```

```
 Start time: Mon Dec 13 05:36:12 EST 2004
```

```
 Stop time: Mon Dec 13 05:52:36 EST 2004
```

```
 Elapsed time: 16 minutes 23 seconds
```

```
GWC-2-UNIT-1: 47.142.128.51
```

```
 States from GWCEM:
```

```
 Current load name: GN090BV
```

```
 Administrative state: unlocked(1)
```

```
 Operational state: enabled(1)
```

```
 Standby state: providingService(3)
```

```
 Fault state: none(0)
```

```
 Alarm state: 00 00 00 00
```

```
 - Critical: 0
```

```
 - Major: 0
```

```
 States from SAM21EM:
```

```
 Card status: Unlocked
```

```
 Operational state: Enabled
```

```
 Availability state: None
```

```
 Total Alarms: 0
```

```
 - Critical: 0
```

```
 - Major: 0
```

```
GWC-2-UNIT-0: 47.142.128.50
```

```
 States from GWCEM:
```

```
 Current load name: GN090BV
```

```
 Administrative state: unlocked(1)
```

```
 Operational state: enabled(1)
```

```
 Standby state: hotStandby(1)
```

```
 Fault state: none(0)
```

```
 Alarm state: 00 00 00 00
```

```
 - Critical: 0
```

```
 - Major: 0
```

```
 States from SAM21EM:
```

```
 Card status: Unlocked
```

```
 Operational state: Enabled
```

```
 Availability state: None
```

```
 Total Alarms: 0
```

```
 - Critical: 0
```

```
 - Major: 0
```

```
--{ Group-2 }-----
```

```
 GWC Node: GWC-4...
```

The screen display repeats the service status of the upgraded GWC nodes. The post-check checks the status of all the upgraded nodes, to ensure that:

- there is no alarm for the in-service GWC unit
- one unit is in service, and the other unit is hot-standby

## 69 Exit GWC Upgrade Tool

When the post-check finishes, exit the Upgrade Menu and return to the Main Menu. Enter:

> **x**

System response:

```
Enter selection (1-5,x): x
```

```
Main Menu for GWC upgrade tool
```

```
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu
```

```
x - Stop upgrade tool and exit CLUI
```

```
Enter selection (1-4,x):
```

## 70 Use the following table to determine your next step.

| If                                       | Do                                  |
|------------------------------------------|-------------------------------------|
| you want to upgrade further GWC nodes    | go back to <a href="#">step 9</a>   |
| all the required GWCs have been upgraded | continue at <a href="#">step 71</a> |



## 71

**CAUTION**

Do not exit the GWC Upgrade Tool before the upgrade successfully completes. Do not press Ctrl+C or close the TERM. If you do so and then start the GWC Upgrade Tool again, the system displays the message:

```
Warning!!! One Upgrade Manager is
running already. It is not recommended
to start a new server. Start a new one
to override it? (Default N) Y/N):
```

After the upgrade completes, stop the GWC Upgrade Tool and exit the CLUI. Enter:

> x

Example system response:

```
Enter selection (1-4,x): x
GWC Upgrade Manager server stopped.
comp5iems-unit0(active):/export/home/ptm>
```

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

## Example screens

### GWC load not available

If the GWC load is not available, the Prepare step fails. You must verify that the GWC load file is installed correctly, then return to the Configuration step to re-input the file name. Refer to the following figure for assistance.

```
Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x): 2

GWC upgrade configuration

[Step 1 - LOAD FILE NAME]
Enter the new load file name (Example: gn070bv.imag): gn090bv.imag
.
.
.

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x): 1

GWC load file doesn't exist.
Available GWC loads in the given directory in SDM/CBM:
- GwcConfig.sh
- gn080bf.imag
- gn080bf_jg.imag
- gn080bg1.imag
```

### Pre-check failure

There are several conditions which may cause the Pre-check step to fail, for example, servers not running, GWC cards with incorrect status. You must correct the problem, then repeat the Pre-check step. Refer to the following figure for assistance.

Upgrade Menu for GWC upgrade tool

- 1 - Prepare
- 2 - Pre-check
- 3 - Upgrade
- 4 - Query upgrade status
- 5 - Post-check

x - exit

Enter selection (1-5,x): 2

```
--{ Group-1 }-----
GWC-10 LARGE_LINENA ... failed
 GWC Node: GWC-10
 Profile: LARGE_LINENA
 Status: Auto discovery in progress.
 Estimated time: 41 minutes 15 seconds
 Paused: Invalid GWC status, unable to perform the upgrade.
GWC-10-UNIT-0: 47.142.128.158
States from GWCEM:
 Current load name: GN080BF
Administrative state: locked(2)
 Operational state: disabled(2)
 Standby state: coldStandby(2)
 Fault state: none(0)
 Alarm state: minor(3) , alarmOutstanding(4)
 - Critical: 0
 - Major: 0
States from SAM21EM:
 Card status: Unlocked
 Operational state: Enabled
 Availability state: None
 Total Alarms: 0
 - Critical: 0
 - Major: 0
GWC-10-UNIT-1: 47.142.128.159
States from GWCEM:
 Current load name: GN080BF
Administrative state: unlocked(1)
 Operational state: enabled(1)
 Standby state: providingService(3)
 Fault state: none(0)
 Alarm state: major(2) , alarmOutstanding(4)
 - Critical: 0
 - Major: 1
 1, Communication with a gateway is down. (MG10/00/5)
States from SAM21EM:
 Card status: Unlocked
 Operational state: Enabled
 Availability state: None
 Total Alarms: 0
 - Critical: 0
 - Major: 0
```

## Pause point

Pause points occur during the upgrade process wherever you specified them in the Configuration step. You must carry out the required manual checks, then enter Continue to allow the upgrade process to continue. Refer to the following figure for assistance.

[Step 8 - PAUSE POINTS]

Values:

0 - no pause points.

(1) For the first GWC node within the same GWC group.

1 - before lock first upgrade unit of "seed" node.

2 - after patch applied to "seed" unit.

3 - before warm-swact.

4 - after warm-swact.

5 - after "seed" node upgraded.

(2) For bulk upgrade GWC nodes with same GWC service type.

6 - before warm-swact.

Separate numbers with comma, for example: 1,3,4

Enter the pause points (Default: 0):1,2,3,4,5

[Step 9 - LOGGING LEVEL]

.

.

.

Group-1 started

Upgrade task started

GWC-10 [1/16] Busy the hot-standby first unit. (GWC-10-UNIT-1)

GWC-10 [2/16] Lock the inactive first unit. (GWC-10-UNIT-1)

Message received from the server:

GWC-10 CHECK-POINT: before lock the first upgrade unit.

Please select from following:

Continue

Answer: continue

GWC-10 [3/16] Change the load of the locked first unit. (GWC-10-UNIT-1)

GWC-10 [4/16] Unlock the first unit. (GWC-10-UNIT-1)

GWC-10 [5/16] Wait for the first unit to become hot-standby. (GWC-10-UNIT-1)

GWC-10 [6/16] Upgraded first unit is hot-standby. (GWC-10-UNIT-1)

GWC-10 [7/16] Apply patch to the upgraded first unit. (GWC-10-UNIT-1)

Apply request was attempted by the NPM server.

GWC-10 [8/16] Patches are applied to the upgraded first unit. (GWC-10-UNIT-1)

Message received from the server:

GWC-10 CHECK-POINT: patches are applied for the "seed" unit.

Please select from following:

Continue

Answer: Continue

GWC-10 [9/16] Wait for the patched unit to become hot-standby (GWC-10-UNIT-1)

### Patch problem

To ignore the error and allow the upgrade process to continue, you can simply enter Continue. If some manual action is needed (for example, launching the NPM CLUI/GUI), carry out the required action, then enter Continue. To invoke the NPM to attempt to apply the patch again, enter Retry. To abort the upgrade for the current GWC node, enter Abort. Refer to the following figure for assistance.

```
Group-1 started
GWC-2: Upgrade task started.
GWC-2 [1/16] Busy the hot-standby first unit. (GWC-2-UNIT-1)
GWC-2 [2/16] Lock the inactive first unit. (GWC-2-UNIT-1)
GWC-2 [3/16] Change the load of the locked first unit. (GWC-2-UNIT-1)
GWC-2 [4/16] Unlock the first unit. (GWC-2-UNIT-1)
GWC-2 [5/16] Wait for the first unit to become hot-standby. (GWC-2-UNIT-1)
GWC-2 [6/16] Upgraded first unit is hot-standby. (GWC-2-UNIT-1)
GWC-2 [7/16] Apply patch to the upgraded first unit. (GWC-2-UNIT-1)
Patch NBF01G09 requires special attention:
 Ftp Error command
Patch NBF02G09 requires special attention:
 ERROR: Patch NBF01G09 needs to be applied in GWC-2-UNIT-1 before NBF02G09 can be
 applied.
Patch NBF03G09 requires special attention:
 ERROR: Patch NBF01G09 needs to be applied in GWC-2-UNIT-1 before NBF03G09 can be
 applied.
.
.
.
Message received from the server:

GWC-2 Warning: NPM can't apply all patches to GWC unit. GWC-2-UNIT-1
Please select from following:
Continue Retry Abort

Answer: retry
GWC-2 [7/16] Apply patch to the upgraded first unit. (GWC-2-UNIT-1)
Apply request was attempted by the NPM server.
GWC-2 [8/16] Patches are applied to the upgraded first unit. (GWC-2-UNIT-1)
GWC-2 [9/16] Wait for the patched unit to become hot-standby (GWC-2-UNIT-1)
GWC-2 [10/16] Patched unit is hot-standby, load imaging starts. (GWC-2-UNIT-1)
```

### Alarm level exceeded

If the actual GWC alarms reach the alarm level defined in the Configuration step, the upgrade pauses. To ignore the alarms and allow the upgrade process to continue, you can simply enter Continue. Otherwise you must enter Abort to stop the upgrade, and correct the problem before continuing. Refer to the following figure for assistance.

```
Group-1 started
Upgrade task started
GWC-10 [1/16] Busy the hot-standby first unit. (GWC-10-UNIT-1)
 GWC-10-UNIT-0: 47.142.128.158
 States from GWCEM:
 Current load name: GN080BE
 Administrative state: unlocked(1)
 Operational state: enabled(1)
 Standby state: providingService(3)
 Fault state: none(0)
 Alarm state: major(2) , alarmOutstanding(4)
 - Critical: 0
 - Major: 1
 1, Communication with a gateway is down. (MG10/00/5)
 States from SAM21EM:
 Card status: Unlocked
 Operational state: Enabled
 Availability state: None
 Total Alarms: 0
 - Critical: 0
 - Major: 0

Message received from the server:

GWC-10 In service unit has more alarms in GWCEM than configured. GWC-10-UNIT-0
Please select from following:
Continue Abort

Answer: Continue
GWC-10 Ignore the alarm states, and continue the upgrade task
```

### Operation timeout

If an operation timeout occurs, the upgrade does not necessarily fail. You can use the CS 2000 Management Tools client and SAM21 Manager client to check the status of the GWC card. After performing the timed-out operation manually (for example, locking the GWC card), you can enter Retry to allow the upgrade process to continue. Refer to the following figure for assistance.

```
Group-1 started
GWC-10: Upgrade task started.
GWC-10 [1/16] Busy the hot-standby first unit. (GWC-10-UNIT-0)
GWC-10 [2/16] Lock the inactive first unit. (GWC-10-UNIT-0)

Message received from the server:

GWC-10 Timeout: SAM21EM can't lock the inactive GWC unit. GWC-10-UNIT-0
Please select from following:
Retry Abort

Answer: retry
GWC-10 [3/16] Change the load of locked first unit. (GWC-10-UNIT-0)
```

## GWC provisioning on MCS

### Purpose of this procedure

This procedure modifies the GWC tab in MCS 5200 Provisioning Manager to indicate the correct MCS discriminator file. This action is necessary to ensure successful MCS-CS 2000 interworking.

### When to use this procedure

Use this procedure after completion of a GWC load upgrade in a CS 2000 environment.

### Prerequisites

This procedure has no prerequisites.

### Action

#### *At the MCS 5200 Provisioning Manager*

- 1 Select the Provisioning client.
- 2 Select Service Nodes.
- 3 Select List Node.
- 4 Select the Node Name for the required GWC.
- 5 Select the Node Type drop-down menu.

*Example system response:*

The screenshot shows the 'Modify Node' page in the Nortel Networks Provisioning Manager. The interface has a blue header with the Nortel Networks logo and 'Unified Network' text. Below the header is a navigation bar with 'HOME' and 'HELP' links. A sidebar on the left contains a tree view with categories like Provisioning, Admins, Domains, Devices, Service Nodes, IPCM Clusters, Voice Mail, Services, Media Portal, Applications, and System. The main content area is titled 'Modify Node' and contains several fields: 'Node Name' (text box with 'co11ngss'), 'Node Address' (radio buttons for 'External Domain' and 'Address Name', with 'Address Name' selected and a dropdown showing 'NGSSGWC011'), 'Node Type' (dropdown menu showing 'CS2K SN09 NGSS' selected), 'Location' (text box with 'CS2K SN08 VRDN'), 'Is Trusted' (text box with 'CS 1000'), 'Behind 1-to-1 NAT' (text box with 'UAS PRI'), and 'Enhanced IM' (text box with 'CS2K SN09 VRDN').



- 6** Refer to the following table to determine your next action.

| <b>If you just completed a</b> | <b>Do</b>                          |
|--------------------------------|------------------------------------|
| Session Server GWC upgrade     | select Node Type<br>CS2K SN09 NGSS |
| VRDN GWC upgrade               | select Node Type<br>CS2K SN09 VRDN |

- 7** Select Update.
- 8** Repeat [step 4](#) to [step 7](#) of this procedure for each MCS gateway whose gateway host points to this CS 2000.
- 9** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## GWC IPS7 provisioning

---

Use this procedure to provision Gateway Controllers (GWC) that handle ISUP traffic as an Application Server (AS) using the USP GUI. Once the GWC has been provisioned as an AS, two IP paths must be set up from the USP to the GWC. Each IP path is set up to a different IPS7 card on the USP. All IP paths between the USP and the GWC are set up to the active GWC. If 4 IPS7 cards are provisioned on the USP, engineering rules determine how the IP paths should be set up to the IPS7 cards based on call capacity.

### Provision GWC IPS7

#### *At the USP GUI*

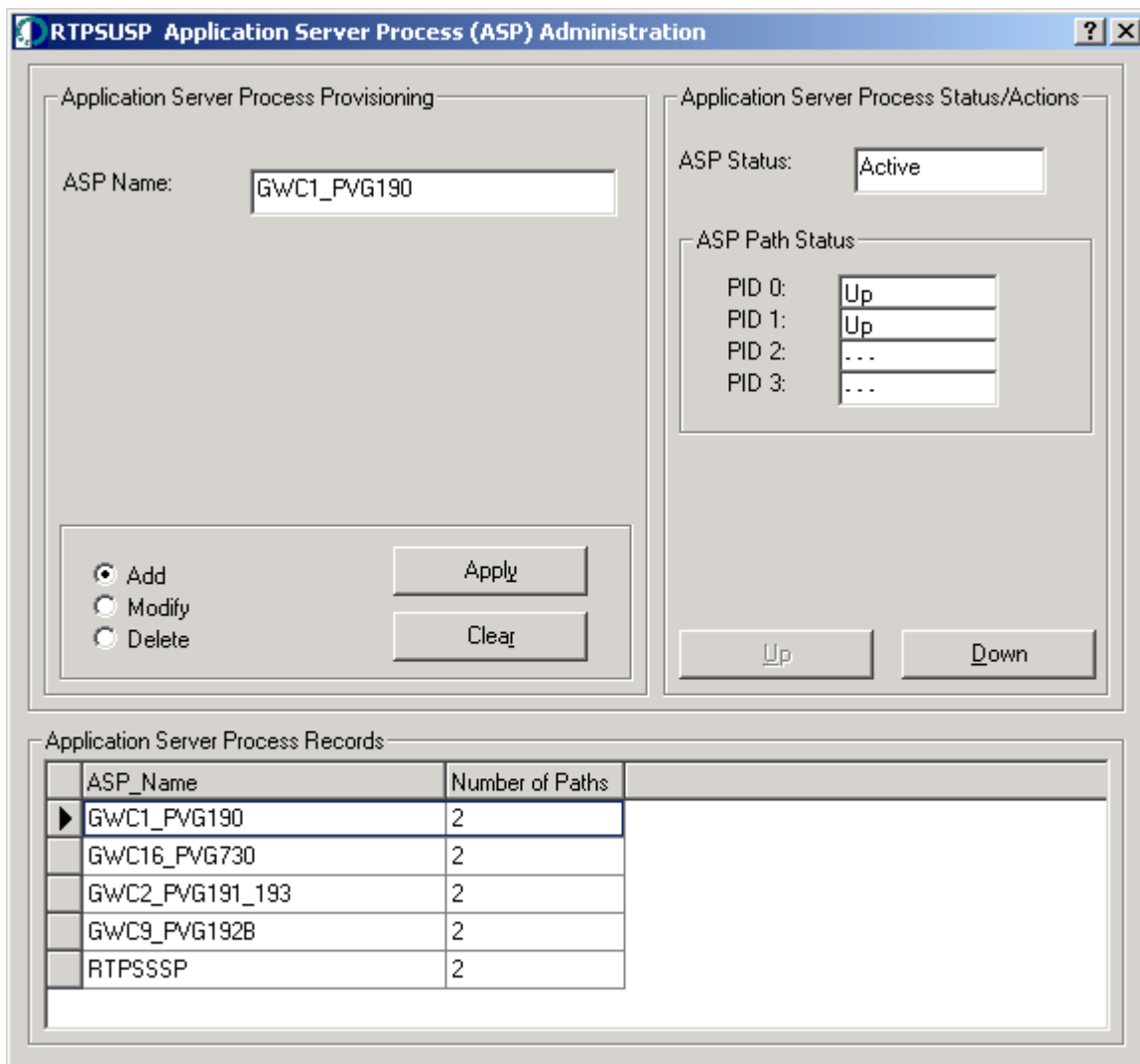
- 1 From the main **USP** menu, click **Network Management**.
- 2 From the **Network Management** window, click **IPS7**.
- 3 In the **IPS7** window, click **ASP**.

- 4 Enter the **ASP Name (GWC)** and click **Apply** and click **OK** to confirm the addition of the ASP and close the **ASP** window.

*The new ASP is listed in the Application Server Process Records window.*

*ASP status reads inactive.*

*No IP paths will be assigned at this stage.*



The screenshot shows the 'RTPSUSP Application Server Process (ASP) Administration' window. It is divided into three main sections. The top-left section, 'Application Server Process Provisioning', contains an 'ASP Name' field with the value 'GWC1\_PVG190'. Below this are three radio buttons: 'Add' (selected), 'Modify', and 'Delete'. To the right of these are 'Apply' and 'Clear' buttons. The top-right section, 'Application Server Process Status/Actions', shows 'ASP Status' as 'Active'. Below this is the 'ASP Path Status' section, which lists four PIDs: PID 0 (Up), PID 1 (Up), PID 2 (...), and PID 3 (...). At the bottom of this section are 'Up' and 'Down' buttons. The bottom section, 'Application Server Process Records', contains a table with two columns: 'ASP\_Name' and 'Number of Paths'.

| ASP_Name        | Number of Paths |
|-----------------|-----------------|
| GWC1_PVG190     | 2               |
| GWC16_PVG730    | 2               |
| GWC2_PVG191_193 | 2               |
| GWC9_PVG192B    | 2               |
| RTPSSSP         | 2               |

- 5 Click **AS** in the **IPS7** window and do the following:
  - a enter the name of the AS in the **Application Server Provisioning** window and
  - b select the corresponding **ASP Name** as the **Primary Process** and click **Apply** and close the **AS** window.
- 6 In the **IPS7** window, click **ASP Paths** and do the following:
  - a Select the **ASP Name**, **Path ID** (enter "0"), **Shelf Name** (USP shelf name) and **System Node Name** (IPS7 card) for the first IP path in the **Application Server Process Path Provisioning** window.
  - b Select **M3UAv2/SCTPv5\_Client** as the Transport Protocol. The **SCTP Parm Index** = 0.
  - c Enter the IP Address of the **Application Server (GWC)** and its associated Remote Port for the IP path. The remote port is **(2905)**.

**Note:** Enter the active ip address of the Application Server (GWC).
  - d Click **Apply** to add the IP Path.

- 7 In the **Application Server Process Path Records** window, do the following:
- Highlight the path and under **Path Actions** click **Up** to activate the IP path.
  - Repeat [step 6](#), adding an entry for the second path. Increment the path id to '1'.

*The following is an example of the **Application Server Process Path Records**.*

**Application Server Process Path (Path) Administration**

**Application Server Process Path Provisioning**

ASP Name:

Path ID:

Shelf Name:

System Node Name:

Transport Protocol:

Sctp Params Index:

IP Address:  Local Port:  Remote Port:

☒ Add ☐ Modify ☐ Delete

**Path Status**

Path State:

**Path Actions**

**Application Server Process Path Records**

| ASP Name        | PID | Shelf Name | Slot Name      | IP Address   |
|-----------------|-----|------------|----------------|--------------|
| GWC1_PVG190     | 1   | RTPSUSP1   | IP_LINK_NOD... | 172.17.40.28 |
| GWC1_PVG190     | 0   | RTPSUSP1   | IP_LINK_NOD... | 172.17.40.28 |
| GWC16_PVG730    | 1   | RTPSUSP1   | IP_LINK_NOD... | 172.17.40.96 |
| GWC16_PVG730    | 0   | RTPSUSP1   | IP_LINK_NOD... | 172.17.40.96 |
| GWC2_PVG191_193 | 1   | RTPSUSP1   | IP_LINK_NOD... | 172.17.40.32 |
| GWC2_PVG191_193 | 0   | RTPSUSP1   | IP_LINK_NOD... | 172.17.40.32 |

- 8** Close the windows as follows:
  - a** Click **Close** to apply the changes and close the **ASP Paths** window.
  - b** Close the **IPS7 Paths** window.
  - c** Close the **Network Management** window.
- 9** Repeat this procedure for each GWC. Each GWC handling ISUP traffic must be set up as an AS and have two IP paths assigned.

---

## Confirming Gateway Controller loads after an upgrade

---

Use this procedure to confirm each Gateway Controller has the correct software load after an upgrade. Repeat this procedure for each Gateway Controller with upgraded software.

### Prerequisites

Perform this procedure after you complete the upgrade of software on a Gateway Controller.

### Action

#### Confirming SAM21 Shelf Controller loads after an upgrade

##### *From the Application Launch Point*

- 1 Launch the CS 2000 Management Tools application. If prompted, enter your Login Name and Password.  
*Response*  
*The main CS 2000 Management Tools window appears.*
- 2 Under Device Types, select Gateway Controller.  
*Response*  
*Network-level information on Gateway Controllers appears.*
- 3 Under Gateway Controllers, select an upgraded Gateway Controller.  
*Response*  
*The Maintenance tab for the selected Gateway Controller appears.*
- 4 Check the value in Loadname for each unit. Make sure the load name identifies the new load for the upgraded Gateway Controller.

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

---

| <b>If the load names for both units</b> | <b>Do</b>                                                                                     |
|-----------------------------------------|-----------------------------------------------------------------------------------------------|
| identify the new load                   | <a href="#">step 6</a>                                                                        |
| anything else                           | Troubleshoot the problem or contact your next level of support. The upgrade was unsuccessful. |

---

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

---

| <b>If you</b>                                       | <b>Do</b>              |
|-----------------------------------------------------|------------------------|
| need to check additional Gateway Controllers        | <a href="#">step 3</a> |
| completed checking all upgraded Gateway Controllers | <a href="#">step 8</a> |

---

- 7 Exit the CS 2000 Management Tools application.

- 8 You have completed this procedure



---

## Rolling back a software upgrade on a standby GWC node

---

### Purpose of this procedure

This procedure describes how to roll back a software upgrade and revert to a previous software load.



#### CAUTION

Downgrades are only supported as part of backing out of the upgrade of an individual GWC type. Call survivability, as specified in this document, is not supported for downgrades once further non-GWC network components have been upgraded or further GWC types have been upgraded. This is especially problematic if the call server or gateways have already been upgraded. Call survivability support during downgrades is limited only to backing out of all instances of the last GWC card type that was being upgraded.

### Restrictions and Limitations

The following restricts apply to using this procedure:

Rollbacks can occur only on a standby GWC card.



#### CAUTION

No provisioning activity can occur on the system while the GWC software downgrade is in progress.



#### CAUTION

Active calls on the GWC node affected may be dropped during a software rollback. Ensure that all steps in this procedure are followed to minimize the risk of calls being dropped.

### Prerequisites

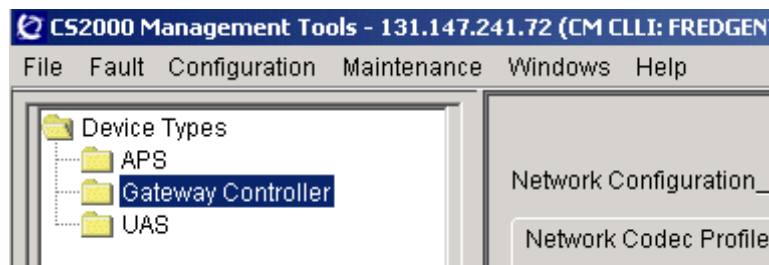
The following prerequisites apply to this procedure:

A GWC software load file from a previous release or a backup image file must be available on the CS 2000 Core Manager or Core and Billing Manager (CBM).

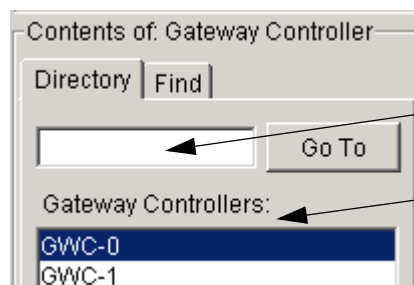
## Action

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

- 1 At the CS 2000 Management Tools window, click on the Gateway Controller folder from the Device Types directory tree in the far left frame.



- 2 From the Contents of: Gateway Controller frame, select the appropriate GWC node you wish to roll back.



Type a GWC node number here  
or  
Select a GWC node from the list  
of provisioned GWC nodes.

- 3 Rollbacks can only occur on a standby GWC card. Select the Maintenance tab and locate the standby card. Busy the standby GWC card by clicking the Busy (Disable) button and confirm this action at the prompt.

GWC-6 Unit 0: 47.104.41.54  
Unit 1: 47.104.41.55

**Maintenance** Provisioning

GWC-6-UNIT-0

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

Save Image Busy (Disable) RTS (Enable) Card View

GWC-6-UNIT-1

|                       |                |                 |                                |
|-----------------------|----------------|-----------------|--------------------------------|
| Administrative state: | unlocked(1)    | Usage state:    | idle(1)                        |
| Operational state:    | enabled(1)     | Stand by state: | coldStandby(2)                 |
| Activity state:       | standby(2)     | Swact state:    | noSwAct(0)                     |
| Isolation state:      | notisolated(2) | Alarm state:    | minor(3) , alarmOutstanding(4) |
| Available state:      | degraded(6)    | Fault state:    | none(0)                        |
| Loadname:             | GI070BN        |                 |                                |

Save Image **Busy (Disable)** RTS (Enable) Card View

☐ Force Warm Swact Cold Swact

- 4 When the Operational state of the standby card is disabled, click the Card View button to access the card view. This action opens the CS 2000 SAM21 Manager.

GWC-6-UNIT-1

|                       |                |                 |                                |
|-----------------------|----------------|-----------------|--------------------------------|
| Administrative state: | locked(2)      | Usage state:    | idle(1)                        |
| Operational state:    | disabled(2)    | Stand by state: | coldStandby(2)                 |
| Activity state:       | standby(2)     | Swact state:    | noSwAct(0)                     |
| Isolation state:      | notIsolated(2) | Alarm state:    | minor(3) , alarmOutstanding(4) |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)                        |
| Loadname:             | GI070BN        |                 |                                |

Save Image Busy (Disable) RTS (Enable) Card View

**At the CS 2000 SAM21 Manager client**

- 5 Select the States tab in the card view.

File View

**Sam21-2 : Slot 12**

Alarms | Equip | **States** | Diags | Provisioning

Summary

| Critical | Major | Minor |
|----------|-------|-------|
| 0        | 0     | 0     |

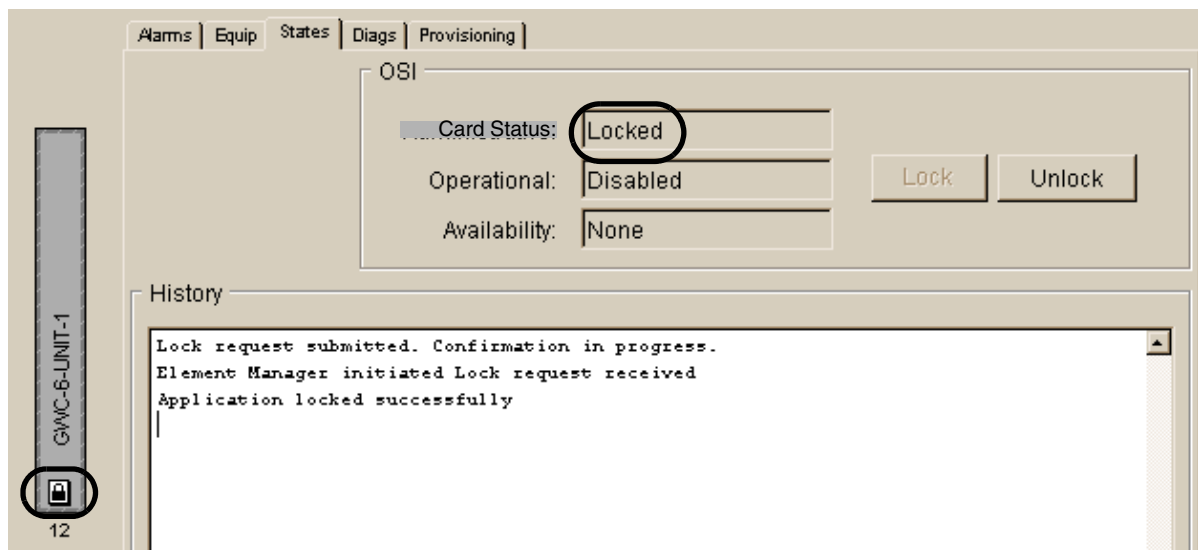
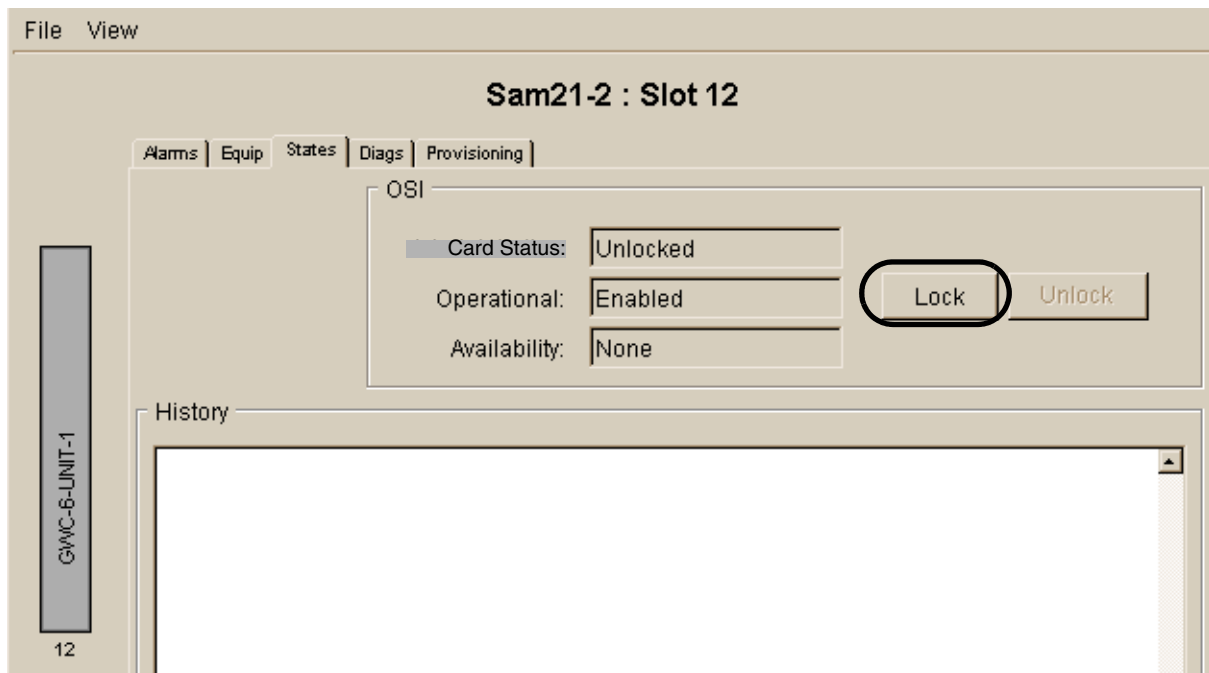
Details

| Equip. | ID | Time | Type | Severity | Reason |
|--------|----|------|------|----------|--------|
|        |    |      |      |          |        |

GWC-6-UNIT-1

12

- 6 Click the Lock button to lock the card. Wait for the message in the History window indicating that the card is locked. Also, notice the lock icon on the card graphic at the left of the screen and the Card Status Locked.



## 7 Select the Provisioning tab in the card view.

File View

**Sam21-2 : Slot 12**

Alarms Equip States Diags **Provisioning**

**General**

IP: 47.104.41.55 Gateway IP: 47.104.41.1

Subnet Mask: 255.255.255.128 FW Version: RM05

MAC Address: 0001AF07A6A0 GWC Number: 6

**NTP**

Primary NTP: 172.25.15.1

Secondary NTP: 172.25.15.1

**GWC-EM**

Host IP: 47.104.41.4

Port: 162

**Load Info**

Server IP: 47.104.41.3

Path: /swd/gwc

Load: gi070bn.imag

☐ FW Flash Enable

**Domain Servers**

Primary: 0.0.0.0 1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

**Modify** Save Clear Cancel Details...

- 8 Click the Modify button to make changes to the provisioning datafill.
- 9 Click the Get Load Files button and select the load to which you want to revert from the drop-down list .

- 10 Click the Save button.

**Note:** Leave the FW (firmware) Flash Enable checkbox unselected.



### CAUTION

For CS 2000 Core Manager the Path: field must be set to /swd/gwc; For CBM the Path: field must be set to /gwc.

Other processes are tied to this directory. For example, the GWC load delivery software places the load in the /swd/gwc directory. Also, GWC auto-imaging is a network file system (NFS) mount of the /swd/gwc directory.

Subnet Mask: 255.255.255.128      FW Version: RM04  
MAC Address: 0001AF07A6A0      GWC Number: 6

NTP  
Primary NTP: 172.25.15.1  
Secondary NTP: 172.25.15.1

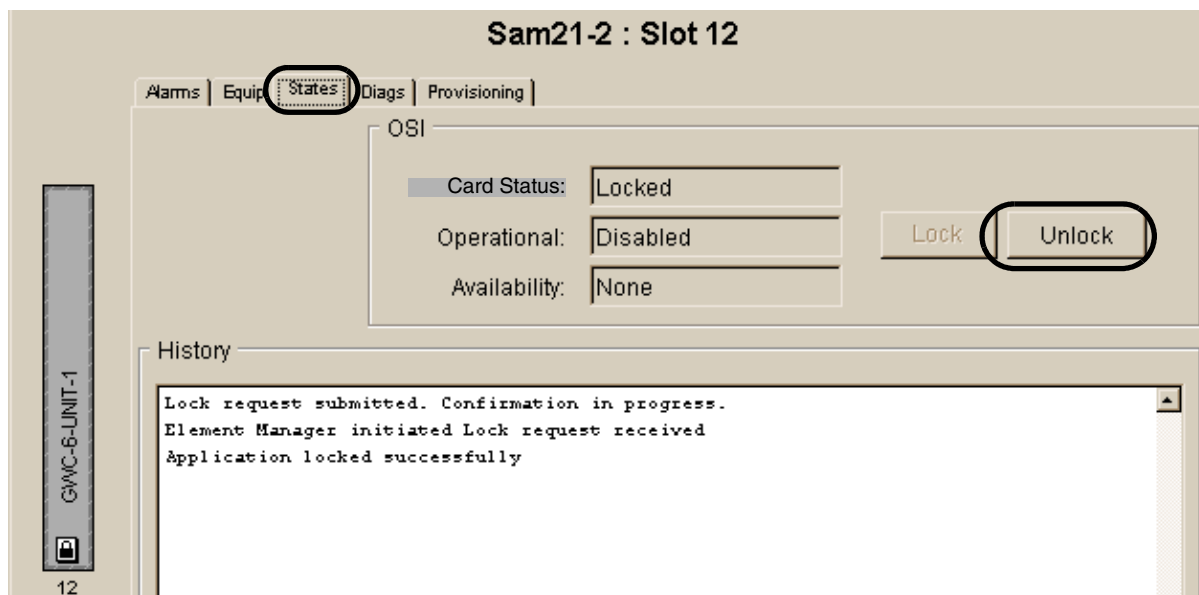
GWC-EM  
Host IP: 47.104.41.4  
Port: 162

Load Info  
Server IP: 47.104.41.3  
Path: /swd/gwc  
Load: gi070bn.imag      Get Load Files  
☐ FW Flash Enable

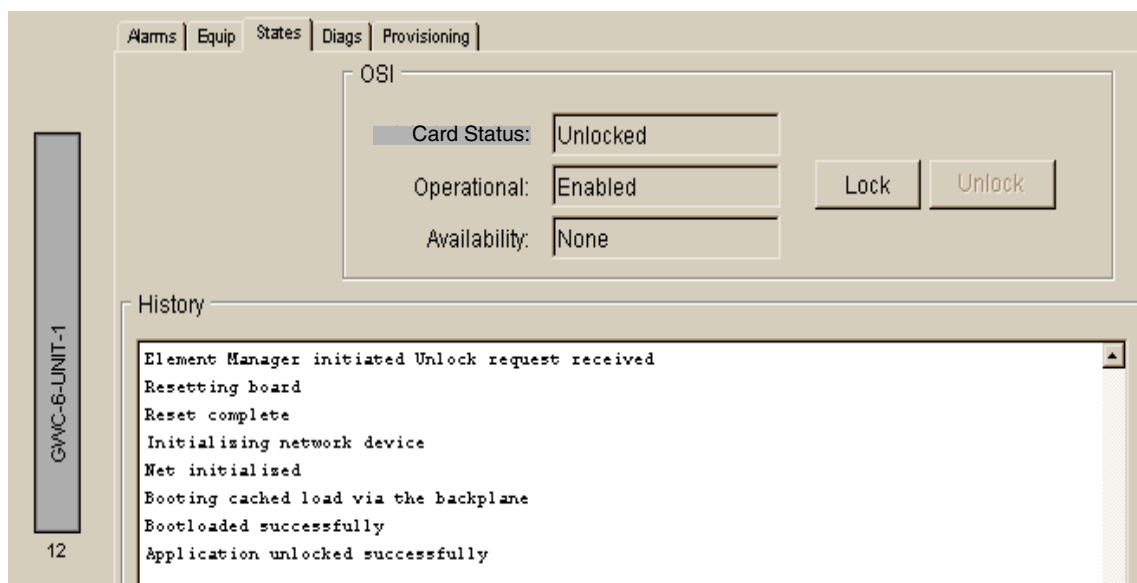
Domain Servers  
Primary: 0.0.0.0      1st Alt: 0.0.0.0  
2nd Alt: 0.0.0.0

Modify      **Save**      Clear      Cancel      Details...

- 11 Select the States tab in the card view.



- 12 Click the Unlock button to load the software you selected previously. Observe the History window display to confirm the the software reload was successful.





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

| If                                                                                                                                                                                                                                                                                | Do                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| you are downgrading the first card in the seed GWC node, and there are patches that must be applied to the earlier software load. (If the image file of the earlier software load already contains the required patches. The following steps to patch the load are not required.) | go to <a href="#">step 14</a> |
| otherwise                                                                                                                                                                                                                                                                         | go to <a href="#">step 16</a> |

- 14** If necessary, patch the seed GWC unit by completing the tasks listed in the following table.

All necessary procedures, as well as the patching checklist and additional patching information, are available in the “Carrier Voice over IP Network patching” section of *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450.

| Task                                             | Procedure                                                                                                                    |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Audit the GWC unit for necessary patch activity. | “Performing a device audit using the NPM” in <i>Nortel Carrier Voice over IP Network Upgrades and Patches</i> , NN10440-450. |
| If you wish, define reports for a GWC.           | “Defining reports using the NPM” in <i>Nortel Carrier Voice over IP Network Upgrades and Patches</i> , NN10440-450.          |
| Apply patches to the standby GWC unit.           | “Applying patches using the NPM” in <i>Nortel Carrier Voice over IP Network Upgrades and Patches</i> , NN10440-450.          |
| Activate the applicable patches.                 | “Activating patches using the NPM” in <i>Nortel Carrier Voice over IP Network Upgrades and Patches</i> , NN10440-450.        |

| Task                                          | Procedure                                                                                                               |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| If required, deactivate any obsolete patches. | “Deactivating patches using the NPM” in <i>Nortel Carrier Voice over IP Network Upgrades and Patches</i> , NN10440-450. |
| If required, remove any obsolete patches.     | “Removing patches using the NPM” in <i>Nortel Carrier Voice over IP Network Upgrades and Patches</i> , NN10440-450.     |

- 15 Take an image of the standby GWC unit. Follow procedure [Take a manual GWC software image on page 1536](#).

**At the CS 2000 GWC Manager client**

- 16 Observe the Standby state field on the inactive GWC card in the Maintenance panel. Wait for the Standby state to transition from coldStandby to hotStandby.

- 17** Apply a warm swact (switch of active cards) by clicking the Warm Swact button at the bottom of the screen.

GWC-6      Unit 0: 47.104.41.54  
Unit 1: 47.104.41.55

Maintenance | Provisioning

GWC-6-UNIT-0

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

Save Image    Busy (Disable)    RTS (Enable)    Card View

GWC-6-UNIT-1

|                       |                |                 |               |
|-----------------------|----------------|-----------------|---------------|
| Administrative state: | unlocked(1)    | Usage state:    | idle(1)       |
| Operational state:    | enabled(1)     | Stand by state: | hotStandby(1) |
| Activity state:       | standby(2)     | Swact state:    | noSwAct(0)    |
| Isolation state:      | notIsolated(2) | Alarm state:    | 00 00 00 00   |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)       |
| Loadname:             | PGC09AV        |                 |               |

Save Image    Busy (Disable)    RTS (Enable)    Card View

☐ Force    **Warm Swact**    Cold Swact

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

| If                                                                                                                             | Do                                                       |
|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| you need to downgrade the mate GWC card (now the new standby GWC card) in the same node                                        | go to <a href="#">step 3</a> and complete this procedure |
| you need to downgrade cards in another GWC node                                                                                | go to <a href="#">step 2</a> and complete this procedure |
| all cards in all GWC nodes have been downgraded (You only need to perform this procedure once for each card in each GWC node.) | go to <a href="#">step 20</a>                            |

- 19** Return to [step 2](#), and repeat this procedure for each GWC node until all units in each node are rebooted from the new image, otherwise continue to the next step.
- 20** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Take a manual GWC software image

---

### Purpose of this procedure

This procedure describes how to save a software image to the CS 2000 Core Manager or Core and Billing Manager (CBM).

A procedure also exists to enable the auto-imaging of a GWC software load once daily.

### When to use this procedure

Use this procedure as a part of upgrading GWC software for an office or as a part of maintenance activity.

Take an image after all patches have been applied to GWC software. Refer to your site operating procedures for information about soak time and how many patches to apply before taking an image. In the absence of this information, Nortel Networks recommends taking an image immediately after applying R or P status patches.



#### CAUTION

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

### Prerequisites

This procedure has no prerequisites.

### Action

#### *At the CS 2000 Core Manager or CBM console*

- 1 Log in to the CS 2000 Core Manager or CBM as the root user.
- 2 Change directory to the GWC software directory.

##### **Example**

```
cd /swd/gwc
```

- 3 Copy the existing GWC software load file to a backup.

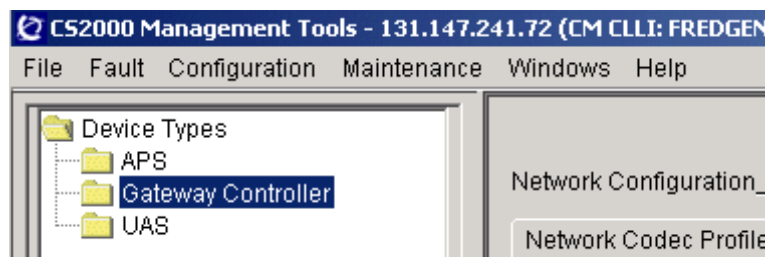
##### **Example**

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

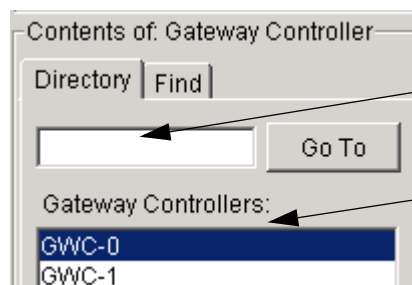
**Note:** You can use any name for the backup file name.

**At the CS 2000 GWC Manager client**

- 4 At the CS 2000 Management Tools window, click on the Gateway Controller folder from the Device Types directory tree in the far left frame.



- 5 From the Contents of: Gateway Controller frame, select the appropriate GWC node from which you want to take an image.



Type a GWC node number here,  
or

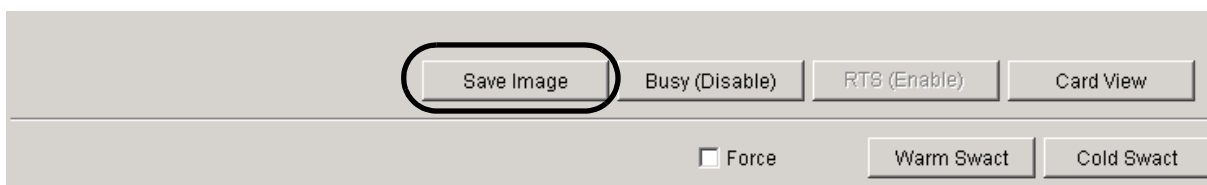
Select a GWC node from the list  
of provisioned GWC nodes.

- 6 Select the Maintenance tab to view the Maintenance panel.
- 7 In the Maintenance panel, identify the GWC card in the node that has an upgraded load already installed. Click the Save Image button for that card to save the software image back to the CS 2000 Core Manager or CBM.

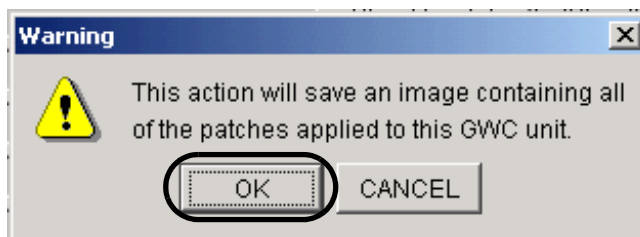
The Save Image command overwrites the existing GWC software load file on the CS 2000 Core Manager or CBM.

**CAUTION**

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



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



**ATTENTION**

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

- 9 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure. To return to the Overall GWC downgrade procedure, refer to [Rolling back a software upgrade on a standby GWC node on page 1524](#).

## Troubleshooting

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

### ***At the CS 2000 Core Manager or CBM console***

- 1 Log in to the CS 2000 Core Manager or CBM as the root user.
- 2 Change directory to the /swd directory by typing  
**# cd /swd**  
and pressing the Enter key.
- 3 Change the permissions for the gwc directory and its file contents by typing  
**# chmod 777 gwc/\***  
and pressing the Enter key.
- 4 Log out of the CS 2000 Core Manager or CBM.
- 5 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## MS 2000 Series upgrade

The Media Server 2000 Series upgrade procedure enables you to apply a maintenance release or patch to a Media Server 2000 Series 2010 or 2020 node.

### New in this release

#### Feature changes

There are no feature changes in the MS 2000 Series upgrade.

#### **ATTENTION**

The MS 2000 Series does not have a new software load for SN09U. Therefore, no upgrade from release SN09 to SN09U is required.

### Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U



## Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade

### Time to complete an upgrade

The following table lists the tasks to upgrade MS 2000 Series node software and the estimated time to complete each task.

**Table 1 Estimated time to complete a software upgrade**

| Task                         | Time              |
|------------------------------|-------------------|
| Preparing for the upgrade    | 30 minutes        |
| Upgrading the software       | 40 minutes        |
| Completing the upgrade       | 10 minutes        |
| Total estimated upgrade time | 1 hour 20 minutes |
| Performing a rollback        | 20 minutes        |

## System Performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade.

## System limitations during upgrade

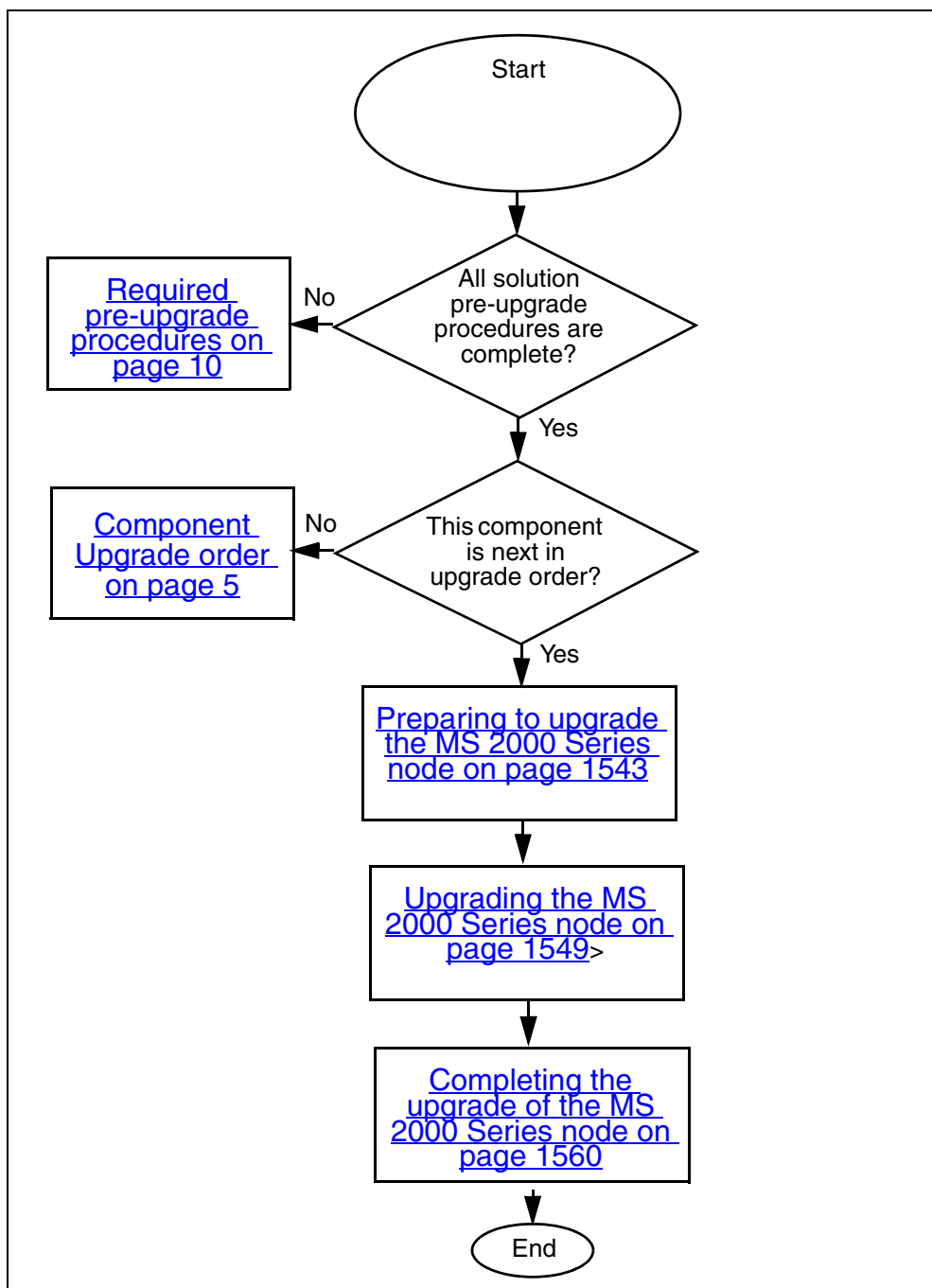
During a software upgrade, the system prohibits the following actions:

- System administration
  - adding, deleting, or modifying users
  - setting time of day
  - changing passwords
- System management
  - modifying the system name
  - adding or deleting system nodes
  - modifying the IP addresses

## MS 2000 Series upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

### MS 2000 Series upgrade tasks



**Aborting an upgrade**

If failure occurs and you need to abort the upgrade, perform [Downgrading an MS 2000 Series node on page 1563](#).

---

## Preparing to upgrade the MS 2000 Series node

---

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

#### Material requirements

This is a software-only procedure and does not require special tools. The following files are provided either on compact disc or through electronic software distribution (ESD):

- CMP file (software executable load)
- INI file (configuration file)
- DAT files containing specific information (such as conference tones, and information to deliver test trunk functionality)
- TXT file (feature key file)

The client workstation must be running the following programs:

- Microsoft Windows 98, NT, 2000, XP, or 2003
- Netscape 6, or higher, or Microsoft Internet Explorer (IE) 6.0, or higher

#### Upgrade prerequisites

The following are prerequisites for a successful MS 2000 upgrade:

- Refer to the release notes and consult with your network administration regarding the tones file to determine if a customized toneset .DAT file is appropriate for your network.

### Action

#### Preparing to upgrade an MS 2000 Series node

***At the server hosting the IEMS. (If this is an HA cluster, connect to the active unit hosting IEMS.)***

- 1 Backing up the current load files must be performed prior to upgrading the server using procedure [Backing up MS 2000 Series files on page 1562](#). Backing up the current load files must be performed prior to upgrading the server.

Please reference *NTP Media Server 2000 Series Configuration Management*, NN10340-511, for procedural information on performing backups on the IEMS GUI.

## 2 Determine the source for the software upgrade files.

### If

the software upgrade files are on CD

### Do

step [3](#)

the software upgrade files have been delivered through ESD

step [10](#)

## 3 Determine whether the audiocodes directory exists:

```
ls -l /data/loads/audiocodes
```

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

### If

the audiocodes directory exists

### Do

step [7](#)

the audiocodes directory does not exist

step [5](#)

## 5 Create the audiocodes directory:

```
mkdir -p /data/loads/audiocodes
```

## 6 Change the permissions on the audiocodes directory:

```
cd /data/loads
```

```
chmod 777 audiocodes
```

## 7 Copy the files from the CD.

**a** Insert the CD into the active CS 2000 Management Tool CD drive.

**b** Enter the following command:

```
cd /cdrom/cdrom0
```

**c** Enter the following command:

```
ls
```

Verify the content of the CD that displays by referring to the patch or release installation instructions to determine the correct release content. You will see .ini, .dat, .cmp, and .txt files listed, as well as an installation script (<filename>.sh or <filename>.pl). The CD may also contain some documentation or a README.file.

**d** Copy the files to the audiocodes directory on the CS 2000 Management Tool by entering the following commands:

```
cp -r * /data/loads/audiocodes
```

- e Enter the following commands:

```
cd /data/loads/audiocodes
ls -ltr
```

Ensure that the files you copied are present in the directory. The newer files will appear near the bottom of the listing.

**Note:** Make a note of the full path name of the .cmp file and of the feature key text file (IPSec-Keys.txt) for use later in this procedure.

- 8 Prepare the .dat file and the .ini file.

- a Log in as root.
- b Change to the audiocodes tools directory by entering the following command.

```
cd /data/loads/audiocodes/Utilities
```

- c Perform an upgrade to the .ini file by entering the following command:

```
perl iniupgrade.pl
/data/loads/audiocodes/AMS_DefaultConfig_<.i
ni file from audiocodes>
/data/loads/audiocodes/<ip address of MS 2000
server>/<old_INI_file>
/data/loads/audiocodes/<ip address of MS 2000
server>/<new_INI_file>
```

where:

**<.ini file from audiocodes>**

is the AMS\_DefaultConfig file located in  
/data/loads/audiocodes

where:

**<old\_INI\_file>**

is the .ini file representing the node's current  
configuration.

The file will be stored on the server in the directory  
/data/loads/audiocodes/<ip address of the MS 2000  
Series node>. The file is named with a timestamp and  
the .ini file extension.

where:

**<new\_INI\_file>**

is the new file you are creating

**Note:** Repeat this step for each MS 2000 Series node.

- 9 Go to [step 15](#).
- 10 Download the new software to the SPFS server. See the procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#)
- 11 Enter the following commands.  

```
cd /tmpmnt
ls
```

Verify the content of the /tmpmnt directory by referring to the patch or release installation instructions to determine the correct release content. You will see .ini, .dat, .cmp, and .txt files listed, as well as an installation script (<filename>.sh or <filename>.pl). There will also be some documentation or a README.file.
- 12 Copy the files to the audiocodes directory on the CS 2000 Management Tool by entering the following commands:  

```
cp -r * /data/loads/audiocodes
```
- 13 Enter the following commands:  

```
cd /data/loads/audiocodes
ls -ltr
```

Ensure that the files you copied are present in the directory. The newer files will appear near the bottom of the listing.

**Note:** Make a note of the full path name of the .cmp file and of the feature key text file (IPSec-Keys.txt) for use later in this procedure.
- 14 Prepare the .dat file and the .ini file.
  - a Log in as root.
  - b Change to the audiocodes tools directory by entering the following command.  

```
cd /data/loads/audiocodes/Utilities
```

- c Copy the <ip address of the MS2000> directory from **/data/loads/ams** to **/data/loads/audiocodes**.
- d Perform an upgrade to the .ini file by entering the following command. Repeat this step for each MS2000 Series node.

```
perl iniupgrade.pl
/data/loads/audiocodes/AMS_DefaultConfig_<.i
ni file from audiocodes directory>
/data/loads/ams/<ip address of MS 2000
server>/<old_INI_file>
/data/loads/audiocodes/<ip address of MS 2000
server>/<new_INI_file>
```

where

**<ini file from audiocodes>**

is the AMS\_Default\_Config file located in  
/data/loads/audiocodes/

where:

**<old\_INI\_file>**

is the .ini file representing the node's current  
configuration.

The file will be stored on the server in the directory  
/data/loads/ams/<ip address of the MS 2000 server>.  
The file is named with a timestamp and the .ini file  
extension.

where:

**<new\_INI\_file>**

is the new file you are creating

**Note:** A message may be output stating that some of the  
values could not be changed. This message is expected.  
The following is an example of this message.

**Example**

```
/data/loads/ams/172.21.195.7/2006-06-28_
13:53:00.Board.ini
```

```
YYYY-MO-DY_HR:MN:SC.Board.ini
```

```
SN09_172.21.195.7_new.ini
```

```
Changing VXMLFILENAME from
'/swd/ams/testtrunk.dat' to '' Changing
CALLPROGRESSTONESFILENAME from
```



```
'/swd/ams/conf-tones.dat' to
'usa_cpt.dat' Value for
MGCPCOMPATIBILITYPROFILE in old file is
16, value in default file is 28. Change
not allowed Value for FAXTRANSPORTMODE in
old file is 1, value in default file is
2. Change not allowed Changing
PRERECORDEDTONESFILENAME from
'/swd/ams/prerecordedtones.dat' to ''
Changing AMSSECONDARYLANGUAGE from spa to
'eng' Value for AMSPROFILE in old file is
1, value in default file is 5. Change not
allowed
```

- 15** You have completed this procedure. Return to [MS 2000 Series upgrade tasks on page 1541](#)

---

## Upgrading the MS 2000 Series node

---

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

You have completed [Preparing to upgrade the MS 2000 Series node on page 1543](#)

### Action

For increased security, the CS 2000 Management Tool and SDM logins are equipped with login timeouts. If at any point in the procedure the user interface or telnet session times out, follow the procedure for logging back in, and continue the procedure from the point at which the timeout occurred.

#### ATTENTION

If you are applying a patch, apply it after the upgrade.

When applying a patch, refer to the instructions contained in the *Admin file* on the Patch CD or in the individual downloaded patch. The *Admin file* explains how to apply the patch and overrides this procedure. If no special instructions are contained in the *Admin file* and a reference to this document is provided, then continue using this document.

## Upgrading the MS 2000 Series node

### *At the Windows desktop interface*

- 1 From the IEMS client, launch the MS 2000 Maintenance and Configuration GUI by right clicking on the node. Scroll down on the MS2000 icon to see the individual MS2010's for maintenance. For more information, refer to *IEMS Basics*, NN10329-111.
- 2 Select the MS 2000 Series node to upgrade and then select the Load Management tab.
- 3 On the left side of the window, choose the Graceful Lock radio button to lock the node. (You will actually initiate the lock in the next step.)

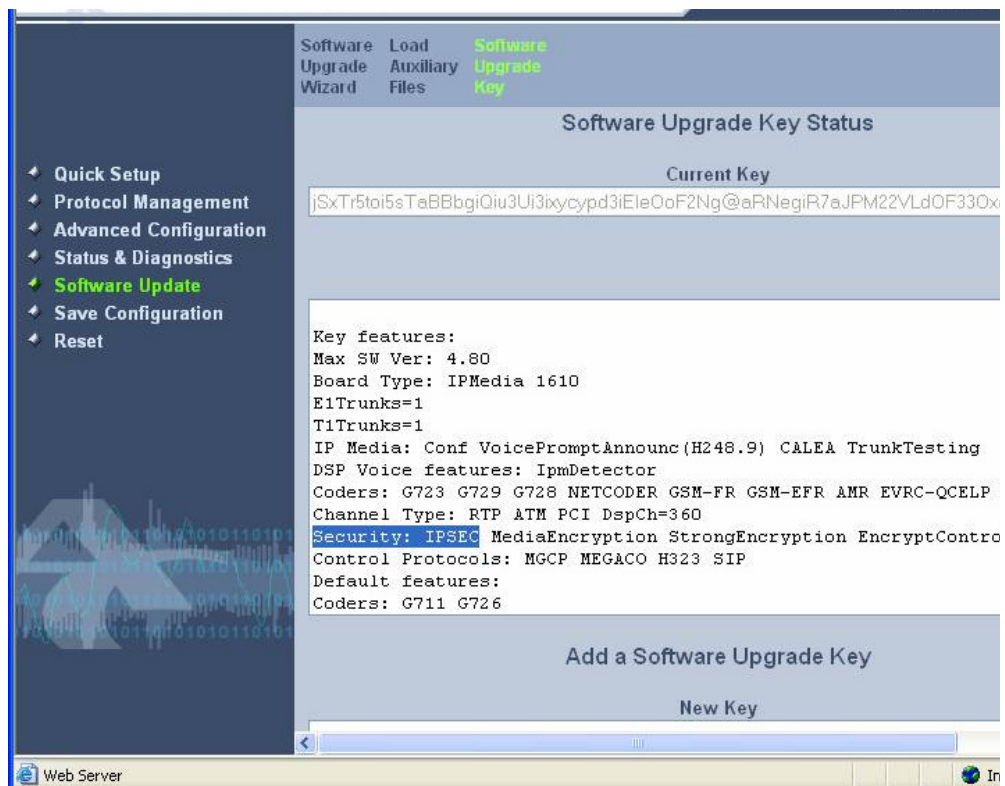
**Note 1:** Performing a Graceful Lock on the node will take it out of service after any active calls have completed.

**Note 2:** If the default MS 2000 server load is 4.40.009.036 or less, IM 24-1463 must be used to upgrade the MS 2000. This load does not work with the IEMS GUI. The load can be found on the General Configuration Tab.

- 4 Select Lock to lock the node.
- 5 Ensure that the MS 2000 is keyed for IPSec. This is a mandatory step that will ensure the MS 2000 is enabled for current and future use of IPSec.

**Note:** If you are not able to launch a web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher) at this point in the procedure, steps 5 through 13 can be performed at a later time. In that event, proceed to step 14 now and then return to step 5 later.

- a Open a standard web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher).
- b Enter the IP address of an MS 2000 Series node in the web-browser address field.
- c In the Enter Network Password window that opens, enter the appropriate user name and password, and then click OK.  
*The main menu buttons located on the left side of the main screen become activated.*
- d Select *Software Update* from the left side panel.
- e Select *Software Upgrade Key* from the top panel.
- f In the list of Key features, check that IPSec is specified, as shown in the following example.



- 6 Refer to the following table to determine the next step.

| If                                             | Do                      |
|------------------------------------------------|-------------------------|
| IPSec is specified in the list of features     | <a href="#">step 14</a> |
| IPSec is not specified in the list of features | <a href="#">step 7</a>  |

- 7 In order to send the key file to the MS 2000 you must copy the file to a location the browser can access. This can be done by ftp-ing the IPSec-Keys.txt file from the IEMS server to the machine that the browser is running on.

#### Example

The following example shows an ftp of the file using a DOS window. The file is placed on the C: directory of the browser PC.

```
C:\ Select C:\WINNT\system32\cmd.exe

G:\>ftp 47.135.43.68
Connected to 47.135.43.68.
220 ProFTPD 1.2.10 Server (Authorized Use Only) [47.135.43.68]
User (47.135.43.68:(none)): maint
331 Password required for maint.
Password:
230 User maint logged in.
ftp> cd /data/loads/audiocodes
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
10.69.33.1
AMS_DefaultConfig_IP_v205.ini
IPM2000_F4.60.009.004.cmp
10.0.5.37
Mediant2000_F4.60.011.005.cmp
IPM2000_F4.60.016.001.cmp
IPSec-Keys.txt
226 Transfer complete.
ftp> 155 bytes received in 0.00Seconds 155000.00Kbytes/sec.
ftp> get IPSec-Keys.txt
200 PORT command successful
150 Opening ASCII mode data connection for IPSec-Keys.txt (538 bytes)
226 Transfer complete.
ftp> 546 bytes received in 0.00Seconds 546000.00Kbytes/sec.
ftp> bye
221 Goodbye.

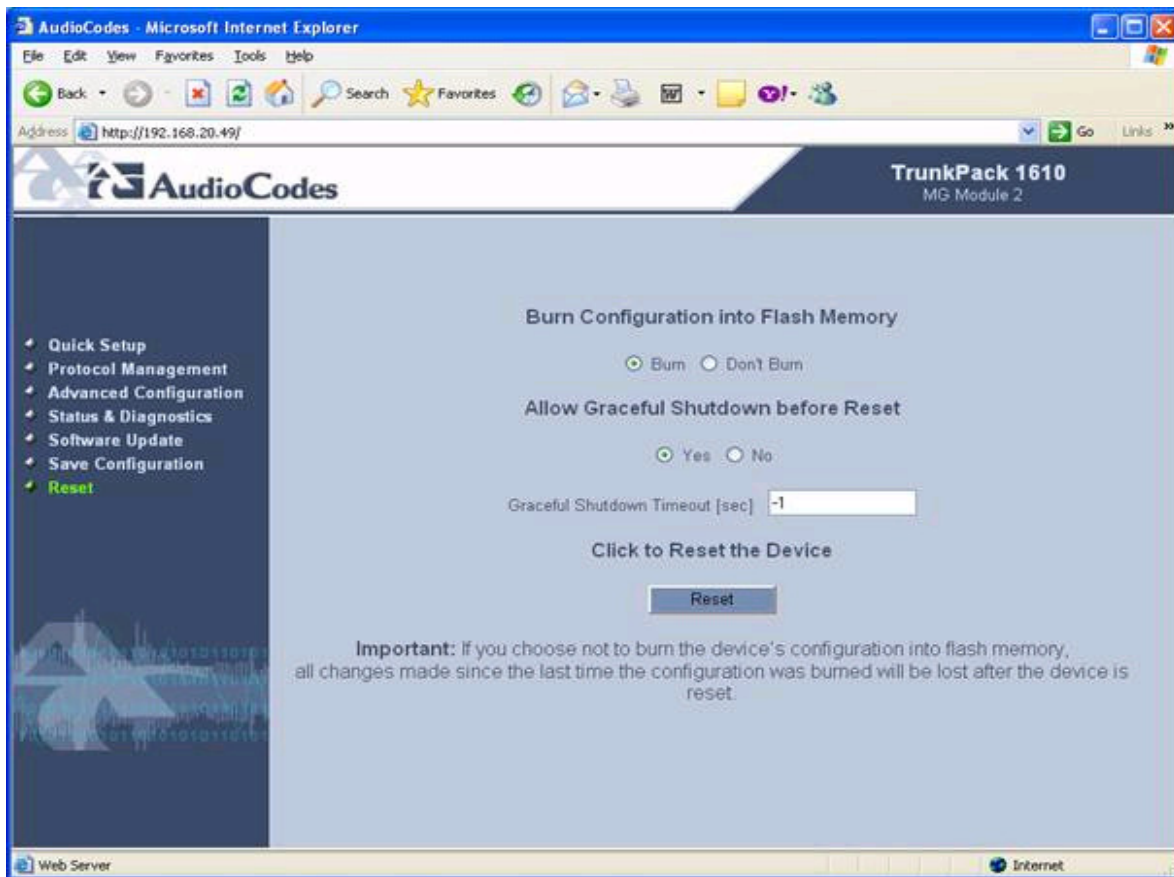
G:\>_
```

- 8 In the browser, scroll to the bottom of the Software Upgrade Key/License screen and locate the window titled Send "License" file from your computer to the device. Click the "Browse" button in this window.
- 9 Locate the Feature Key text file (IPSec-Keys.txt) that was saved to your machine in [step 7](#) and click the "Open" button.
- 10 Click the "Send File" button.

The feature key file is downloaded to the TPM.

The TPM software searches the feature key file for its serial number.

When the serial number is found, the TPM software validates the associated feature key, burns the new key into the TPM memory.



Perform a reset by pressing the RESET key, located at the left side of the screen.

**Note:** If you encounter any errors contact Nortel Support.

- 11 After the reset completes (usually 1-2 minutes) re-launch the MS 2000 Web Server utility, as shown in [step 5](#).
- 12 Validate the new key by scrolling through the list of Key features and verifying the presence of IPSec.
- 13 Close the MS 2000 Web Server utility.
- 14 Select the CMP and INI files to upload from the pull down menus at the bottom of the Load Management window in the MS 2000 IEMS Maintenance and Configuration GUI.

**Note 1:** The CMP and INI files associated with the new software load must be installed on the MS 2000 Series nodes. These are the files you copied in the procedure [Preparing to upgrade an MS 2000 Series node on page 1543](#)

**Note 2:** If you upgraded the INI file in the procedure [Preparing to upgrade an MS 2000 Series node on page 1543](#), you will see the upgraded file in the pull down list. Select this upgraded INI file to upload to the MS 2000 Series node.

- 15 Select the Send Files button to start the upgrade (load the files to the node).

The status logs section at the bottom of the Load Management window displays the load that is being sent. Also, periodic updates display information on how long the burn process has been progressing.

#### Example

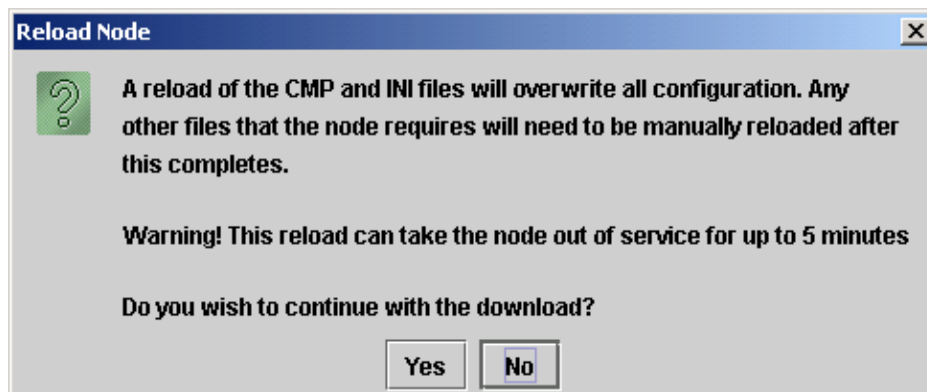
Waiting for load to be burned into flash. Time from burn start is 2 minutes 1 secs

Waiting for load to be burned into flash. Time from burn start is 2 minutes 21 secs

Download of 2004-11-19\_13:19:16.Board.ini starting.

Download of 2004-11-19\_13:19:16.Board.ini completed.

While executing the upgrade, the following message displays.

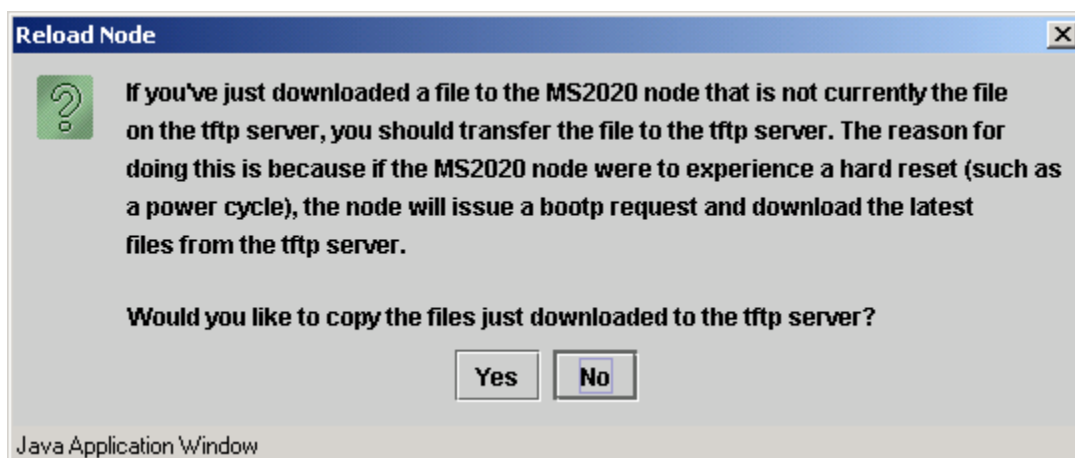


**Note:** The call progress tone, pre-recorded tone, and test trunk dat files are **not** automatically updated with this procedure. If these files have changed, the files should be copied to the appropriate directories on the CBM or SDM. Access the CBM and copy the files to the /data/swd/ams directory or access the SDM and copy the files to the /swd/ams directory. The files to be copied are located in the /data/loads/audiocodes directory on the IEMS server.

- 16 Select Yes to proceed with the upgrade.

Once the loads have been sent, the following screen displays prompting you to save the file to the tftp server if it is different

from the file already there. Because this is an upgrade, the file you just loaded is not yet on the tftp server.



**17** Select Yes to save the file to the tftp server.

#### ATTENTION

If both MS2020's and MS2010's are in the office, then the boot file in the bootptab entry must be unique for MS2020 and MS2010 entries. This allows a separate soft link for both the MS2020 load and the MS2010 load can be built.

**Note:** This step will download the CMP file to the tftp server, but before it can be used, you must reset the softlink, and change the permissions on the cmp file through the following steps:

1. Telnet to the CBM or SDM, as the root user.
2. Change directory to appropriate ams directory:

On SDM: **cd /swd/ams**



On CBM: **cd /data/swd/ams**

3. Remove the existing (old) ams.cmp file:

| If                                    | Do                                                                                                                                                        |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP or ATM-only (non-tri-mode) network | <b>rm ams.cmp</b>                                                                                                                                         |
| Tri-mode network                      | Remove the unique softlink<br>for the type of MS20x0 being<br>upgraded:<br><br>For example:<br><b>rm ams_ms2010.cmp</b><br>or<br><b>rm ams_ms2020.cmp</b> |

**Note:** If the softlink name returned above is ams.cmp, and you need to convert from a IP-only or ATM-only network to a tri-mode network, the softlink should be unique to allow both MS2010 and MS2020 to reside on the same network, otherwise there is a potential to load one of the nodes with an invalid load. The procedure [Updating the MS2000 to Unique Softlink Names on page 1569](#) contains the steps to create unique softlinks.

4. Change permission on the new CMP file to read/write access that was TFTP to the SDM or CBM:

**chmod 755 <CMP file>**

where <CMP file> is the name of the new CMP file.

### Example

```
chmod 755 IPM2000_F4.60.016.001.cmp
```

- Establish a soft link to the CMP file by entering the link command:

| If                                       | Do                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP or ATM-only<br>(non-tri-mode) network | <p><b>In -sf &lt;CMP file&gt; ams.cmp</b></p> <p>where ams.cmp is the<br/>&lt;generic_symbolic_link_name&gt;</p> <p>For example:<br/><b>In -sf IPM2000_F4.60D.016.001.cmp<br/>ams.cmp</b></p>                                                                                                                                                                                                                                                          |
| Tri-mode network                         | <p>For the <b>MS2010</b> enter the link command:</p> <p><b>In -sf &lt;CMP file&gt; ams_ms2010.cmp</b></p> <p>For the <b>MS2020</b> enter the link command:</p> <p><b>In -sf &lt;CMP file&gt; ams_ms2020.cmp</b></p> <p>Where ams_ms20x0.cmp is the<br/>&lt;generic_symbolic_link_name&gt;</p> <p>For example:</p> <p><b>In -sf IPM2000_F4.60D.016.001.cmp<br/>ams_ms2010.cmp</b></p> <p><b>In -sf TP6310_F4.60D.016.001.cmp<br/>ams_ms2020.cmp</b></p> |

**Note:** If the softlink name returned above is ams.cmp, and you need to convert from a IP-only or ATM-only network to a tri-mode network, the softlink should be unique to allow both MS2010 and MS2020 to reside on the same network, otherwise there is a potential to load one of the nodes with an invalid load. The procedure **Updating The MS2000 To Unique Softlink Names** contains the steps to create unique softlinks.

- Verify that the checksum for the symbolic link matches the checksum for the new release file. Type:

```
sum *cmp
```

**Note:** For tri-mode networks, the checksum for both the cmp files for both the MS2010 and MS2020 servers need to be verified. The sum command for tri-mode networks should be executed twice. The IPM1610...cmp file is applicable for the MS2010 and the TP6310...cmp file is applicable for the MS2020 server.

**Example**

```
31637 3665 IPM1610_F#.##.###.###.cmp
```

```
31637 3665 ams_ms2010.cmp
```

7. Older software in this directory that will no longer be used should be removed from the bootp/tftp server. Older loads no longer used typically have load numbers in the filenames that are smaller numerically and have older timestamps.

To remove these files, enter the following commands:

```
ls -l -t
```

**Example**

```
lrwxrwxrwx 1 root other 12 Apr 25 16:32 ams.cmp ->
```

```
IPM2000_F4.016.001.cmp
```

```
-rwxrwxrwx 1 root other 4321321 Apr 25 15:31
```

```
IPM2000_F4.60.016.001.cmp
```

```
-rwxrwxrwx 1 root other 4215234 Feb 28 12:34
```

```
IPM2000_F4.60.001.001.cmp
```

```
-rwxrwxrwx 1 root other 4215234 Jan 12 12:34
```

```
IPM2000_F4.60.000.099.cmp
```

**Note:** In the example system response above, ams.cmp is the symbolic link that points to the IPM2000\_F4.60.016.001.cmp load file. This symbolic link was created in the previous step.

**rm <load file>**

where <load file> is an older load file that is no longer used.

**Example**

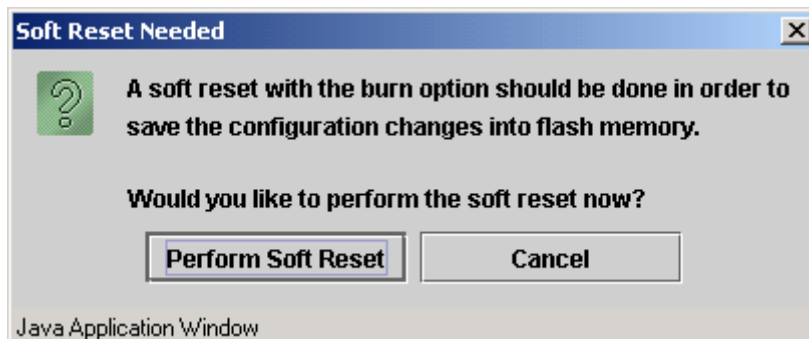
In the Example system response shown above, the loads IPM2000\_F4.60.001.001.cmp and IPM2000\_F4.60.000.099.cmp are older loads no longer used and may be removed:

```
rm IPM2000_F4.60.000.099.cmp
```

```
rm IPM2000_F4.60.001.001.cmp
```

**Note:** The load files shown above are examples only and are used to illustrate how removal of older loads should be performed. Your software load file names will differ from these examples.

- 18 After the upgrade completes, the following screen displays.



- 19 Select Perform Soft Reset to complete this procedure.
- It may take several minutes for the system reset to complete. When the system reset is complete, a list of messages like those shown below will display in the Status Logs pane of the MS 2000 Maintenance and Configuration GUI window:

Soft reset completed  
Requesting data for table atmPortLoopbackConfigTable  
Requesting data for table acSysIKEPolicyTable  
Successfully retrieved trusted managers table for node 172.16.0.65  
Successfully retrieved trap destination table for node 172.16.0.65  
Successfully retrieved table data  
Successfully retrieved table data

- 20 The Lock State indicator in the Maintenance pane located in the left panel of the Maintenance and Configuration Tool window shows the administrative state of the MS 2000 Series node. A locked state is an out-of-service state; an unlocked state indicates that the node is in service. Check the Lock State of the MS 2000 Series node. If the Lock State indicates that the node is locked, unlock the node to place it in service by clicking the Unlock button.
- 21 This procedure is complete. Return to [MS 2000 Series upgrade tasks on page 1541](#). If you experienced any errors, please see [Downgrading an MS 2000 Series node on page 1563](#).

---

## Completing the upgrade of the MS 2000 Series node

---

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

You have completed [Upgrading the MS 2000 Series node on page 1549](#)

### Action

#### Completing the upgrade of the MS 2000 Series node

##### *At your workstation*

- 1 On the left side of the MS 2000 Maintenance and Configuration GUI window, select Unlock to unlock the node.
- 2 Perform this procedure for additional MS 2000 Series nodes you are upgrading.
- 3 Determine the source for the software upgrade files.

---

| If                                                    | Do                     |
|-------------------------------------------------------|------------------------|
| the software upgrade files were on CD                 | step <a href="#">4</a> |
| the software upgrade files were delivered through ESD | step <a href="#">6</a> |

---

- 4 Eject the CD-ROM by entering the following commands:

```
cd /
```

```
eject cdrom
```

- 5 Go to step [11](#)

- 6 Begin unmounting the ISO image using the command line interface:

```
cli
```

- 7 Enter the number next to the Other option in the menu.

- 8 Enter the number next to the umount\_image option in the menu.

**Note:** You must unmount the image file using the umount command before removing the image file. If the file is deleted while it is mounted by the operating system, it can interfere

with normal operation of runtime applications running on this server.

- 9 Exit each menu level of the command line interface to eventually return to the root level:

```
select - x
```

- 10 Change directory to the ESD load file directory and remove the directory and files you created earlier in this procedure. For example:

**Example**

```
cd /data/esd_iso
```

```
rm -r /MS2000X0.X0.V.NCL.NAP.VAULT.X.D
```

```
or
```

```
rm -r /MS2A00X0.X0.V.NCL.NAP.VAULT.X.D
```

- 11 Edit the object properties in the IEMS for the MS2000 network element you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the Device Version field.
- [Editing and viewing object properties using Java Web Start Client on page 2255](#)
  - [Editing and viewing object properties using Web Client on page 2261](#)
- 12 Remove the .iso file from the CMT **/data/esd\_iso** directory
- 13 You have completed this procedure. Return to [MS 2000 Series upgrade tasks on page 1541](#)

---

## Backing up MS 2000 Series files

---

When upgrading from software release SN08 or SN09, perform a file backup using the IEMS GUI.

Before starting this procedure, review any documentation included with the software. The documentation included with the software can override or supplement this procedure.

### Backing up the current load files

For increased security, the CS 2000 Management Tool and SDM logins are equipped with login timeouts. If at any point in the procedure the user interface or telnet session times out, follow the procedure for logging back in, and continue the procedure from the point at which the timeout occurred.

1        in .

### Backing up MS 2000 files

#### *At the Windows desktop interface*

- 1        Back up the SN08 INI file in the /data/loads/audiocodes/<ip address of the MS 2000 node> directory by performing the following steps:
  - a        From the IEMS client, launch the MS 2000 Maintenance and Configuration GUI. Consult your system administrator for instructions about how to access the GUI.
  - b        In the MS 2000 Maintenance and Configuration window, select the Load Management tab.
  - c        On the left side of the window, choose the Backup INI to tftp Server.
  - d        Click on the INI Backup button to initiate the backup.
  - e        Repeat steps [1a](#) to [1d](#) for each MS 2000 node that is being upgraded.
  - f        Close the IEMS GUI.
- 2        This procedure is complete. Return to step [2](#) in [Preparing to upgrade the MS 2000 Series node](#)

---

## Downgrading an MS 2000 Series node

---

This procedure enables you to downgrade a MS 2000 Series node to a previous release. The MS 2000 Series node can be either an MS 2010 or an MS 2020.

### Downgrading an MS 2000 Series node

#### *At the Windows desktop interface*

- 1 Open a telnet window and log into the IEMS server:  
Become the root user: **su – root**  
**password:** <enter the root password>
- 2 On the IEMS server, copy the existing **.cmp** file from **/data/loads/ams** to **/data/loads/audiocodes** for selection in the GUI
- 3 Copy the existing **.ini** file from **/data/loads/ams** to **/data/loads/audiocodes/<ip address>** for selection in the GUI.

#### **Example**

**/data/loads/audiocodes/10.165.54.111**

- 4 Open a second telnet session to the CBM server.  
Delete the **ams.cmp** on the CBM
- 5 On the CBM, execute the following command to create a soft link to point to the existing **.cmp** file  
**ln -sf <CMP file> ams.cmp**  
This will ensure that the existing file is loaded during a reboot.
- 6 Open a browser window and insert the following in the address bar: **https://<virtual\_iems\_ip>:9091/**.

#### **Example**

**https:// https://47.105.68.154:9091/**

- 7 Select the Media Server 2000 node to downgrade. Right mouse click on the MS you are downgrading and select "Config and Maintenance tools", then select the Load Management tab.  
Choose **Applications -> IEMS Topologies ->Network Elements**. There is an "MS 2000" tree if the MS 2000 device has been added into IEMS. Click on "MS 2000". The right side window will show all MS 2000 devices.



- 8 On the left side of the window, choose the Graceful Lock radio button to lock the node. (You will actually initiate the lock in the next step.)

**Note:** Performing a Graceful Lock on the node will take it out of service after any active calls have completed.

### WARNING

There is no confirmation window. Once lock is selected it will lock the MS

- 9 Select Lock to lock the node.
- 10 Select the CMP and INI files to upload from the pull down menus at the bottom of the Load Management screen.

In this situation, the user must manually put the (CMP and INI) files in the directory (/data/loads/audiocodes/<MS\_IP>), so the files are visible from the IEMS GUI and the downgrade is possible from IEMS.

#### Example

**/data/loads/audiocodes/10.165.54.111**

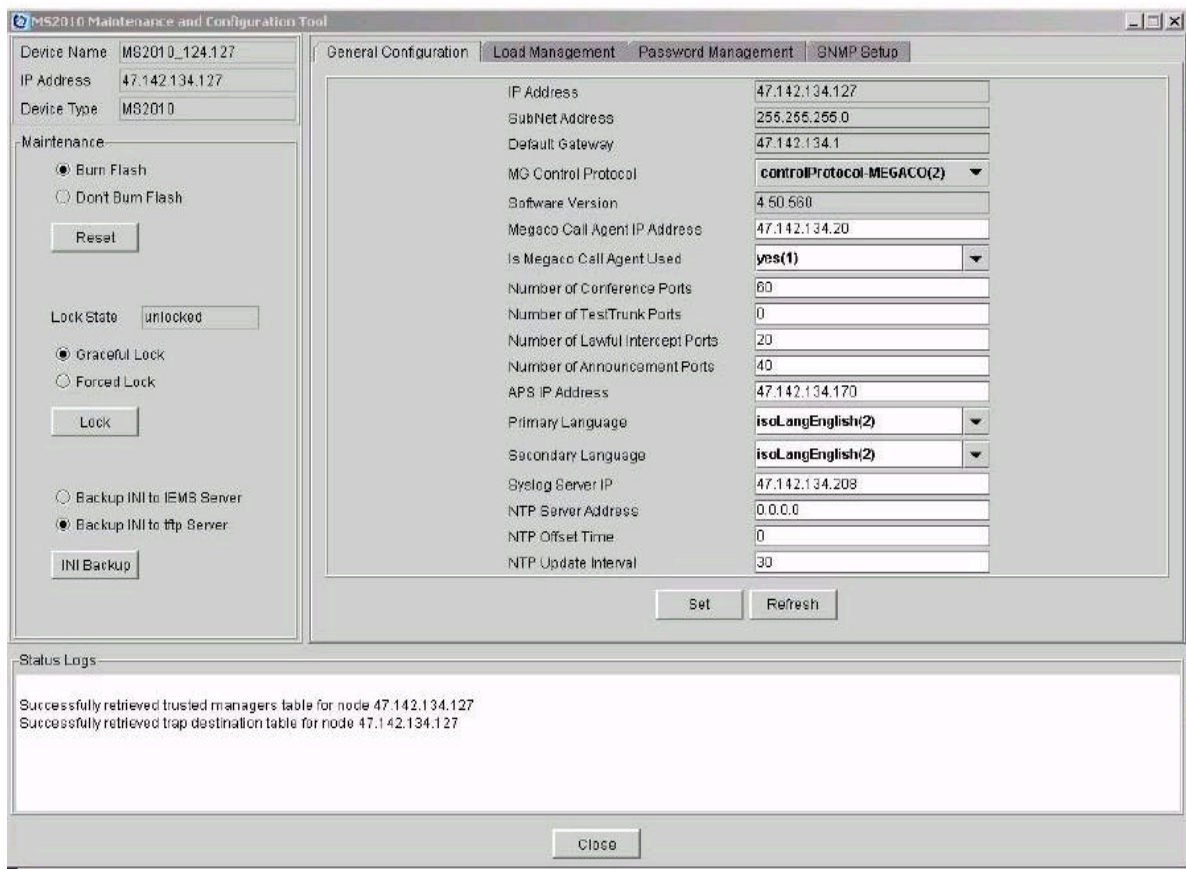
This can be accomplished by retrieving the load files that were FTP'ed from the CBM (assume the old CMP and INI file are on the bootp server) to the CMT server

(/data/loads/audiocodes/<MS\_IP>). If the load files are not on the CBM and have been removed, then load the lower software release file (CMP) from the original MS20x0 CD for the software release to be downgraded into /data/loads/audiocodes directory.

Locate the INI file for lower software release for the MS20x0 node on the bootp server (CBM) or if this is not possible, use the default INI file from the original MS20x0 CD and add site specific settings for configuration using the "General Configuration" tab in IEMS GUI for the MS20x0.

The loading of the INI file from CD is performed ONLY if the INI file for the lower software release cannot be located.

The default INI file is a configuration file which is missing site specific settings like the call agent IP address, this is the GWC IP address and other site specific settings. Use the "General Configuration" tab the IEMS GUI after the default INI file from the MS20x0 CD has been located and downloaded to the MS20x0. See the screen shot below.



- 11 Select the Send Files button to start the downgrade (load the files to the node).

The status logs section that displays at the bottom of the Load Management window shows the load that is being sent. Also, periodic updates display information on how long the burn process has been progressing.

**Note:** Please use the existing version of the **.cmp** and **.ini** file that was copied to **/data/loads/audiocodes** directory.

#### Example

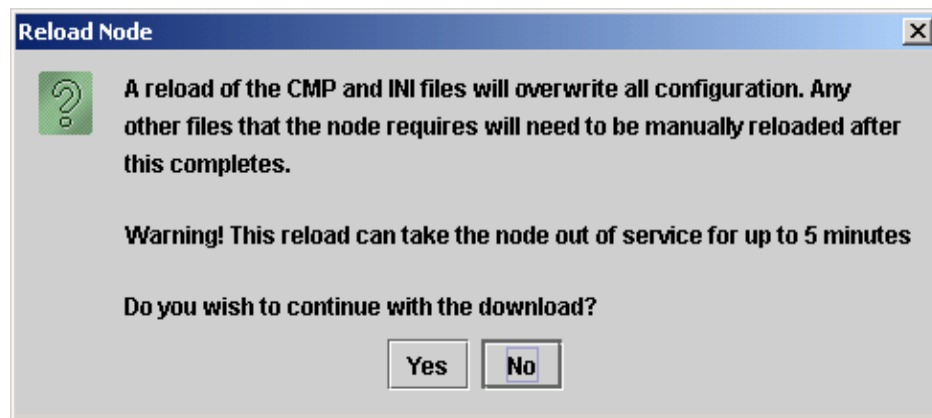
Waiting for load to be burned into flash. Time from burn start is 2 minutes 1 secs

Waiting for load to be burned into flash. Time from burn start is 2 minutes 21 secs

Download of 2004-11-19\_13:19:16.Board.ini starting.

Download of 2004-11-19\_13:19:16.Board.ini completed.

While executing the downgrade, the following message displays.



### ATTENTION

The download of the CMP and INI file from IEMS to the MS20x0 occurs using HTTP. If there are failures, please verify the media server web user id and password and SNMP community strings are correct for the MS20x0 in the IEMS GUI. This can be verified using the three screen shots below. Right click on the MS20x0 icon and selecting "Object Properties".

MS20x0 web user ID and password by default are: **"Admin"** and **"Admin"**

**SNMP Default Setting:**

Port = **161**

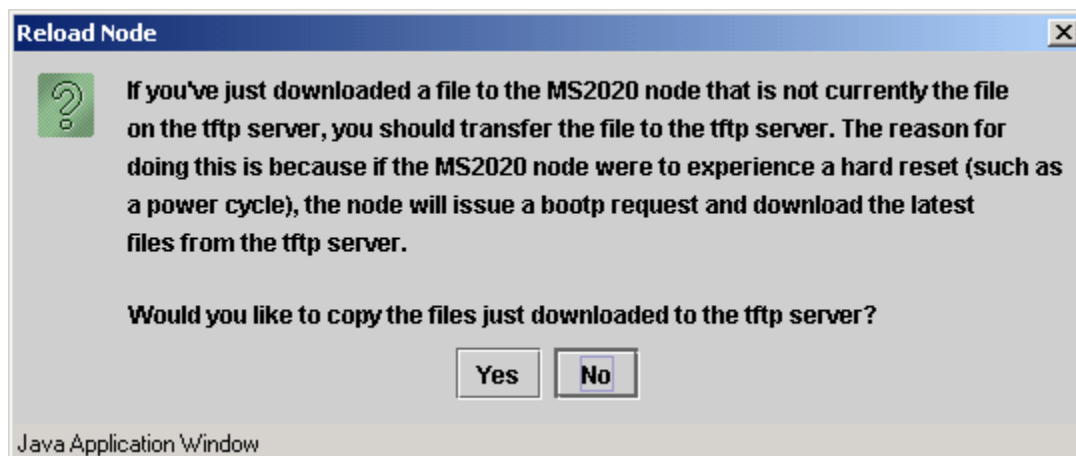
Community is = **Public**

Write Community = **Private**

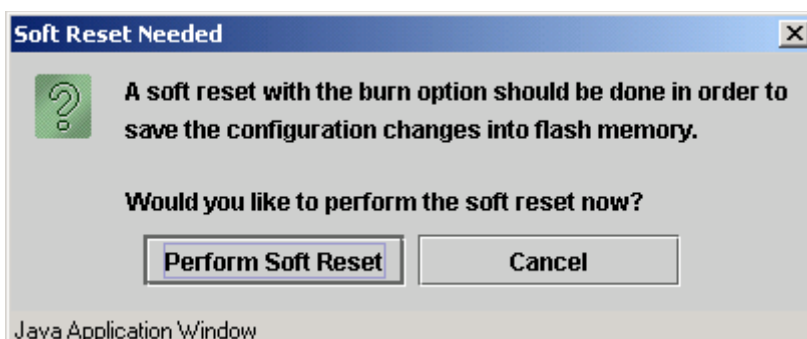
Version = **v2c**

- 12 Select Yes to proceed with the downgrade.

Once the loads have been sent the following screen displays prompting you to save the file to the tftp server if it is different from the file already there.



- 13 Select Yes to save the file to the tftp server.
- 14 After the downgrade completes, the following screen displays.



- 15 Select Perform Soft Reset to complete this procedure.
- 16 Unlock the MS from the IEMS GUI after the CMP and INI files have been downgraded.  
When the "Config and Maintenance tools" shows, left side window shows node that can be locked or unlocked. If the node is unlocked, there is a lock button; if the node is locked, there is an unlock button.
- 17 Perform the instruction in the following table.

| If                                                    | Do                           |
|-------------------------------------------------------|------------------------------|
| Downgrading Media Server 2000 nodes                   | Go to <a href="#">step 3</a> |
| There are no more Media Servers 2000 nodes to upgrade | Continue to next step.       |

- 18** Log out of IEMS, CMT and CBM. At the Solaris prompt, enter:  
**exit**
- 19** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Updating the MS2000 to Unique Softlink Names

---

### Application

Use this procedure to change a non-unique softlink name (ams.cmp) for the MS2000, to a unique softlink name for the MS2010 (ams\_ms2010.cmp) and MS2020 (ams\_ms2020.cmp). Unique softlink names are required in a tri-mode network (those with both MS2010s (IP) and MS2020s (ATM)).

Contact Nortel Support at any point during this procedure for assistance.

### Prerequisites

Refer to [Upgrading the MS 2000 Series node on page 1549](#).

### Action

***From the workstation, update the softlink name on the server***

- 1 Telnet to the SPFS-based server:  
**telnet <IP address>**  
where <IP address> is the IP address of the server.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user  
**\$ su - root**
- 4 When prompted, enter the root password.
- 5 Access the command line interface.  
**# cli**

#### **Example**

Command Line Interface

- 1 - View
  - 2 - Configuration
  - 3 - Other
  - X - exit
  - select -
- 6 Enter 2 to access the Configuration menu.

#### **Example**

Configuration

- 1 - NTP Configuration
  - 2 - Apache Proxy Configuration
  - 3 - DCE Configuration
  - 4 - OAMP Application Configuration
  - 5 - CORBA Configuration
  - 6 - IP Configuration
  - 7 - DNS Configuration
  - 8 - Syslog Configuration
  - 9 - Database Configuration
  - 10 - NFS Configuration
  - 11 - Bootp Configuration
  - 12 - Restricted Shell Configuration
  - 13 - Security Services Configuration
  - 14 - Login Session
  - 15 - Location Configuration
  - 16 - Cluster Configuration
  - 17 - Succession Element Configuration
  - 18 - snmp\_poller (SNMP Poller Configuration)
  - 19 - backup\_config (Backup Configuration)
  - X - exit
- Select -

- 7 Enter 11 to access the Bootp Configuration.

**Example**

Example response

Bootp Configuration

- 1 - bootp\_add (Add Entries To The Bootptab File)
- 2 - bootp\_del (Delete Entries From The Bootptab File)
- 3 - bootp\_list (List Out The Bootptab File)
- 4 - bootp\_restore (Restore Bootptab File From The Last Version)

X - exit

select -

- 8 Enter 3 to list the bootp information.
- 9 Make a copy of the information associated with the IP of the MS20x0 you want to change.

**Example**

47.142.134.127:\

bf=MS2010.cmp

-fb;/swd/ams/47.142.134.127.ini:\

gw=47.142.134.1:\

hd=/swd/ams:\

ht=ether:\

ha=00908F042B46:\

ip=47.142.134.127:\

sa=47.142.134.124:\

sm=255.255.255.0:\

vm=rfc1048:

You are returned to the bootp configuration menu.

**Note:** If you copy and paste the information from the old board (above), do not include the colon backslash (:\) when you paste the text. The colon backslash is not part of the data.

- 10 Enter 2 to delete the bootp information for the previous BootP file you are replacing.
- 11 Enter the MAC address (hardware address [ha]) of the old BootP file containing the old softlink name.
- 12 Enter ok to accept the current settings you just entered.

**Example**

in remove

after sed

Asking bootpd at pid 24554 to reload /etc/bootptab.

=== "bootp\_del" completed successfully

- 13 Enter 1 to add the MS20x0 to the bootp file.



- 14** Enter the information associated with the old MS20x0 softlink name you removed, with the exception of the softlink name (boot file [bf]). For the hardware [bf] info, enter the new softlink name.

**Example**

ams\_ms2010.cmp

or

ams\_ms2020.cmp

**Note:** The information from the previous BootP needs to be associated with the new BootP file. The Boot file is the only thing different.

- 15** Enter ok to accept the current settings you just entered.

**Example**

Asking bootpd at pid 24554 to reload /etc/bootptab.

=== "bootp\_add" completed successfully

- 16** Enter 3 to list the bootp information.
- 17** Verify that the new information for the MS20x0 softlink was entered correctly.
- 18** If you are modifying a second nodes softlink information, repeat steps [10](#) through [17](#) above.
- 19** Enter X until you have backed out of the CLI tool.
- 20** Type **exit**. You have completed this procedure.



## MG 9000 upgrade

The Nortel Networks Media Gateway 9000 (MG 9000) is an access gateway positioned at the edge of the Succession Network, offering a wide range of voice, data, and video services.

Universal Access-AAL1 (UA-AAL1) applications provide voice, DSL, and private lines services over a unified ATM network in the North American market. The UA-AAL1 solution uses the ATM transport network to carry packetized voice, call control signaling, OAM and data traffic.

Universal Access IP (UA-IP) applications use the IP network to carry packetized voice, call control signaling, OAM and data traffic to provide end office plain old telephone service (POTS), P-Phone, and Coin lines services, trunking services, and DSL services in International and North American markets.

When upgrading the MG 9000 network element from SN08 to SN09U or SN09 to SN09U, the following activities take place in the following order:

- follow procedure [Upgrading MG 9000 Manager software from SN08 or SN09 to SN09U on page 1076](#)
- install the GUI client application
- provision userids
- upgrade software in MG 9000 cards

Refer to the following related procedures:

- downgrading the MG 9000 software in [Downgrading the MG 9000 and MG 9000 Manager from SN09U to SN08 or SN09 on page 2495](#)
- upgrading the MG 9000 cards individually, by card type, or all cards is described in *MG 9000 Configuration Management*, NN10096-511.

## What's new in MG 9000 Upgrades in (I)SN09U

### Feature changes

Modified procedures reflecting support for upgrade to SN09U.

### Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 to SN09U
- SN09 to SN09U
- SN09U to SN09U

### Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

### Time to complete an upgrade

The following table lists the tasks to upgrade MG 9000 network element software and the estimated time to complete each task.

#### Estimated time to complete a software upgrade

| Task                         | Application               | Time         |
|------------------------------|---------------------------|--------------|
| Preparing for the upgrade    |                           | 15 mins      |
| Upgrading the software       | MG 9000 (single shelf NE) | 1 hr 44 mins |
| Completing the upgrade       |                           |              |
| Total estimated upgrade time |                           | 2 hours      |

### Service impacts

The upgrade of MG 9000 network element software does not impact service.

### Additional information

The following additional information applies to the upgrade of MG 9000 software:

- Warnings for all components and services impacted during upgrade
  - No data provisioning can be performed during upgrades. During the upgrade of a given NE, the MG 9000 Manager blocks any attempt to change data for that NE. The MG 9000 Manager displays a minor warning indicating provisioning is halted and the database is unavailable for that NE.
  - PM collection cannot be performed while the MG 9000 Manager master server is not running.
  - OC3 carriers must not be in split-mode. For details, refer to the procedure “Recovery from APS Split-mode” in *MG 9000 Fault Management*, NN10074-911.

**Note:** If the node is in the split-mode state, and if this state was initiated by the system, the recovery process must be performed, including a 24-hour soak period. To determine if the split mode state is a result of a system action, refer to *MG 9000 Fault Management*, NN10074-911.

- Refer to the following table to identify the PEC codes for SN08-SN09 cards.

### SN09U upgrade PEC codes

| Card type               | Pre-SN08 PEC codes        | SN08 new hardware PEC codes | SN09U new hardware PEC codes |
|-------------------------|---------------------------|-----------------------------|------------------------------|
| ITP                     | NTNY30AA or NTNY30BA (IP) | NTNY30BA or NTNY30CB        |                              |
| ITX                     | NTNY41AA                  | NTNY41BA                    |                              |
| DS-512 ABI              | NTNY43AA                  | NTNY43BA or NTNY43BB        |                              |
| DCC-OC3 (SCO)           | NTNY45AA                  | NTNY45CA                    |                              |
| Hybrid DCC-OC3 (OC3)    | NTNY45AA                  |                             |                              |
| DCC-DS1IMA (SCI hybrid) | NTNY45BA                  | NTNY45BA                    |                              |

## SN09U upgrade PEC codes

| Card type | Pre-SN08 PEC codes   | SN08 new hardware PEC codes | SN09U new hardware PEC codes |
|-----------|----------------------|-----------------------------|------------------------------|
| DCC-GigE  |                      | NTNY45FA                    |                              |
| MTA       |                      | NTNY42AB                    |                              |
| GLC       | NTNY53AA<br>NTNY53AB |                             | NTNY53BA<br>NTNY53CA         |

- Recommendations for limiting service impact: none

## Upgrade strategy

The following high-level strategy summarizes network upgrade procedures required when upgrading the MG 9000 NE:

1. Upgrade the Communication Server 2000 (CS2000) Management Tools software to ensure node and line provisioning applications are updated ([CS 2000 Management Tools upgrade on page 272](#)).
2. Upgrade the SPFS software ([Upgrading SPFS software on page 403](#)). This includes the SPFS on the MG 9000 Manager master and mid-tier servers.

**Note:** The CS 2000 Management Tools and the SPFS platform software must be upgraded to SN09 before upgrading the MG 9000 Manager server and mid-tier software ([step 4](#)).

3. Remove the existing SN08 or SN08 software packages. Perform this activity just after upgrading the Server Platform Foundation Software (SPFS). SN08 or SN09 SPFS software does not operate with SN09U SPFS software.
4. Upgrade the MG 9000 Manager software in the following order: server, mid-tier.
5. Upgrade all of the MG 9000 intelligent cards and the MTA and xDSL cards to SN09U from an image received on CD or through electronic software delivery (ESD) using the mg9kuptool accessible from the command line interface (CLI) on the MG 9000 master server.

## Tools and utilities

The MG 9000 supports software upgrades and downgrades. Procedures in this document reference these activities. For MG 9000 Manager software downgrade procedures, refer to [Downgrading the](#)

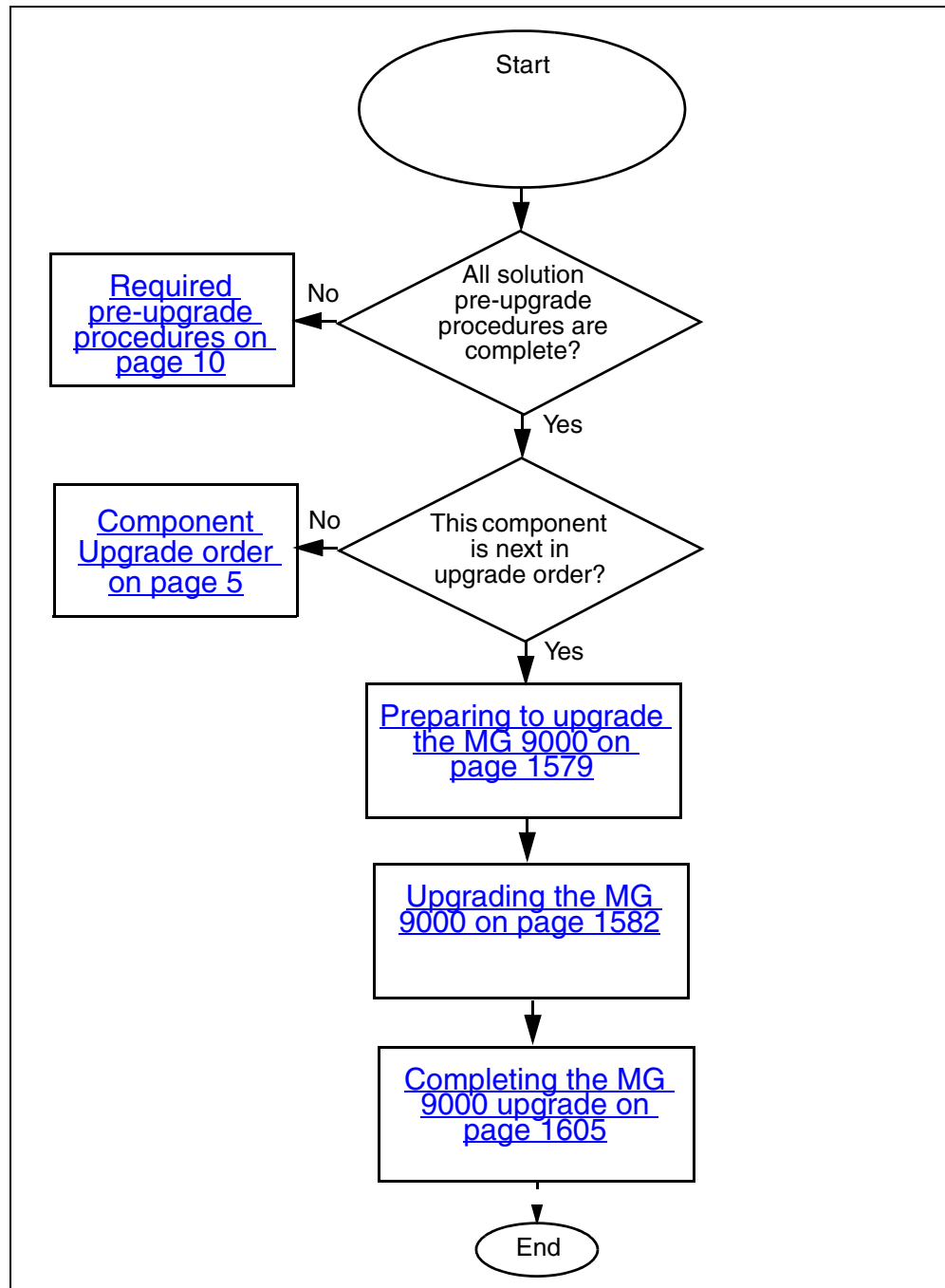
[MG 9000 and MG 9000 Manager from SN09U to SN08 or SN09 on page 2495.](#)

The MG 9000 Manager supports patching through the network patch manager (NPM). Patching procedures and information are located in [Carrier Voice over IP Network patching on page 2265.](#)

The command line interface (CLI) mg9kuptool provides an automated software upgrade for the MG 9000 cards, including the MTA and xDSL cards. The mg9kuptool can upgrade multiple MG 9000 NE devices. The mg9kuptool automates device patching after the upgrade. Although the mg9kuptool does not provide upgrade process status messages, those messages can be obtained by performing a telnet to the server and enter the mg9kuptool -query command. The mg9kuptool upgrade procedure is described in [Upgrading the MG 9000 using the mg9kuptool on page 1588.](#)

## **MG 9000 upgrade tasks**

This taskflow shows you the sequence of tasks you perform to upgrade this component.

**MG 9000 upgrade tasks**

---

## Preparing to upgrade the MG 9000

---

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

Perform the previous required upgrade according to the order listed in the table [Component Upgrade Order on page 6](#). The required upgrade is the previous component in the list according to your network configuration.

### Pre-upgrade requirements

Ensure the CS 2000 Manager has been upgraded to SN09U before upgrading any MG 9000s to SN09U.

The MG 9000 Manager must be upgraded to SN09U before the MG 9000 cards are upgraded to SN09U. An MG 9000 Manager at software level SN09U is capable of managing an MG 9000 NE operating at SN08, SN09, or, SN09U.

**Note:** All alarms on the MG 9000 Manager and MG 9000 network element must be cleared prior to proceeding with the SN08 or SN09 to SN09U upgrade process.

Do not provision any new data to the NEs during upgrade activities.

### Entry criteria

The following are the criteria for entering the SN08 or SN09 to SN09U upgrade process:

- host names and IP addresses required for:
  - the MG 9000 Manager mid-tier server
  - the MG 9000 Manager server
  - the CS 2000 Manager (Oracle database), required
  - the Security Authentication Host, typically the mid-tier IP address
  - the Imaging FTP Server Host, typically the SDM
- user id and password for the Imaging FTP Server Host must have overwrite privileges



- hardware and software baseline:
  - MG 9000 card loads must be at SN08 or SN09 with all patches applied
  - MG 9000 Manager software must be at SN09U with all patches applied and enabled
- tools required: database browser (optional)
- run a getpatch to retrieve all SN09U patches before the upgrade starts. Refer to [Transferring patches delivered on CD to the NPM database on page 2297](#) or [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#) for more information.
- upgrade interdependency:
  - SPFS on MG 9000 Manager master and mid-tier servers must be upgraded to SN09U ().
  - CS 2000 Management Tools must be upgraded to SN09U prior to upgrading the MG 9000 Manager to SN09U.
  - ensure MG 9000 PSEs are configured correctly before the upgrade starts as described in the MG 9000 Manager upgrade procedures [Upgrade interdependencies on page 1069](#).
  - MG 9000 card upgrades are addressed in [Upgrading the MG 9000 using the mg9kuptool on page 1588](#).

**Exit criteria**

The following are the criteria for exiting from the SN08 or SN09 to SN09U upgrade process:

- The upgrade was successful
  - after the MG 9000 NE is successfully discovered in SN09U
- Recommended testing
  - Make sure alarms are received (temporarily set a cooling unit breaker on the IBIP to off).
  - Select a VMG from the Switched Line Services View. Select a termination and make sure that the termination properties show correctly.
  - Select a Private lines service, if provisioned, and get the properties for it. Make sure the Svc OperStatus from the Service Properties View is connected for full and active endpoint services

- Log reports or operational measurements (OM): check the customer logs for audit messages indicate clean up failures.
- Equipment state verification: access the Oracle database and verify the same number of terminations exists (optional).

**Applying software fixes**

When it is necessary to apply software fixes, the following methods are available:

- Maintenance Release upgrade process: refer to procedure [Upgrading the MG 9000 Manager software to a maintenance release on page 2512](#).
- The MG 9000 uses the Network Patching Manager (NPM) patching system. Any device requiring patching must first be audited to determine the load name compatibility with the patch before applying the patch.

For more information on patching refer to [Carrier Voice over IP Network patching on page 2265](#).

**Action**

Proceed to [Upgrading the MG 9000 on page 1582](#) and use the [SN08 or SN09 to SN09U MG 9000 upgrade checklist on page 1582](#) to follow the steps for upgrading the MG 9000.

## Upgrading the MG 9000

The following checklist provides the high-level steps to upgrade the MG 9000. Where applicable, a reference to the step-by-step procedure is provided.

### SN08 or SN09 to SN09U MG 9000 upgrade checklist

Use the following table as a checklist for a high-level MG 9000 NE upgrade summary when upgrading the MG 9000 from SN08 or SN09 to SN09U. This checklist references detailed procedures that are provided later in the document. Enter a check mark (✓) in the ✓ column as each step or procedure is completed.

#### MG 9000 SN08 or SN09 to SN09U upgrade checklist

| Activity                                        |                                                                                                                                                                                       | Procedure                                                                                                                                                                                              | ✓ |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| <b>On the Inactive node</b>                     |                                                                                                                                                                                       |                                                                                                                                                                                                        |   |
| <b>For each network element in SN08 or SN09</b> |                                                                                                                                                                                       |                                                                                                                                                                                                        |   |
| <b>1</b>                                        | Ensure all MG 9000 Patch Image (PI) load files have been copied to the CS2000 Core Manager (SDM) to support upgrade / downgrade activity from CD-ROM or Electronic Software Delivery. | Refer to <a href="#">Installing MG 9000 loads into CS 2000 Core Manager from CD-ROM on page 1606</a> or <a href="#">Preparing MG 9000 software delivered through ESD for an upgrade on page 1608</a> . |   |
| <b>2</b>                                        | Provisioning a floating IP address.                                                                                                                                                   | Refer to <a href="#">Provisioning a floating IP address on page 1610</a> .                                                                                                                             |   |
| <b>3</b>                                        | If this is an SN08 to SN09U upgrade, ensure the Preshared Keys match.                                                                                                                 | Refer to "Changing NE Encryption Keys" in <i>MG 9000 Security and Administration</i> , NN10162-611.                                                                                                    |   |

**MG 9000 SN08 or SN09 to SN09U upgrade checklist**

| Activity                        | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ✓ |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| <b>4</b> Image server<br>userid | <p>Login into MG9KSERVER as root</p> <p>Check the image server userid on MG9KSERVER by typing <b>/opt/nortel/mg9ks*/bin/mg9kserver config</b> and choose the option next to display current settings.</p> <p>If the image server userid is root or mgsmim, telnet to SDM/CBM as root or mgsmim to determine if communication between MG 9000 Manager and SDM/CBM is established. If successful, proceed to checklist activity <a href="#">6</a>.</p> <p>If the communication fails for root: Contact next level of support.</p> <p>If the communication fails for mgsmim: Proceed to check list number <a href="#">5</a>.</p> <p><b>Note:</b> It is recommended that either root or mgsmim should be used as image server userid on MG9KEM.</p> |   |

**MG 9000 SN08 or SN09 to SN09U upgrade checklist**

|   | Activity                                                                                                   | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ✓ |
|---|------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 5 | Creating the image server userid on SDM/CBM                                                                | <p>To create an image server userid on SDM/CBM, login as root and perform the following:</p> <pre># mkuser pgrp=maint groups=maint maxage=0 minlen=0 minalpha=0 minother=0 home=/home/mgsmim shell=/bin/ksh mgsmim</pre> <p><b># passwd mgsmim (set initial password to new2day)</b></p> <pre>#chown -R &lt;imaging userid&gt;:&lt;userid group&gt; /swd/mg9k</pre> <p><b>where</b></p> <p>imaging userid is the user id for the image server<br/>userid group is the group to which the userid belongs</p> <p><b>Example</b></p> <pre>chown -R mgsmim:maint /swd/mg9k</pre> <p><b># telnet to SDM/CBM (to set permanent password)</b></p> <pre>login: mgsmim mgsmim's Password: new2day 3004-610 You are required to change your password. Please choose a new one. mgsmim's New password: feb2006 Enter the new password again: feb2006</pre> |   |
| 6 | Steps to change the image server settings on the MG 9000 Manager                                           | <p>Login to MG9KSERVER as root.</p> <p>The image server IP address is the same as the SDM/CBM IP address on which the MG 9000 loads are stored. The same userid and password must be used in the CLUI upgrade.</p> <p>The image server IP address, userid, or password can be changed by typing<br/><b>/opt/nortel/mg9ksrv*/bin/mg9kserver config</b> and selecting the option corresponding to Change Imaging Server settings on the MG9KSERVER.</p>                                                                                                                                                                                                                                                                                                                                                                                           |   |
| 7 | Perform a card upgrade on the following cards on the NE: all MTA, xDSLs, DS1s, ABIs, ITPs, ITXs, and DCCs. | <p>Perform the procedure <a href="#">Upgrading the MG 9000 from SN08 or SN09 to SN09U using the mg9kuptool without options on page 1593</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |   |

**MG 9000 SN08 or SN09 to SN09U upgrade checklist**

|   | Activity                                                                                    | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ✓ |
|---|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
|   | <b>Note:</b> This is a safe stopping point.                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |   |
| 8 | Create patched images of all MG 9000 loads, only if patches were applied during the upgrade | <p>After the MG 9000 cards have been upgraded to SN09U and the MG 9000 Manager upgraded to SN09U, perform the following procedure to image the network element (NE) cards for use in upgrading the cards in other NEs.</p> <p><b>Note 1:</b> Perform the following steps after the following conditions are met:</p> <ul style="list-style-type: none"> <li>the NPM is at SN09U</li> <li>the suite of MG 9000 Manager servers are running SPFS09U</li> </ul> <p><b>Note 2:</b> The following are the high level step to create patched images of all MG 9000 loads. This will be accomplished by upgrading, patching, and then imaging three MG 9000s (one DCC-OC3 MG 9000, one DCC-DS1-IMA MG 9000, and one DCC-GigE MG 9000). Ensure the NEs selected include all MG 9000 intelligent card types in the office.</p> <ol style="list-style-type: none"> <li>Upgrade all the intelligent cards on a DCC-OC3 MG 9000 using the latest available PI loads. During the upgrade, any available patches that were not included on the PI load are applied. After patching is complete, take an image of the DCC-OC3 MG 9000 using the NPM.</li> <li>Upgrade a DCC-IMA MG 9000 using the PI loads just created. During the upgrade, any available patches for any remaining intelligent card types (including the DCC-DS1-IMA) that were not patched during the DCC-OC3 MG 9000 upgrade are applied. After the upgrade is complete, take an image of the DCC-DS1-IMA MG 9000 using the NPM</li> </ol> |   |

**MG 9000 SN08 or SN09 to SN09U upgrade checklist**

| Activity                                           | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | ✓ |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| Create patched images of all MG 9000 loads (contd) | <ul style="list-style-type: none"> <li>c. Upgrade a DCC GigE MG 9000 using the PI loads just created. During the upgrade, any available patches for any remaining intelligent card types (including the DCC GigE) that were not patched during the DCC-OC3 or DCC-GigE MG 9000 upgrade are applied. After the upgrade is complete, take an image of the DCC-GigE MG 9000 using the NPM.</li> <li>d. Use the following to determine the next step. <ul style="list-style-type: none"> <li>• if there were additional patches added to the pre-patched image loadfile, go to step <a href="#">e</a></li> <li>• if there were no additional patches added to the pre-patched image loadfile, go to step <a href="#">f</a></li> </ul> </li> <li>e. Apply remaining SN09U patches to all cards on this NE with DCC OC3 cards.</li> <li>f. Take an image of the inactive cards on this NE with DCC OC3 cards. Refer to <a href="#">Performing a device image using the NPM on page 2327</a> for steps on performing a device image. Select SmartImage-&gt;MG9KDEVICES.</li> <li>g. Upgrade one NE with DCC-DS1-IMA cards with the SN09U MG 9000 patched images just created in the previous step. Load all cards on this NE with the supplied image.</li> <li>h. Apply the remaining patches to all cards on this NE with DCC DS1-IMA cards.</li> <li>i. Take an image of the inactive cards on this NE with DCC DS1-IMA cards that were not imaged in step <a href="#">f</a> above. Refer to <a href="#">Performing a device image using the NPM on page 2327</a> for steps on performing a device image. Select SmartImage-&gt;MG9KDEVICES.</li> <li>j. Upgrade one NE with DCC GigE cards with the SN09U MG 9000 patched images created in step <a href="#">i</a>. Load all cards on this NE with the supplied image.</li> </ul> |   |

**MG 9000 SN08 or SN09 to SN09U upgrade checklist**

| <b>Activity</b>                                                                                                                                                                                                                                                                                                                                         | <b>Procedure</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | √ |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| Create patched images of all MG 9000 loads (contd)                                                                                                                                                                                                                                                                                                      | k. Apply the remaining patches to all cards on this NE with DCC DS1-IMA cards.<br>l. Take an image of the inactive cards on this NE with DCC GigE cards that were not imaged in step f or step j. Refer to <a href="#">Performing a device image using the NPM on page 2327</a> for steps on performing a device image. Select SmartImage->MG9KDEVICES.<br>m. Use the images created in the previous steps to upgrade all the of the cards on all the remaining NEs to be upgraded to SN09U. |   |
| <b>9</b> Configure Community of Influence, if applicable                                                                                                                                                                                                                                                                                                | Go to the Subnet View, click the affected NE, and select Configuration->Internodal ESA from the menu bar. Make any required Community of Interest changes.<br>Refer to procedure "Provisioning Internodal ESA and community of interest" in <i>MG 9000 Configuration Management</i> , NN10096-511.                                                                                                                                                                                           |   |
| <b>Note:</b> This is a safe stopping point.                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |   |
| After all NEs are at SN09U and there is no need to downgrade to SN08 or SN09 proceed to the next step:<br><br><b>Note:</b> If it is necessary to downgrade the MG 9000 and MG 9000 Manager, perform procedure <a href="#">Downgrading the MG 9000 and MG 9000 Manager from SN09U to SN08 or SN09 on page 2495</a> . Otherwise proceed to the next step. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |   |
| <b>Note:</b> Proceed to the next step only after the one night process (ONP) is complete.                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |   |
| <b>10</b>                                                                                                                                                                                                                                                                                                                                               | This procedure is complete. If applicable, return to the higher lever task flow or procedure that directed you to this procedure.                                                                                                                                                                                                                                                                                                                                                            |   |



## Upgrading the MG 9000 using the mg9kuptool

The upgrade of the MG 9000 is performed using the command line interface (CLI) mg9kuptool.

**Note:** Fix upgrade problems by using the [Software upgrade errors and problem resolution on page 1613](#). Once the problem has been resolved, re-enter the command which failed for the single NE. After successfully completing the command for the single NE, continue with the next step in the mg9kuptool for all NEs being upgraded. For example, while downloading NE 1, 2, and 3, NE 2 fails. Clear the download failure with NE 2, open another mg9kuptool, and download NE 2. Once NE 1, 2, and 3 have all completed the download step successfully, proceed with the precheck step for NEs 1, 2, and 3.

The mg9kuptool enables the upgrade process to be separated into the following two time frames, thereby using operating company personnel time more effectively.

- preparation phase, which includes downloading of the card loads that takes place outside of the maintenance window, with no service impact

**Note:** This phase can be performed 24-48 hours prior to the maintenance window.

- upgrade phase, which occurs within the maintenance window

The following table shows the command options used in the mg9kuptool.

### mg9kuptool command options

| Time frame                                         | Command options | Description                                                                                                                                                                                                                                                                          |
|----------------------------------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preparation phase - outside the maintenance window | -configure      | Provides the configuration of the upgrade tool. This includes the list of NEs to upgrade, the name and location of the card loads.                                                                                                                                                   |
|                                                    | -prepare        | Provides information to the user to determine if the system is prepared for the upgrade. It is executed for each node in the target list <-n>.                                                                                                                                       |
|                                                    | -download       | Downloads the card loads as defined in the upgrade plan. It is executed for each node in the target list <-n>.                                                                                                                                                                       |
|                                                    | -precheck       | Reviews the overall system health of each node in the target list <-n> in preparation for the upgrade. Any problems discovered are returned so that action can be taken to correct the issue before the upgrade begins.                                                              |
| Upgrade phase - inside the maintenance window      | -upgrade        | Executes the actual upgrade process defined in the upgrade plan. It is executed for each node in the target list <-n>. When the upgrade is complete, all available patches will be applied.                                                                                          |
|                                                    | -postcheck      | Determines if any alarms were raised and reports any patches that were not applied. This command is executed for each node in the target list <-n>.                                                                                                                                  |
|                                                    | -query          | Provides status information regarding the upgrade process for each node in the target node list <-n>.                                                                                                                                                                                |
|                                                    | -abort          | Terminates the upgrade step being executed for each node in the target node list <-n>.                                                                                                                                                                                               |
|                                                    | -n              | Describes the list of nodes on which to apply the operation.<br><br>This is a comma separated list of NE numbers. If the list is specified as ALL then the operations is applied to all nodes in the plan. This option may be used on all commands except <configure> and <prepare>. |

When the mg9kuptool is executed, with or without options, an MGEM714 log is output. The MGEM714 log is accessible from custlog.

For information on retrieving custlog, refer to "Retrieving MG 9000 logs" in *MG 9000 Fault Management*, NN10074-911.

## Limitations and restrictions

The following limitations and restrictions apply to the use of the mg9kuptool.

- Do not use the **abort** option from another uptool when the configure command is in progress. Since the **configure** option creates an upgrade plan for all of the network elements, the abort command issues on a particular network element will not affect the in progress configure command. However, the configure command can be aborted by typing Ctrl and C key.
- The mg9kuptool does not prevent two users from modifying the configuration data. However, this could produce unexpected results.
- Configure only the NEs which should be upgraded at the same time. However, the number of NEs that can be configured simultaneously is four.
- Minor and Warning alarms on the NEs are not indicated as an error since the MG 9000 will allow upgrades on the cards.
- The maximum number of mg9kuptool sessions that can be launched is five.
- When the user performs the download command, the MG 9000 will download the specified load, even if the MG 9000 already has that load.
- After a successful download command is performed on a card, the upgrade command will download a new patched image (PI) only if the requested PI base loadname is different from the PI base loadname specified for the prepare download. Note that patch content does not alter the PI base loadname.
- If a new image of an existing MG 9000 load is created, the only way the new load can be downloaded to the cards is to use the download command.
- The download command is not supported for card types MTA and XDSL.
- The mate load functionality on the MG 9000 does not copy over prepare (prep) download files.

- The mg9kuptool provides support only for a full node upgrade. The mg9kuptool does not allow
  - single cards to be upgraded
  - protection group upgrades
  - load from mate
- If an upgrade fails, there is no retry mechanism. However, if all cards of a specific type (for example, ITP cards) are running the desired load and do not have a load in the prep download area, this card type is skipped during the upgrade command. This assumes that the upgrade command is re-entered due to some failure. Patching of these cards is not skipped.
- The abort command stops processing the card type which is upgrading once the MG 9000 completes the command it is currently processing (such as, once the apply step is complete). If other card types are already upgraded, they remain on the upgraded or downgraded load.
- Auto processes on the NPM are not automatically turned off nor automatically turned on. The customer must turn off auto processing at the NPM prior to upgrading. The precheck only alerts the customer to ensure auto processes are turned off in the NPM. The upgrade and postcheck alerts the customer to manually check and turn auto processing on again.
- The download and upgrade times are only estimates.
- The following limitations apply to MTA and xDSL cards as part of the mg9kuptool upgrades:
  - Prior to upgrading MTA or xDSL cards, the MG 9000 Manager verifies that all the cards are in an Unlocked/Enabled state. If any card is not in the correct state, the MG 9000 Manager will not perform the upgrade.
  - To upgrade MTA and xDSL cards, the MG 9000 Manager will lock the card, download the load to the card, and then unlock the card. The order in which the MG 9000 Manager upgrades XDSL or MTA cards cannot be specified as part of the upgrade.
  - The lock request of an xDSL card will fail if the card has an active call. If the lock request fails for a given xDSL card, the MG 9000 Manager will note the failure and attempt to upgrade the remaining xDSL cards. Once the MG 9000 Manager has upgraded the remaining xDSL cards, the MG 9000 Manager will halt the upgrade process. The MG 9000 Manager will report that some of the xDSL cards could not be upgraded.

- If the download or unlock of any MTA or XDSL card fails, the MG 9000 Manager immediately halts the upgrade process.
- If an MTA or xDSL card already has the load file specified in the upgrade request, the MG 9000 Manager will consider the card already upgraded and move on to the next card to upgrade.
- When upgrading xDSL cards, the MG 9000 Manager can upgrade only those cards with supported hardware. If a given xDSL card does not have a CLEI code of VA1AAAAAA, the MG 9000 Manager will skip that card and move on to the next card to upgrade.
- If the user aborts an upgrade while the MG 9000 Manager is upgrading the xDSL or MTA cards, the MG 9000 Manager will return all cards to an unlocked state. However, the MG 9000 Manager will not roll back the loads on any of the cards. For instance, assume the user is upgrading all five xDSL cards on a given node. Assume the user aborts the upgrade after the first two cards have upgraded and a third card is in the process of upgrading. The MG 9000 Manager halts the upgrade process after the third card completes its upgrade. In the end, three XDSL cards are running the new load and two XDSL cards are running the old load.
- When the user enters the upgrade command, normally the cards already have a load in the prep load area and do not require another download from the SDM. Exceptions to this are if
  - the card does not have a prep download file
  - the card's prep download file contains a different base load name from the specified load file

## Prerequisites

The mg9kuptool requires secure access by performing a telnet over Secure SHell (SSH). Root privileges are required to use the mg9kuptool.

## Action

Perform the following procedure to upgrade the component.

### Upgrading the MG 9000 from SN08 or SN09 to SN09U using the mg9kuptool without options

*At the MG 9000 Manager workstation CLI (server for t1400/N240 simplex or active unit on N240 cluster)*

1

#### ATTENTION

Steps [1](#) through [8](#) must be executed outside the maintenance window using the mg9kuptool. This can be performed 24 to 48 hours prior to the maintenance window.

Use the query option in the mg9kuptool script to check the status of the NEs prior to the upgrade. Upgrade can be completed only on the NEs for which download and precheck has been completed prior to the maintenance window. If the configure option is executed, this will reset the upgrade plan and the user must repeat the steps again.

Log in to the server through the console port using the root user id and password by typing

```
znc0y0jm console login: root
```

The system responds with the following:

Password:

```
<enter the root password>
```

2 Enter the password.

- 3 To start the mg9kuptool in interactive mode, type
- ```
# /opt/nortel/mg9ksrv_09_1/bin/mg9kuptool.sh
```

The system responds with the following

```
1 configure
2 prepare
3 download
4 precheck
5 upgrade
6 postcheck
7 abort
8 query
x exit
```

Please select an option:

Note: From another telnet window, another mg9kuptool session can be launched and the number next to the query option can be entered to monitor the progress of any step throughout the upgrade.

- 4 Ensure all loads are FTPd to the SDM/CBM.

Note: All loads must be FTPd to the SDM/CBM before proceeding. Even missing a single load prevents moving ahead. The load list is: MTA, DSL, DS1, ABI, ITP, ITX, SCO, SCG, and SCI.

- 5 To configure an NE, or up to 20 NEs for upgrade, type.

\$ 1

The system responds with the following:

Which NE(s) do you want to upgrade/downgrade?
Enter NE number. If more than 1 NE, separate
them with commas (e.g. 8,9)?

Enter a directory where the loads reside?
(Default: /swd/mg9k)

Note 1: When a new upgrade plan is created using the Configure option, it will overwrite the existing plan. For example, if NEs 1 and 2 are configured in the first plan and if the technician plans to configure a second plan with NEs 3 and 4, it will overwrite the existing plan for NEs 1 and 2. Use the Configure option with care. Contact Nortel support for assistance.

Note 2: To identify the NEs to be upgraded, go the MG 9000 Manager. From the Subnet View, click once on an MG 9000 icon. From the menu bar, select Configuration->View/Modify NE Properties and retrieve the NE number from the Properties view.

- a Enter the NE number, for example

8

- b Enter the directory where the loads reside or accept the default by pressing Enter.

The system responds with the following:

220 wnc0y0m0 FTPD Server (Version 21.43.4.0
Oct 20 2004) ready.

Loads found on system:

MTAG08BW_GZ

MTAG09AK_GZ

MTAG09AB_1_GZ

Enter a load name for the MTA card?

- c** Enter the MTA card load to be used, for example

MTAG09AB_1_GZ

The system responds with the following:

Loads found on system:
DSLA08BW.bin
DSLA09AE.bin
DSLA09AB_1.bin

Enter a load name for the XDSL card?

- d** Enter the DSL card load to be used, for example

DSL09AB_1.bin

The system responds with the following:

Loads found on system:
DS1G09AL_GZ.tar
DS1G09AB_1_GZ.tar
DS1G08BW_GZ_wk39.tar

Enter a load name for the DS1 card?

- e** Enter the DS1 card load to be used, for example

DS1G09AB_1_GZ

The system responds with the following:

Loads found on system:
ABIG09AL_GZ.tar
ABIG09AB_1_GZ.tar
ABIG08BX_GZ_wk39.tar
Enter a load name for the ABI card?

- f** Enter the ABI card load to be used, for example

ABIG09AB_1_GZ

The system responds with the following:

Loads found on system:
ITPA09AL_GZ.tar
ITPA09AB_1_GZ.tar
ITPA08BY_GZ_wk42.tar
Enter a load name for the ITP card?

- g** Enter the ITP card load to be used, for example

ITPA09AB_1_GZ

The system responds with the following:

Loads found on system:

ITXA09AL_GZ.tar

ITXA09AB_1_GZ.tar

ITXA08BW_GZ.tar

ITXA08BW_GZ_wk39.tar

Enter a load name for the ITX card?

- h** Enter the ITX card load to be used, for example

ITXA09AB_1_GZ

The system responds with the following:

Loads found on system:

SCOA09AL_GZ.tar

SCOA09AB_1_GZ.tar

SCOA08BW_GZ_wk39.tar

Enter a load name for the SCO card?

- i** Enter the SCO card load to be used, for example

SCOA09AB_1_GZ

The system responds with the following:

Loads found on system:

SCIA09AL_GZ.tar

SCIA09AB_1_GZ.tar

SCIA08BW_GZ_wk42.tar

Enter a load name for the SCI card?

- j** Enter the SCI card load to be used, for example

SCIA09AB_1_GZ

The system responds with the following:

Loads found on system:

SCGA08AL_GZ.tar

SCGA09AX_GZ.tar

SCGA09AB_1_GZ.tar

Enter a load name for the SCG card?

- k** Enter the SCG card load to be used, for example

SCGA09AB_1_GZ

6 To prepare the NE(s) for upgrade, type

\$ 2

Note 1: If faults appear, clear them and return to this step and re-enter the command.

Note 2: If the prepare step fails for any reason, review the alarm raised at the Alarm Browser in the MG 9000 Manager and refer to [Software upgrade errors and problem resolution on page 1613](#) to correct the failure. Once the failure reason has cleared, open a new mg9kuptool window, choose option 2, and prepare the NE. Once the failed NE has completed the prepare step and other NEs have completed the prepare step, proceed with the download step on all NEs in the first mg9kuptool window.

Note 3: The Prepare command normally takes less than 5 minutes. However, if no response is received within 5 minutes, perform the following steps to escape this situation:

1. Open another mg9kuptool session in another window and enter the Abort command.
2. Press Ctrl+C in the window that is hung in the Prepare state to end the mg9kuptool session.
3. Launch a new mg9kuptool session.

The system responds with the following:

```
Enter the node number or the node number list
for the prepare request. Press Enter to
continue.
```

The system responds with the following:

```
Have you put the patch files on the NPM? Y/N
```

- a Verify that patch files have been moved to the NPM and are available for loading and patching activities. After this is complete, type

Y

The system responds with the following:

```
Upgrading to loads:
/swd/mg9k/MTAG09AB_1_GZ
/swd/mg9k/DSLA09AB_1
/swd/mg9k/DS1G09AB_1_GZ.tar
patchlist:
none
/swd/mg9k/ABIG09AB_1_GZ.tar
patchlist:
AMZ05UFM
/swd/mg9k/ITPA09AB_1_GZ.tar
patchlist:
AMZ06UFM
HDD13UFM
HDD14UFM
HDD15UFM
/swd/mg9k/ITXA09AB_1_GZ.tar
patchlist:
none
/swd/mg9k/SCOA09AB_1_GZ.tar
patchlist:
AMZ07UFM
AMZ08UFM
HDD16UFM
/swd/mg9k/SCIA09AB_1_GZ.tar
patchlist:
AMZ08UFM
/swd/mg9k/SCGA09AB_1_GZ.tar
patchlist:
AMZ08UFM
```

Please compare the patchlists above against the Nortel web page.

```
NE# 8: time to download is 60 minutes
time to upgrade is 30 minutes
time to patch is 27 minutes
```

Note: Look for any errors after all the NE upgrade and patching times are listed.

- 7 To download the software to the cards, type

\$ 3

The system responds with the following:

Enter the node number or node number list for the download request:

Press Enter to continue.

Note 1: Wait for the system response. This may take a few minutes, depending on the size of the MG 9000 being downloaded. Also look for any error messages.

Note 2: If the download fails, it can be due to an SSH key mismatch. Remove the SSH keys using the procedure [MG 9000 SN08 or SN09 to SN09U upgrade checklist](#), step 6 on [page 1584](#)

Note 3: If the prepare step fails for any reason, review the alarm raised at the Alarm Browser in the MG 9000 Manager and refer to [Software upgrade errors and problem resolution on page 1613](#) to correct the failure. Once the failure reason has cleared, open a new mg9kuptool window, choose option 2, and prepare the NE. Once the failed NE has completed the prepare step and other NEs have completed the prepare step, proceed with the download step on all NEs in the first mg9kuptool window.

- 8 To perform a precheck of the system prior to upgrading the system, type

\$ 4

Note 1: If faults appear, clear them and return to this step and re-enter the command. If necessary, repeat until no faults appear.

Note 2: If the prepare step fails for any reason, review the alarm raised at the Alarm Browser in the MG 9000 Manager and refer to [Software upgrade errors and problem resolution on page 1613](#) to correct the failure. Once the failure reason has cleared, open a new mg9kuptool window, choose option 2, and prepare the NE. Once the failed NE has completed the prepare step and other NEs have completed the prepare step, proceed with the download step on all NEs in the first mg9kuptool window.

The system responds with the following:

```
Enter the node number or node number list for
the precheck request:
```

Press Enter to continue.

9 To proceed with the upgrade of the system, type

```
$ 5
```

Note 1: This step is performed in the maintenance window.

Note 2: Check the upgrade time for each NE that was displayed in the prepare. If multiple NEs are being upgraded, add the upgrade times together to determine the amount of time required for the upgrade to run.

Note 3: Wait for the system to respond before proceeding. To check the status of the upgrade process, start another telnet over SSH process and perform a query using procedure [Query the status of an upgrade step on page 1604](#).

Note 4: If the prepare step fails for any reason, review the alarm raised at the Alarm Browser in the MG 9000 Manager and refer to [Software upgrade errors and problem resolution on page 1613](#) to correct the failure. Once the failure reason has cleared, open a new mg9kuptool window, choose option 2, and prepare the NE. Once the failed NE has completed the prepare step and other NEs have completed the prepare step, proceed with the download step on all NEs in the first mg9kuptool window.

The system responds with the following:

```
This process will affect DSL traffic and should
be performed during a maintenance window only.
```

```
Enter the node number or node number list for
the upgrade request:
```

Press Enter to continue.

Note: If multiple NEs are being upgraded and one NE fails the upgrade process, perform a postcheck of NEs that successfully completed the upgrade before attempting to fix the NE. Proceed to the next step to perform the postcheck. If the postcheck on the successful NEs is not performed, it will not be known if all the patches were applied successfully on the NEs unless the upgrade is attempted again.

- 10 To perform a postcheck of the system after the upgrade of the system is complete, type

\$ 6

Note: If the prepare step fails for any reason, review the alarm raised at the Alarm Browser in the MG 9000 Manager and refer to [Software upgrade errors and problem resolution on page 1613](#) to correct the failure. Once the failure reason has cleared, open a new mg9kuptool window, choose option 2, and prepare the NE. Once the failed NE has completed the prepare step and other NEs have completed the prepare step, proceed with the download step on all NEs in the first mg9kuptool window.

The system responds with the following:

```
Enter the node number or node number list for
the postcheck request:
```

Press Enter to continue.

Did any NEs fail to upgrade? Fix the problem and go back to step [9](#).

- 11 This procedure is complete. Go to step [8 on page 1585](#) of the [MG 9000 SN08 or SN09 to SN09U upgrade checklist](#) and continue with the upgrade process.

Note: If the mg9kuptool has locked up, use Ctrl+C to come out of the tool lockup. If a download or upgrade step is in progress, Ctrl+C will behave the same as the Abort command used in the following procedure.

Aborting an upgrade step

At the MG 9000 Manager workstation CLI

- 1 Log in as root by typing

```
$ su - root
```

The system responds with the following:

Password:

<enter the root password>

- 2 Enter the password.

- 3 To start the mg9kuptool in interactive mode, type

```
# /opt/nortel/mg9ksrv_09_1/bin/mg9kuptool.sh
```

The system responds with the following

```
1 configure
2 prepare
3 download
4 precheck
5 upgrade
6 postcheck
7 abort
8 query
x exit
```

Please select an option:

- 4 To abort an upgrade step, type

```
$ 7
```

Enter the node number or node number list for the abort request:

Press Enter to continue.

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Query the status of an upgrade step

At the MG 9000 Manager workstation CLI

- 1 Log in as root by typing

```
$ su - root
```

The system responds with the following:

Password:

<enter the root password>

- 2 Enter the password.

- 3 To start the mg9kuptool in interactive mode, type

```
# /opt/nortel/mg9ksrv_09_1/bin/mg9kuptool.sh
```

The system responds with the following

```
1 configure
2 prepare
3 download
4 precheck
5 upgrade
6 postcheck
7 abort
8 query
x exit
```

Please select an option:

- 4 To query the status of the upgrade process, type

```
$ 8
```

Enter the node number or node number list for the query request:

<the displayed default is the list of all NEs in the plan>

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Completing the MG 9000 upgrade

Perform the next required upgrade according to the order listed in the table [Component Upgrade Order on page 6](#). The required upgrade is the next component in the list according to your network configuration.

Installing MG 9000 loads into CS 2000 Core Manager from CD-ROM

Purpose of this procedure

This procedure describes how to install the MG 9000 software loads onto the CS 2000 Core Manager from CD-ROM.

When to use this procedure

This procedure is to be used when a maintenance non-computing load (MNCL) software release or standard NCL is delivered to the customer site.

Prerequisites

When supporting an upgrade from SN08 or SN09 to SN09USN09U, ensure the SN08 or SN09 loads are currently in the SDM/CBM in the event there is a need to perform a software downgrade from SN09U to SN08 or SN09.

Action

Installing MG 9000 loads into the CS 2000 Management Tools Manager from CD-ROM

At the CS 2000 Management Tools Manager

- 1 Insert the CD-ROM into the CD-ROM tray. If the unit is a Netra 240 in a cluster configuration, use the active Netra 240 unit. The active unit is identified by a lit USER LED on the front of the unit.

The CD-ROM label for the SAM21 Shelf Controller software includes the product code, MG9K0091, on the lower half of the label.

At the CS 2000 Management Tools console or terminal window

- 2 Log in and then use the su command to gain root privilege.

login: username
Password: <password>
Last login: Fri Jun 30 12:48:18 from <otherhost>
su - root
Password: <password>

- 3 Execute the platform_load_install.sh script by typing
- ```
/opt/nortel/sspfs/Scripts/platform_load_install.sh
```

The system responds with the following.

```
Welcome to the Platform Installation Tool
Version 3.2
```

```
=====
RPM INSTALLATION/REMOVAL
=====
1) Install RPM from CDROM 2) Install RPM from
 Disk
3) Uninstall RPM 4) Query all RPMs

OTHER
=====
C) Change Rotation Parameters P) View Rotation
 Parameters
V) MG9K Platform Version X) Exit
Installed
```

Please choose one of the following:

- 4      To install the software type 1 and press the Return key.
- The screen clears and the contents of the .rpm package are displayed.
- Note:** If the message There is no cd in the CDROM drive, please check drive is displayed, ensure that the CD-ROM is inserted in the tray for this unit.
- 5      To proceed with the software installation, type Y.
- The software is extracted from the .rpm package. The .rpm package is transferred to the CS 2000 Core Manager.
- 6      Enter the root password for the CS 2000 Core Manager. The software is installed on the CS 2000 Core Manager.
- 7      Enter the Eject command to eject the CD from the CD-ROM drive.
- ```
# eject
```
- 8 Log out of the CS 2000 Management Tools server.
- 9 Remove the CD-ROM.
- 10 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Preparing MG 9000 software delivered through ESD for an upgrade

Purpose of this procedure

This procedure describes how to prepare MG 9000 software delivered through Electronic Software Delivery (ESD) method for an upgrade of the MG 9000.

Note: For information on how to install MG 9000 load from CD-ROM, refer to procedure [Installing MG 9000 loads into the CS 2000 Management Tools Manager from CD-ROM on page 1606](#).

When to use this procedure

Use this procedure after you perform the procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#).

Prerequisites

Your operating company must have an ESD agreement with Nortel Networks. When the agreement was established, the operating company furnished Nortel Networks with the location of an electronic drop box and a user name and password pair for delivering software loads. When Nortel Networks delivers a software load to the drop box, an electronic mail notification is sent to the e-mail address specified by the telephone operating company when the ESD agreement was established.

Action

At a CS 2000 Management Tools server terminal

- 1 Make sure you are logged in as root. If necessary, perform the following steps.
 - a Change to the root user by typing

```
$ su -
```

and pressing the Enter key.
 - b When prompted, enter the root password.
- 2 List the contents of the /tmpmnt directory by typing

```
# ls -l /tmpmnt/noarch
```
- 3 Record the name of the .rpm file.
- 4 Execute the installation script by typing

```
# platform_load_install.sh
```

- 5 When prompted, select the option Install RPM from Disk by typing:
`> 2`
- 6 When prompted, enter the .rpm filename.
- 7 When prompted, enter the location of the .rpm file by typing:
`# /tmpmnt/noarch`
The system displays the contents of the .rpm file package.
- 8 To proceed with the software installation, type:
`y`
The software is extracted from the .rpm package. The .rpm package is transferred to the CS 2000 Core Manager.
- 9 Enter the root password for the CS Core 2000 Manager.
The system installs the software on the CS 2000 Manager, the transferred .rpm package is deleted
The system installs the software on the CS 2000 Core Manager.
After the load file is installed on the CS 2000 Core Manager, the transferred .rpm package is deleted from the CS 2000 Core Manager.
Note: An additional confirmation prompt can display requesting acceptance of the RSA key. Confirm the following sample prompt by typing yes.

RSA key fingerprint is:
26:b5:2a:97:49:cb:a6:7d:ee:c2:db:96:97:db:34:a5.
Are you sure you want to continue connecting (yes/no)?
- 10 Exit the installation program by typing:
`#x`
- 11 Unmount the ESD file. Perform procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).
- 12 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Provisioning a floating IP address

Purpose of this procedure

The MG 9000 Manager assigns the floating IP address to the card being upgraded dynamically. The floating IP address is provisioned from the MG 9000 Manager as described in the following procedure. Provisioning a floating IP address should be performed during initial installation and commissioning. The floating IP address persists in the MG 9000 Manager data.

When to use this procedure

This procedure is provided only if the need arises to change, correct, or add the floating IP address.

Prerequisites

Before beginning, ensure you have the correct privileges to perform this procedure.

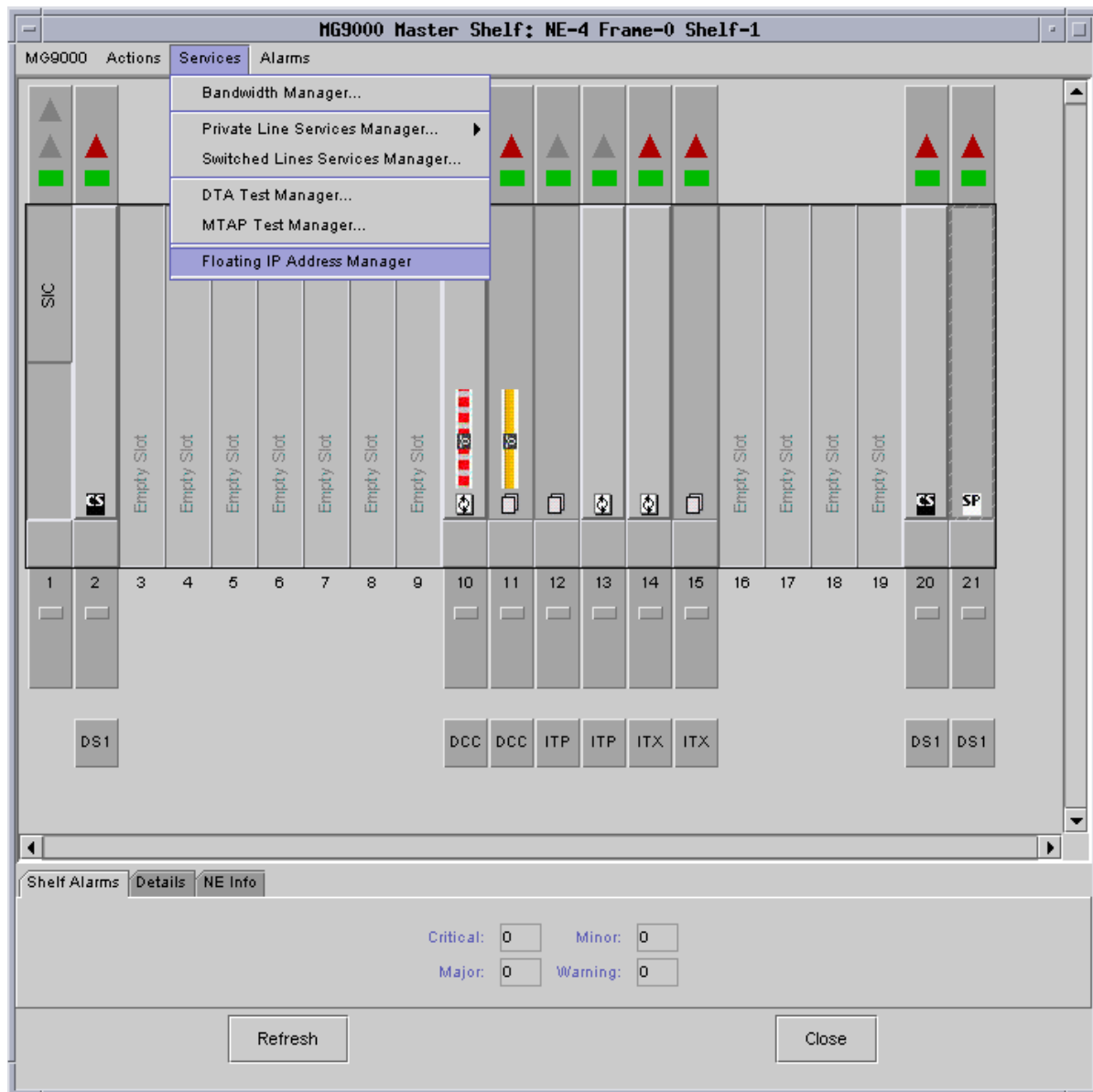
Contact your network administrator to obtain a new IP address when a new floating IP address must be provisioned.

Action

Provisioning a floating IP address

At the MG 9000 Manager

- 1 Verify whether a floating IP address has already been provisioned at the MG 9000 Manager by selecting Services->Floating IP Address Manager from the menu bar of any Frame, Shelf, or Card View. This address must be in the same subnet as the MG 9000.
- 2 To provision a floating IP address in the MG 9000 Manager if necessary, perform the following steps:
 - a From any Frame, Shelf, or Card view select the menu Services. From within Services select Floating IP Address Manager, as shown in the following figure.

Floating IP Address Manager accessed from Shelf View

- b** Enter the IP address in the Floating IP Address Manager and select Apply. The address will be displayed under existing IP addresses. When finished, select Close.

Floating IP Address Manager View



- c If the floating IP address must be replaced, delete the entry first. To delete an entry select the entry, select the Delete check box, then press Apply. When finished select Close.
 - d If the floating IP address is correct, select Close.
- 3 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Software upgrade errors and problem resolution

The following table lists the potential errors that arise at various steps in the MG 9000 software upgrade process, the cause, and recovery actions.

MG 9000 software upgrade errors and problem resolution

Error type	Possible cause	Recovery action
Upgrade provisioning errors		
Invalid file type	This error is received if the card type selected is invalid for the load file name provided. Every load file name has the card type embedded within it.	Ensure the load file name is valid for the card type to be provisioned, then try again.
Invalid Version	This error is received if the version number embedded within the load file name is invalid for this gateway. For example, if it is only valid to upgrade to versions 5 or 6 and the loadfile name contains version 8, an error is displayed.	Ensure the load file name version is valid for the attempted upgrade, then try again.
Invalid State	This card is locked or active.	If this card is active and does have a mate, the request will be denied. First Swact/Spare the card to its mate and continue. If this card is inactive, but locked, first unlock the card and continue.

MG 9000 software upgrade errors and problem resolution

Error type	Possible cause	Recovery action
Download errors		
FTP server related	- incorrectSDM loadfile/path permissions - floating IP configuration error - network connection failure identified during the provisioning activity - Preshared keys between the MG 9000 and the MG 9000 Manager do not match	Abort the upgrade. Check provisioned data for validity and provision another upgrade.
Corrupt File	- an incompatible load file provisioned for this card. For instance, if the card type is ITP, the load file name must include ITP. The same is true for other cards. - insufficient memory for an image file	Abort the upgrade. - For the incompatible load file error, check the file name type and provision another upgrade. - For the insufficient memory error, go to dshell and do a filesys/finfo and look at the freespace on the volume. It should be about three times the size of the image file.
Node Not Responding	The card is undergoing a maintenance operation or is in an otherwise invalid state (such as, restarting) or is not running.	Go to the Card View and verify the card status. If the card status appears correct, the error is possibly due to a longer than expected communication delay. Abort the upgrade and try again
Flash exhaust	There is insufficient flash memory to allow the download of the software to the card.	Please retry the Upgrade. If the problem persists, kindly contact Nortel for assistance to restore space on the flash memory.
Apply errors		

MG 9000 software upgrade errors and problem resolution

Error type	Possible cause	Recovery action
State	If this card is Active, an Apply will fail if this card has a mate.	Abort the upgrade. Cause a redundancy action (Swact or Spare) to occur. This card was possibly Inactive during the provisioning of the upgrade. A card is no longer Active when a redundancy action occurs.
Node Not Responding	This card is undergoing a maintenance operation, is in an otherwise invalid state (such as, restarting) or is not running.	Go to the Card View and verify the card status, if the card status appears correct the error is possible due to a longer than expected communication delay. Abort this upgrade and try again.
SwactDataSync Multi-Node Only	Mate cards in a protection group are NOT in data sync; a required Swact has failed or will not be executed	Go to the Card View and lock the card, then go to the Card View for the Inactive mate and unlock the card. The unlock action will cause a restart (since they are not in data sync). Once the Inactive card has completed its restart, attempt to Abort. Note: If after multiple tries data sync is not achieved, contact Nortel Networks for further guidance. Additional upgrades are not possible until this problem is resolved.
SwactMateState Multi-Node Only	For reasons other than not in DataSync, the Active card refuses to give up activity (possibly due to faults on the InActive card).	Determine what the fault state or problem with the InActive card is and correct it. Once the InActive card is in a valid state, attempt to Abort. Note: If you cannot correct the error, contact Nortel Networks for further guidance. Additional upgrades are not possible until this problem is resolved.

MG 9000 software upgrade errors and problem resolution

Error type	Possible cause	Recovery action
SwactMateUnav ailable Multi-Node Only	A communication problem exists between the Inactive and the Active cards. A Swact is not allowed.	Resolve the communication problem. Once the Inactive card is in a valid state, attempt to Abort. Note: If you cannot correct the error, contact Nortel Networks for further guidance. additional upgrades are not possible until this problem is resolved.
SwactError Multi-Node Only	A generic error associated with a Swact request, but enough information cannot be obtained for the Upgrade subsystem to identify the cause.	Contact your maintenance administrator to identify and resolve the problem. Once the card(s) are in a valid state, attempt to Abort. Note: If you cannot correct the error, contact Nortel Networks for further guidance. additional upgrades are not possible until this problem is resolved.
Generic	See the previous entry.	Contact Nortel Networks.
Accept errors		
Node Not Responding	The card is undergoing a maintenance operation, is in an otherwise invalid state (such as restarting) or is not running.	Go to the Card View and verify the card status. If the card status appears correct the error is possibly due to a longer than expected communication delay. Abort the upgrade and try again.
GENERIC	See the previous entry.	Contact Nortel Networks.
Abort errors		
Node Not Responding	The card is undergoing a maintenance operation, is in an otherwise invalid state (such as restarting) or is not running.	Go to the Card View and verify the card status. If the card status appears correct, the error is possibly due to a longer than expected communication delay. Abort this upgrade and try again.

MG 9000 software upgrade errors and problem resolution

Error type	Possible cause	Recovery action
SwactDataSync	Mate cards in a protection group are NOT in data sync; a required Swact has failed or will not be executed	Go to the Card View and lock, then go to the Card View for the inActive mate and unlock the card. The unlock action will cause a restart (since they are not in data sync). Once the inActive card has completed its restart, attempt to Abort. Note: If after multiple tries data sync is not achieved, contact Nortel Networks for further guidance. Additional upgrades are not possible until this problem is resolved.
SwactMateState	For reasons other than not in DataSync, the Active card refuses to give up activity (possibly due to faults on the Inactive card).	Determine the fault state or problem with the inActive card and correct it. Once the Inactive card is in a valid state, attempt to Abort. Note: If you cannot correct the error, contact Nortel Networks for further guidance. Additional upgrades are not possible until this problem is resolved.
SwactMateUnavailale	There is a communication problem between the Inactive and Active cards. A Swact is not allowed.	Resolve the communications issue. Once the Inactive card is in a valid state, attempt to Abort. Note: If you cannot correct the error, contact Nortel Networks for further guidance. Additional upgrades are not possible until this problem is resolved.
SwactError	This is a generic error associated with a Swact request, but enough information cannot be obtained for the Upgrade subsystem to identify the cause.	Contact your maintenance administrator to identify and resolve the problem. Once the card(s) are in a valid state, attempt to Abort. Note: If you cannot correct the error, contact Nortel Networks for further guidance. Additional upgrades are not possible until this problem is resolved.
GENERIC	See the previous entry.	Contact Nortel Networks



Nortel USP Upgrades

ATTENTION

Perform all software upgrade procedures from the alternate boot server, unless otherwise noted. You must have administrative privileges to perform a software upgrade.

New in this release

Feature changes

In SN09U (USP11.1), there are no new feature changes that affect the USP upgrade.

Upgrade paths

Nortel Networks supports the following direct in-service upgrade paths:

- USP10.0.x/SN08 to USP11.1.x/SN09U
- USP11.0.x/SN09 to USP11.1.x/SN09U
- USP11.1.x/SN09U to USP11.1.y/SN09U (maintenance release)

If upgrading from a USP9.0 or lower release, upgrade to USP10.0.x before continuing with this upgrade.

Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

Time to complete an upgrade

The following table lists the tasks to upgrade USP software and the estimated time to complete each task.

Table 1 Estimated time to complete a software upgrade

Task	Card	Time
Preparing for the upgrade		35 minutes
Upgrading the software	RTC	20 minutes per card
	IPLINK	15 minutes per card
	SS7IPLINK	15 minutes per card
	NPC	15 minutes per card
	NPE	15 minutes per card
	NPS	15 minutes per card
	other link nodes	5 minutes per node
	CC card	2 minutes per card
Completing the upgrade		30 minutes
Total estimated upgrade time		4 to 8 hours

Large systems and small systems

A small USP system typically requires less time to perform an upgrade than a large USP system.

- A small USP system consists of one or two shelf systems. You can upgrade most small USP systems in a single six-hour maintenance window.
- A large USP system consists of three or more shelves. Most large USP systems require two or more six-hour maintenance windows for a software upgrade.

The following table lists sizes of USP systems and the time to complete a software upgrade for each size.

Table 2 USP systems and upgrade times

System size	Length of time	Maintenance windows
1 shelf	2 hours	1
2 shelves	5 hours	1
3 shelves	8 hours	2
4 shelves	10 hours	2
5 shelves	12 hours	2
8 shelves	20 hours	4

Service impacts

The upgrade of USP software does not impact service. Traffic is maintained through redundant links configured on different link cards. A loss of network redundancy occurs when a blade is taken out of service.

The CLI is not available for use during an upgrade.

Additional information

This section provides additional information on USP software upgrades.

Auto-negotiate

Auto-negotiate for the CS LAN can be enabled during a USP software upgrade.

Core Bounce cutover

The procedures for cutover from Core Bounce to Direct Messaging are not performed during an upgrade. Contact Nortel Networks for more information.

In-service cutover

An in-service cutover is not performed during an upgrade. Contact Nortel for more information.

Routemaster

The Routemaster application is beyond the scope of upgrades. Contact Nortel for more information on using Routemaster for end office consolidation.

USP software releases

USP software releases use the following naming convention:

USPnn.n.n

The first and second numbers identify a major USP software release, and the third number identifies a maintenance release.

The following table lists examples of USP major releases and USP maintenance releases.

Table 3 USP software releases

Major release	Maintenance releases
USP10.0.0	USP10.0.3
USP10.1.0	USP10.1.2
USP11.0.0	USP11.0.3

Scope of document

This document supports major release upgrades and maintenance release upgrades.

- A major release upgrade is an upgrade from one release to a another release. Following is an example of a major upgrade.
USP10.0.3 to USP11.0.0
- A maintenance release upgrade is an upgrade from one release to a another release within the same major release.
USP10.0.2 to 10.0.3

Upgrade order**Small systems and one maintenance window**

The card upgrade order for a one maintenance window upgrade varies slightly for one- and two-shelf systems.

For a one-shelf system, upgrade the following cards:

- upgrade RTC 15
- upgrade CC1 in slot 1

- upgrade the link cards
- upgrade the NP cards
- upgrade CC2 in slot 18
- upgrade RTC 12

For a two-shelf system, upgrade the following cards:

- upgrade RTC 15
- upgrade CC1 in slot 1 on the control shelf
- upgrade CC1 in slot 1 on the extension shelf
- upgrade the link cards on the extension shelf
- upgrade the link cards on the control shelf
- upgrade the NP cards in the control shelf
- upgrade the NP cards in the extension shelf
- upgrade CC2 in slot 18 on the control shelf
- upgrade CC2 in slot 18 on the extension shelf
- upgrade RTC 12

For a list and detailed procedures of the card upgrade order for a one-and two-shelf system, see [Upgrading the system nodes for one maintenance window upgrades on page 1663](#).

Large systems and multiple maintenance windows

When performing a large system upgrade that requires more than one maintenance window to complete, you must upgrade the entire Control CAM shelf and one card for each unique card type before the end of the first maintenance window. The subsequent windows are used to upgrade the remaining cards in the system.

For upgrades spanning multiple maintenance windows, upgrade the following cards:

- upgrade RTC 15
- upgrade CC1 in slot 1 on the control shelf
- upgrade link cards in the control shelf
- upgrade NP cards in the control shelf
- upgrade CC2 in slot 18 on the control shelf
- upgrade one card for each unique card type on any extension shelf

- SWACT RTC 12; if you cannot SWACT RTC 12, upgrade a card of a type that you have not yet upgraded
- perform test calls and monitor the system for at least 15 minutes to evaluate your acceptance of the upgrade
- upgrade RTC 12

Note: The RTC12 upgrade completes the upgrade requirement for the first maintenance window. You can continue the upgrade in this current maintenance window and in the next maintenance window.

- upgrade CC1 in slot 1 on the extension shelf
- upgrade the link cards on the extension shelves
- upgrade the NP cards in the extension shelves
- upgrade CC2 in slot 18

For a list and detailed procedures of the card upgrade order for a multiple shelf systems, see [Upgrading the system nodes for multiple maintenance window upgrades on page 1665](#).

NP chain upgrade considerations

The four possible NP card configurations to consider when planning to perform an upgrade over multiple maintenance windows are as follows:

1. All NP cards on the Control Shelf if:

- both NPCs on the control shelf
- all the chain related NPx cards on the control shelf

All NP cards will be upgraded during the first window as all cards must be upgraded in the Control shelf during the first window.

2. Only the NPC on the Control Shelf and other NP cards on Extension shelves if:

- both NPCs are on the control shelf
- at least one chain associated NPx on an extension shelf

You must finish upgrading both NPC associated chains and all NPx cards on the first maintenance window.

3. NPCs on an Extension shelf and other NP cards on the Control shelf if:

- both NPCs are on an extension shelf
- at least one chain related NPx provisioned on the control shelf

You must finish upgrading all NPx cards associated to that chain in the first maintenance window.

Note: Nortel Networks suggests locating both NPCs on the control shelf to avoid extension shelf isolation.

4. All NP cards on Extension shelves if:

- both NPCs are on one extension shelf
- all the chain associated NPx also provisioned on extension shelves

You can choose to finish upgrading one NPC associated chain and one NPS associated chain (If an alternate NPS is already involved with the selected NPC associated chain, the NPS associated chain does not have to be upgraded in the first maintenance window).

Note: Nortel Networks suggests locating both NPCs on the control shelf to avoid extension shelf isolation.

System capacity

The software upgrade procedure can impact the system capacity. This means that additional disk space on the OAMP workstation and the RTC system nodes are required for converting existing databases.

The pre-checking procedure checks for adequate disk space on the RTC system nodes. A message box informs you if your disk space is too low. If disk space is too low, delete any old snapshots.

Once the update is complete, the additional disk space is no longer required and is made available for use.

System performance

The software upgrade procedure can impact USP system performance in the following ways:

- An upgrade database conversion is necessary due to internal USP data format changes. This affects the RTC system node in slot 15 (the inactive RTC system node). The RTC in slot 15 is the first system node upgraded to the new version.
- Depending on the scope of data format changes, the inactive RTC in slot 15 takes approximately 20 minutes to load and convert internal data to the new format. During this time, the inactive RTC

system node is not enabled and the system operates with a single RTC system node.

- You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade. This is because the Link system nodes must be reloaded during the upgrade. As a result, all SS7 traffic is rerouted from the links and linksets that reside on the disabled Link system node.

System limitations during upgrade

During a software upgrade, the system prohibits the following actions, listed by subsystem:

- System administration
 - adding, deleting, or modifying users
 - setting the time of day
 - changing passwords
- System management
 - modifying the system name or shelf names
 - adding or deleting RTC, CC, or application system nodes
 - modifying the IP address or the PEC of the RTC system nodes
- SS7 management (MTP Level 3)
 - adding, deleting, or modifying a system identity
 - adding, deleting, or modifying a capability code
 - adding, deleting, or modifying links, linksets, linkset groups, combined linksets, or routesets
 - adding, deleting, or modifying ASP, AS, ASP Paths, AS destinations, or AS assignments
- SS7 management (MSU/Gateway Screening)
 - deleting gateway screening criteria files
- SS7 management (Global Title Translations)
 - adding, deleting, or modifying all GTT results
 - adding, deleting, or modifying all GTA results
 - adding, modifying, or deleting GTT translation type text
 - adding, modifying, or deleting GTT translations

- SS7 management (Special Study Operational Measurements)
 - adding, deleting, or modifying SSOMs
 - enabling/disabling SSOMs on linksets
- SS7 management (SCCP)
 - adding or deleting remote point codes (RPCs)
 - adding, deleting, or modifying remote subsystems (RSSs)
 - adding or deleting concerned point codes
 - adding, deleting, or modifying local subsystems (LSSs)
 - adding or deleting
 - local subsystems concerned point codes (CPCs)
 - adding or deleting LSS instances
- IPS7 management
 - adding, deleting, or modifying application server process
 - adding, deleting, or modifying application server process path
 - adding, deleting, or modifying application server
 - adding, deleting, or modifying application server destination
 - adding, deleting, or modifying application server assignment

OAMP workstation functionality

The GUI allows multiple sites to be configured on an OAMP workstation at one time. Since the sites are not upgraded at the same time, the following conditions apply:

- If the GUI is upgraded and the USP is not, you can access existing USP capabilities. You cannot use the new capabilities.
- The new USP GUI allows you to log in to a previous system, a new system, or a USP system that has an upgrade in progress.
- You cannot use a previous version of the GUI to log in to a newer version of the USP software.
- Only one version of the GUI can be installed at a time, because the GUI upgrade requires the conversion of local files.

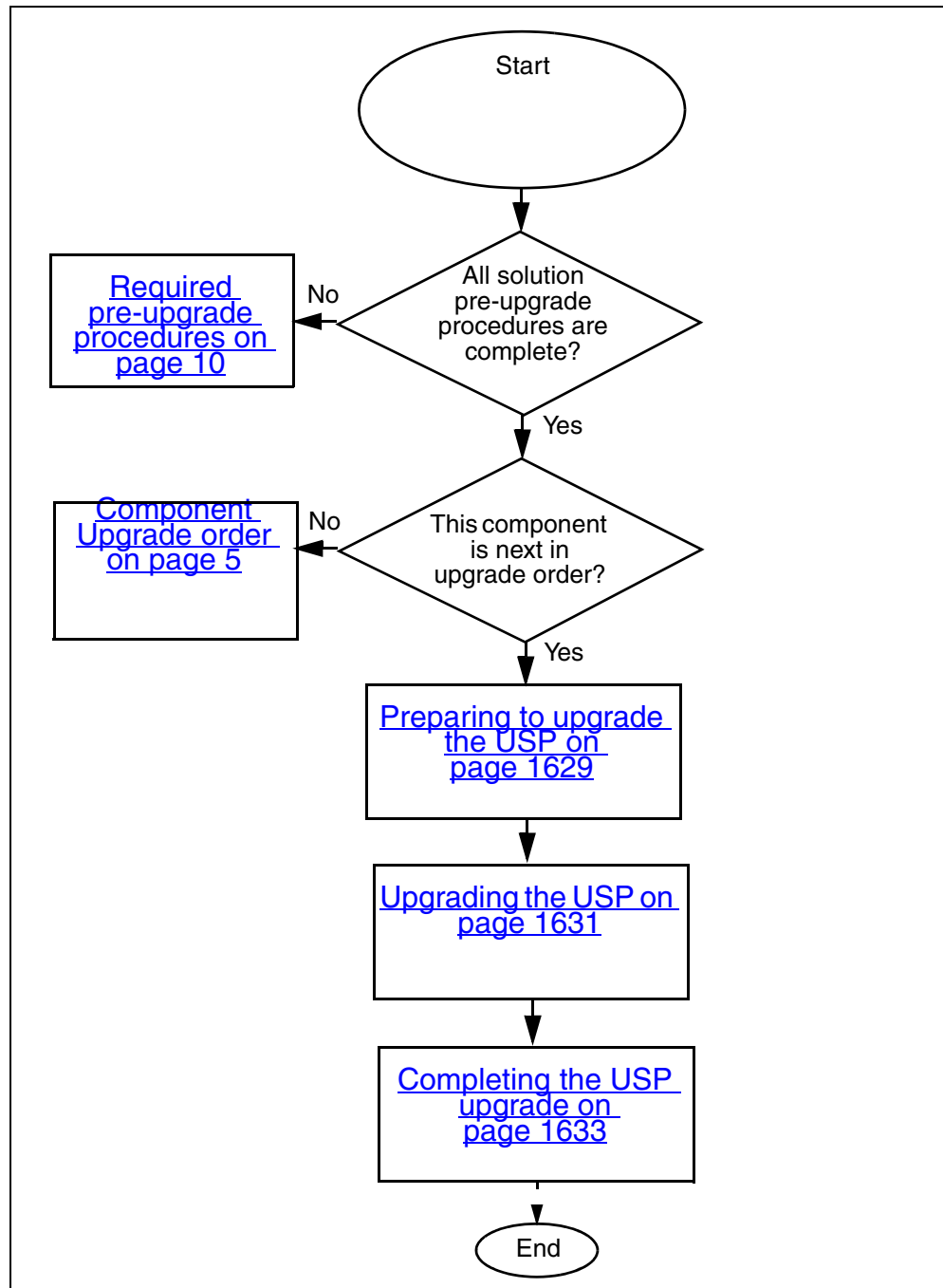
Aborting an upgrade

If you need to abort the USP upgrade, perform [Aborting an Upgrade on page 1743](#).

USP upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

USP upgrade tasks



Preparing to upgrade the USP

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

This procedure has the following prerequisites:

- any prerequisites identified at the start of this document, have been completed
- all components that precede the USP, as identified at the start of this document, have been upgraded
- for CS 2000 Management Tools-based workstations, procedure [Upgrading the ABS software on the CS 2000 Management Tools server on page 519](#) was completed during the CS 2000 Management Tools upgrade.

Action

Perform the following tasks to prepare the USP for an upgrade.

At the OAMP workstation

- 1 Log in to the USP GUI.

For detailed steps, refer to procedure [Logging in to the USP GUI on page 1691](#).

At the USP GUI

- 2 Determine the release that is running on the USP, which is indicated in the status bar as "Connected to <lab_name> <load_version>", and ensure the USP is running the latest point release of the current major release. Check for any RMR bulletins to determine the latest point release.
- 3 Determine if the office uses Route Master.
For detailed steps, refer to procedure [Checking Route Master status on page 1636](#).
- 4 Make sure all system nodes are operating in one of the following statuses:
 - in-service and unlocked
 - offline

For detailed steps, refer to procedure [Verify the USP is running on page 1637](#).

- 5 Take corrective action to clear all outstanding alarms.
For details refer to *USP Fault Management*, NN10071-911.
- 6 Make sure each IPS7 card has no more than 16 paths. If your system has IPS7 cards with more than 16 paths, redistribute the paths among the system nodes.
For details, refer to section "Application Server Process Paths Configuration" in *USP Configuration Management*, NN10093-511.
- 7 Delete old and unused snapshots.
For detailed steps, refer to procedure [Delete a data snapshot on page 1639](#).
- 8 Take an alternate boot data snapshot.
For detailed steps, refer to procedure [Creating an alternate boot data snapshot on page 1642](#).
- 9 Perform test calls and verify the calls complete successfully.
- 10 Reinitialize each RTC system node.
For detailed steps, refer to procedure [Reinitializing an RTC system node on page 1645](#).
- 11 You have completed this procedure. Proceed to [Upgrading the USP on page 1631](#).

Upgrading the USP

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

Complete the following tasks:

1. [Preparing to upgrade the USP on page 1629](#)
2. Review the upgrade schedule and office records to determine if ABS software on the CS 2000 Management Tools (CMT) server has been upgraded during this upgrade cycle.
3. Determine whether you are upgrading using a CD or Electronic Software Delivery (ESD), and if upgrading using a CD, ensure you have the CD for the release you are upgrading to.

Action

Perform the following tasks procedures to upgrade the component.

Upgrading the USP

At the OAMP workstation

- 1 Use the following table to determine your first step.

If you are upgrading USP on a	Do
non-CMT-based OAMP workstation (Windows-based)	step 2
CMT-based OAMP workstation	step 4

- 2 Perform one of the following tasks:
 - If you receive new USP software on CD, insert the CD in the CD drive of your workstation.
 - If you receive new software through ESD, perform [Installing Using ESD on page 514](#).
- 3 Upgrade the ABS and USP GUI using procedure [Upgrading the ABS and USP GUI on a Windows-based workstation on page 1647](#):

4 Use the upgrade wizard. See [Using the Upgrade Wizard on page 1659](#)

5 Use the following table to determine your next step.

If	Do
you are running the ABS on a non-CMT-based OAMP workstation in a CVoIP network	step 6
otherwise	step 7

6 Migrate the ABS to the CS 2000 Management Tools (CMT) server. Refer to [Migrating the Alternate Boot Server \(ABS\) from USP PC to CS 2000 Management Tools on page 1693](#).

7 You have finished upgrading the software on the USP. Go to [Completing the USP upgrade on page 1633](#).

Completing the USP upgrade

The USP Upgrade Wizard performs most upgrade completion tasks. No additional procedures are needed to complete the USP upgrade.

Follow office policy in the removal and storage of extra copies of new USP software.

- If you used a CD to upgrade the USP software, remove the CD from the CD drive and store the CD.
- If you used an ESD software load to upgrade the USP software, archive or delete the following files:
 - ESD software load
 - compressed USP software
 - any extra copies of new USP software on your PC
- Upgrade the next component in the end-to-end upgrade. Refer back to [Component Upgrade order on page 5](#).

Configuring Exceed for an upgrade

Perform the following procedure to configure the Exceed application for an upgrade of alternate boot server (ABS) software.

Prerequisites

Familiarity with starting the Exceed Xconfig application. Depending on the setup of your PC, you can start Xconfig through any of the following methods:

- Double-click a desktop shortcut.
- Select the menu option from Programs->Exceed or Programs->Hummingbird
- Double-click the xconfig.exe file in the Exceed folder.
- Type the directory path and name of the xconfig.exe file in Start->Run or a DOS prompt.

Action

The following configuration steps apply to the Hummingbird version 10.0.0.0. For other versions please consult your Hummingbird documentation.

Configuring Exceed for an upgrade

At your PC

- 1 Start the Exceed Xconfig application.

Response

The Xconfig window opens.

- 2 Switch to "classic view" and select the Security icon.

Response

The Security window opens.

- 3 Under Host Access Control List, choose host access. Select the Green check mark on the toolbar to save and exit.

Response

The Security window closes and the Xconfig window opens.

- 4 Select the Communication icon.

Response

The Communication window opens.

- 5** Make sure Mode is set to Passive. Select the Green check mark on the toolbar to save and exit.

Response

The Communication window closes and the Xconfig window opens.
- 6** Double-click the Screen Definition window.

Response

The Screen Definition window opens.
- 7** Select the tab Screen 0.
- 8** Under Window Mode, make sure Multiple is selected. Select the Green check mark on the toolbar to save and exit.

Response

The Screen Definition window closes and the Xconfig window opens.
- 9** Close the Xconfig window. From the menu bar, select File->Exit.

Response

The Xconfig window closes.
- 10** You have completed this procedure.

Checking Route Master status

Use the following procedure to determine if an office uses Route Master. Perform this procedure before a USP software upgrade.

Prerequisites

This procedure has no prerequisites.

Action

Perform the following steps to complete this procedure.

Checking Route Master status

At the OAMP workstation

- 1 Log in to the USP GUI.

For detailed steps, refer to procedure [Logging in to the USP GUI on page 1691](#).

At the USP GUI

- 2 Open the Route Master provisioning window through **Configuration>rm>system-id-mapping**.
- 3 Under the Search tab, click **Retrieve**.
A list of provisioned Route Master system IDs appears. If the office does not use Route Master, no system IDs appear.
- 4 Use the following table to determine your next step.

If	Do
a list of system IDs appears	step 5
otherwise	step 6
- 5 Record that the office uses Route Master. You will perform additional test calls after the upgrade.
- 6 Close the Route Master provisioning window.
- 7 You have completed this procedure. Return to [Preparing to upgrade the USP on page 1629](#).

Verify the USP is running

Before beginning upgrade procedures, complete this check from the USP GUI to make sure your system is running in a predictable, stable manner.

Prerequisites

This procedure has no prerequisites.

Action

Perform the following steps to complete this procedure.

Verify the USP is running

At the OAMP workstation

- 1 Log in to the USP GUI.
For detailed steps, refer to procedure [Logging in to the USP GUI on page 1691](#).

From the USP GUI

- 2 Display the node maintenance and provisioning window by selecting **Configuration>platform>node**.
- 3 Display the graphical view by selecting **Graphical View**.
- 4 Make sure that the icon for each in-service system node is green.

If	Do
all icons for every in-service system node are green	step 5
any icon for any in-service system node is any other color	Do not continue with the upgrade. Troubleshoot the problem or contact your next level of support.

- 5 Make sure that the icon for each offline node are yellow.

If	Do
all icons for every offline system node are yellow	step 6
any icon for any offline system node is any other color	Do not continue with the upgrade. Troubleshoot the problem or contact your next level of support.

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

If your USP system contains	Do
a single shelf	step 7
multiple shelves	Repeat this procedure for each USP shelf in the office.

- 7 You have completed this procedure. Return to [Preparing to upgrade the USP on page 1629](#).

Delete a data snapshot

Use this procedure to delete old or unused data snapshots. Perform this procedure before a USP software upgrade.

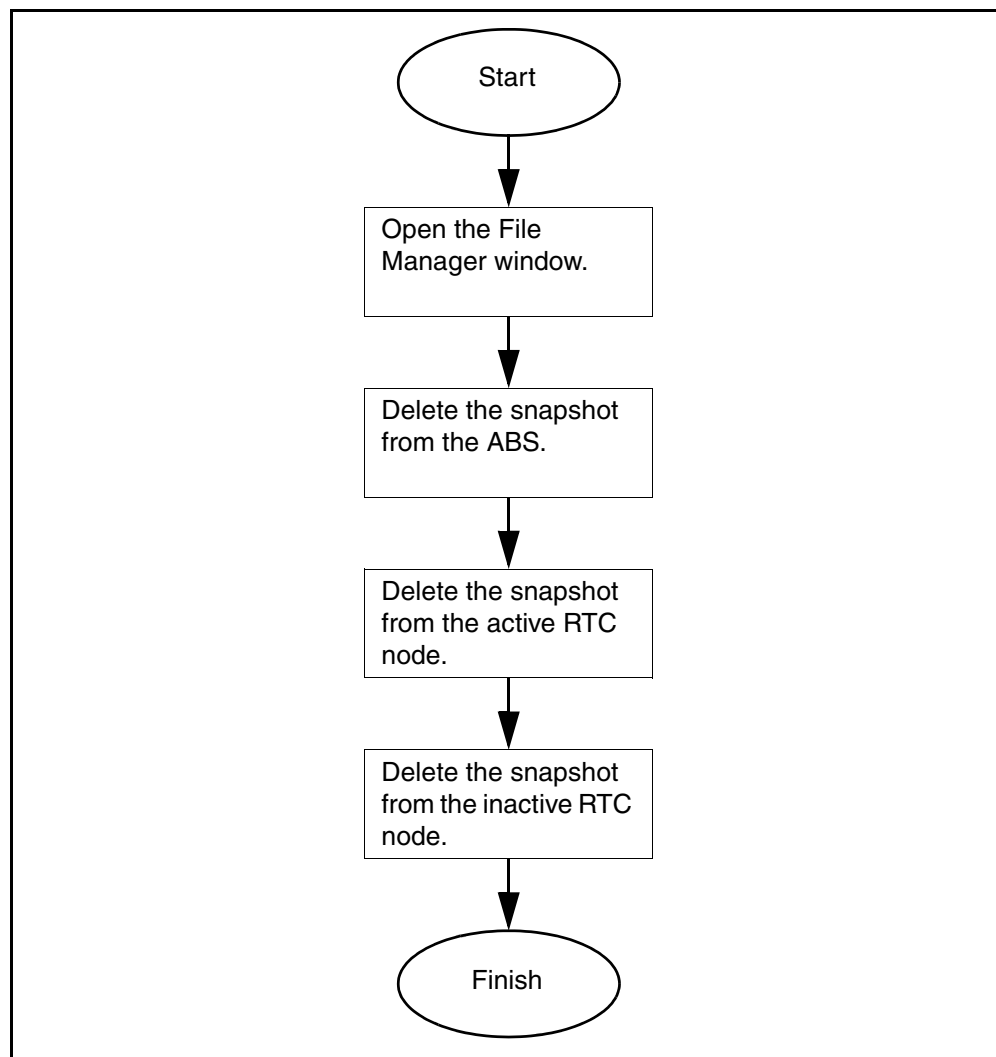
Prerequisites

This procedure has no prerequisites.

Action

The following figure shows the high-level steps of this procedure. Use the step-by-step instructions that follow the figure to perform the procedure.

Delete an old data snapshot



Delete a data snapshot

At the OAMP workstation

- 1 Log in to the USP GUI.

For detailed steps, refer to procedure [Logging in to the USP GUI on page 1691](#).

At the USP GUI

- 2 Open the File Manager window by selecting **Administration>file-manager**.

Response

The File Manager window appears.

- 3 At the Source portion of the window, select a snapshot to delete and click Delete.

Note: The Source portion is the left side of the window under Alternate Boot Server.

Response

An hourglass appears while the USP Manager deletes the snapshot from the Alternate Boot Server. The information under Alternate Boot Server refreshes when the snapshot is deleted.

- 4 Repeat [step 3](#) for each snapshot you want to delete from the Alternate Boot Server.

- 5 At the Destination portion of the window, make sure the active RTC node is selected.

Note: The Destination portion is the right side of the window under the RTC selection.

- 6 Expand the Snapshot folder and the folder for the previous version of software.

- 7 Select the snapshot and click Delete.

Response

An hourglass appears while the USP Manager deletes the snapshot from the active node. The information refreshes when the snapshot is deleted.

- 8 Repeat steps [step 6](#) and [step 7](#) for each snapshot on the active RTC node you want to delete.

- 9 At the RTC selection, select the inactive RTC node.

- 10 Expand the Snapshot folder and the folder for the previous version of software.

- 11 Select the snapshot and click Delete.

Response

An hourglass appears while the USP Manager deletes the snapshot from the inactive node. The information refreshes when the snapshot is deleted.

- 12 Repeat steps [step 10](#) and [step 11](#) for each snapshot on the inactive RTC node you want to delete.
- 13 You have completed this procedure. Return to [Preparing to upgrade the USP on page 1629](#).

Creating an alternate boot data snapshot

During the upgrade, you will be making many changes to the system. To ensure you have a backup in case a change has a performance degradation impact, you must take a snapshot when your system is operating properly. This allows you to revert the system to that snapshot. You must take a snapshot before you start the upgrade and once again after completing the upgrade.

Prerequisites

This procedure has no prerequisites.

Action

To create an alternate boot data snapshot, perform the following steps:

Creating an alternate boot data snapshot

At the OAMP workstation

- 1 Log in to the USP GUI.

For detailed steps, refer to procedure [Logging in to the USP GUI on page 1691](#)

At the USP GUI

- 2 Click **Administration>backup**.
- 3 Enter a description of the data snapshot in the Description box. You can enter up to 32 characters.

Use the following format for the description so the file can be easily identified in the future:

- pre_upgrd_<site>_<date> for backup pre-upgrade snapshot
- post_upgrd_<site>_<date> for backup post-upgrade snapshot

where

<site>

is the site name

<date>

is the current date

- 4 Click the corresponding checkboxes to activate the following options, as appropriate:
 - transfer snapshot to alternate boot server

Note: Nortel Networks recommends that you enable this option. If you do not select this option, a warning dialog box will appear; select yes to continue.
 - set as active snapshot on alternate boot server

Note: Nortel Networks recommends that you enable this option. If you do not select this option, a warning dialog box will appear; select yes to continue.
 - delete oldest snapshot on alternate boot server if maximum reached (16)
 - delete oldest snapshot on rtc if maximum reached (5)
- 5 Click **Create** to create the data snapshot.

A Confirmation required dialog box appears, stating: Backup create command can take up to 20 minutes, during which time system write access will be disabled. Do you want to continue? Click **Yes** to continue.
- 6 When the data snapshot command is complete, close the Administration backup window by clicking the X in the top right corner.
- 7 If you selected both transfer snapshot to alt boot server and set as active snapshot on alternate boot server, go to step [15](#). If you only selected transfer snapshot to alt boot server, go to step [14](#).
- 8 Click **Administration>File Manager**.
- 9 Select the active RTC system node from the drop-box.
- 10 Open the snapshot folder.
- 11 Open the folder corresponding to the version of the USP software that you are running.
- 12 Select the snapshot file you want to copy. When you select a file, its description is displayed in the Description box.
- 13 Copy the snapshot to the ABS by clicking <. An hourglass appears while the data snapshot is copied. The folders in ABS portion of the window are updated with the information for the copied data snapshot when the copy operation is complete.

Note: These files are large and can take several minutes, depending on system activity, to copy from an RTC system node to your alternate boot server.

- 14** Update the ABS Active Snapshot using the ABS Settings window:

 - Open the Alternate Boot Server (ABS) window by clicking **Administration> alternate-boot-server**
 - Select the snapshot you have just created from the Snapshot name drop-down list.
 - Click **Modify** to save your changes and close the window.
A Confirmation dialog box appears, asking if you want to continue with the ABS Modify command. Click **Yes** to continue.
- 15** This procedure is complete. If applicable, return to the higher-level procedure or task flow that directed you to this procedure.

Reinitializing an RTC system node

Perform the following procedure to download a boot image and re-initialize the RTC system node before a USP software upgrade.

Prerequisites

This procedure has no prerequisites.

Action

Perform the following steps to complete this procedure.

Reinitializing an RTC system node

At the OAMP workstation

- 1 Log in to the USP GUI.

For detailed steps, refer to procedure [Logging in to the USP GUI on page 1691](#).

At the USP GUI

- 2 Open the system node provisioning window by selecting **Configuration>platform>node**.
- 3 Display the graphical view by selecting **Graphical View**.
- 4 Double-click the icon for the inactive RTC system node, which is the one with no check mark.
- 5 Check the status of the node.

If the inactive RTC system node is	Do
unlocked	step 6
locked	step 8

- 6 Click **Lock**.
- 7 If a confirmation dialog box appears, Click **Yes** to confirm the change.
- 8 Click **Load** to download the RTC system node boot image and re-initialize the RTC system node.
- 9 If a confirmation dialog box appears, Click **Yes** to confirm the change.
- 10 Display the graphical view by selecting Graphical View.
- 11 Wait for the card to display in green. Green indicates initialization is complete.

- 12 Double-click the icon for the inactive RTC system node, which is the one with no check mark.
- 13 Click **Unlock** to unlock the RTC.
- 14 If a confirmation dialog box appears, Click **Yes** to confirm the change.
- 15 Click **SWACT** to make the inactive RTC system node Active.
- 16 If a confirmation dialog box appears, Click **Yes** to confirm the change.
- 17 Use the following table to determine your next step.

If you reinitialized	Do
one RTC system node	step 3
both RTC system nodes	step 18

- 18 Make sure that the RTC system node in slot 12 (RTC12) is the active RTC system node.

If RTC12	Do
inactive	step 19
active	step 21

- 19 Click **SWACT** to make RTC12 the active system node.
- 20 If a confirmation dialog box appears, Click **Yes** to confirm the change.
- 21 This procedure is complete. Return to [Preparing to upgrade the USP on page 1629](#).

Upgrading the ABS and USP GUI on a Windows-based workstation

Use this procedure to upgrade the ABS and USP GUI on a Windows-based OAMP workstation.



CAUTION

The GUI will not function properly with non-ASCII based character sets. Ensure that the OAMP workstation is set to either English or German language character sets.

Prerequisites

This procedure has no prerequisites.

Action

Perform the following tasks to complete this procedure:

1. [Uninstalling the ABS and USP GUI from Windows-based workstations on page 1647](#)
2. [Installing the new ABS and USP GUI on a Windows-based workstation on page 1649](#)
3. If the workstation serves as the alternate boot server, the Signaling Server Monitor, Alternate Boot Server Configuration Manager, and the three Distinct servers start up automatically when the workstation restarts.

If this is the first time to install ABS on this windows workstation, you need to configure three Distinct servers. For detailed steps, refer to [Configuring the Distinct BOOTP, FTP and NFS Servers for Windows on page 1652](#).

Uninstalling the ABS and USP GUI from Windows-based workstations

At the OAMP workstation

- 1 If you are upgrading ABS server, identify the current installation path. From Distinct FTP server window, select **configure-->server-->export**, then record the exported folder's path.
- 2 Close all open applications and exit the USP Distinct Servers (if running) and Signaling Server Monitor (if running).
- 3 Click the Windows **Start** button on your desktop taskbar.

- 4 On the Settings menu, select **Control Panel**.
- 5 In the Control Panel window, double-click **Add/Remove Programs**.
- 6 In the Change or Remove Programs tab of the Add/Remove Programs window, select Universal Signaling Point from the alphabetical list of programs.
- 7 Click the **Change/Remove** button. A uninstall pop-up window appears prior to removing the application and its components.
- 8 Wait for the uninstall window to open and click **Next** when it appears.
- 9 Click **Completely Uninstall**, then click **Next**. All installed components will be uninstalled.

If you want to uninstall ABS or USP GUI only, click **Uninstall specific components**. Then use the following table to determine your action:

If	Do
Uninstalling ABS	uncheck USP Software Loads and ABS Manager, then click uninstall
Uninstalling USP GUI	uncheck USP Graphical Interface Client, then click uninstall

- 10 Click **Done**.
- 11 This procedure is complete. Restart your computer and go to [Installing the new ABS and USP GUI on a Windows-based workstation on page 1649](#).

Installing the new ABS and USP GUI on a Windows-based workstation

ATTENTION

Installing this USP software on a workstation other than your Nortel Networks-approved workstation may overwrite some system files used by other applications. This can cause failure of existing applications. Also, installing software other than Nortel Networks-approved applications on your USP OAMP workstation can cause failure of the USP application.

ATTENTION

When adding the ABS and USP GUI on an NTST30DA workstation, install the GUI using the Add/Remove Programs utility in the Windows Control Panel.

At the OAMP workstation

- 1 Close any open applications.
- 2 Use the following table to determine your next step.

If the new USP software is located	Do

on a CD	step 3
in a directory on your PC	Open the directory with the new USP software and go to step 6 .

- 3 Insert the USP Software CD-ROM disk into the CD-ROM drive.
- 4 Double-click the **My Computer** icon on your desktop.
- 5 Double-click the CD-ROM disk icon.
- 6 Double-click **Install.exe**.
Note: When adding the USP GUI on an NTST30DA workstation, install the GUI using the Add/Remove Programs utility in the Windows Control Panel.
- 7 At the Introduction window for the USP setup program, click **Next**.

- 8 Select the package(s) that you want to install on this workstation.
 - Select USP Software Loads and ABS manager if you want this workstation to act as the alternate boot server.

Each USP system needs one workstation configured as an alternate boot server. Do not configure more than one alternate boot server for each USP system.
 - Select USP Graphical User Interface Client if you want this workstation to be able to log into the USP site.
 - Select USP User Manuals and Documentation Suite to install the complete collection of FCAPS documents, Marconi TNX-210 ATM Switch Manuals, and Interface Specifications.
 - Select USP GR-310 Mediation Application to install a SEAS OSS Interface.
 - Select Acrobat Reader if you do not have a version of Adobe Acrobat Reader installed on this workstation.
- 9 Select **Next**. If you select GR-310 Mediation Application, enter your Nortel Networks provided serial number when prompted by the system.
- 10 Select an Installation Directory and click **Install**.

If you selected the ABS pkg, the following pop-up will appear:

Prior to installing the Alternate Boot Server Package please ensure that all unnecessary snapshots and old release loads (i.e. maintenance releases that are no longer in use) are deleted. This will ensure adequate disk space is available during the install procedure.

Select **OK** and then select an installation directory.

If this is to upgrade the ABS server, please select the installation directory where the old release was installed, refer to the installation path recorded in [step 1](#) of [Uninstalling the ABS and USP GUI from Windows-based workstations on page 1647](#).

The Copying Program Files window appears with a status bar to show progress in copied files.

If you chose to install Acrobat reader, a Welcome window for the Adobe Acrobat Reader Setup Program appears. Adobe Acrobat Reader is required to view the Solution information. If Adobe Acrobat Reader is already installed on this workstation, click **No**. Click **Yes** to the "Are you sure" message. Proceed to the next step.

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

If	Do
you want to install Adobe Acrobat Reader	step 12
otherwise	step 16

- 12** Click **Next**. The Acrobat Reader License Agreement appears.

- 13** Click **Yes** to accept the terms of the agreement. The Acrobat Reader Destination Location window appears.

- 14** Click **Next**.

Note: Do not modify the destination path for Acrobat Reader.

- 15** The Acrobat Reader Setup Complete window appears. Click **OK**.

- 16** Log in to the USP from the new release of the USP GUI and monitor the OAMP workstation for 10 minutes while logged into the USP. Check logs during this time. Your USP GUI is now upgraded. You will use the GUI to upgrade your USP software.

Note: When you first connect the GUI it will detect that the lab is running a prior version and will logout and log back in automatically to re-initialize based on the older feature set (it is expecting the new release by default).

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

If you	Do
freshly installed ABS software during this procedure	proceed to Configuring the Distinct BOOTP, FTP and NFS Servers for Windows on page 1652
otherwise	step 18

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

Configuring the Distinct BOOTP, FTP and NFS Servers for Windows

At the OAMP workstation

1



CAUTION

Make a record of the password immediately.

ATTENTION

For upgrading ABS server, if the installation directory is the same as the one before uninstallation, procedure [Configuring the Distinct BOOTP, FTP and NFS Servers for Windows](#) can be ignored.

If this is the initial install of the ABS, a pop-up window prompts you to create a password for the Alternate Boot Server Configuration Manager.

- 2 Click the **Distinct BOOTP Server** button on the taskbar to maximize the Distinct BOOTP Server window.
- 3 Click the **Configure** menu and select **Administrator** and then **Login** to display the Distinct BOOTP Login window.
- 4 Enter your administrator password in the Enter the administrator password field and click **OK** to log into the server.
The Distinct BOOTP Login window closes.
- 5 Click the **Configure** menu and select **Server** to display the Configure BOOTP window.
- 6 In the Addresses tab window, view the contents of the field at the bottom of the window, next to the Add, Modify, and Remove buttons. This field should contain the hexadecimal Ethernet hardware addresses of the RTC system nodes in your system.
- 7 Select the Ethernet hardware address that matches the Ethernet hardware address for the RTC system node in slot 12 of your system. The information for that Ethernet hardware address should appear in the various fields.
- 8 In the Boot File field, change the value to **/c/ntssgusp/abs/sites/<site_name>/rtc1/rtcboot** (site_name

is the name of your system as it appears in the site configuration information).

- 9 Click **Modify** to save the changes.
- 10 Select the Ethernet hardware address that matches the Ethernet hardware address for the RTC system node in slot 15 of your system. The information for that Ethernet hardware address should appear in the various fields.
- 11 In the Boot File field, change the value to **/c/ntssgusp/abs/sites/<site_name>/rtc2/rtcboot** (site_name is the name of your system as it appears in the site configuration information).
- 12 Click **Modify**, then **Apply** to save the changes.
- 13 Open the Alternate Boot Server Configuration Manager.
- 14 Log in to the Alternate Boot Server Configuration Manager.
- 15 Under the File drop-down menu, select **ABS Configuration**.
- 16 Select a site from the Site list.
- 17 Confirm that the Alternate Boot Loads displayed for each RTC are for the pre-upgrade load.
- 18 Confirm that the Alternate Boot Snapshot display is the snapshot taken earlier in this procedure. A pre-upgrade snapshot
- 19 Click **Apply** to save the changes.
- 20 Log out of the Alternate Boot Server Configuration Manager.

Configuring the FTP server

- 21 Click on the Distinct FTP Server in the task bar.
- 22 From the Distinct FTP Server window, select **Configure->Administrator->Login**.
- 23 In the query dialog box, type **SERVICE** for password and select **OK**.
- 24 From the Distinct FTP Server window, select **Configure->Server**.
- 25 From the Server Properties window, select the **Users** tab window.
 - For User Name, enter **ntssg**.
 - For User Password, enter **1ntssgstp** (number 1 followed by ntssg in lowercase).

- For Confirm Password, enter **1ntssgstp**.
 - Select **Add**.
- 26** From the Server Properties window, select the **Exports** tab window. Important:
- The **Browse** Button must be used to find the C:\ directory, do not type the choice into the field.
- Select **ntssg** from the Users droplist.
 - For Folder, use Browser button to select **C:**
 - For Export Name, enter: **/c**
 - Check all permissions (Download, Upload, List, Delete).
 - Select **Add**.
- 27** From the Server Properties window, select **OK**.
- 28** From the Distinct FTP Server window, select **Configure->Administrator->Logout**.
- 29** Select **OK**.
- 30** Minimize the Distinct FTP Server to the Taskbar.

Configuring the NFS server

- 31** Click on the **Distinct NFS Server** in the task bar.
- 32** From the Distinct NFS Server window, select **Configure->Administrator->Login**.
- 33** In the query dialog box, type **SERVICE** for password and select **OK**.
- 34** From the Distinct NFS Server window, select **Configure->Server**.
- 35** From the Configure the NFS Server window, select the **Groups** tab window.
- For Group Name, enter **ssg** (in lower case).
 - For Group ID, enter **453**.
 - Then select **Add**.
- 36** From the Configure the NFS Server window, select the **Users** tab window.
- For User Name, enter **ntssg** (in lower case).
 - For User Password, enter **1ntssgstp**.
 - For User ID, enter **50015**.

- For Group Name, select **ssg** from the droplist.
 - Select **Add**.
- 37** From the Configure the NFS Server window, select the **Exports** tab window.
- For Path, use Browser button to select C:\ and double-click on **C:**.
 - Select **OK**. In the Path Edit Box, ensure that C:\ is the only entry.
 - For Owner, select **ntssg** from the droplist.
 - Show Hidden Files attribute is not checked.
 - Show System Files attribute is not checked.
 - Read, write, execute for Owner permissions is checked.
 - Read, execute for Group permissions is checked.
 - Read, execute for World permissions is checked.
 - Select **Export**.
 - Select **Apply**.
- 38** From the Configure the NFS Server window, select the **General** tab window.
- Enter the path of the Log Folder as **C:\PROGRAM FILES\DISTINCT\LOG**
 - Under Prompt Dialogs, the On Application Exit is checked.
 - The Set Spool Folder is not checked.
 - From the Configure the NFS Server window, select **OK**.
- 39** From the Distinct NFS Server window, select **Configure->Administrator->Logout**.
- 40** When a window Are you sure you want to Logout? appears, Select **Yes**.
- 41** Minimize the Distinct NFS Server to the Taskbar.
- 42** This procedure is complete. If applicable, return to the higher-level procedure or task flow that directed you to this procedure.

Upgrading the USP GUI on a CS 2000 Management Tools-based OAMP workstation



CAUTION

The GUI may not function properly with non-ASCII based character sets. Ensure that the OAMP workstation is set to either English or German language character sets.

ATTENTION

If you installed the USP ABS software and GUI during the CS 2000 Management Tools upgrade, use the procedure [Using the Upgrade Wizard on page 1659](#) to upgrade the USP GUI.

Use this procedure to use console mode to upgrade the USP GUI on a CS 2000 Management Tools OAMP workstation.

Prerequisites

This procedure has no prerequisites.

Action

Perform the following tasks to complete this procedure:

1. [Uninstalling the USP GUI on the CS 2000 Management Tools workstation on page 1656](#)
2. [Installing the new USP GUI on the CS 2000 Management Tools workstation on page 1657](#)

Uninstalling the USP GUI on the CS 2000 Management Tools workstation

At the OAMP workstation

- 1 Launch the USP uninstall procedure.

```
> cd <original install path>/ntssgusp/
```

where
original install path
is /data/usp for offices at USP10 and lower
is /opt/usp for offices at USP11 and higher

```
>./Uninstall_Universal_Signaling_Point -i
console
```

Note: A space precedes -i in the above command line.

- 2 Press Enter in the Introduction window.
- 3 In the Uninstall Options step, press Enter to uninstall the USP GUI.
- 4 Press Enter to complete the installation and to exit.
- 5 You have uninstalled the USP GUI. Go to [Installing the new USP GUI on the CS 2000 Management Tools workstation on page 1657](#).

Installing the new USP GUI on the CS 2000 Management Tools workstation

At the OAMP workstation

- 1 Change directories:

If the new USP-Compact software is located	Do
in a CD	>cd /cdrom/cdrom0
on the CS 2000 Management Tools server	>cd /data/esd_iso

- 2 List the directory and locate the install.bin file:

```
>ls
```

- 3 Launch the installation program, which can take several minutes to finish launching.

```
>./install.bin -i console
```

- 4 Press Enter in the Introduction step.
- 5 Press Enter in the Component Selection step.
- 6 In the Pre-Installation Summary step, confirm that USP Graphical Interface Client is included in Software Components. Press Enter to continue.
- 7 Press Enter in the Installation Directory step to accept the default installation directory.

Note: Executing the Component Installation step can take several minutes to run.
- 8 Press Enter to complete the Installation and exit.

- 9 You have completed this procedure. Return to [Upgrading the USP on page 1631](#).

Using the Upgrade Wizard

Use the following procedure to upgrade USP software.

ATTENTION

Do not use the software upgrade wizard to upgrade NPC/NPS/NPE system nodes if there are NPE chains provisioned. Manually upgrade these nodes instead. See [Upgrade of NPC, NPS, and NPE nodes on page 1670](#).

Upgrading NPC, NPS, and NPE system nodes is only applicable to systems that include the optional Universal Number Portability Master (UNPM) capability.

Setup

The system performs the following actions to prepare the USP for an upgrade:

- copies upgrade package to the RTCs from Alternate Boot Server
- copies software loads to RTCs from Alternate Boot Server
- sets the target upgrade software version

Note: Prior to running the setup, ensure that the maximum number of files permitted in the file system has not been reached. Otherwise, the setup procedure will fail.

Running the setup

At the OAMP workstation

- 1 Log in to the USP GUI.
For detailed steps, refer to procedure [Logging in to the USP GUI on page 1691](#).
- 2 Click **Fault>Log**. Display the Realtime log list by selecting Realtime View. Any new logs generated by the system are displayed on the screen.
- 3 Click the Clear button to clear the Realtime log.
- 4 Click the Start button.
- 5 Click **Administration>software-upgrade**. Select the software release you are installing in the Target Version text box. Use the notation vn.n.n (for example v11.0.0).

- 6 Click the **Run Setup** button. A confirmation dialog box is displayed.
- 7 Click **Yes**.
Note: Setup can take up to an hour to complete. A confirmation that the setup is complete will appear at the bottom left corner of the dialog box.
- 8 Click **Next** when you see the message "command completed" at the bottom left corner of the window.
- 9 Proceed to the next section ([Precheck](#)).

Precheck

Run the precheck to ensure that the upgrade is ready to proceed. The system confirms the following:

- Both RTCs are in-service with an operational state of enabled.
- RTC in slot 12 of control shelf is the current active RTC.
- The alternate boot server is configured properly for current system configuration for both RTCs.
- All other system nodes are in-service with an operational state of enabled or have an availability state of offline.
- Software upgrade packages have been transferred to both RTCs.

If any of the checks fail, resolve them before proceeding with the upgrade.

Running the precheck

At the OAMP workstation

- 1 Click the **Run Precheck** button.
- 2 Click **Yes** to confirm the action.
- 3 Click **Next** when you see the message "upgrade precheck successful" at the bottom left corner of the dialog box.
- 4 If the status panel indicates that the precheck is successful, proceed to the next section ([Limit user access](#)). If the precheck was not successful, address any error messages and repeat the precheck before you proceed. For example, if the precheck status panel indicates that disk space is low, delete any unused snapshots and loads from the RTC SCSI disk using the File Manager.

Limit user access

Before you begin a software upgrade, limit connections to the USP to prevent other users from accidentally modifying provisioning data while the upgrade is in progress.

Although the following procedure is not a part of the Upgrade Wizard, it is performed at this point since you are now ready to proceed with the upgrade.

To view or restrict user access to the USP during a software upgrade, perform the following procedure.

Viewing and restricting user access to the USP

At the OAMP workstation

- 1 To modify user account information, click **Security>user-account**.
- 2 Click the **Search** tab.
- 3 Select **All** from the **Records** drop-down menu.
- 4 Click **Retrieve**.
- 5 Select all records by clicking the first one and then holding the shift key down, and clicking the last record.

Do not include your own user account with the records you have selected. Find your own record in the list and while holding down the Ctrl key, click on your record. This will de-select your record, while keeping the others selected.
- 6 Click on **Post**. An X appears to the left of all the records.
- 7 Create a record showing the currently enabled and disabled users as follows:
 - a Click on the **Export posted records** icon (the second button to the left of the context-sensitive Help button). A message box appears, asking: "Do you want to continue?". Answer **Yes**.
 - b The **Export** dialog box appears. Enter a filename and specify a file type for the exported records file. Click **Save**.

The file you have just created is a list of all user accounts. It shows which users were enabled or disabled before beginning the upgrade procedure. Use this list to restore the correct user account status when directed to do so in [Complete the upgrade on page 1682](#).

- 8 Double-click on any posted record. The Administration tab then appears.
- 9 Ensure the **enabled** option is not selected. Uncheck the enabled option if it is checked.
- 10 Click **Modify**.
A confirmation dialog box appears.
- 11 Use the following table to determine your next step.

If	Do
only one user was posted in step 6	click Yes and proceed to step 14
multiple users were posted in step 6	click Posted , which displays the multi-modify field selection dialog box, and proceed to step 12

- 12 Select the **enabled** option field. The letter n should appear to the right.
- 13 Click **OK**. All posted users will be disabled once the command completes.
- 14 Proceed to section [Start the upgrade](#).

Start the upgrade

Run the Start Upgrade procedure to begin the software upgrade. All pre-check conditions must be met before the upgrade is allowed to start. All upgrade packages and target software loads must be transferred to both RTCs.

Running the Start Upgrade procedure

At the OAMP workstation

- 1 Click the **Start Upgrade** button.
- 2 Click **Yes** to confirm.
- 3 Click **Next**.
Note: To abort the software upgrade, all nodes must be running the original back-level release (no nodes must have an upgrade-status of upgraded. If nodes are upgraded, they must be downgraded before you click the Stop Upgrade button.
- 4 Proceed to section [Software load setup](#).

Software load setup

The Software Load Setup builds a mapping between the current software loads and the target software loads and automatically re-maps the software load pointer to the new target software release.

The system creates a default mapping based on the current software version and the target upgrade version specified during setup. All current software loads must be mapped to the target software loads. If a software mapping does not exist for the current load, you must resolve the missing pairing.

The current load list contains all software loads available on the active RTC that match the current software release.

The upgrade load list contains all software loads available on the active RTC that match the target upgrade software release.

Running the software load setup

At the OAMP workstation

- 1 Review the software mapping displayed in the software load setup. Confirm the mapping is correct.
- 2 Click the **Next** button.
- 3 Proceed to the next section ([Upgrade the system nodes](#)).

Upgrade the system nodes

Run the node upgrade to perform the software upgrade for a specific node. You can also select multiple nodes to upgrade using the Shift+Ctrl keys or Ctrl+click with a mouse.

Upgrading the system nodes for one maintenance window upgrades

Upgrade the system nodes for a one-shelf or two-shelf system using the procedure that follows.

At the OAMP workstation

- 1 Upgrade the inactive RTC in slot 15. For detailed steps, refer to [Upgrading the inactive RTC in slot 15 on page 1666](#).

- 2 Upgrade the CC in slot 1 on the control CAM shelf. For detailed steps, refer to [Upgrade a CC node on page 1668](#).

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

If you have a	Do
one-shelf system	step 5
two-shelf system	step 4

- 4 For a two-shelf system, also upgrade the CCs in slot 1 on the extension CAM shelf. For detailed steps, refer to [Upgrade a CC node on page 1668](#).

- 5 Upgrade the link system nodes on the control shelf. For detailed steps, refer to [Upgrade a link node on page 1668](#).

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

If you have a	Do
one-shelf system	step 8
two-shelf system	step 7

- 7 For a two-shelf system, also upgrade the link system nodes on the extension CAM shelf. For detailed steps, refer to [Upgrade a link node on page 1668](#).

- 8 If your system includes the optional Universal Number Portability Master (UNPM) capability, upgrade the NPC, NPS and NPE nodes on the control CAM shelf. For detailed steps, refer to [Upgrade of NPC, NPS, and NPE nodes on page 1670](#).

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

If you have a	Do
one-shelf system	step 12
two-shelf system	step 10

- 10 For a two-shelf system, also upgrade the NPC, NPS and NPE nodes on the extension CAM shelf. For detailed steps, refer to [Upgrade of NPC, NPS, and NPE nodes on page 1670](#).

- 11 Upgrade the CCs in slot 18 on the control CAM shelf. For detailed steps, refer to [Upgrade a CC node on page 1668](#).

- 12 Upgrade the CC in slot 18 on the extension CAM shelf. For detailed steps, refer to [Upgrade a CC node on page 1668](#).

- 13 Switch activity (SWACT) between RTCs, and upgrade the inactive RTC in slot 12. For detailed steps, refer to [Perform a SWACT and upgrade the Inactive RTC node in slot 12 on page 1677](#).
- 14 Activate new features. For detailed steps, refer to [Activate features on page 1681](#).
- 15 Monitor the USP for 15 minutes, and ensure the USP performs without degradation. If there is a degradation in service, complete section [Deactivate upgrade features on page 1681](#). If there is no degradation and you want to keep the features activated, proceed to section [Cleanup on page 1682](#).

Upgrading the system nodes for multiple maintenance window upgrades

When performing a large system upgrade that requires more than one maintenance window to complete, you must upgrade the entire Control CAM shelf before the end of the first maintenance window. Use the additional window to upgrade the cards in the extension shelves.

Note: If your system includes NPC, NPS and/or NPE nodes, you must upgrade the NPC, NPS and NPE system nodes (on all shelves if you have a dual-shelf or multi-shelf system) in a specific order depending on the local subsystem assignment. (See [Upgrade of NPC, NPS, and NPE nodes on page 1670](#).) Re-ordering of the upgrade sequence may be required if performing a multi-node upgrade operation.

Upgrade the system nodes with three or more shelves using the procedure that follows:

At the OAMP workstation

- 1 Upgrade the inactive RTC in slot 15. For detailed steps, refer to [Upgrade of the inactive RTC node in slot 15 on page 1666](#).
- 2 Upgrade the CC in slot 1 on the control CAM shelf. For detailed steps, refer to [Upgrade a CC node on page 1668](#).
- 3 Upgrade the CCs in slot 1 on the extension CAM shelves. For detailed steps, refer to [Upgrade a CC node on page 1668](#).
- 4 Upgrade the link system nodes on the control CAM shelf. For detailed steps, refer to [Upgrade a link node on page 1668](#).
- 5 If your system includes the optional Universal Number Portability Master (UNPM) capability, upgrade the NPC, NPS and NPE nodes on the control CAM shelf. For detailed steps, refer to [Upgrade of NPC, NPS, and NPE nodes on page 1670](#).

- 6 Upgrade the CCs in slot 18 on the control CAM shelf. For detailed steps, refer to [Upgrade a CC node on page 1668](#).
Note: When you perform the SWACT command in [step 7](#), you will be informed if you have not upgraded one card of each unique card type in your system. In this case, upgrade the card which will be on an extension shelf. You can perform the SWACT again until it is successful.

7

ATTENTION

Before upgrading RTC12, perform test calls to ensure the system is performing properly. Once RTC 12 is upgraded, the abort of the upgrade requires an out-of-service alternate boot to the snapshot taken before starting the upgrade.

Switch activity (SWACT) between RTCs, and upgrade the inactive RTC in slot 12. For detailed steps, refer to [Perform a SWACT and upgrade the Inactive RTC node in slot 12 on page 1677](#).

Note: The required cards have been upgraded for the first maintenance window. You can continue to upgrade cards now or in the next maintenance window.

- 8 Upgrade the link system nodes on the extension CAM shelves. For detailed steps, refer to [Upgrade a link node on page 1668](#).
- 9 If your system includes the optional Universal Number Portability Master (UNPM) capability, upgrade the NPC, NPS and NPE nodes on the extension CAM shelves. For detailed steps, refer to [Upgrade of NPC, NPS, and NPE nodes on page 1670](#).
- 10 Upgrade the CCs in slot 18 on the extension CAM shelves. For detailed steps, refer to [Upgrade a CC node on page 1668](#).

Upgrade of the inactive RTC node in slot 15

The upgrade of the RTC in slot 15 can take up to 20 minutes to complete.

Upgrading the inactive RTC in slot 15

At the OAMP workstation

- 1 Click on the appropriate row to select the RTC15 node to upgrade from the list of available nodes in the software upgrade wizard. The RTC node is in slot 15, with a slot type of rtc.

- 2 Click the **Upgrade** button. A confirmation dialog box appears. Click **Yes** to continue.
- 3 Wait for the upgrade to complete. The upgrade-status will change to upgraded on completion.

Note: If the automatic node upgrade fails to complete successfully, perform the upgrade manually. For detailed steps, refer to [Upgrade nodes manually on page 1678](#).
- 4 Click **Fault>Log**. Display the Realtime log list by selecting Realtime View to monitor the USP to ensure it performs normally and does not report any LOG_SWERRS or LOG_TRAPS. If it does, contact your next level of support.
- 5 Set the alternate boot load for RTC system nodes to the new upgrade load.

The alternate boot settings are used when an RTC is not able to boot from disk. After upgrading RTC15, if RTC15 were to boot, it would be able to data sync from RTC12 and upgrade. But if RTC12 were to boot, it would be booting the old release load and would not be able to data sync from RTC15, which is now running the upgrade load. So RTC12 would alternate boot. If the alternate boot load is the old release load, RTC 12 would again, not be able to data sync and become enabled. This is why the active alternate boot loads for both RTCs must be changed to the new upgrade load, thus permitting RTC12 to alternate boot the upgrade load and then data sync with RTC15 (also running the upgrade load).

A special case occurs if both RTCs were to alternate boot at the same time, before you changed the active snapshot to one taken with the active RTC running the upgrade load. In this case, you will have to change the active alternate boot loads to the old release loads, since the snapshot would contain data from the old release.
 - a Click **Administration>alternate-boot-server**.
 - b Update RTC 12 to the new release version by selecting the new release from the ABS Active Loads drop-down menu.
 - c Update RTC 15 to the new release version by selecting the new release from the ABS Active Loads drop-down menu.
 - d Click **Modify**.
- 6 This procedure is complete. Return to [Upgrade the system nodes on page 1663](#) to determine your next step.

Upgrade a CC node

To upgrade a CC node, perform the following steps:

Note: Start with CC1 on the control shelf.

Upgrading the CC node

At the OAMP workstation

- 1 Select the node to upgrade in the list of available nodes in the software upgrade wizard.
- 2 Click the **Upgrade** button. The system asks for confirmation.
- 3 Wait for the node upgrade to complete (the upgrade-status will change to upgraded on completion).
Note: If the automatic node upgrade fails to complete successfully, perform the upgrade manually.
- 4 Click **Fault>Log**. Display the Realtime log list by selecting Realtime View to monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade, contact your next level of support.
- 5 This procedure is complete. Return to [Upgrade the system nodes on page 1663](#) to determine your next step.

Upgrade a link node

ATTENTION

To upgrade an NPC, NPS, or NPE node see [Upgrade of NPC, NPS, and NPE nodes on page 1670](#).

ATTENTION

Traffic is maintained through redundant links configured on different link cards. To maintain the traffic, ensure there are redundant links configured on different link cards before upgrading the link card.

To upgrade a single system node, perform the following steps:

Upgrading a link node

At the OAMP workstation

- 1 Select the node to upgrade in the list of available nodes in the software upgrade wizard.
- 2 Click the **Upgrade** button. The system asks for confirmation.
- 3 Wait for node upgrade to complete (upgrade-status will change to upgraded on completion).
- 4 Click **Fault>Log**. Display the Realtime log list by selecting Realtime View to monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.
- 5 Repeat this procedure for all remaining link nodes.
- 6 This procedure is complete. Return to [Upgrade the system nodes on page 1663](#) to determine your next step.

Upgrade multiple link nodes

ATTENTION

To upgrade an NPC, NPS, or NPE node, see [Upgrade of NPC, NPS, and NPE nodes on page 1670](#).

To upgrade multiple system nodes, perform the following steps.

Upgrading multiple link nodes

At the OAMP workstation

- 1 **Shift-click** or **ctrl-click** to select a range of nodes to upgrade in the list of available nodes in the software upgrade wizard.
- 2 Select the delay interval between each successive node upgrade. This will be used to soak the upgraded node before moving to the next system node.
- 3 Click the **Upgrade node** button. The system asks for confirmation.
- 4 Wait for the node upgrade to complete (upgrade-status will change to upgraded on completion).
Note: If the automatic node upgrade fails to complete successfully, perform the upgrade manually.
- 5 The upgrade will now delay for the selected interval before continuing to the next node to upgrade. Upgrade of nodes can

be cancelled at any time by clicking the **Stop** button. To skip the delay count down, click **No delay** and the next node will be upgraded immediately.

- 6 Click **Fault>Log**. Display the Realtime log list by selecting Realtime View to monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.
- 7 Repeat this procedure for all remaining link nodes.
- 8 This procedure is complete. Return to [Upgrade the system nodes on page 1663](#) to determine your next step.

Upgrade of NPC, NPS, and NPE nodes

The upgrade of an NPC, NPS or NPE node or all nodes, requires special handling to ensure that the local subsystem instances associated with an NPC, NPS and NPE chain, have been deactivated. Also, the node to upgrade must not be the active NPC node. If the node to upgrade is the active node, then a switch of activity must be performed prior to upgrading the node.

Note: Upgrading NPC, NPS and NPE nodes is only applicable to systems that include the optional Universal Number Portability Master (UNPM) capability.



CAUTION

Potential for NPDB corruption

If upgrading the NP nodes/chains, the connection to the LSMS will need to be released on the LSMS. Refer to the LSMS operation manual for release methods. Contact Nortel Networks Technical Support for more information. Failure in doing so will result in NPDB corruption.

For a multiple maintenance window, upgrade the NPC and NPS system nodes without NP chains, as indicated in the procedure that follows.

In the first maintenance window

- 1 Upgrade the inactive NPC system node.
- 2 Upgrade one NPS system node.

In subsequent maintenance windows

- 3 Upgrade the remaining NPS system nodes.
- 4 Switch activity (SWACT) to the newly-upgraded NPC node.

5 Upgrade the inactive NPC system node.

For a multiple maintenance window, upgrade the NPC, NPS, and NPE system nodes with NP chains as indicated in the procedure that follows.

In the first maintenance window

- 1 Upgrade the inactive NPC system node, the NPE nodes in that chain, and any associated NPS nodes.
- 2 If no NPS cards have been upgraded, upgrade one NPS node and the NPE nodes in its chain.

In subsequent maintenance windows

- 3 Upgrade the remaining NPS chains, their associated NPS nodes, and the NPE nodes in those chains.
- 4 Switch activity (SWACT) to the newly-upgraded NPC node.
- 5 Upgrade the final NPC system node, the NPE nodes in that chain, and any associated NPS nodes.

Upgrading NPC, NPS, and NPE nodes

On LSMS

- 1 Release all SMI connections to the UNPM. Refer to the LSMS operation manual for release methods.

At the OAMP workstation

- 2 In the menu bar, click **Administration>Platform>Node**.
- 3 Select the NPC you want to upgrade, and check the activity state of the NPC.
- 4 Use the following table to determine your next step.

If the NPC is	Do
active	Perform a SWACT, then continue to step 5 .
inactive	Continue to step 5 .

- 5 Deactivate the NP local subsystem instance running on the inactive NPC system node as follows:

Click

Configuration>SCCP>shared-local-subsystem-instance, select the desired NPx, and click **Deactivate**.

- 6** If an NPE chain has been provisioned with this NPC node as the master and with an alternate NPS system node, then deactivate the local subsystem instance running on the alternate NPS as follows:

Click

Configuration>SCCP>shared-local-subsystem-instance, select the desired NPx, and click **Deactivate**.

- 7** Using the software upgrade wizard, select the NPC node to upgrade in the list of available nodes.
- 8** Click the **Upgrade node** button. The system asks for confirmation.
- 9** Wait for node upgrade to complete (the upgrade-status will change to upgraded on completion).

Note: If the automatic node upgrade fails to complete successfully, perform the upgrade manually.

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

If	Do
an NPE chain is provisioned with this NPC node as master	repeat step 7 to step 9 for each NPE system node and the alternate NPS system node associated with this chain.
there is no NPE chain associated with this NPC node	proceed to step 11

- 11** Wait for the local subsystem instance to be deactivated/prohibited.
- 12** Reactivate the local subsystem instance running on the inactive NPC as follows:

Click

Configuration>SCCP>shared-local-subsystem-instance, select the desired NPx, and click **Activate**.

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

If	Do
an NPE chain is provisioned with an alternate NPS system node	step 14

	If	Do
	there is no NPE chain provisioned with an alternate NPS system node	step 15
14	Wait for the local subsystem instance to be deactivated/prohibited, and then reactivate the local subsystem instance running on the alternate NPS as follows: Click Configuration>SCCP>shared-local-subsystem-instance , select the desired NPx, and click Activate .	
15	Wait for the reactivated local subsystem instances to return to the activated/allowed state.	
16	Click Fault>Log . Display the Realtime log list by selecting Realtime View to monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.	
17		
	If	Do
	NPS system nodes are provisioned without a chain, or NPS system nodes which are masters of a chain	select an NPS system node to be upgraded. This node cannot be an NPS system node already upgraded in the previous steps or the NPS system node associated with the currently active NPC chain.
	there are no further NPS system nodes to be upgraded	proceed to step 30 .
18	Deactivate the NP local subsystem instance running on the NPS system node as follows: Click Configuration>SCCP>shared-local-subsystem-instance , select the desired NPx, and click Deactivate .	
19	If an NPE chain has been provisioned with an alternate NPS for the selected NPS, deactivate the NP LSS instance running on the alternate NPS system node as follows: Click Configuration>SCCP>shared-local-subsystem-instance , select the desired NPx, and click Deactivate .	

- 20** Using the software upgrade wizard, select the NPS node to upgrade in the list of available nodes
- 21** Click **Upgrade node**.
- 22** Wait for node upgrade to complete (upgrade-status will change to upgraded on completion).
- Note:** If the automatic node upgrade fails to complete successfully, perform the upgrade manually.
- 23** Use the following table to determine your next step.

If	Do
an NPE chain has been provisioned for this NPS node	repeat step 20 to step 22 for each NPE system node and the alternate NPS system node associated with this chain.
there is no NPE chain associated with this NPS node	step 24

- 24** Wait for the local subsystem instance to be deactivated/prohibited.
- 25** Reactivate the local subsystem instance running on the NPS as follows:
Click
Configuration>SCCP>shared-local-subsystem-instance, select the desired NPx, and click **Activate**.
- 26** If an NPE chain has been provisioned with an alternate NPS system node:
- a** Wait for the local subsystem instance to be active/allowed.
 - b** Reactivate the NP local subsystem instance running on the alternate NPS as follows:
Click
Configuration>SCCP>shared-local-subsystem-instance select the desired NPx, and click **Activate**.
- 27** Wait for the reactivated local subsystem instances to return to the activated/allowed state.
- 28** Click **Fault>Log**. Display the Realtime log list by selecting Realtime View to monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.

- 29 Repeat [step 17](#) to [step 28](#) for any remaining NPS system nodes in the system, otherwise proceed to [step 30](#).
- 30 Switch activity between the active and inactive NPC nodes as follows:

Click **Administration>platform>node** for the currently active NPC node, then click **Swact**.
- 31 Deactivate the NP local subsystem instance running on the inactive NPC system node as follows:

Click
Configuration>SCCP>shared-local-subsystem-instance, select the desired NPx, and click **Deactivate**.
- 32 If an NPE chain has been provisioned with an alternate NPS system node, deactivate the local subsystem instance running on the alternate NPS as follows:

Click
Configuration>SCCP>shared-local-subsystem-instance, select the desired NPx, and click **Deactivate**.
- 33 Using the software upgrade wizard, select the newly inactive NPC node to upgrade in the list of available nodes.
- 34 Click the **Upgrade node** button.
- 35 Wait for the node upgrade to complete (upgrade-status will change to upgraded on completion).

Note: In the event that the automatic node upgrade fails to complete successfully, perform the upgrade manually.
- 36 If an NPE chain has been provisioned for this NPC, repeat [step 33](#) to [step 35](#) for each NPE system node and the alternate NPS system node associated with this chain.
- 37 Wait for the local subsystem instance to be deactivated/prohibited, then, reactivate the local subsystem instance running on the inactive NPC as follows:

Click
Configuration>SCCP>shared-local-subsystem-instance, select the desired NPx, and click **Activate**.
- 38 If an NPE chain has been provisioned with an alternate NPS system node, wait for the local subsystem instance to be deactivated/prohibited, then reactivate the local subsystem instance running on the alternate NPS as follows:

Click
Configuration>SCCP>shared-local-subsystem-instance, select the desired NPx, and click **Activate**.

- 39** Wait for the reactivated local subsystem instances to return to the activated/allowed state.
- 40** Click **Fault>Log**. Display the Realtime log list by selecting Realtime View to monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.
- 41** Ensure the activity state of the NPC is set to not-active as follows:
- Click **Administration>shared>local-subsystem**. If the NPC's activity state is currently active then go to [step 38](#), otherwise go to [step 39](#).
- | If: | Do: |
|--|--------------------------------------|
| the NPC's activity state is currently active | proceed to step 42 . |
| the NPC's activity state is currently inactive | proceed to step 43 . |
- 42** Switch activity between the active and inactive NPC nodes as follows:
- Click **Administration>platform>node** for the currently active NPC node, then click **Swact**.
- 43** Click **Fault>Log**. Display the Realtime log list by selecting Realtime View to monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If it does, do not continue with the node upgrade.

On LSMS

- 44** Re-establish all SMI connections to the UNPM. Refer to the LSMS operation manual for release methods.
- 45** This procedure is complete. Return to [Upgrade the system nodes on page 1663](#) to determine your next step.

Perform a SWACT and upgrade the Inactive RTC node in slot 12

ATTENTION

After completing [step 5](#) in the procedure that follows, you will not be able to abort the upgrade process, except by performing an out-of-service alternate boot to the data snapshot taken before you started the upgrade procedure.

Upgrade of the RTC in slot 12 can take up to 20 minutes to complete.

Performing a SWACT and upgrade for the inactive RTC node in slot 12

At the OAMP workstation

- 1 Verify that RTC15 is the active RTC.
 - a In the menu bar, click **Configuration>platform>node**.
 - b Click the **Graphical view** tab.
 - c Double-click the RTC in slot 15.

If:	Do:
the Activity State is Active	step 2
the Activity State is not Active	perform a SWACT, then proceed to step 2

- 2 Select the RTC12 node to upgrade from the list of available nodes in the software upgrade wizard.
- 3 Use the following table to determine your next step.

If	Do
you want to proceed with the upgrade	step 5
you want to abort the upgrade process	step 4

- 4 Verify that RTC12 is the active RTC.
 - a In the menu bar, click **Configuration>platform>node**.
 - b Click the **Graphical view** tab.
 - c Double-click the RTC in slot 12.

If:	Do:
the Activity State is Active	Downgrading Using the Wizard on page 1744
the Activity State is not Active	perform a SWACT and proceed to Downgrading Using the Wizard on page 1744

- 5 Click the **Upgrade** button.
- 6 Wait for the node upgrade to complete (upgrade-status will change to upgraded on completion).

Note: In the event that automatic node upgrade fails to complete successfully, perform the upgrade manually.
- 7 Wait 10 minutes and then perform a SWACT.
- 8 Click **Fault>Log**. Display the Realtime log list by selecting Realtime View to monitor the USP to ensure it performs normally and does not report any LOG_SWERRs or LOG_TRAPs. If LOG_SWERRs or LOG_TRAPs are reported, do not continue with the node upgrade. If the upgrade was successful, proceed to the next step.
- 9 Click **Next** and continue with [Activating new features on page 1681](#).
- 10 This procedure is complete. Return to [Upgrade the system nodes on page 1663](#) to determine your next step.

Upgrade nodes manually

Perform the steps in the following procedure to manually upgrade any system node type including link nodes, as appropriate.

ATTENTION

The procedure that follows provides the general steps on how to upgrade a system node. However, nodes must be upgraded in a specific order. Refer to section [Upgrading the system nodes for one maintenance window upgrades on page 1663](#) or [Upgrading the system nodes for multiple maintenance window upgrades on page 1665](#) as appropriate.

Upgrading nodes manually

At the OAMP workstation

- 1 If you are manually upgrading a system link node and if the system link node is unlocked and enabled, proceed to [step 2](#); otherwise, proceed to [step 3](#).

If you are manually upgrading a non-link node, and if the system node is unlocked and enabled proceed to [step 5](#), otherwise, proceed to [step 4](#).
- 2 Inhibit all of the links on the system node, if applicable. See the USP Configuration Management guide for these procedures.

Note: You cannot inhibit IPS7 links. If there is only one available link on a linkset, you will not be able to inhibit it. If it is a one-link linkset, proceed to [step 3](#) without inhibiting the link. If there are other links on the linkset, make at least one of them available before attempting to inhibit the link.
- 3 Deactivate all of the links or paths on the system node, as applicable to the system node. See the USP Configuration Management guide for these procedures.
- 4 Set the boot image of the node by completing the following steps. For link nodes, complete substeps [a](#) - [f](#). For non-link nodes, complete substeps [a](#) - [d](#) and then [f](#).
 - a Click **Configuration>platform>node**.
 - b Click **Graphical View**.
 - c Click the slot for the node you need to upgrade to open the node in the Administration panel.
 - d Select the drop-down menu to set the boot image to the new release version.
 - e For link nodes, you also need to set its HA boot image to the new HA release version.

Note: IPS7 and IP high-speed (HSL) link cards do not require HA loads.
 - f Click **Modify**.

Note: The card must be reloaded immediately after the boot image is set to the new release version.
If the system node is off-line, the setting of the boot image reset the status to Upgraded. There are no alarms for an offlined node.

- 5 Lock and load the system node. See the USP Configuration Management guide for these procedures.
- 6 When the system node becomes enabled, **unlock** it.
- 7 Verify that the running load is the new version. If not, make sure that the correct image is selected in the platform-node Administration panel. If not, contact your next level of support.
- 8 For link nodes, **Activate** and **uninhibit** all of the links on the system link node.
- 9 Click **Fault>Log**. Display the Realtime log list by selecting Realtime View to monitor the USP for 15 minutes after you upgrade the first card and each unique card type in the system (for example, ATM and IP). Make sure the USP performs normally and does not report any LOG_SWERRs or LOG_TRAPs. During this period, perform test calls to verify that the newly loaded system node performs consistently with its pre-upgrade status. Take steps to ensure test calls are routed through links on this Link system node.
- 10 After the first linkset is upgraded (a linkset upgrade requires the upgrade of several link cards), perform a test call to make sure all of the link cards in the linkset have been correctly upgraded. If there are any errors, contact your next level of support. The test call for the linkset is required only for the first linkset upgraded.
- 11 Repeat [step 1](#) to [step 9](#) for the remaining system nodes on the remaining CAM shelves. Upgrade the system nodes from the lowest slot on the lowest-numbered shelf to the highest slot on the highest-numbered shelf. After you have successfully upgraded the first system node, remaining system nodes only need to be monitored for stability. A complete set of test calls will be performed when all system nodes are upgraded.
- 12 Perform a complete set of test calls when all system nodes are upgraded.

If it was determined prior to the upgrade, that the site is using a route master configuration, perform the following test calls:

 - network to host
 - network to donor
 - host to donor
 - migrated donor to donor
- 13 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Activate features

You must activate the new features of the software load. All system nodes must be upgraded to activate features.

ATTENTION

When you activate new features, all GUI connections will log out and log back in automatically to re-initialize in order to pick up the new features. Select Administration>software-upgrade. Click Next to go to the feature activation screen.

Activating new features

At the OAMP workstation

- 1 Click **Activate Features**.
- 2 Click **Yes** to accept the activation and continue.
- 3 Perform test calls to verify that messages are correctly routed.
If it was determined prior to the upgrade that the site is using a route master configuration, the following test calls must be performed:
 - network to host
 - network to donor
 - host to donor
 - migrated donor to donorClick **Fault>Log**. Display the Realtime log list by selecting Realtime View to monitor the USP to ensure it does not report any LOG_SWERRs or LOG_TRAPs.
- 4 This procedure is complete. Return to [Upgrade the system nodes on page 1663](#) to determine your next step.

Deactivate upgrade features

Complete this procedure only if you want to deactivate new features from a software upgrade (for instance, in the event of a degradation in service). If features for the new release were activated, deactivate the features using the Upgrade Administration window.

Deactivating new features

At the OAMP workstation

- 1 Open the Upgrade Administration window as follows:
Click **Administration>software-upgrade> Deactivate New Features**.
A confirmation dialog box appears.
- 2 Click **Yes** to deactivate or **No** to leave features active.
- 3 You have completed this procedure. Proceed to the next section ([Cleanup](#)).

Cleanup

The cleanup stage, deletes some of the upgrade files that were used during the upgrade.

Running the cleanup

At the OAMP workstation

- 1 Click **Administration>software-upgrade**.
- 2 Ensure that the new features are activated.
- 3 Click **Next**.
- 4 Click **Run Cleanup**.
A confirmation dialog box appears.
- 5 Click **Yes**.
- 6 Proceed to the next section ([Complete the upgrade](#)).

Complete the upgrade

The complete stage stops the upgrade, shuts down the wizard, creates a data snapshot, restores access privileges, and checks the donor switch for SS7 alarms.

Stopping the upgrade

At the OAMP workstation

- 1 Click **Administration>software-upgrade**
- 2 Click **Stop Upgrade**. A confirmation dialog box appears. To inform the system that the upgrade has completed successfully, click **Yes**.
- 3 Click the X at the top right corner of the wizard action panel to close the wizard.

- 4 Set user privileges back to pre-upgrade settings and re-enable any user accounts that were disabled during the upgrade. Refer to the file you created in "Limit user access" section, step [7](#) for the correct user status. Refer to the sections Security: User accounts and Security: User session in the USP Administration and Security guide for additional information.
- 5 Create a data snapshot, copy it to the alternate boot server and set the alternate boot server snapshot. Refer to procedure [Creating an alternate boot data snapshot on page 1642](#).
- 6 If it was determined prior to the upgrade that the site is using a route master configuration, check the donor switch for SS7 alarms.
- 7 Determine whether the USP is installed on the IEMS. Launch the IEMS Java Web Start Client (refer to "Launching IEMS Java Web Start Client" in *IEMS Basics*, NN10329-111).
- 8 Select the Network Elements topology panel in the IEMS Topologies tree.
- 9 In the list of network elements that displays, determine whether the USP is present.
- 10 Use the following table to determine your next step.

If the USP is	Do
configured in IEMS	step 11
not configured in IEMS	step 12

- 11 Update the software version in the Device Version field by editing the Managed Object Properties in IEMS for the USP that you just upgraded to reflect the new software version.
Refer to either of the following procedures to update the Device Version field:
 - [Editing and viewing object properties using Java Web Start Client on page 2255](#)
 - [Editing and viewing object properties using Web Client on page 2261](#).
- 12 Exit from the IEMS Java Web Start Client.

13 You have completed this procedure.

If	Do
you have a Nortel Ethernet Routing Switch 8600 in your solution and you want to enable auto-negotiate	Configure the Nortel Ethernet Routing Switch port to auto-negotiate on page 1684
otherwise	Post-upgrade checklist on page 1688

Configure the Nortel Ethernet Routing Switch port to auto-negotiate**ATTENTION**

Perform this procedure if you have a Nortel Ethernet Routing Switch 8600 in your solution, and you want to enable auto-negotiation.

If you are not using auto-negotiation, skip this procedure and proceed to [Post-upgrade checklist on page 1688](#).

To enable auto-negotiation of the Ethernet port speed and duplex state, perform the following steps at the command line interface to the Nortel Ethernet Routing switch.

Note: After you execute [step 1](#) of this procedure and you confirm that you will need to modify auto-negotiate, lock the IPS7 card before you make the 8600 port change. After the port change, load and unlock the card. Perform these steps at the USP OAMP workstation.

Configuring the Nortel Ethernet Routing Switch port

At the CLI for the Nortel Ethernet Routing Switch

- 1 Determine the slot and port on the Nortel Ethernet Routing Switch that connects to the device:

```
> show ip arp info <ip_address>
```

ip_address

is the physical IP address of the IPS7 GW card.

The slot and port are reported.

```
prompt:cpu> show ip arp info 172.30.242.25
```

```
=====
                                     Ip Arp
=====
 IP_ADDRESS      MAC_ADDRESS      VLAN  PORT  TYPE  TTL
-----
 172.30.242.25   00:90:69:1a:d4:fc   200   1/2   DYNAMIC 272
```

If the response indicates MLT instead of the slot and port, perform this operation from the mate Nortel Ethernet Routing Switch unit. If the response indicates that no arp entry is found, ping the IP address from the CLI, and retry the command.

- 2 Determine if the ports are already set to auto-negotiate by typing:

```
> show port info config port <slot>/<port>
```

and pressing the Enter key.

where

<slot>

is the slot number from the previous step

<port>

is the port number from the previous step

```
prompt:cpu> show port info config port 1/2
```

Port Config											
PORT NUM	TYPE	AUTO NEG.	SFFD	ADMIN DUPLX	SPD	OPERATE DUPLX	SPD	DIFF-SERV EN	QOS TYPE	MLT LVL	ID
1/2	100BaseTX	false	false	half	100	full	100	fals	core	1	0

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

If the ports	Do
are already set to auto-negotiate	step 10
are not set to auto-negotiate	step 4

At the OAMP workstation

- 4 Lock the IPS7 card connected to the 8600 port as follows:
- Click **Configuration>platform>node**.
 - Click the **Graphical View** tab.
 - Double-click the slot of the IPS7 card you want to lock.
 - Click **Lock**. A confirmation dialog box appears.
 - Click **Yes**.

At the CLI for the Nortel Ethernet Routing Switch

- 5 Set the slot and port to auto-negotiate:
- ```
> config ethernet <slot>/<port> auto-negotiate enable
```

*The slot and port are reconfigured to auto-negotiate and the prompt returns.*

```
prompt:cpu> config ethernet 1/2 auto-negotiate enable
prompt:cpu>
```

**6** Verify the port configuration:

> **show port info config port <slot>/<port>**

*The slot and port configuration is displayed.*

```
prompt:cpu> show port info config port 1/2
```

```
=====
Port Config
=====
```

| PORT<br>NUM | TYPE      | AUTO<br>NEG. | SFFD  | ADMIN<br>DUPLX | SPD | OPERATE<br>DUPLX | SPD | DIFF-SERV<br>EN | TYPE | QOS<br>LVL | MLT<br>ID |
|-------------|-----------|--------------|-------|----------------|-----|------------------|-----|-----------------|------|------------|-----------|
| 1/2         | 100BaseTX | true         | false | half           | 100 | full             | 100 | fals            | core | 1          | 0         |

**7** Commit the change:

> **save config**

**At the OAMP workstation****8** Load the IPS7 card as follows:

- Click **Configuration>platform>node**.
- Click **Graphical View**.
- Double-click the slot of the IPS7 card you want to load.
- Click **Load**. A confirmation dialog box appears.
- Click **Yes**.

**9** Unlock the IPS7 card as follows:

- Click **Configuration>platform>node**.
- Click the **Graphical View** tab.
- Double-click the slot of the IPS7 card you want to unlock.
- Click **Unlock**. A confirmation dialog box appears.
- Click **Yes**.

**10** This procedure is complete. Proceed to the next section ([Post-upgrade checklist](#)).

## Post-upgrade checklist

This checklist provides system cleanup on your upgraded USP. Perform this checklist on your alternate boot server. To complete the post-upgrade checklist, perform the following steps:

**Note:** Wait 24 hours after completing all of the upgrade procedures.

### Performing the post-upgrade checklist

#### *At the OAMP workstation*

- 1 Begin a new log time period to end the upgrade log tracking time period as follows:

Click **Fault>Log>New Period**.

- 2 Delete all snapshots associated with the previous USP release from both RTC system nodes as follows:

**Note:** If you have changed your boot image file for a new release, Nortel Networks recommends that you delete the out-of-date image file from your system using the File Manager function.

- a In the File Manager panel, select the data snapshot to be deleted from the Snapshot field in the RTC portion of the window.

**Note:** You cannot delete the boot data snapshot. If you attempt to delete the boot data snapshot, you will receive an error message.

- b Expand the Snapshot folder.
    - c Expand the folder for the previous version of the software.
    - d Click **Delete** to delete the snapshot. An hourglass appears while the data snapshot is deleted. When the deletion operation is complete, snapshot is removed from the RTC side of the File Manager panel.

- 3 Delete old loads from the Alternate Boot Server:

- a Open the ABS configuration manager application. If your ABS is on a PC, then open the configuration manager from the Windows **Start** menu and perform substeps [d](#) to [f](#). If your ABS is on the CMT, then proceed to substep [b](#).

- b There are two versions of the ABS Configuration Manager available on the CMT. One is graphically-based and the other is console-based. If you want to use graphically-based ABS Configuration Manager, perform substeps [c](#) to [f](#). If you want to use the console-based ABS Configuration Manager, perform substeps [g](#) to [h](#).
  - c For the graphically-based ABS Configuration Manager on the CMT, perform the following:
    - i Ensure that your X-Windows server software is running and that host access permissions are allowed for the CMT. Refer to your X-Windows server software manual for details.
    - ii Log in to the CMT as root.
    - iii Enter **DISPLAY=<IP address of your PC>:0.0**. To find the IP address of the PC you are using, enter **ipconfig** from a DOS window.
    - iv Enter **export DISPLAY**. To confirm the export, enter **echo \$DISPLAY**.
    - v Enter **cd /<USP install path>/ntssgusp/abs**.
    - vi Launch the ABS Configuration Manager. Type **./ABS&**
  - d Click **File>uninstall Release**. The uninstall existing release window appears.
  - e Select the release to be deleted from the drop-down menu.
  - f Click **Apply**.
  - g Enter **./console\_abs** to launch the console-based ABS Configuration Manager application. You will be prompted with the **ABSCM>** prompt.
  - h Enter **ABSCM>release uninstall <release-name>**

**Note:** Refer to the ABS\_Specification.pdf document for all the command syntax of the console-based ABS Configuration manager.
- 4 Delete old snapshots from the Alternate Boot Server.
  - a Click the **Administration** button on the main menu.
  - b Click **File Manager**.
  - c In the Alternate Boot Server window, navigate to the release associated with the snapshots you wish to remove.
  - d Click on the snapshot you want to delete.
  - e Click **Delete**.

- 5 Perform a hard disk defragmentation on your alternate boot PC. On a Windows 2000 machine, open the Disk Defragmenter utility (**Start>Programs>Accessories>System Tools>Disk Defragmenter**). Select the **Analyze** option. If Windows recommends that the disk be Defragmented, run the utility.
- 6 This procedure is complete. Return to [Upgrading the USP on page 1631](#) to determine your next step.

## Logging in to the USP GUI

The following procedure provides the instructions to log in to the USP GUI that is installed on either a Windows-based workstation or the CS 2000 Management Tools (CMT) server.

### *At your workstation*

- 1 Log in to the USP GUI.

| If the USP GUI is installed on   | Do                     |
|----------------------------------|------------------------|
| a Windows-based OAMP workstation | <a href="#">step 2</a> |
| the CMT server                   | <a href="#">step 5</a> |

### *At the windows-based OAMP workstation*

- 2 Click the Windows Start button on your desktop.
- 3 Select **Programs->Universal Signaling Point->Universal Signaling Point GUI**.

The USP Interface Client window appears with either the Session-Login or Site Manager dialog box displayed in the window.

- 4 Proceed to [step 10](#).

### *At your workstation*

- 5 Launch your web browser.
- 6 In the Address field, enter the name or IP address of the CMT server.  
The Application Launch Point page appears.
- 7 Click **Application Launcher**.  
The Login window appears.
- 8 Enter your user name and password, then click **Log In**.  
The Application Launch Point window appears after a valid login.
- 9 Click the **Universal Signaling Point Interface Client** link to launch the GUI.

The USP Interface Client window appears with either the Session-Login or Site Manager dialog box displayed in the window.



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

| <b>If the</b>                    | <b>Do</b>               |
|----------------------------------|-------------------------|
| Site Manager dialog box appears  | <a href="#">step 11</a> |
| Session-Login dialog box appears | <a href="#">step 14</a> |

- 11** Click **New**, and enter the site name, the rtc-12 ipaddress and rtc-15 ipaddress.
- 12** Click **Apply**.
- 13** Click **OK**.  
The Session-Login dialog box appears.
- 14** Enter the login account and password.
- 15** You have completed this procedure. If applicable, return to the higher level task or procedure that directed you to this procedure.

## Migrating the Alternate Boot Server (ABS) from USP PC to CS 2000 Management Tools

The purpose of this method is to provide information and instructions for migrating the Alternate Boot Server (ABS) from the USP EM PC to the CS 2000 Management Tools (CMT) server on the SPFS platform

### Material requirements

The following is a list of material requirements.

#### Required documents

The required documents are listed as follows:

- Job Site Information Package
- Customer Information Documentation (CI or CNCD)
- Installation Safety Manual (ISM/IMO). This document can be requested from the Regional Tool Facility.
- EHS (European Health and Safety) EHS\_MAN\_002
- WMS (Workmanship Standards) WMS-001

#### Tools

The tools listed in the following table are required.

| U.S. tools | Canadian tools | Description               |
|------------|----------------|---------------------------|
| E003389    | E003389        | Installation Data Toolkit |

#### Software

Software for USP11.0.0, USP Compact, or BBSTP on CD is required.

### Precautions

Observe the general safety precautions against personal injury and equipment damage outlined in the ISM/IMO at all times.

Due to the nature of the BOOTP protocol, the BOOTP server must either be located on the same IP subnet as the USP or be used with a BOOTP server and router that support BOOTP forwarding.

Do not power down a terminal if connected to a console port on the T240. Powering down the terminal will take the T240 down.

Do not disconnect a serial connection to the Netra T240 before closing any application that was previously using the port. This will cause the

server to lock-up and will have to be powered down to gain access once again.

Prior to integrating any equipment into the network it is critical to verify the IP Address assigned to the new equipment is not already assigned to existing equipment on the network. Perform a Ping test prior to assigning IP Addresses to any equipment to verify the IP Address is not currently assigned. Verify no response is received when performing the Ping test prior to integrating any equipment into the network.

## Preparations

Prior to starting the operations presented in this method, arrange all materials, tools, and test equipment at the work location so as to minimize fatigue and inconvenience.

For the installation, you can use either a graphical interface (Hummingbird suite) or a command line interface. If you require it, ensure the FT laptop has Hummingbird installed and contains FTP and Exceed. If you use Exceed, make sure the application is configured to support the upgrade. See [Configuring Exceed for an upgrade on page 1634](#).

The following information must be provided by the customer or site specific documentation. Use the following table to help insert the customer provided information throughout the method. The following table will be used for an initial install.

| System variable                                                                                                                          | Actual value |
|------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <b>Client PC Information (Current ABS)</b>                                                                                               |              |
| PC HostName                                                                                                                              |              |
| PC IP Address                                                                                                                            |              |
| List all PC usernames and passwords that will be needed<br>DISTINCT BOOTP/FTP/NFS Server passwords<br>ABS Configuration Manager password |              |
| Configured Sites                                                                                                                         |              |
| Alternate Boot Loads<br>RTC-12<br>RTC-15                                                                                                 |              |

| System variable                                 | Actual value                                                              |
|-------------------------------------------------|---------------------------------------------------------------------------|
| ABS Snapshot                                    |                                                                           |
| <b>CS2000 Management Tools Server (new ABS)</b> |                                                                           |
| CMT HostName                                    |                                                                           |
| CMT IP Address                                  |                                                                           |
| Root user<br>Root password                      | root<br>(root password is set to root during factory loading of the SPFS) |
| User account<br>Password                        | FIELD<br>SERVICE                                                          |
| <b>BOOTP settings</b>                           |                                                                           |
| SiteName                                        |                                                                           |
| Gateway IP Address                              |                                                                           |
| RTC-12 MAC address                              | Note: Do not include the :’s                                              |
| RTC-15 MAC address                              | Note: Do not include the :’s                                              |
| Host IP Address                                 | Note: This is the RTC IP address                                          |
| Server IP Address                               | Note: This is the CMT IP address                                          |
| Subnet Mask                                     |                                                                           |

## Overview

In the Carrier Voice over IP Solution, a customer has the option of moving the existing PC ABS function to the CS 2000 Management Tools (CMT) server. The following method will provide the procedures to complete the migration of the ABS and install the USP EM on the CMT server.

This method contains the following procedures:

- [Preparing the PC ABS workstation on page 1696](#)
- [Creating a user account for the CMT Server on page 1697](#)

- Install/configure the ABS application using only one of the following procedures:
  - [Install and configure the ABS application using Exceed on page 1698](#)
  - [Install and configure the ABS application using a console on page 1699](#)
- [Access verification and pre-migration completion on page 1701](#)
- [CMT Server migration on page 1703](#)
- [Verification procedure on page 1711](#)

## PC ABS workstation

To prepare the PC ABS workstation for installation and configuration procedures, perform the following steps.

### Preparing the PC ABS workstation

#### *From the ABS PC workstation*

- 1 To reduce the amount of data that will need to be moved, uninstall any unused releases from the ABS Manager. To do this, perform the following steps:
  - Note:** The tool checks to ensure that no existing USP sites are using the release loads files and snapshots.
  - a Log in to the ABS Configuration Manager: Click **File>Login**.
  - b Type **SERVICE** for the password and click **OK**.
- 2 Select **File>Uninstall Release**.
- 3 Click on the release that you want to uninstall and select **apply**.
  - Note:** Do not remove the current release.
- 4 Close the Uninstall window when all unused releases have been removed.
- 5 Delete any old snapshots from the existing USP sites if they are no longer required.

To open the ABS Configuration Window, select **File>ABS Configuration**.
- 6 Select each Site using the drop-down menu. Using the drop-down menu, select the Snapshot record you want to delete.
- 7 Click **Delete**.
  - Note:** You will only be able to delete snapshots that begin with bv\*\*\*\*\*. Keep at least one recent snapshot.

- 8 Click **OK** when all old snapshots have been removed.
- 9 Repeat for all sites in office.
- 10 In the ABS Configuration window, record all the sites that are configured along with their Alternate Boot loads and Snapshot records. (See the table provided on page [1694](#).)
- 11 Log out of the ABS Configuration Manager.
- 12 Click **YES** to confirm and minimize window.
- 13 Record the BOOTP settings for reference when setting up the CMT as follows:
  - a Open the Distinct BootP Server window.

**Note:** You may have to log in using **File>Login** (FIELD passwd SERVICE).
  - b Click **Configure>Server**.
  - c Click on each of the Address and Networks tabs.
  - d Capture data.
- 14 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## CMT Server user account

Complete the setup of the FIELD user account on the SPFS server. By default, the FIELD account is created in the Carrier Voice over IP group. However, the password now needs to be set.

### Creating a user account for the CMT Server

#### *Setup UserID and Password for ABS Server on CMT*

- 1 Open a Telnet session. To do this, click **Start>Run**.
- 2 Enter the <CMT IP address>:  
**Telnet <CMT IP address>**
- 3 Click **OK**.  
The session opens.
- 4 Log in as maint:  
Type: **maint**  
Type: **<maint password>**
- 5 Switch user to root:  
Type: **su -root**

Type: **<root password>**

**Note:** The FIELD user is created as part of the SPFS install.

- 6 Change the password to SERVICE:

Type: **passwd FIELD**

- 7 Type: **SERVICE**

You will be prompted to re-enter your new password.

- 8 Do not close the Telnet window.

## Install and configure the ABS application using Exceed

### ATTENTION

The procedures in this section assume that you are using the software distribution CD.

When installing the BPS/USP EM on the SPFS server, you will have to export the display to your PC. If you prefer to use a command line interface for this installation, see [Install and configure the ABS application using a console on page 1699](#). The SPFS is a headless server (no keyboard or monitor) and therefore a GUI install must be re-routed to a PC with a display.

In this procedure, use Exceed to assist in the installation of the USP EM.

### Installing and configuring the ABS application using Exceed

#### *From the FT Laptop PC*

- 1 Make sure Exceed is configured to support the upgrade. See the Preparations section of this procedure and [Configuring Exceed for an upgrade on page 1634](#).

- 2 To start an Exceed session, click **Programs>Hummingbird Suite>Exceed>Exceed**.

The program will be running and minimized to the task bar.

- 3 Return to your Telnet session.

Type: **DISPLAY=<IP address of your PC>:0.0**

**Note:** To find the IP address of the PC you are using, type: ipconfig from a DOS window.

- 4 Type: **export DISPLAY**

- 5 Type: **echo \$DISPLAY**

You will see <IP address of your PC>:0.0.

**6** Type: **cd /cdrom/cdrom0**

Type: **ls**

Ensure that you see the file install.bin.

**7** Type: **./install.bin**

This can take several minutes to launch. You will see the following response:

- Preparing to install...
- Extracting the JRE from the installer archive...
- Unpacking the JRE...
- Extracting the installation resources from the installer archive...
- Configuring the installer for this system's environment...
- Launching installer...
- .....
- (new PC window)

A new window will appear on your PC (from the Exceed session).

**8** Click **Next** and you will see the selection of components to install.

**9** Select the components you want to install using the **Choose** button.

**10** Click **Next** and you will see a warning for disk space.

**11** Click **OK**.

**12** When the installation is complete, close the window by selecting **Done**.

**13** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Install and configure the ABS application using a console

If you have already performed this installation with Exceed in the last procedure, skip this procedure.



## Installing and configuring the ABS application using a console

### From the FT Laptop PC

- 1 To switch to the CDROM, enter **cd /cdrom**.  
This command can be slightly different depending on the system you are using.
- 2 To ensure that the file is there, type **ls**.  
Check that you see the file **install.bin**.
- 3 Enter **./install.bin -i console**.  
You will now see preparations for console mode installation. This can take a few minutes.
- 4 Press **Enter** to continue.
- 5 Use the following table to determine your next step.

| If you are                                                  | Do                     |
|-------------------------------------------------------------|------------------------|
| using the CS 2000 Management Tools webstart application     | <a href="#">step 6</a> |
| not using the CS 2000 Management Tools webstart application | <a href="#">step 8</a> |

- 6 Change the selected packages. Type **1** to select item 1 **USP Software Loads and ABS Manager**.

#### *Example of Package Selection panel*

```

1 - [X] USP Software loads and ABS Manager
2 - [X] USP Graphical Interface Client
3 - [X] USP User Manuals and Documentation Suite
Enter software component numbers and press
<Enter> to continue.
```

- 7 Press **Enter** and go to [step 10](#).
- 8 Change the selected packages.
  - Type **1** to select item 1 **USP Software Loads and ABS Manager**.
  - Type **2** to deselect item 2 **USP Graphical Interface Client**

#### *Example of Package Selection panel*

```

1 - [X] USP Software loads and ABS Manager
2 - [] USP Graphical Interface Client
```

3 - [X] USP User Manuals and Documentation Suite  
Enter software component numbers and press  
<Enter> to continue.

- 9 Press **Enter** to continue.
- 10 You will be asked to confirm your selection.  
For non-CMT platforms, press **Enter** to see the default USP directory. You can change this if you wish.
- 11 Press **Enter** again to start the installation. You will be updated with the installation progress.
- 12 Press **Enter** to exit.
- 13 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Access verification and pre-migration completion

This procedure will verify the access to the ABS Configuration Manager and ensure that there are no sites at this time.

This procedure will also locate the ntssgusp/abs directory in preparation for the migration.

### Verifying access and completing pre-migration steps

#### *From the FT laptop PC*

- 1 Type: **su -root**  
password <root password>
- 2 Type: **cd /<USP install path>/ntssgusp/**  
Type: **chown -R FIELD:maint2 abs**  
Type: **chmod -R 775 abs**
- 3 Check to ensure permissions are set correctly.  
Type: **ls -l**  
Response:  
*drwxrwxr-x 2 FIELD maint2 \*date\* \*time\* abs*
- 4 Exit from the root user shell. Type: **exit**
- 5 Move to the abs directory. Type: **cd abs**
- 6 There are two versions of the ABS Configuration Manager available on the CMT. One is graphically-based and the other is console-based. If you want to use the graphically-based ABS

Configuration Manager, perform steps [7](#) to [12](#). If you want to use the console-based ABS Configuration Manager, perform steps [13](#) to [16](#).

- 7 Ensure that DISPLAY is set correctly.
- 8 The following command will start the ABS Configuration Manager and export the display back to the IP assigned in the previous steps.  
Type: **./ABS**  
You will be prompted to set your password.
- 9 Enter the Password twice:  
Type: **SERVICE**  
Type: **SERVICE**  
Click **OK**.
- 10 Log in to the ABS Configuration Manager. To do this, click **File>Login**.
- 11 Enter **SERVICE** as the password and click **Login**.
- 12 If you successfully logged into the ABS Configuration Manager, you have verified access.  
**Note:** The window will appear blank. Click on the File pull-down menu. If logout is highlighted then you are logged in.  
You can minimize the ABS window.
- 13 Enter **./console\_abs** to launch the console-based ABS Configuration Manager application.  
You will be prompted with **ABSCM>** prompt.
- 14 Set your password. Enter **ABSCM>passwd set**.  
Supply password as **SERVICE** and re-enter the same again for confirmation.
- 15 Log in to the ABS to go through.  
Type: **ABSCM> login**.  
Supply password as **SERVICE**.
- 16 If you successfully logged into the ABS Configuration Manager, you have verified access.
- 17 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## CMT Server migration

To migrate to the CMT Server, perform the following procedures:

- Configure the FTP and NFS servers on the CMT to allow the transfer of files from existing PC ABS. see [Configuring the FTP and NFS servers on page 1703](#).
- Set permissions on the ABS files. See [Setting permissions on the ABS files \(CMT\) on page 1706](#).
- Verify the data transfer. See [Verifying the data transfer on page 1707](#).
- Enable and configure the BOOTP server on the CMT ABS. See [Enabling and configuring the BOOTP server on the CMT ABS on page 1708](#).
- Disable the BOOTP server on the PC ABS. See [Disabling the BOOTP server on the PC ABS on page 1709](#).
- Verify correct settings for the USP (RTC). See [Verifying correct settings for the USP \(RTC\) on page 1710](#).

### Configuring the FTP and NFS servers

#### *From the FT Laptop PC*

- 1 Open a new Telnet session to the CMT Server.  
**maint**  
**<maint password>**
- 2 Switch to user root.  
**su -root**  
**<root password>**  
Root privileges are required for SPFS modifications.
- 3 From the # prompt,  
Type: **cli**
- 4 Enter the number next to the Configuration menu option.
- 5 Enter the number next to the NFS Configuration menu option.
- 6 Enter the number next to the **usp\_nfs\_on** (turn on the USP NFS configuration) menu option.  
  
You will see this message, followed by the NFS Configuration options:

=== Executing "usp\_nfs\_on"

USP NFS successfully turned on

=== "usp\_nfs\_on" completed successfully

**Note 1:** You need root privileges to enable/disable NFS on the CMT.

**Note 2:** Before executing usp\_NFS\_on, log in again after running the USP installer.

**Note 3:** After executing usp\_NFS\_on, select list\_nfs to check if the directory used to install the USP is mounted.

7 Select **X** three times to exit the CLI tool.

8 Minimize the Telnet session.

**Note:** The next several steps will move the existing ABS data from the USP EM PC over to the CMT Server. These steps will be performed from the Field Technician's laptop. An abstemp folder will need to be created on the FT laptop to temporarily hold the data during the transfer.

9 Open a DOS prompt. To do this, click **Start >Run**. Type **cmd** and click **OK**.

10 Type: **cd \**.

11 Type: **mkdir abstemp**.

12 Type: **dir /w**.

13 Ensure that the abstemp folder is present, and close the DOS window.

14 Before any transfer of data, the FT laptop **MUST** disable the CyberArmor Personal Firewall.

Mouse over the CyberArmor icon in the task bar (right lower corner of the screen).

a Right-click on the CyberArmor.

b Select **Stop Profile** from the pop-up menu.

c When prompted to stop the profile, click **Yes**.

15 To open an FTP session, click: **Start>Programs>Hummingbird suite>Host Access>FTP for windows Explorer**.

The Hummingbird Neighborhood window appears.

16 To connect to the USP EM PC, click: **File>New FTP Profile**.

17 Complete the FTP Site Properties in the General tab window:  
Host Address: **<USP PC IPaddress>**

User Name: **ntssg**

Password: **1ntssgstp** (note: 1 is the #1)

Account:

Initial Directory: **/c/ntssgusp/abs**

**18** In the FTP Site Properties window, select the **Advanced** tab.

**19** De-select **Enable Directory Caching**.

**20** De-select **Passive Mode**.

**21** In the FTP Site Properties window, select the **Other** tab.

Use the drop-box to select **Binary** for Uploading and Downloading.

**22** Click **OK**.

**23** Save the FTP profile:

Type: **USP PC**

Click **OK**.

**24** Double-click the **USP PC**.

A new Explorer window appears.

**25** Ensure that the FT Laptop PC FTP window has the c:\abstemp directory expanded (use the + to expand the directory structure).

Ensure that the USP PC has the ntssgusp\abs directory expanded.

**26** Copy the releases folder from the USP PC to the FT laptop PC.

Right-click on the releases folder and drag it to the C:\abstemp folder. Select **Copy Here**.

You will see the file transfer window while copying the files.

**27** Copy the sites folder from the USP PC to the FT laptop PC.

**28** Right-click on the sites folder and drag it to the C:\abstemp folder. Select **Copy Here**.

**29** Check the C:\abstemp folder to ensure that the releases and sites folders exist (and sub-folders).

**30** Close the Explorer window.

**31** Double-click the **CMT server**.

A new Explorer window appears.

**Note:** The CMT Server profile was created in [Creating a user account for the CMT Server on page 1697](#).

- 32 Ensure that the FT Laptop PC has the abstemp directory expanded and that the CMT has the /opt/usp directory expanded.
- 33 Copy folders from the FT Laptop PC to the CMT Server by holding down the Ctrl key and selecting all releases that are not currently present on the CMT Server. Drag and drop these folders by right-clicking **Copy Here**.
- 34 Ensure that the FT Laptop PC has the abstemp/sites directory expanded. Ensure that the CMT has the /opt/usp directory expanded.
- 35 Copy all files and folders from the FT Laptop PC to the CMT Server.
- 36 Right-click and drag and drop the entire Sites folder onto the /opt/usp/ntssgusp/abs directory.
- 37 Check to ensure that all data was transferred correctly by expanding the CMT server /opt/usp/ntssgusp/abs directory.
- 38 Expand each of the releases and sites folders to ensure correct data.
- 39 Close the Explorer window and the Hummingbird FTP program.
- 40 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Setting permissions on the ABS files (CMT)

#### *From the FT Laptop PC*

- 1 Open/restore a Telnet session to the CMT Server.
- 2 Ensure that you are logged in as root.  
**su -root**
- 3 Type: **cd /**  
Type: **chmod -R 775 /<USP install path>**
- 4 Ensure permissions are set correctly.  
Type: **cd /<USP install path>/../**  
Type: **ls -l**  
Look for the following line:  
*drwxrwxr-x 5 FIELD maint2 \*date\* \*time\* usp*
- 5 Minimize the Telnet session.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Verifying the data transfer

### *From the FT Laptop PC*

- 1 Restore or open the ABS Configuration Manager on the CMT Server. There are two versions of the ABS Configuration Manager available on the CMT. One is graphically-based and the other is console-based. If you restored or opened the graphically-based ABS Configuration Manager, perform steps [2](#) to [6](#). If you restored or opened the console-based ABS Configuration Manager, perform steps [7](#) to [13](#).
- 2 Click on **File>ABS Configuration**.  
The Alternate Boot Server window appears.
- 3 Verify that all required sites and releases are present.
- 4 Select each site in the drop down menu and verify the following:
  - RTC loads
  - Snapshots
- 5 Click the **Apply** button for each site. When you click the Apply button, the ABS Configuration Manager will rebuild the site-specific configuration files based on the CMT directory structure.
- 6 Minimize the ABS Configuration Manager window.
- 7 Enter the **ABSCM>site show <site-name>** command to view the site's details.
- 8 To view all the available loads, enter **ABSCM>load show all**
- 9 To view all the snapshots for a specified site, enter:  
**ABSCM>snapshot show <site-name>**
- 10 To modify the RTC12-load of the specified site, enter:  
**ABSCM>site mod <site-name> rtc12-load <new-rtc12-load-name>**
- 11 To modify the RTC15-load of the specified site, enter:  
**ABSCM>site mod <site-name> rtc15-load <new-rtc15-load-name>**
- 12 To modify the snapshot name of the specified site, enter:  
**ABSCM>site mod <site-name> snapshot <new-snapshot-name>**
- 13 When the site mod command is executed, the ABS Configuration Manager will rebuild the site-specific configuration files based on the CMT directory structure.



- 14 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

**Note:** Refer to the *ABS\_Specification.pdf* document for the complete details of all the console-based ABS Configuration Manager commands.

## Enabling and configuring the BOOTP server on the CMT ABS

### From the FT Laptop PC

- 1 Open a new Telnet session to the CMT Server.
- 2 Ensure that you are logged in as root:  
**su -root**  
Root privileges are required for SPFS modifications.
- 3 From the # prompt,  
Type: **cli**
- 4 Enter the number next to the Configuration menu option.
- 5 Enter the number next to the Bootp Configuration menu option.
- 6 Enter the number next to the **bootp\_add** menu option.  
*=== Executing "bootp\_add"*  
**Note:** RTC 12 or 15
- 7 Enter the bootfile value [bf] for bootp entry.
- 8 The following value is for RTC12. Type:  
**/<USP install path>/ntssgusp/abs/sites/<sitename>/rtc1/rtcboot**  
For RTC 15, type:  
**/<USP install path>/ntssgusp/abs/sites/<sitename>/rtc2/rtcboot**
- 9 Enter the gateway IP address [gw] for bootp entry.  
Type: **<gateway IP address>**
- 10 Enter the home directory [hd] for bootp entry.  
Type: **.**  
**Note:** The character is a period [.].
- 11 Enter the hardware type [ht] for bootp entry.  
Type: **ethernet**

- 12 Enter the hardware address [ha] for bootp entry.  
**Note:** Do not include the colon [:] character. The following is an example: (010080E944056B)  
Type: **<MAC address>**
- 13 Enter the host IP address [ip] for bootp entry.  
Type: **<Host IP address>**  
**Note:** RTC IP Address
- 14 Enter the server IP address [sa] for bootp entry.  
Type: **<Server IP address>**  
**Note:** CMT IP Address
- 15 Enter the subnet mask value [sm] for bootpentry.  
Type: <subnet mask> Bootfile: \*\*\*\*\*  
Gateway IP Address: \*\*\*\*\*  
Home Directory: .  
Hardware Type: **ethernet**  
Hardware Address: \*\*\*\*\*  
Host IP Address:\*\*\*\*\*  
Server IP Address: \*\*\*\*\*  
Subnet Mask: \*\*\*\*\*  
Type **ok** to accept current settings.
- 16 Ensure that all data you entered is correct. If not, type anything other than OK and press Enter. Re-enter the data.  
Type: **ok**
- 17 Repeat [step 1](#) to [step 15](#) for RTC#2 which is called RTC15.
- 18 Type: **X**  
You will see the Configuration options.
- 19 Select **X** three times to exit the CLI tool.
- 20 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Disabling the BOOTP server on the PC ABS

#### *From the USP EM PC*

- 1 Restore the (PC) Distinct BOOTP Server window.

- 2 Click **Configure>Disabled**.
- 3 Exit the Distinct BOOTP Server window. To do this, click **File>Exit**. Click **Yes**.
- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Verifying correct settings for the USP (RTC)

#### *From the BOOTP server*

- 1 You can use the USP EM PC to perform [step 1](#) to [step 5](#) or log in to the CMT and perform the steps.
- 2 Telnet to RTC-12 or RTC-15.
- 3 Log in with a valid username and password.
- 4 Type: **admin abs test rtc-12**  
Verify the prompt is returned after issuing the command. This can take a couple of seconds to respond.  
The following response indicates that there were no issues.  
*CMD>*
- 5 Type: **admin abs test rtc-15**  
Verify the prompt is returned after issuing the command. This can take a couple seconds to respond.  
The following response indicates that there were no issues.  
*CMD>*
- 6 Type: **admin abs show all**  
Verify that the abs-ipaddress is the address of the CMT ABS and that the correct RTC loads and snapshot are selected.  
(Example response ONLY for a site named Ireland):  
*~CMD>admin abs show all*  
*rtc-12-loadname = ss7rtc\_ppc750\_09\_00\_03\_47c*  
*rtc-15-loadname = ss7rtc\_ppc750\_09\_00\_03\_47c*  
*snapshot-version = v9.0.3*  
*snapshot-name = bv2\_0-6277d3091d27*  
*snapshot-date = 07/29/2004 09:39:39*  
*snapshot-description = usp9.0.3.47c\_02\_purge*  
*abs-ipaddress = 47.142.142.26*  
*abs-path = /opt/usp/ntssgusp /abs/sites/Ireland/rtc2/rtcboot*  
*virtual-index = 1*  
*~CMD>*

- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Verification procedure



### CAUTION

Do not perform [step 17](#) to [step 35](#) if this is an in-service site.

## Verifying and testing your work

### *From the USP EM PC*

- 1 Launch the Application Launch Point.
- 2 Launch the USP GUI.
- 3 Click **File>session-login**.
- 4 Log in to the site:  
**FIELD**  
**SERVICE**
- 5 Click **Administration**, then select **alternate-boot-server**.  
Verify that the BootP response displays the IP address of the CMT Server. Also verify that the bootP path matches what was set during the procedure [Enabling and configuring the BOOTP server on the CMT ABS](#).
- 6 Click **Test**.  
Click **OK**.
- 7 Check the logs using the **Logs** button on the USP GUI. The Site log window appears.
- 8 Verify that the test completed successfully for each RTC and that there are no ABS related alarms.  
In the information field you should see abs test: success.
- 9 In the Alternate Boot settings window, click **Modify** and verify that the ABS settings are successfully applied (no adverse logs, alarms or pop-ups).  
In the log information field you should see abs mod:success.
- 10 From the USP GUI, click **Administration>Backup**.

- 11 Enter a snapshot description of CMT ABS Test Snapshot. Click **Backup**.

**Note:** This action can take up to 10 minutes.

When the action is complete, a Successful snapshot window will open.

- 12 Click **OK** and close the backup window.
- 13 From the USP GUI, click **Administration>File Manager**.

After a couple of minutes, the File Manager panel opens.

- 14 In the right-hand side of the screen (RTC \*\*), double-click **snapshots**.

Double-click the appropriate v11.0.x release folder and locate the snapshot that was just created.

**Note:** Highlight each snapshot and view the description field to find the snapshot called CMT ABS Test snapshot or use the date field.

- 15 Select the snapshot and click the left arrow in the middle of the screen to transfer the snapshot to the CMT ABS.

The transfer will be completed when Ready is displayed in the bottom left corner of the GUI.

- 16 In the left-hand side of the screen (Alternate Boot Server), double-click **snapshots**.

Double-click the appropriate v11.0.x release folder and locate the snapshot that was just transferred.

**Note:** Use the description field to ensure that you are using the correct snapshot.

- 17 Select the snapshot on the ABS (located on the left side of the file manager screen). Click the **delete** button.

Verify that the snapshot is deleted (no adverse logs, alarms or pop-ups). Use the Log manager to verify the logs.

- 18 Select the snapshot on the RTC side (located on the right side of the file manager screen). Click the **delete** button.

Verify that the snapshot is deleted (no adverse logs, alarms or pop-ups). Use the Log manager to verify the logs.

- 19 Close the window.

**Note:** Do not perform [step 20](#) to [step 37](#) if this is an in-service site. If this is an in-service site, skip to [step 37](#).

**From the FT laptop PC**

- 20 Establish an Exceed connection to the CMT Server and launch the ABS Configuration Manager (refer to the procedure [Verifying the data transfer](#) to open the ABS Configuration Manager from the CMT Server). There are two versions of the ABS Configuration Manager available on the CMT. One is graphically-based and the other is console-based. To use the graphically-based ABS Configuration Manager, perform steps [21](#) and [22](#). If you want to use the console-based ABS Configuration Manager, perform steps [23](#) and [24](#).
- 21 Select **File>Login**. Enter the password **SERVICE**.
- 22 Select **File>SSMON**.  
The Signaling Server Monitor window will open.
- 23 Log in to the console-based ABS Configuration manager.  
Type: **ABSCM> login**. Enter the password **SERVICE**.
- 24 To read ssmon logs from the ssmon.log file type either of the following commands:  
**ABSCM>ssmonlog show all**  
or  
**ssmonlog show last-num-logs <no-of-logs>**  
**Note:** The console-based ABS Configuration Manager does not display ssmon logs in real time. Instead, it reads from the ssmon.log file and display logs. Refer to the *ABS\_Specification.pdf* document for complete details.
- 25 Leave the Signaling Server Monitor window open on the FT laptop and perform the next steps from the USP EM PC.

**From the USP EM PC**

- 26 Start the USP EM GUI and log in.
- 27 Click **System Mgmt**.  
The Site System Management window will open.
- 28 Click the first shelf on the top left.  
The control shelf window will open.
- 29 Look at the graphical representation of the RTC cards in slot 12 and slot 15. The active RTC will have a check mark in a small box. You must perform this test on the inactive RTC.

- Click the inactive RTC to open the screen and note the IP address for this card. This IP address is used in the next step as the <Inactive IP address>.
- 30 Click **Start>Run** and type: **FTP <Inactive IP address>**.
  - 31 Log in using the FIELD username with password SERVICE account.
  - 32 Type: **cd /sd0 \*\*\* Changed directory to "/sdo"**.
  - 33 Type: **del sysconf**.
  - 34 From the USP GUI, click the lock button on the inactive RTC that is currently open. Click **Yes**.  
The RTC changes to LOCK status.
  - 35 From the USP GUI, click the load button on the inactive RTC that is currently open. Click **Yes**.  
**Note:** Several pop-ups can be generated indicating a loss of connection to the RTC (This step can several minutes).
  - 36 Monitor the SSMON window for status messages as the RTC performs an alternate boot. The entire process can take up to 15 to 30 minutes.
  - 37 When connectivity to the RTC is restored (a pop-up message will open). Click **OK**.
  - 38 Click the unlock button on the inactive RTC that is currently open.
  - 39 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## USP High-Speed Link Cutover Procedure

---

**CAUTION**

Conduct the cutover during a maintenance window, where the low speed link traffic is below 0.2 erlang.

To cutover from 16 LSL to two HSLs, the low speed link traffic must be less than 0.1 erlang.

This section details procedures for converting a Common Channel Signaling System 7 (SS7) low-speed link (LSL) linkset into an high-speed link (HSL) linkset.

Throughout this document, links originating on DS0A, V.35 or Channelized E1/T1 link system nodes are referred to as low-speed links (LSLs). Links originating on high-speed link or SS7 IP link system nodes are referred to as high-speed links (HSL). The ATM high-speed link system node physically consists of the T1/E1 Transition Module (TM) and a link mission card. The computing engine mission card consists of a Power/SCSI/Ethernet (PSE) TM, an SS7 IP link mission card, and an MTP2 E1 HSL.

This section also provides the procedures to transition from low-speed link (LSL) linksets to high-speed link (HSL) linksets.



## Hardware requirements

The following hardware is required for ATM high-speed links:

- T1/E1 Transition Module NTST81BA, or NTST81AB
- Link Mission Card
  - NTST10BA (base link card)

The following hardware is required for E1 MTP2 high-speed links:

- T1/E1 Transition Module NTST81BA
- Link Mission Card
  - NTST10CA

The following hardware is required for SS7 IP High Speed links:

- PSE TM NTST09AA, NTST09AB, or NTST09AC
- IP Link Mission Card which includes:
  - NTST11BA (LE3)

For further information about issues related to hardware installations involving high-speed links (HSL), contact the installation prime.

## Software requirements

Software release USP8.0 or later is required for this cutover.

## HSL cutover process

### **ATTENTION**

Ensure that the network to be converted and all connecting nodes and network connections are in service.

Ensure that all alarms have been cleared before proceeding with the cutover procedure.

Review and coordinate the cutover procedure with other operating companies in the network that are involved in the cutover procedure.

Up to sixteen ATM/E1 or MTP2 HSL system nodes can be commissioned on an extension shelf (12 on a control shelf). For IP HSLs, up to eight HSL can be commissioned on each shelf. On a fully populated system, an LSL link system node must be decommissioned before installing each HSL system node. Existing links on the LSL system node must be moved to other link system nodes or decommissioned. If your system is fully populated, contact your next level of support.

The cutover procedure requires operating company personnel to be present at each office that is affected by a link change during any step of the procedure. Nortel Networks recommends that you appoint a cutover project manager to coordinate all the steps for the cutover.

### **HSL cutover guidelines**

Note the following guidelines when performing the HSL cutover:

- The high-speed link system node can support HSLs for C-links, B/D links, or A-links.
- Carry out the C-linkset cutover before the signaling transfer point (STP) quad B/D-linkset cutover because only two nodes are involved in the C-linkset cutover.
- An HSL system node provides a single port in the same space that an LSL system node provides four or eight ports. Therefore, on a full system, four or eight LSL ports must be decommissioned for each HSL added.

The HSL cutover applies to:

- C-linkset cutover for a signaling transfer point (STP) pair
- B-linkset cutover for an STP quad
- D-linkset cutover for an STP quad
- A-links-to-service control point (SCP) cutover
- A-links-to-SSP cutover

**Note:** Nortel Networks recommends performing the C-linkset cutover for an STP pair before attempting the B-linkset and D-linkset cutover for an STP quad.

### HSL cutover procedures

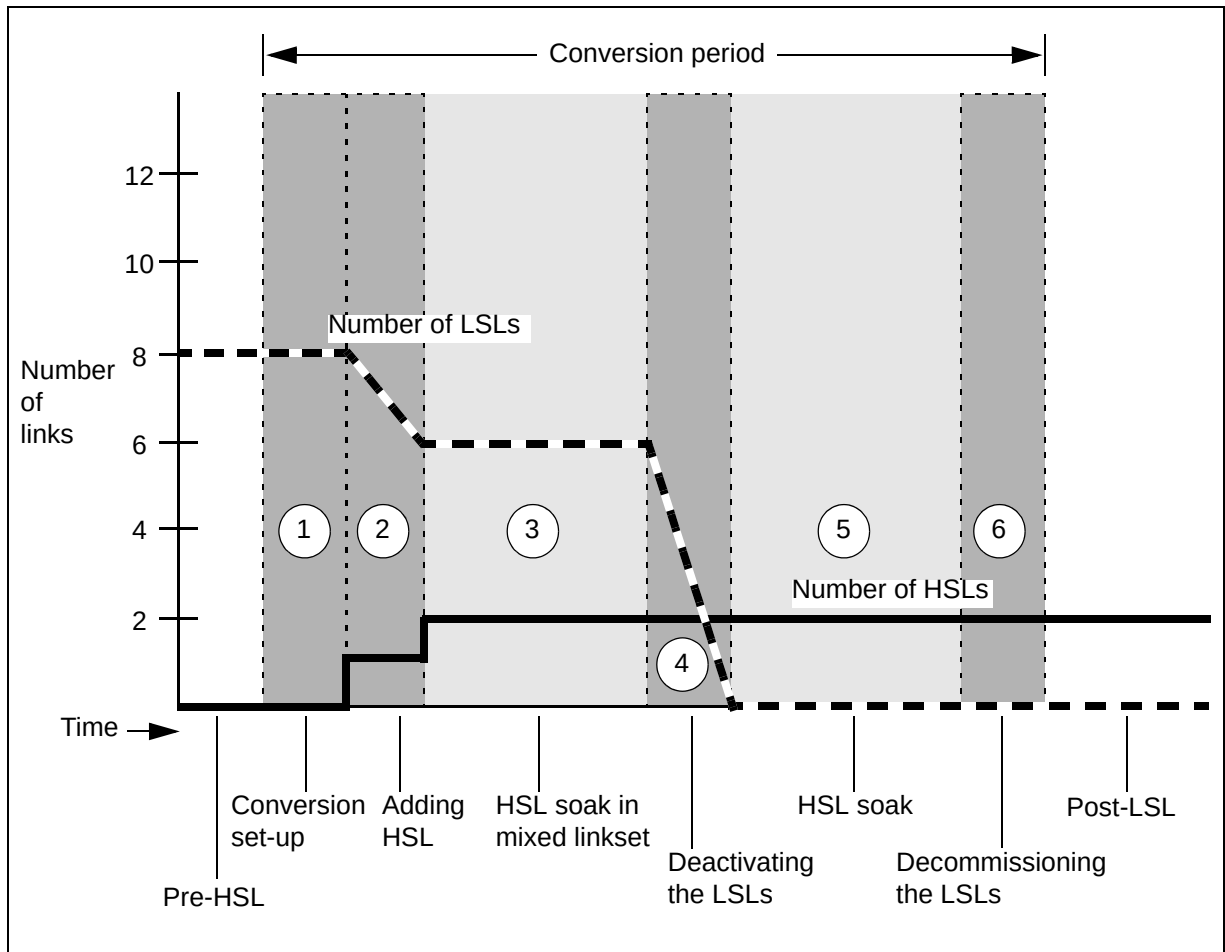
#### **ATTENTION**

During cutover, HSLs and LSLs are supported in the same mixed linkset. The USP supports mixed HSL and LSL linksets only during the cutover procedure. After the cutover is complete, linksets s will be homogeneous.

#### **ATTENTION**

Contact your next level of support to determine the correct version of the engineering bulletin and to determine if any other engineering bulletins apply.

The following figure shows the cutover steps.

**Link count during cutover**

The HSL cutover requires completing the following procedures:

1. Cutover setup.
  - a. Configure the HSL system node. Refer to the procedure “Provisioning Links” in the Operational Configuration section of the customer documentation.
  - b. Configure ports. Refer to the procedure “Provisioning Links” in the Operational Configuration section of the customer documentation.

**Note:** For MTP2 E1 HSLs the cable must be connected to RJ45 cable.

  - c. Load the HSL system nodes. Refer to the procedures “Provisioning Links” in the Operational Configuration section of the customer documentation.
2. Add HSLs.
  - a. Configure SAAL timers. Refer to the procedure “Adding a SAAL Timer or Parameter Index” in the Operational Configuration section of the customer documentation.
  - b. Configure SAAL parameters. Refer to the procedure “Adding a SAAL Timer or Parameter Index” in the Operational Configuration section of the customer documentation.
  - c. Deactivate LSLs. Refer to the procedure “Activating and Deactivating Links” in the Operational Configuration section of the customer documentation.
  - d. Delete LSLs. Refer to the procedure “De-provisioning links” in the Operational Configuration section of the customer documentation.
  - e. Configure HSLs. Refer to the applicable ATM, E1 MTP2, or IP HSL procedure in the Operational Configuration section of the customer documentation.
  - f. Perform BERT on ATM and E1 MTP2 before RTSing the links, “Perform BERT” in the Security and Administration guide.
  - g. RTS the link. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
3. Soak the HSLs in a mixed linkset. Refer to the procedure [Soaking the HSLs on page 1722](#).

#### 4. Offline the LSLs.

- a. Calculate LSL traffic. Refer to the procedure “Performing USP traffic calculations” in the Operational Configuration section of the customer documentation.

**Note:** If the Erlang level is above 0.2 E, contact the personnel responsible for your next level of support. Use Operational Measurements to calculate traffic and to determine if you can proceed with the cutover.

- b. Calculate LSL traffic on the mate node. Refer to the procedure “Performing USP traffic calculations” in the Operational Configuration section of the customer documentation.

**Note:** If the Erlang level is above 0.2 E, contact the personnel responsible for your next level of support. Use Operational Measurements to calculate traffic and to determine if you can proceed with the cutover.

- c. Deactivate the LSL. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
- d. Deactivate all remaining LSLs in the linkset. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
- e. Deactivate the LSL on the mate node. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
- f. Deactivate all remaining LSLs in the linkset on the mate node. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.

5. Soak the HSLs. Refer to the procedure [Soaking the HSLs on page 1722](#).
6. Decommission the LSLs.
  - a. Delete the datafill for the LSLs. Refer to the procedure “De-provisioning links” in the Operational Configuration section of the customer documentation.
  - b. Delete LSLs for remaining links in the linkset. Refer to the procedure “De-provisioning links” in the Operational Configuration section of the customer documentation.
  - c. Delete the datafill for the LSLs on the mate node. Refer to the procedure “De-provisioning links” in the Operational Configuration section of the customer documentation.
  - d. Delete LSLs for remaining links in the linkset on the mate node. Refer to the procedure “De-provisioning links” in the Operational Configuration section of the customer documentation.

### Soaking the HSLs

#### ATTENTION

If a failure occurs at any time during this phase, refer to [Performing the recovery procedure for HSL failure on page 1723](#).

- 1 Allow the system to soak for one hour.
- 2 Check the logs for the system. Click **Fault>Logs** on the main menu to open the Logs window.
- 3 Check the alarms for the system. To view alarms, click the alarm banner. The Alarms window appears. Check for alarms.
- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Recovery procedure for HSL failure

If an HSL fails during either phase, traffic is redistributed over the remaining links in the linkset or combined linkset. The following steps describe the HSL recovery procedure.

## Performing the recovery procedure for HSL failure

### *At the OAMP workstation*

- 1** Deactivate and offline the failed HSL. Refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
- 2** Perform a remote Loopback at the far end of the link. Refer to the procedure “Remote Loopback” in the Fault Management section of the customer documentation. On the local end of the link, perform a BERT Operation. Refer to the procedure “Performing Bert” in the Security and Administration guide. Clear any faults before proceeding.
- 3** RTS the HSL. To RTS the link, refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
- 4** Select one of the following options.:

| If                           | Do                                   |
|------------------------------|--------------------------------------|
| the failure condition exists | continue to step <a href="#">5</a> . |
| the failure condition clears | step <a href="#">8</a>               |
- 5** Provision LSLs. Refer to the procedure “Provisioning links” in the Operational Configuration section of the customer documentation.
- 6** RTS the LSLs. To RTS the link, refer to the procedure “Activating and deactivating links” in the Operational Configuration section of the customer documentation.
- 7** Contact your next level of support.
- 8** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## In-Service Introduction of Inter-CAM Communication Media (ICCMs)

**CAUTION****Service interruption**

To reduce the risk of service-affecting issues, Nortel recommends that you perform the procedure during low traffic periods in the maintenance time frame.

**CAUTION****Service degradation**

If your system has a mate system, do not perform maintenance activities on the mate while you perform the conversion procedure on the first node. Performing maintenance activities during an inservice conversion can affect service.

**ATTENTION**

Make sure that the dual-shelf system is working properly before starting the conversion procedure. Check alarm information to make sure there are no alarms pointing to problems with CC cards, RTC cards, fibre-optic cable states, loss of communication redundancy (LOCR), isolation, or shelf states. Make sure that all connecting nodes and network connections are in service. Review and coordinate the conversion procedure with other operating companies in the network.

Use this procedure for an in-service conversion of the USP from a dual-shelf system, that links directly through OC-3 cables, to a system where the shelves link through two Inter-CAM Communication Media (ICCM). The system can be expanded to a multi-shelf system with up to eight Communications Application Module (CAM) shelves.

One shelf remains designated as the control CAM shelf and the additional shelves are designated as extension CAM shelves. Each extension shelf contains two CCs and a maximum of 16 additional system nodes.

To maintain the existing redundancy and availability of the Signaling Server platform, two ICCMs are deployed in the system configuration. One CC node on each shelf is connected to the first ICCM. The other CC node on each shelf is connected to the second ICCM. This configuration allows full redundancy of SS7 messaging as well as the inservice upgrade capability of the ICCMs. The servicing of one ICCM can take place while the second ICCM carries traffic. This ensures no service impact to SS7 traffic on the link cards.

## Prerequisites

This procedure has the following prerequisites:

- The USP software upgrade must be complete, and all nodes in the system must be running the same load.
- The USP must be provisioned with all hardware required for a dual-shelf system.
- The RTC must be provisioned with a CE3 (Computing Engine 3 with PP4), running a PP4 750-based load.
- Two ICCMs and associated cabling must be available on-site.

## Hardware requirements

The following tables describe the additional minimum hardware requirements needed for the in-service conversion.

### Additional minimum hardware required for dual-shelf in-service conversion

| Name                                  | PEC      | Quantity                |
|---------------------------------------|----------|-------------------------|
| ICCM (Marconi TNX-210 ATM Switch)     | NTST87AA | 2 for the system        |
| RTC CE3 (Computing Engine 3 with PP4) | NTST11BA | 2 for the control shelf |
| OC-3 Fibre Cables                     | NTST88AA | 4 (2 for each shelf)    |

**Additional minimum hardware required for four-shelf in-service conversion**

| Name                                  | PEC      | Quantity                |
|---------------------------------------|----------|-------------------------|
| ICCM (Marconi TNX-210 ATM Switch)     | NTST87AA | 2 for the system        |
| RTC CE3 (Computing Engine 3 with PP4) | NTST11BA | 2 for the control shelf |
| OC-3 Fibre Cables                     | NTST88AA | 8 (2 for each shelf)    |

**Additional minimum hardware required for five-shelf in-service conversion**

| Name                                  | PEC      | Quantity                |
|---------------------------------------|----------|-------------------------|
| ICCM (Marconi TNX-210 ATM Switch)     | NTST87AA | 2 for the system        |
| RTC CE3 (Computing Engine 3 with PP4) | NTST11BA | 2 for the control shelf |
| OC-3 Fibre Cables                     | NTST88AA | 10 (2 for each shelf)   |

**Additional minimum hardware required for eight-shelf in-service conversion**

| Name                                  | PEC      | Quantity                |
|---------------------------------------|----------|-------------------------|
| ICCM (Marconi TNX-210 ATM Switch)     | NTST87AA | 2 for the system        |
| RTC CE3 (Computing Engine 3 with PP4) | NTST11BA | 2 for the control shelf |
| OC-3 Fibre Cables                     | NTST88AA | 16 (2 for each shelf)   |

Each ICCM provides room for expansion to up to 16 OC-3 ports. The ICCM terminates the OC-3 links from the CAM shelves and provides routing between the CAM shelves on the system.

Nortel arranges the provisioning of the ICCMs to allow the CAM shelves to communicate properly. Once the ICCMs are powered up, they are ready to route ATM messages. If a routing error occurs, contact your next level of support.

The OC-3 fibre cable between the CCs and the ICCMs is a standard multi-node fibre cable with SC connectors. This cable is custom-built for the application. The same OC-3 cable is used for connection of dual-shelf systems. Nortel Networks recommends that you have extra OC-3 cables on site in case of fibre optic cable failure.

For additional information on provisioning the hardware, contact your installation prime.

## In-service introduction of ICCMs process



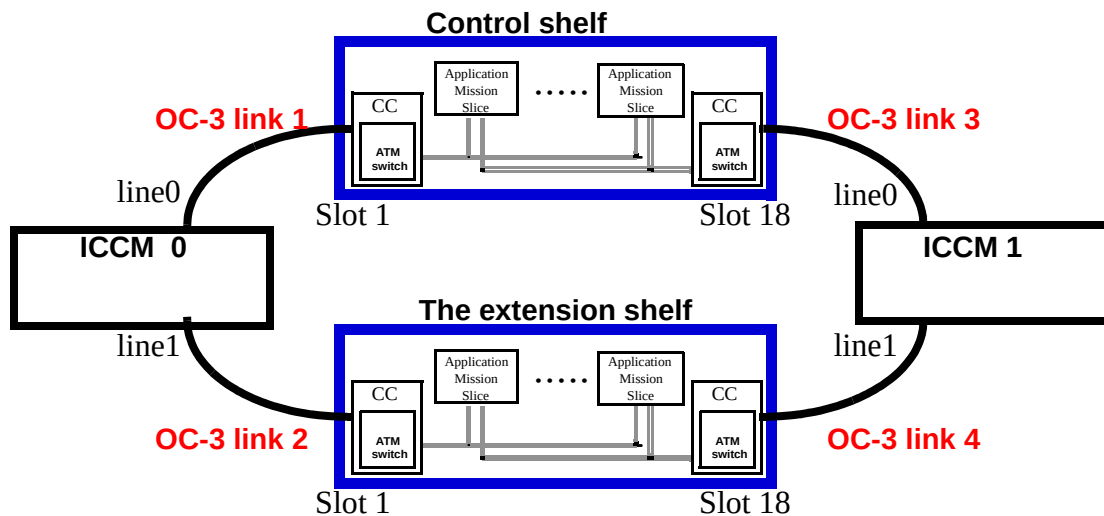
### **CAUTION**

#### **Non-redundant system**

During most of the conversion procedure, the system operates without redundancy. Nortel recommends that the conversion take place during low traffic periods in the maintenance window in order to avoid loss of service.

This section describes the step-by-step in-service conversion procedure for converting a system from a dual-shelf system, that links directly through OC-3 fibre optic cables, to a system where the CAM shelves link through ICCMs.

## ICCM connectivity with system shelves



A dual-shelf system with ICCMs uses four OC-3 cable links. The following is a summary of the cable connections:

- OC-3 link 1 connects the CC in slot 1 on the control CAM shelf to line 0 on line card 0 of ICCM 0.
- OC-3 link 2 connects the CC in slot 1 on the extension CAM shelf to line 1 on line card 0 of ICCM 0.
- OC-3 link 3 connects the CC in slot 18 on the control CAM shelf to line 0 on line card 0 of ICCM 1.
- OC-3 link 4 connects the CC in slot 18 on the extension CAM shelf to line 1 on line card 0 of ICCM 1.

In order for the pre-configured ICCMs to operate correctly with the CAM shelves, the system must be connected as specified in this document.

To avoid disruption to service, only one set of the CCs is disabled at one time, and all traffic is carried on the other set of CCs during the conversion procedure. In this document, conversion of the CCs in slot 1 occurs first, followed by the conversion of the CCs in slot 18.

### In-service introduction of ICCMs procedures

In-service introduction of ICCMs in a dual-shelf system requires the completion of the following separate procedures:

1. Upgrade USP software.
2. Log in and check alarms.
3. Disable and offline the CC in slot 1 on the extension CAM shelf.

4. Disable and offline the CC in slot 1 on the control CAM shelf.
5. Remove OC-3 cable connections for the CCs in slot 1 and connect the CCs to ICCM 0.
6. Enable the CC in slot 1 on the control CAM shelf.
7. Enable the CC in slot 1 on the extension CAM shelf.
8. Check OMs to ensure messaging goes through ICCM 0.
9. Soak the system after conversion of the CCs in slot 1.
10. Disable and offline the CC in slot 18 on the extension CAM shelf.
11. Disable and offline the CC in slot 18 on the control CAM shelf.
12. Remove OC-3 cable connections for the CCs in slot 18 and connect the CCs to ICCM 08.
13. Enable the CC in slot 18 on the control CAM shelf.
14. Enable the CC in slot 18 on the extension CAM shelf.
15. Check OMs to ensure messaging goes through ICCM 1.
16. Add ICCMs to the system GUI.
17. Soak the dual-shelf system.

### **Upgrading the USP software**

Use the procedures in this document.

### **Logging in and checking alarms**

#### ***At the OAMP workstation***

- 1 Double-click the system icon on your OAMP workstation to display the login window.
- 2 To log in to the system GUI, select a site and enter a user identification and password.
- 3 Check alarm information to make sure there are no alarms pointing to problems with CC cards, RTC cards, fibre-optic cable states, loss of communication redundancy (LOCR), isolation, or shelf states. To view alarms, click the alarm banner. The Alarms window appears.
- 4 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

**Disabling and offlining the CC in slot 1 on the extension CAM shelf*****On the system GUI***

- 1 Click Configuration>platform>node>Graphical View.
- 2 Click the icon for the extension shelf to open the shelf\_name window for the extension CAM shelf.
- 3 Click the icon for the CC in slot 1 to open the CC in slot 1 on the graphical view window for the extension CAM shelf.
- 4 Click Lock to lock the CC in slot 1. A pop-up window appears. Click Yes to confirm the change. Check the Administrative state (the word Locked should be highlighted).
- 5 Click Offline to offline the CC in slot 1. A pop-up window appears. Click Yes to confirm the change. Click OK to continue. Check the Availability status in the Maintenance portion of the window. The word Offline should be highlighted.
- 6 Click Close to return to the shelf\_name window for the extension CAM shelf. Click Close to return to the System Configuration window.
- 7 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

**Disabling and offlining the CC in slot 1 on the control CAM shelf*****On the system GUI***

- 1 Click Configuration>platform>node>graphical view.
- 2 Click the icon for the control CAM shelf to open the shelf\_name window for the control CAM shelf.
- 3 Click the icon for the CC in slot 1 to open the CC in slot 1 on the maintenance and provisioning window for the control CAM shelf.
- 4 Click Lock to lock the CC in slot 1. A pop-up window appears. Click Yes to confirm the change. Check the Administrative state in the Maintenance portion of the window. The word Locked should be highlighted.
- 5 Click Offline to offline the CC in slot 1. A pop-up window appears. Click Yes to confirm the change. Click OK to continue. Check the Availability status in the Maintenance portion of the window. The word Offline should be highlighted.
- 6 Click Close to return to the shelf\_name window for the control CAM shelf. Click Close to return to the System Configuration window.

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



## Removing OC-3 cable connections for the CCs in slot 1 and connecting the CCs to ICCM 0



### CAUTION

#### Service interruption

When you remove the OC-3 cable, make sure that you remove the cable from the CCs in slot 1. Removal of the OC-3 cable from the CCs in slot 18 can disrupt service. Make sure that the LED on the CC TM is OFF before you remove the OC-3 cable. If the LED is ON, the CC is enabled, and loss of service can occur.

### *On the system*

- 1 Remove the OC-3 cable connecting the CC in slot 1 on the control CAM shelf to the CC in slot 1 on the extension CAM shelf.
- 2 Use the OC-3 cable to connect the CC in slot 1 on the control CAM shelf to line 0 on line card 0 of the ICCM 0. Check the lights on the ICCM 0 for line 0. A green light indicates the cable connection is correct. If the red light is on, a line error occurred. If a problem occurs, perform the steps in the [Troubleshooting an OC-3 cable connection on page 1740](#).
- 3 Use an OC-3 cable to connect the CC in slot 1 on the extension CAM to line 1 on line card 0 of the ICCM 0. Check the lights on the ICCM 0 for line 0. A green light indicates the cable connection is correct. If the red light is on, a line error occurred. If a problem occurs, perform the steps in the [Troubleshooting an OC-3 cable connection on page 1740](#).
- 4 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Enabling the CC in slot 1 on the control CAM shelf

### *On the system GUI*

- 1 Click Configuration>platform>node>graphical view.
- 2 Click the icon for the control CAM shelf to open the shelf\_name window for the control CAM shelf.
- 3 Click the icon for CC in slot 1 to open the CC in slot 1 on the maintenance and provisioning window for the control CAM shelf.

- 4 Click Load to load the CC in slot 1. A pop-up window appears. Click Yes to confirm the change. Check the Operational state in the Maintenance portion of the window to verify the changes. The word Unlocked should be highlighted.
- 5 Click Unlock to unlock the CC in slot 1. A pop-up window appears. Click Yes to confirm the change. Check the Administrative state in the Maintenance window. The word Unlocked should be highlighted.
- 6 Click **Close** to return to the shelf\_name window for the control CAM shelf. Click Close to return to the System Configuration window.
- 7 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### **Enabling the CC in slot 1 on the extension CAM shelf**

#### ***On the system GUI***

- 1 Click Configuration>platform>node>graphical view.
- 2 Click the icon for the extension CAM shelf to open the shelf\_name window for the extension CAM shelf.
- 3 Click the icon for CC in slot 1 to open the CC in slot 1 on the maintenance and provisioning window for the extension CAM shelf.
- 4 Click Load to load the CC in slot 1. A pop-up window appears. Click Yes to confirm the change. Check the Operational state in the Maintenance portion of the window to verify the changes. The word Unlocked should be highlighted.
- 5 Click Unlock to unlock the CC in slot 1. A pop-up window appears. Click Yes to confirm the change. Check the Administrative state in the Maintenance window. The word Unlocked should be highlighted.
- 6 Click **Close** to return to the shelf\_name window for the extension CAM shelf. Click Close to return to the System Configuration window.
- 7 Wait for at least 10 minutes after enabling the CC in slot 1 on the extension shelf. Check the system logs and OMs for any unusual events.
- 8 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Checking OMs to ensure messaging goes through LCCM 1

### *On the system GUI*

- 1 Click **Performance>om**.
- 2 Click **Search**.
- 3 In the criteria box select:
  - application-name from the **Field** drop-down menu
  - equal from the **Condition** drop-down menu
  - ATM Driver Messaging from the **Value** drop-down menu
- 4 Click **Retrieve**.
- 5 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Soaking the system after the conversion of CCs in slot 1

### *At the OAMP workstation*

- 1 Allow the system to soak for one hour after the conversion of the CCs in slot 1.
- 2 Check the logs for the system. Click Logs on the main menu to open the Logs window.
- 3 Check the alarms for the system. To view alarms, click the alarm banner. The Alarms window appears. Check alarm information to make sure there are no alarms pointing to problems with CC cards, RTC cards, fibre-optic cable states, loss of communication redundancy (LOCR), isolation or shelf states.

If a problem or failure occurs at any time during soak do not proceed until the problem is resolved and the alarm clears. If you cannot resolve the problem, contact your next level of support.
- 4 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Disabling and offlining the CC in slot 18 on the extension CAM shelf

### *On the system GUI*

- 1 Click Configuration>platform>node>graphical view.
- 2 Click the icon for the extension CAM shelf to open the shelf\_name window for the extension CAM shelf.

- 3 Click the icon for the CC in slot 18 to open the CC in slot 18 on the maintenance and provisioning window for the extension CAM shelf.
- 4 Click Lock to lock the CC in slot 18. A pop-up window appears. Click Yes to confirm the change. Check the Administrative state in the Maintenance portion of the window. The word Locked should be highlighted.
- 5 Click Offline to offline the CC in slot 18. A pop-up window appears. Click Yes to confirm the change. Click OK to continue. Check the Availability state in the Maintenance portion of the window. The word Offline should be highlighted.
- 6 Click Close to return to the shelf\_name window for the extension CAM shelf. Click Close to return to the System Configuration window.
- 7 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### **Disabling and offlining the CC in slot 18 on the control CAM shelf**

#### ***On the system GUI***

- 1 Click Configuration>platform>node>graphical view.
- 2 Click the icon for the control CAM shelf to open the shelf\_name window for the control CAM shelf.
- 3 Click the icon for the CC in slot 18 to open the CC in slot 18 on the maintenance and provisioning window for the control CAM shelf.
- 4 Click Lock to lock the CC in slot 18. A pop-up window appears. Click Yes to confirm the change. Check the Administrative state in the Maintenance portion of the window. The word Locked should be highlighted.
- 5 Click Offline to offline the CC in slot 18. A pop-up window appears. Click Yes to confirm the change. Click OK to continue. Check the Availability state in the Maintenance portion of the window. The word Offline should be highlighted.
- 6 Click Close to return to the shelf\_name window for the control CAM shelf. Click Close to return to the System Configuration window.
- 7 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Removing the OC-3 cable connections for the CCs in slot 18 and connecting the CCs to ICCM 1



### CAUTION

#### Service interruption

When you remove the OC-3 cable, make sure that you remove the cable from the CCs in slot 18. Removal of the OC-3 cable from the CCs in slot 1 can disrupt service. Make sure that the LED on the CC TM is OFF before you remove the OC-3 cable. If the LED is ON, the CC is enabled, and loss of service can occur.

### *On the system*

- 1 Remove the OC-3 cable connecting the CC in slot 18 on the control CAM shelf to the CC in slot 18 on the extension CAM shelf.
- 2 Use the OC-3 cable to connect the CC in slot 18 on the control CAM shelf to line 0 on line card 0 of the ICCM 1. Check the lights on the ICCM 1 for line 0. A green light indicates the cable connection is correct. If the red light is on, a line error occurred. If a problem occurs, perform the steps in the [Troubleshooting an OC-3 cable connection on page 1740](#).
- 3 Use an OC-3 cable to connect the CC in slot 18 on the extension CAM to line 1 on line card 0 of the ICCM 1. Check the lights on the ICCM 1 for line 0. A green light indicates the cable connection is correct. If the red light is on, a line error occurred. If a problem occurs, perform the steps in the [Troubleshooting an OC-3 cable connection on page 1740](#).
- 4 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Enabling the CC in slot 18 on the control CAM shelf

### *On the system GUI*

- 1 Click Configuration>platform>node>graphical view.
- 2 Click the icon for the control CAM shelf to open the shelf\_name window for the control CAM shelf.
- 3 Click the icon for CC in slot 18 to open the CC in slot 18 on the maintenance and provisioning window for the control CAM shelf.

- 4 Click Load to load the CC in slot 18. A pop-up window appears. Click Yes to confirm the change. Check the Operational state in the Maintenance portion of the window to verify the changes. The word Unlocked should be highlighted.
- 5 Click Unlock to unlock the CC in slot 18. A pop-up window appears. Click Yes to confirm the change. Check the Administrative state in the Maintenance window. The word Unlocked should be highlighted.
- 6 Click **Close** to return to the shelf\_name window for the control CAM shelf. Click Close to return to the System Configuration window.
- 7 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### **Enabling the CC in slot 18 on the extension CAM shelf**

#### ***On the system GUI***

- 1 Click Configuration>platform>node>graphical view.
- 2 Click the icon for the extension CAM shelf to open the shelf\_name window for the extension CAM shelf.
- 3 Click the icon for CC in slot 18 to open the CC in slot 18 on the maintenance and provisioning window for the extension CAM shelf.
- 4 Click Load to load the CC in slot 18. A pop-up window appears. Click Yes to confirm the change. Check the Operational state in the Maintenance portion of the window to verify the changes. The word Unlocked should be highlighted.
- 5 Click Unlock to unlock the CC in slot 18. A pop-up window appears. Click Yes to confirm the change. Check the Administrative state in the Maintenance window. The word Unlocked should be highlighted.
- 6 Click **Close** to return to the shelf\_name window for the extension CAM shelf. Click Close to return to the System Configuration window.
- 7 Wait for at least 10 minutes after enabling the CC in slot 18 on the extension shelf.
- 8 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Checking OMs to ensure messaging goes through ICCM 1

### *On the system GUI*

- 1 Click OMs on the main menu to open the Operation Measurements window.
- 2 Set the interval to five minutes in the Interval Type field. Click Query Interval Data to open the OMBrowser Interval Selection window.
- 3 Click on the bottom line of the window to select the last five-minute interval. Click Get Selected Intervals. A pop-up window appears. Click Yes to confirm your change.
- 4 Click Open Filter Selection Window to open the Operational Measurements Filter window.
- 5 Select ATM Driver Messaging in the Application Filter list.
- 6 Select the CC in slot 18 on the extension shelf in the Element Filter list.
- 7 Click Close to return to the Operational Measurements window.
- 8 In the Register portion of the window, locate “Plane 1 Message Count” and “Plane 2 Message Count”. The OM Value should be the same for each count. If the OM value is not the same for the two counts, contact your next level of support.
- 9 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Adding ICCMs on the system GUI

### *On the system GUI*

- 1 Click System mgmt on the main menu to open the System Configuration window.
- 2 Click Add ICCM. A pop-up window appears. Click Yes to confirm the change. Click OK to continue. Two ICCMs appear on the GUI.
- 3 Check the OC-3 link state indicator on the GUI to make sure all the OC-3 links are up.  
  
If an OC-3 link is down, the OC-3 link indicator changes to show a broken link in the black square below the shelf.
- 4 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Soaking the dual-shelf system

### ATTENTION

If a failure occurs at any time during this phase, refer to [Conversion failure management on page 1740](#). If you cannot resolve the problem, contact your next level of support.

### ATTENTION

When you complete this procedure, you can now install additional shelves on the system. Refer to the section “Adding an Extension Shelf” in the Configuration Management guide.

### *At the OAMP workstation*

- 1 Allow the system to soak for one hour after the conversion to a system with two ICCMs.
- 2 Check the logs for the system. Click Logs on the main menu to open the Logs window.
- 3 Check the alarms for the system. To view alarms, click the alarm banner. The Alarms window appears. Check for alarms pointing to problems with CC cards, RTC cards, fibre-optic cable states, loss of communication redundancy (LOCR), isolation or shelf states.
- 4 Check the OC-3 link state indicator on the system GUI. Make sure all of the OC-3 links are up.
- 5 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Troubleshooting and system recovery

This section provides the procedures for troubleshooting and recovering a system from problems encountered during the conversion process.

Each line on the ICCM has a green light and a red light. A green light indicates a correct OC-3 cable connection. A red light indicates a problem with the connection. After you connect the CAM shelves to the ICCMs using OC-3 cables, check the lights. If the red light is on, perform the following steps:



## Troubleshooting an OC-3 cable connection

### *At the ICCM*

- 1** A reversal of the RX and TX nodes on the OC-3 cable can be the problem. To solve the problem, unplug the cable, switch the RX and TX nodes, and plug the cable in again. If the green light is on, continue with the conversion procedure. Otherwise, perform the next step.
- 2** Use another OC-3 cable to replace the current cable. Make sure that you connect the RX and TX nodes correctly.
- 3** You have completed this procedure. If the green light is on, continue with the conversion procedure. If the problem continues, contact your next level of support.

## Conversion failure management

To abort the conversion, perform the following backout procedures:

1. Remove ICCMs on the system GUI.
2. Perform a back out for the ICCM 1.
3. Remove the ICCM and connect the CCs with direct OC-3 cable links.
4. Perform a back out for the ICCM 0.

### Removing ICCMs from the system GUI

#### **ATTENTION**

If you added ICCMs on the system GUI, perform the following steps to remove them. If no ICCMs were added, skip this procedure.

### *At the OAMP workstation*

- 1** On the system GUI, open the System Configuration window. To do this, click Configuration>platform>system.
- 2** Click **Delete ICCM**. A pop-up window appears. Click **Yes** to confirm. Click **OK** to continue. The system removes the ICCMs from the GUI.
- 3** You have completed this procedure. Continue the backout procedure or contact your next level of support

## Performing a back out for ICCM 1

### *At the OAMP workstation*

- 1 Disable and offline the CC in slot 18 on the extension shelf. See [Disabling and offlining the CC in slot 18 on the extension CAM shelf on page 1734](#).
- 2 Disable and offline the CC in slot 18 on the control shelf. See [Disabling and offlining the CC in slot 18 on the control CAM shelf on page 1735](#).
- 3 Remove ICCM 1 and connect the CCs in slot 18 with direct OC-3 cable links. See [Removing the OC-3 cable connections for the CCs in slot 18 and connecting the CCs to ICCM 1 on page 1736](#).
- 4 Enable the CC in slot 18 on the control shelf. See [Enabling the CC in slot 18 on the control CAM shelf on page 1736](#).
- 5 Enable the CC in slot 18 on the extension shelf. See [Enabling the CC in slot 18 on the extension CAM shelf on page 1737](#).
- 6 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Removing the ICCM and connecting the CCs with direct OC-3 cable links



#### **CAUTION**

##### **Service interruption**

When you remove the OC-3 cables, make sure that you remove the OC-3 cables from the CCs in slot 18 connecting to ICCM 1. Removal of the OC-3 cables from the CCs in slot 1 connecting to ICCM 0 can result in loss of service. Make sure that the LED on the CC TM card is OFF before removing the OC-3 cables. If the LED is ON, the CC is enabled and service can be disrupted.

### *At the system*

- 1 Remove the OC-3 cable connecting the CC on the control CAM shelf to the line card of the ICCM.
- 2 Remove the OC-3 cable connecting the CC on the extension CAM shelf to the line card of the ICCM.
- 3 Use an OC-3 cable to connect the CC on the control CAM shelf to the CC on the extension CAM shelf.

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

### **Performing a back out for ICCM 0**

#### ***At the system***

- 1 Disable and offline the CC in slot 1 on the extension shelf. See [Disabling and offlining the CC in slot 1 on the extension CAM shelf on page 1730](#).
- 2 Disable and offline the CC in slot 1 on the control shelf. See [Disabling and offlining the CC in slot 1 on the control CAM shelf on page 1730](#).
- 3 Remove ICCM 0 and connect the CCs in slot 1 with direct OC-3 cable links. See [Removing OC-3 cable connections for the CCs in slot 1 and connecting the CCs to ICCM 0 on page 1732](#).
- 4 Enable the CC in slot 1 on the control shelf. See [Enabling the CC in slot 1 on the control CAM shelf on page 1732](#).
- 5 Enable the CC in slot 1 on the extension shelf. See [Enabling the CC in slot 1 on the extension CAM shelf on page 1733](#).
- 6 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Aborting an Upgrade

The following sections describe the procedures used to abort a software upgrade before it has been completed. When you have completed this process, your system runs the previous software version.

To abort an upgrade, downgrade only the system nodes that have been upgraded.



### CAUTION

Once you complete the upgrade of the RTC in slot 12, the only way to return to the previous configuration is to perform an alternate boot from a data snapshot created prior to the upgrade. Do not upgrade the RTC in slot 12 until you perform test calls and ensure the system is ready for completion of the upgrade.



### CAUTION

Before you begin any downgrade procedure, make sure that you have a recent data snapshot on the alternate boot server.

### *At the OAMP workstation*

- 1 Use the following table to determine the procedure you need to start with to downgrade your system.

| If                                                         | Do                                                                        |
|------------------------------------------------------------|---------------------------------------------------------------------------|
| RTC 12 has been upgraded                                   | <a href="#">Downgrade the USP from a data snapshot on page 1744</a>       |
| RTC 12 is not upgraded, but other cards have been upgraded | <a href="#">Downgrading Using the Wizard on page 1744</a>                 |
| RTC 15 has been upgraded                                   | <a href="#">Downgrading the inactive RTC node in slot 15 on page 1754</a> |

- 2 When all the cards in the system are running the original release loads, complete the following sections:
  - [Stop the upgrade and delete the upgrade package on page 1764](#)
  - [Downgrade the GUI on page 1766](#)
- 3 You have completed this procedure.

## Downgrade the USP from a data snapshot

If you upgraded RTC12, you can only return to the previous software version by restoring the data snapshot created before you upgraded the GUI. The downgrade process contains the following procedures:

### *At the OAMP workstation*

- 1 Restore the data snapshot you created before beginning the upgrade. For the restore procedure, refer to *USP Security and Administration*, NN10159-611.  
  
For the procedure to create a data snapshot, refer to [Creating an alternate boot data snapshot on page 1642](#).
- 2 You have completed this procedure. If applicable, return to the higher level task or procedure that directed you to this procedure.

## Downgrading Using the Wizard

Perform the following procedures to prepare the system for the software downgrade using the Wizard.

## Downgrade the system nodes

Run the Wizard node downgrade to perform the software downgrade for a specific node. You can also select multiple nodes to downgrade using the Shift+Ctrl keys or Ctrl+click with a mouse.

### Downgrade order

#### **ATTENTION**

If you have not yet upgraded RTC12 prior to this downgrade, then follow the downgrade order listed below. Otherwise, refer to [Downgrade the USP from a data snapshot on page 1744](#).

Downgrade the system nodes in the following order:

1. CC in slot 18 on control CAM shelf, see [To downgrade a CC node: on page 1745](#).
2. CCs in slot 18 on extension CAM shelves, see [To downgrade a CC node: on page 1745](#).
3. NPC, NPS and NPE nodes on control and extension CAM shelves, see [To downgrade NPC, NPS, and NPE nodes: on page 1746](#).
4. Link system nodes on control and extension CAM shelves, see [To downgrade a single Link node: on page 1751](#).
5. CCs in slot 1 on extension CAM shelves, see [To downgrade a CC node: on page 1745](#).
6. CC in slot 1 on control CAM shelf, see [To downgrade a CC node: on page 1745](#).
7. Inactive RTC in slot 15, see [To downgrade the inactive RTC in slot 15: on page 1754](#).

### Downgrading a CC node

The following procedure is used to downgrade a CC node using the wizard.

#### To downgrade a CC node:

##### *At the OAMP workstation*

- 1 Select the node to downgrade in the list of available nodes in the software upgrade wizard.
- 2 Click the **Downgrade** button. The system asks for confirmation.
- 3 Wait for the node downgrade to complete (the upgrade-status will change to not-upgraded on completion).

**Note:** In the event that the automatic node downgrade fails to complete successfully, perform the downgrade manually. See [Manually downgrading system nodes on page 1755](#).

- 4 Monitor the USP to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs. If it does, do not continue with the node downgrade, contact your next level of support.
- 5 This procedure is complete. Continue to downgrade the next system node in the order appropriate to your system.

## Downgrading the NPC, NPS, and NPE nodes

The downgrade of an NPC, NPS and/or NPE node requires special handling to ensure that the local subsystem instances associated with an NPC, NPS and an NPE chain have been deactivated. Also, the downgrading node must not be the active NPC node. If it is, then a switch of activity must be performed prior to downgrading the node.



### CAUTION

#### Potential for NPDB corruption

If downgrading the NP nodes/chains, the connection to the LSMS will need to be released on the LSMS. Contact Nortel Networks Technical Support for more information. Failure in doing so will result in NPDB corruption.

### ATTENTION

Do not use the software upgrade wizard to downgrade NPC/NPS/NPE system nodes if there are NPE chains provisioned. Manually downgrade these nodes instead, as detailed in [Manually downgrading the NPC, NPS, and NPE system nodes on page 1759](#).

## To downgrade NPC, NPS, and NPE nodes:

### On LSMS

- 1 Release all SMI connections to the UNPM. Refer to the LSMS operation manual for release methods.

### At the OAMP workstation

- 2 In the menu bar, click **Administration>Platform>Node**.
- 3 Select the NPC you want to downgrade.
- 4 Check the activity state of the NPC.

| If                  | Do                                                         |
|---------------------|------------------------------------------------------------|
| the NPC is active   | Perform a SWACT, then continue to <a href="#">step 5</a> . |
| the NPC is inactive | Continue to <a href="#">step 5</a> .                       |

- 5 Click **Lock**.

- 6 Deactivate the NP local subsystem instance running on the inactive NPC system node. To do this, click **configuration>sccp>shared-local-subsystem-instance**, select the NPx of interest and click **Deactivate**.
- 7 If an NPE chain has been provisioned with this NPC node as the master and with an alternate NPS system node, then deactivate the local subsystem instance running on the alternate NPS. To do this, click **configuration>sccp>shared-local-subsystem-instance**, select the NPx of interest and click **Deactivate**.
- 8 Using the software upgrade wizard, select the NPC node to downgrade in the list of available nodes.
- 9 Click the **Downgrade node** button. The system asks for confirmation.
- 10 Wait for node downgrade to complete (the upgrade-status will change to not-upgraded on completion).

**Note:** In the event that the automatic node downgrade fails to complete successfully, perform the downgrade manually. See [Manually downgrading the NPC, NPS, and NPE system nodes on page 1759](#).

11

| If                                                       | Do                                                                                                                                          |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| an NPE chain is provisioned with this NPC node as master | repeat steps <a href="#">8</a> to <a href="#">10</a> for each NPE system node and the alternate NPS system node associated with this chain. |
| there is no NPE chain associated with this NPC node      | continue this procedure.                                                                                                                    |

- 12 Wait for the local subsystem instance to be deactivated/prohibited.
- 13 Re-activate the local subsystem instance running on the inactive NPC To do this, click **configuration>sccp>shared-local-subsystem-instance**, select the NPx of interest and click **Activate**.



14

| If                                                                  | Do                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| an NPE chain is provisioned with an alternate NPS system node       | Wait for the local subsystem instance to be deactivated/prohibited. Re-activate the local subsystem instance running on the alternate NPS To do this, click <b>Configuration&gt;SCCP&gt;local-subsystem</b> , select the NPx of interest and click <b>Activate</b> . |
| there is no NPE chain provisioned with an alternate NPS system node | continue this procedure.                                                                                                                                                                                                                                             |

15 Wait for the re-activated local subsystem instances to return to the activated/allowed state.

16 Monitor the USP to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs. If it does, do not continue with the node downgrade.

17

| If                                                                                                 | Do                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NPS system nodes are provisioned without a chain, or NPS system nodes which are masters of a chain | select an NPS system node to be downgraded. This node cannot be an NPS system node already downgraded in the previous steps or the NPS system node associated with the currently active NPC chain. |
| there are no further NPS system nodes to be downgraded                                             | Proceed to <a href="#">step 30</a> .                                                                                                                                                               |

18 Deactivate the NP local subsystem instance running on the NPS system node. To do this, click **configuration>sccp>shared-local-subsystem-instance**, select the NPx of interest and click **Deactivate**.

19 If an NPE chain has been provisioned with an alternate NPS for the selected NPS, deactivate the NP LSS instance running on the alternate NPS system node. To do this, click **configuration>sccp>shared-local-subsystem-instance**, select the NPx of interest and click **Deactivate**.

**20** Using the software upgrade wizard, select the NPS node to downgrade in the list of available nodes

**21** Click the **Downgrade node** button.

**22** Wait for node downgrade to complete (upgrade-status will change to not-upgraded on completion).

**Note:** In the event that the automatic node downgrade fails to complete successfully, perform the downgrade manually.

[Manually downgrading the NPC, NPS, and NPE system nodes on page 1759.](#)

**23**

| If                                                  | Do                                                                                                                                           |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| an NPE chain has been provisioned for this NPS node | repeat steps <a href="#">20</a> to <a href="#">22</a> for each NPE system node and the alternate NPS system node associated with this chain. |
| there is no NPE chain associated with this NPS node | continue this procedure.                                                                                                                     |

**24** Wait for the local subsystem instance to be deactivated/prohibited.

**25** Re-activate the local subsystem instance running on the NPS. To do this, click **configuration>scdp>shared-local-subsystem-instance**, select the NPx of interest and click **Activate**.

**26** If an NPE chain has been provisioned with an alternate NPS system node:

- a** Wait for the local subsystem instance to be activated/allowed.
- b** Re-activate the NP local subsystem instance running on the alternate NPS. To do this, click **configuration>scdp>shared-local-subsystem-instance**, select the NPx of interest and click **Activate**.

**27** Wait for the re-activated local subsystem instances to return to the activated/allowed state.

**28** Monitor the USP to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs. If it does, do not continue with the node downgrade.

**29** Repeat steps [17](#) to [28](#) for any remaining NPS system nodes in the system, otherwise proceed to step [30](#).

- 30 Swact the active NPC node. To do this, click **Administration>platform>node** for the currently active NPC node, then click the **Swact** button.
- 31 Deactivate the NP local subsystem instance running on the inactive NPC system node. To do this, click **configuration>sccp>shared-local-subsystem-instance**, select the NPx of interest and click **Deactivate**.
- 32 If an NPE chain has been provisioned with an alternate NPS system node, then deactivate the local subsystem instance running on the alternate NPS. To do this, click **configuration>sccp>shared-local-subsystem-instance**, select the NPx of interest and click **Deactivate**.
- 33 Using the software upgrade wizard, select the newly inactive NPC node to downgrade in the list of available nodes.
- 34 Click the **Downgrade node** button.
- 35 Wait for the node downgrade to complete (upgrade-status will change to not-upgraded on completion).  
**Note:** In the event that the automatic node downgrade fails to complete successfully, perform the downgrade manually. [Manually downgrading the NPC, NPS, and NPE system nodes on page 1759](#).
- 36 If an NPE chain has been provisioned for this NPC, repeat steps [33](#) to [35](#) for each NPE system node and the alternate NPS system node associated with this chain.
- 37 Wait for the local subsystem instance to be deactivated/prohibited, then, re-activate the local subsystem instance running on the inactive NPC. To do this, click **configuration>sccp>shared-local-subsystem-instance**, select the NPx of interest and click **Activate**.
- 38 If an NPE chain has been provisioned with an alternate NPS system node, wait for the local subsystem instance to be deactivated/prohibited, then re-activate the local subsystem instance running on the alternate NPS. To do this, click **configuration>sccp>shared-local-subsystem-instance**, select the NPx of interest and click **Activate**.
- 39 Wait for the re-activated local subsystem instances to return to the activated/allowed state.
- 40 Monitor the USP to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs. If it does, do not continue with the node downgrade.

- 41** Ensure that the activity state of the NPC is set to not-active. To do this click **Administration>shared>local-subsystem**.

**If****Do**

the NPC's activity state is currently active

continue to step [42](#).

the NPC's activity state is currently inactive

continue to step [43](#).

- 42** SWACT the currently active NPC node. To do this click **Administration>platform>node**.
- 43** Monitor the USP to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs. If it does, do not continue with the node downgrade.

**On LSMS**

- 44** Re-establish all SMI connections to the UNPM. Refer to the LSMS operation manual for release methods.
- 45** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

**Downgrading a single Link node****ATTENTION**

To downgrade an NPC, NPS, or NPE node see [Downgrading the NPC, NPS, and NPE nodes on page 1746](#).

The following procedure is used to downgrade a single system node using the wizard.

**To downgrade a single Link node:****At the OAMP workstation**

- 1** Select the node to downgrade in the list of available nodes in the software upgrade wizard.
- 2** Click the **Downgrade** button. The system asks for confirmation.

- 3 Wait for node downgrade to complete (upgrade-status will change to not-upgraded on completion).  
**Note:** If the automatic node downgrade fails to complete successfully, perform the downgrade manually. See [Manually downgrading system nodes on page 1755](#).
- 4 Monitor the USP to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs. If it does, do not continue with the node downgrade.
- 5 Repeat this procedure for all remaining link nodes.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Downgrading multiple Link nodes

### ATTENTION

To downgrade an NPC, NPS, or NPE node, see [Downgrading the NPC, NPS, and NPE nodes on page 1746](#).

The following procedure is used to downgrade multiple system nodes using the wizard.

### To downgrade multiple Link nodes:

#### *At the OAMP workstation*

- 1 **Shift-click** or **ctrl-click** to select a range of nodes to downgrade in the list of available nodes in the software upgrade wizard.
- 2 Select the delay interval between each successive node downgrade. This will be used to soak the downgraded node before moving to the next system node.
- 3 Click the **Downgrade node** button. The system asks for confirmation.
- 4 Wait for the node downgrade to complete (upgrade-status will change to not-upgraded on completion).  
**Note:** If the automatic node downgrade fails to complete successfully, perform the downgrade manually. See [Manually downgrading system nodes on page 1755](#).
- 5 The downgrade will now delay for the selected interval before continuing to the next node to downgrade. Downgrade of nodes can be cancelled at any time by clicking the **Stop** button. To skip the delay count down, click **No delay** and the next node will be downgraded immediately.
- 6 Monitor the USP to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs. If it does, do not continue with the node downgrade.
- 7 Repeat this procedure for all remaining link nodes.
- 8 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Downgrading the inactive RTC node in slot 15

The downgrade of the RTC in slot 15 can take up to 20 minutes to complete.

### To downgrade the inactive RTC in slot 15:

#### *At the OAMP workstation*

- 1 Verify that RTC15 is the inactive RTC.
  - a In the menu bar, click **Configuration>platform>node**.
  - b Click the **Graphical view** tab.
  - c Double-click the RTC in slot 15.

| If                             | Do                                                         |
|--------------------------------|------------------------------------------------------------|
| the Activity State is inactive | Continue to <a href="#">step 2</a> .                       |
| the Activity State is active   | Perform a SWACT, then continue to <a href="#">step 2</a> . |
- 2 Select the RTC15 node to downgrade from the list of available nodes in the software upgrade wizard.
- 3 Click the **Downgrade** button. A confirmation dialog box appears. Click **Yes** to continue.
- 4 Wait for node downgrade to complete (the upgrade-status will change to not-upgraded on completion).
 

**Note:** If the automatic node downgrade fails to complete successfully, perform the downgrade manually. See [Manually downgrading system nodes on page 1755](#).
- 5 Monitor the USP to ensure it performs normally and does not report any LOG\_SWERRS or LOG\_TRAPS. If it does, contact your next level of support.
- 6 Set the alternate boot load for RTC system nodes to the downgrade load.
 

**Note:** The alternate boot settings are used when an RTC is not able to boot from disk.

  - a Click **Administration>alternate-boot-server**.
  - b Update RTC 12 to the old release version by selecting the old release from the ABS Active Loads drop-down menu.
  - c Update RTC 15 to the old release version by selecting the old release from the ABS Active Loads drop-down menu.

- d Select the data snapshot taken before starting the upgrade from the Alt. Boot Data Snapshot list. Once the snapshot is selected, the window displays the Description.
        - e Click **Modify**.
- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Manually downgrading system nodes

You can only downgrade system nodes if the RTC in slot 12 is not upgraded. Nortel Networks recommends that you downgrade the cards in the reverse order as you upgraded the cards.



### CAUTION

Do not downgrade RTC 15 until all other cards have been downgraded. If you downgrade RTC 15 before you have downgraded all the other cards in the system, and an upgraded card reboots, the upgraded card is orphaned and will not enable because there is no upgraded RTC to provide the upgraded data. To recover this orphaned card, change the boot load to the older release.

The procedures in this section describe how to perform a downgrade for each of the following nodes:

- CC system node
- Link system nodes
- NPC, NPS, and NPE system nodes
- RTC system node in slot 15; this must be the last card downgraded

Perform each downgrade only as necessary (if you upgraded the system node).



### **Manually downgrading a CC system node**

The following procedure is used to manually downgrade the CC system node.

#### **To manually downgrade a CC system node:**

##### ***At the OAMP workstation***

- 1** Click **Configuration>platform>node**.
- 2** Double-click the slot for this node to open the node in the **Administration** panel.
- 3** Click **Graphical View**.
- 4** Select the drop-down menu to set the boot image to the previous release version.
- 5** Lock and load the CC system node.
- 6** When the CC system node becomes enabled, unlock it.
- 7** Verify that the running load is the downgraded load. If not, double-check that the correct image is selected on the maintenance and provisioning window.
- 8** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Manually downgrading the Link system nodes

Downgrade the Link system nodes one at a time, beginning with the lowest slot number and proceeding to the highest slot number.

### ATTENTION

To manually downgrade an NPC, NPS, or NPE node see [Manually downgrading the NPC, NPS, and NPE system nodes on page 1759](#).

## To manually downgrade the Link system nodes:

### *At the OAMP workstation*

- 1 Click **Configuration>platform>node**.
- 2 Click **Graphical View**
- 3 Double-click the slot for the link node to open the node in the **Administration** panel.
- 4 Select the drop-down menu to set its boot image to the previous Link release version. Set the HA boot image to the previous HA release version, if applicable.  
**Note:** IP high-speed link (HSL) link cards do not require HA loads.
- 5 Inhibit all the links on the Link system node, if applicable.  
**Note 1:** You cannot inhibit IPS7 links.  
**Note 2:** If there is only one available link on a linkset, you cannot inhibit it. If there are other links on the linkset, make at least one of them available before attempting to inhibit the link. If it is a one-link linkset, proceed to step [6](#) without inhibiting the link.
- 6 Deactivate all of the links or paths on the Link system node, as applicable.
- 7 Lock and load the Link system node.
- 8 When the Link system node becomes enabled, unlock it.
- 9 Verify that the running load is the downgraded load. If not, double-check that the correct image is selected on the maintenance and provisioning window.
- 10 Activate and uninhibit all of the links on the Link system node.
- 11 Repeat steps [4](#) to [10](#) for the remaining Link system nodes.

- 12** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Manually downgrading the NPC, NPS, and NPE system nodes

If your system includes the optional Universal Number Portability Master (UNPM) feature, you must downgrade the NPC, NPS, and NPE system nodes (on all shelves if you have a dual-shelf or multi-shelf system). If your system does not include the UNPM feature, skip this section.



### CAUTION

#### Potential for NPDB corruption

If downgrading the NP nodes/chains, the connection to the LSMS will need to be released on the LSMS. Refer to the LSMS operation manual for release methods. Contact Nortel Networks Technical Support. Failure in doing so will result in NPDB corruption.

## To manually downgrade the NPC, NPS, and NPE system nodes:

### On LSMS

- 1 Release all SMI connections to the UNPM. Refer to the LSMS operation manual for release methods.

### At the OAMP workstation

- 2 Click **Configuration>platform>node**.
- 3 Click **Graphical View**.
- 4 Double-click the slot for this node to open the node in the **Administration** panel.
- 5 Select the drop-down menu to set the boot image to the previous release version.
- 6 If an NPE chain has been provisioned for this NPC, repeat steps [2](#) to [5](#) for the NPE system nodes and the alternate NPS system node associated with this chain.
- 7 Deactivate the NP LSS instance running on the inactive NPC system node, using the Local Subsystem Instance window.
- 8 If an NPE chain has been provisioned with an alternate NPS, deactivate the NP LSS instance running on the alternate NPS system node, using the Local Subsystem Instance window.
- 9 Lock and load the inactive NPC system node.
- 10 If an NPE chain has been provisioned for this NPC, lock and load each NPE system node and the alternate NPS system node associated with this chain.

- 11 When the inactive NPC system node becomes enabled, unlock it.
- 12 If an NPE chain has been provisioned for this NPC, when each NPE system node and the alternate NPS system node becomes enabled, unlock each of these nodes.
- 13 Contact Nortel Networks Technical support to continue the downgrade.  
**Note:** NPDB raises a critical alarm, this is expected due to Nortel Networks technical support issuing commands on the NPDB.
- 14 Wait for the LSSI to be Deactivated/Prohibited, then re-activate the local subsystem instance running on the inactive NPC system node.
- 15 If an NPE chain has been provisioned with an alternate NPS, wait for the LSSI to be Deactivated/Prohibited, then re-activate the NP LSS instance running on the alternate NPS system node.
- 16 Verify that the load running for the inactivate NPC system node is the previous version. If not, make sure that the correct image is selected on the maintenance and provisioning window. If the right image is selected but the incorrect load is running, stop the downgrade procedures and contact Nortel Networks technical support.
- 17 When the re-activated local subsystem instance(s) enter the allowed/activated state, monitor the USP for 15 minutes to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs.
- 18 If NPS system nodes are provisioned, select an NPS system node to be downgraded. Note, that this can not be an NPS system node already downgraded in the previous steps. If there are no NPS system nodes to be downgraded, skip to step [31](#).
- 19 In the provisioning and maintenance window of the selected NPS system node, set its boot image to the previous NPS release version.
- 20 If an NPE chain has been provisioned for the selected NPS, repeat steps [2](#) to [5](#) for the NPE system nodes and the alternate NPS system node associated with this chain.
- 21 Deactivate the local subsystem (LSS) instance associated with the NPS system node.
- 22 If an NPE chain has been provisioned with an alternate NPS for the selected NPS, deactivate the NP LSS instance running on

- the alternate NPS system node, using the Local Subsystem Instance window.
- 23** Lock and load the selected NPS system node.
  - 24** If an NPE chain has been provisioned for this NPS, lock and load each NPE system node and the alternate NPS system node associated with this chain.
  - 25** When the NPS system node becomes enabled, unlock it.
  - 26** If an NPE chain has been provisioned for this NPS, when each NPE system node and the alternate NPS system node becomes enabled, unlock each of these nodes.
  - 27** Wait for the LSSI to be Deactivated/Prohibited, then re-activate the LSS instance on the NPS system node.
  - 28** If an NPE chain has been provisioned with an alternate NPS, wait for the LSSI to be Deactivated/Prohibited, then re-activate the NP LSS instance running on the alternate NPS system node.
  - 29** Verify that the running load is the previous version. If not, make sure that the correct image is selected on the provisioning and maintenance window.
  - 30** Repeat steps [17-29](#) for any remaining NPS system nodes in the system.
  - 31** Once the re-activated local subsystem instance(s) enter the allowed/activated state, monitor the USP for 15 minutes to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs.
  - 32** In the provisioning and maintenance window of the active NPC system node, click the SWACT button to switch the active NPC system node.
  - 33** In the provisioning and maintenance window of the newly inactive NPC system node, set its boot image to the previous NPC release version.
  - 34** If an NPE chain has been provisioned for this NPC, repeat steps [2](#) to [5](#) for the NPE system nodes and the alternate NPS system node associated with this chain.
  - 35** Deactivate the local subsystem instance on the newly inactive NPC system node.
  - 36** If an NPE chain has been provisioned with an alternate NPS, deactivate the NP LSS instance running on the alternate NPS system node, using the Local Subsystem Instance window.
  - 37** Lock and load the newly inactive NPC system node.

- 38 If an NPE chain has been provisioned for this NPC, lock and load each NPE system node and the alternate NPS system node associated with this chain.
- 39 When the newly inactive NPC system node becomes enabled, unlock it.
- 40 If an NPE chain has been provisioned for this NPC, when each NPE system node and the alternate NPS system node becomes enabled, unlock each of these nodes.
- 41 Wait for the LSSI to be Deactivated/Prohibited, then re-activate the local subsystem instance on the newly inactive NPC system node.
- 42 If an NPE chain has been provisioned with an alternate NPS, wait for the LSSI to be Deactivated/Prohibited, then re-activate the NP LSS instance running on the alternate NPS system node.
- 43 Verify that the load running is the previous version. If not, make sure that the correct image is selected on the maintenance and provisioning window. If the right image is selected but the incorrect load is running, stop the downgrade procedures and contact Nortel Networks technical support.
- 44 In the provisioning and maintenance window of the newly inactive NPC system node, click the SWACT button to switch the active NPC system node.
- 45 Once the re-activated local subsystem instance(s) enter the allowed/activated state, Monitor the USP for 15 minutes to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs.

#### ***On LSMS***

- 46 Re-establish all SMI connections to the UNPM. Refer to the LSMS operation manual for release methods.
- 47 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

**Manually downgrading the RTC system node in slot 15**

The following procedure is used to manually downgrade the RTC system node in slot 15.

**To manually downgrade the RTC system node in slot 15:*****At the OAMP workstation***

- 1** Click **Configuration>platform>node**.
- 2** Click **Graphical View**.
- 3** Double-click the slot 15 for this RTC node to open the node in the **Administration** panel.
- 4** Select the drop-down menu to set the boot image to the previous release version.
- 5** Lock and load the inactive RTC system node.
- 6** When the inactive RTC system node becomes enabled, unlock it.
- 7** Verify that the running load is the downgraded version. If not, make sure that the correct image is selected on the Provisioning and Maintenance window. If the correct image is selected, but the incorrect image is running, stop the downgrade procedures and contact your next level of support.
- 8** Set the alternate boot load for both RTC 12 and RTC15 to the previous load.
- 9** After downgrading the RTC, perform a test call to make sure the call is routed correctly. If there are any errors, contact your next level of support.  
  
Proceed to the section [Stop the upgrade and delete the upgrade package on page 1764](#).
- 10** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Stop the upgrade and delete the upgrade package

When you abort a software upgrade procedure, perform the procedure: Stopping the upgrade.

Remove the upgrade package from both RTC system nodes. To do this, perform the procedure: Deleting the upgrade package.

You then must delete the new loads from RTC12 and RTC15, delete all snapshots associated with the unwanted USP release from both RTC system nodes, and delete the loads and snapshots from the Alternate Boot Server.

### Stopping the upgrade

#### *At the OAMP workstation*

- 1 Click Stop Upgrade. A confirmation dialog box appears.
- 2 Click Finish on the wizard action and navigation panel.
- 3 Create a data snapshot, copy it to the alternate boot server and set the alternate boot server snapshot
- 4 Set user privileges back to pre-upgrade settings and re-enable any user accounts that were disabled during the upgrade. Refer to the file you created in "Limit user access" section, step [7](#) for the correct user status. Refer to the sections Security: User accounts and Security: User session in the *USP Administration and Security* guide for additional information.
- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Deleting the upgrade package

#### *At the OAMP workstation*

- 1 Open the File Manager panel. To do this, click **Administration>File Manager**.
- 2 Highlight RTC12 in the list.
- 3 Open the upgrade folder.
- 4 Open the required version folder.
- 5 Select the required upgrade file.
- 6 Click **Delete**.
- 7 Repeat steps [2](#) to [6](#) for the RTC in slot 15.
- 8 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Deleting the new loads from RTC12 and RTC15

### *At the OAMP workstation*

- 1 Open the File Manager panel. To do this, click **Administration>File Manager**.
- 2 Select the RTC system node from which you want to delete the load image file from the RTC drop box.
- 3 Expand the Loads folder.
- 4 Expand the folder for the new release.
- 5 Select the files to be deleted from the Loads.  
**Note:** Make sure you select the correct loads before deleting them.
- 6 Click **Delete**.
- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Deleting snapshots from the RTCs

### *At the OAMP workstation*

- 1 Open the File Manager panel. To do this, click **Administration > File Manager**.
- 2 Select the RTC system node from which you want to delete the snapshot from the RTC drop box.  
**Note:** You cannot delete the boot data snapshot. If you attempt to delete the boot data snapshot, you will receive an error message.
- 3 Expand the Snapshot folder.
- 4 Expand the folder for the new release.
- 5 Click Delete to delete the snapshot. An hourglass appears while the data snapshot is deleted. When the deletion operation is complete, snapshot is removed from the RTC side of the File Manager window.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Deleting loads from the alternate boot server

### *At the OAMP workstation*

- 1 Open the ABS configuration manager. There are two versions of ABS Configuration Manager available on the CMT. One is graphically-based and the other is console-based. If you opened the graphically-based ABS Configuration Manager, perform steps [2](#) to [4](#). If you opened the console-based ABS Configuration Manager, proceed to step [5](#).
- 2 Click on file, then select **uninstall release** from the drop-down menu. The uninstall existing release window appears.
- 3 Select the load to be deleted from the drop-down menu.
- 4 Click **Apply**, and proceed to [step 6](#).
- 5 Enter **ABSCM>release uninstall <release-name>**.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Deleting old snapshots from the alternate boot server

### *At the OAMP workstation*

- 1 Open the File Manager panel. To do this: click **Administration>File Manager**.
- 2 Expand the Snapshot folder.
- 3 Expand the folder for the new release.
- 4 Click **Delete** to delete the snapshot. An hourglass appears while the data snapshot is deleted. When the deletion operation is complete, the snapshot is removed from the Alternate Boot Server side of the File Manager window.
- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Downgrade the GUI

When aborting a software upgrade, you can choose to uninstall the new version of the USP GUI from your workstation(s) and then install the previous version.

However, downgrading the GUI is not required. The new version of the GUI is backward-compatible with the previous USP software.

If you choose to downgrade the GUI, uninstall the upgraded version and install the downgrade version on your alternate boot server first, and then repeat both procedures for the other OAMP workstations in your system, as necessary. To do this, see the procedure [Uninstalling the upgraded USP GUI on page 1767](#)

If you uninstall the new version of the GUI, you must then install the previous version. To do this, see the procedure [Installing the previous version of the USP GUI on page 1767](#). Finally, after you have downgraded the GUI and restarted the workstation, you must reset the alternate boot server to the original configuration. To do this, see the procedure [Modifying the alternate boot server on page 1769](#).

## Uninstalling the upgraded USP GUI

### *At the OAMP workstation*

- 1 Close any open applications and exit all USP Distinct servers.
- 2 In Windows, click **Start** on your desktop.
- 3 On the Settings menu, select **Control Panel**.
- 4 In the Control Panel window, double-click the **Add/Remove Programs** icon.
- 5 In the Install/Uninstall tab window of the Add/Remove Programs Properties window, select Universal Signaling Point from the alphabetical list of programs.
- 6 Click **Change/Remove**. A pop-up menu asks if you are sure you want to completely remove the USP and all of its components.
- 7 Click **Next**.
- 8 Click **Complete UnInstall**.
- 9 Click **Yes** to confirm your choice. All of the files are removed.
- 10 Restart your computer.
- 11 This procedure is complete. After your computer restarts, proceed to the next section .

## Installing the previous version of the USP GUI

### **ATTENTION**

To install the previous version of the USP GUI, you will require a Window-based OAMP workstation.

***At the OAMP workstation***

- 1** Insert the previous version of the USP software CD-ROM disk into the CD-ROM drive.
- 2** Double-click the **My Computer** icon.
- 3** Double-click the CD-ROM disk icon.
- 4** Double-click **Setup.exe**.
- 5** A pop-up window appears with the warning that installing this software on a workstation other than a Nortel Networks-approved workstation can overwrite some system files used by other applications. If this is a Nortel Networks-approved workstation, click **Yes** to continue.
- 6** At the Welcome window for the setup program, click **Next**. The Copying Program Files window appears with a status bar while the files are copied.
- 7** A pop-up window asks if you want to configure this workstation as an alternate boot server. Each USP system needs one workstation configured as an alternate boot server. If this workstation is your alternate boot server, click **Yes**. If not, click **No**.

**Note:** Do not configure more than one alternate boot server for each USP system.

If you answer yes, then after completing these installation steps, follow the additional steps to configure the three distinct servers (the BOOTP server, the NFS server, and the FTP server).

- 8** If Adobe Acrobat Reader is already installed on this workstation, skip to step [12](#). If not, a Welcome window for Adobe Acrobat Reader Setup Program appears. Click **Next**.
- 9** The Acrobat Reader Licence Agreement appears. Click **Yes** to accept the terms of the agreement.
- 10** The Acrobat Reader Destination Location window appears. Click **Next**. Do not modify the destination path for Acrobat Reader.
- 11** The Acrobat Reader Setup Complete window appears. Click **Finish**. The Acrobat Reader Setup Complete window appears again. Click **OK**.
- 12** The Installation Setup Complete window appears.
- 13** Click the radio button next to the option "Yes, I want to restart my computer now".
- 14** Click **Finish**. The computer restarts.

- 15 Remove the USP software disk from the drive. Keep the disk handy to the USP hardware.
- 16 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Modifying the alternate boot server

### *At the OAMP workstation*

1



#### CAUTION

Make a record of the password immediately.

A pop-up window prompts you to create a password for the Alternate Boot Server Configuration Manager.

- 2 Click the **Distinct BOOTP Server** button on the taskbar to maximize the Distinct BOOTP Server window.
- 3 Click the Configure menu and select Administrator and then Login to display the Distinct BOOTP Login window.
- 4 Enter your administrator password in the Enter the administrator password field and click **OK** to log into the server.  
The Distinct BOOTP Login window closes.
- 5 Click the Configure menu and select Server to display the Configure BOOTP window.
- 6 In the Addresses tab window, view the contents of the field at the bottom of the window, next to the Add, Modify, and Remove buttons. This field will contain the hexadecimal Ethernet hardware addresses of the RTC system nodes in your system.
- 7 Select the Ethernet hardware address that matches the Ethernet hardware address for the RTC system node in slot 12 of your system. The information for that Ethernet hardware address will appear in the various fields.
- 8 In the Boot File field, change the value to **/d/ntssgusp/abs/sites/<site\_name>/rtc12/rtcboot** (where site\_name is the name of your system as it appears in the site configuration information).
- 9 Click **Modify** to save the changes.

- 10 Select the Ethernet hardware address that matches the Ethernet hardware address for the RTC system node in slot 15 of your system. The information for that Ethernet hardware address will appear in the various fields.
- 11 In the Boot File field, change the value to **/d/ntssgusp/abs/sites/<site\_name>/rtc15/rtcboot** (where *site\_name* is the name of your system as it appears in the site configuration information).
- 12 Click **Modify**, then **Apply** to save the changes.
- 13 Open the Alternate Boot Server Configuration Manager. There are two versions of the ABS Configuration Manager available on the CMT. One is graphically-based and the other is console-based. If you opened the graphically-based ABS Configuration Manager, perform steps [14](#) to [20](#). If you opened the console-based ABS Configuration Manager, perform steps [21](#) to [29](#).
- 14 Log in to the Alternate Boot Server Configuration Manager.
- 15 Under the File drop-down menu, select ABS Configuration.
- 16 Select a site from the Site list.
- 17 Confirm that the Alternate Boot Loads displayed for each RTC are for the pre-upgrade load.
- 18 Confirm that the Alternate Boot Snapshot display is the snapshot taken earlier in this procedure. A pre-upgrade snapshot
- 19 Click **Apply** to save the changes.
- 20 Log out of the Alternate Boot Server Configuration Manager and proceed to [step 30](#).
- 21 Log in to the console-based Alternate Boot Server Configuration Manager.  
Type: **ABSCM>login**
- 22 Enter the **ABSCM> site show <site-name>** command to view the site's details.
- 23 To view all the available loads, enter **ABSCM>load show all**.
- 24 To view all the snapshots for a specified site, enter:  
**ABSCM>snapshot show <site-name>**
- 25 To modify the RTC12-load of the specified site, enter:  
**ABSCM>site mod <site-name> rtc12-load  
<new-rtc12-load-name>**
- 26 To modify the RTC15-load of the specified site, enter:

**ABSCM>site mod <site-name> rtc15-load  
<new-rtc15-load-name>**

- 27** To modify the snapshot of the specified site, enter:

**ABSCM>site mod <site-name> snapshot  
<new-snapshot-name>**

- 28** Confirm that the Alternate Boot Snapshot display is the snapshot taken earlier in this procedure. It should be a pre-upgrade snapshot.
- 29** Log out of the Alternate Boot Server Configuration Manager.
- 30** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

**Note:** Refer to the *ABS\_Specification.pdf* document for the complete details of all the console-based ABS Configuration Manager commands.





# USP-Compact upgrade

## New in this release

### Feature changes

This release introduces no feature changes that affect upgrades.

### Other changes

The following other changes in this release affect upgrades.

- Numerous changes were made throughout the guide to document specific upgrade procedural changes related to the new release.
- Minor errors were corrected throughout.

## Upgrade paths

This procedure provides the high-level steps to prepare for an upgrade from:

- USPc10.0/(I)SN08 to USPc11.1/(I)SN09U (described in this document)
- USPc11.0/(I)SN09 to USPc11.1/(I)SN09U (described in the Readme file for this release.)
- USPc11.1/(I)SN09U to USPc11.1/(I)SN09U (described in the Readme file for this release.)

## Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

### Time to complete an upgrade

The following table lists the tasks to upgrade USP-Compact software and the estimated time to complete each task.

**Table 1 Estimated time to complete a software upgrade**

| Task                         | Time                                 |
|------------------------------|--------------------------------------|
| Preparing for the upgrade    | 15 minutes                           |
| Upgrading the software       | 20 minutes for each USP-Compact card |
| Completing the upgrade       | 27 minutes                           |
| Total estimated upgrade time | up to 2 hours                        |

**Note:** All times are estimates. The steps to gather software are not service affecting and can be performed before the software upgrade.

### Service impacts

The upgrade of USP-Compact software does not impact service. Traffic is maintained through redundant links configured on different link cards. A loss of network redundancy occurs when a blade is taken out of service.

### Additional information

None

### System capacity

The software upgrade procedure can impact the system capacity. This means that additional disk space on the OAMP workstation and the SAM21 disk complex are required for converting existing databases. The pre-checking procedure checks for adequate disk space on the disk complex. A message box informs you if your disk space is too low. If disk space is too low, delete any old snapshots. Once the update is complete, the additional disk space is no longer required and is made available for use.

## System performance

The software upgrade procedure can impact USP-Compact system performance in the following ways:

- An upgrade database conversion is necessary due to internal USP-Compact data format changes. This affects the inactive USPc card (card on the right in the shelf).
- Depending on the scope of data format changes, the inactive USPc card takes approximately 15 minutes to load and convert internal data to the new format. During this time, the inactive USPc card is not enabled and the system operates with a single USPc card.
- The network capacity is reduced during software upgrade. This results from taking down one of the USPc cards which takes down approximately half of the SS7 signaling links. Therefore, you must perform software upgrade procedures during maintenance periods.

## Limitations

The following limitations apply, listed by subsystem:

- System administration
  - adding, deleting, or modifying users
  - setting the time of day
  - changing passwords
- System management
  - modifying the system name or shelf names
  - adding or deleting system nodes
  - modifying the IP address or the PEC of the USPc cards
- SS7 management (MTP Level 3)
  - adding, deleting, or modifying a system identity
  - adding, deleting, or modifying a capability code
  - adding, deleting, or modifying links, linksets, linkset groups, combined linksets, or routesets

- SS7 management (MSU Trace Screening)
  - deleting MSU Trace criteria file
- IPS7 management
  - adding, deleting, or modifying application server process (ASP)
  - adding, deleting, or modifying application server process path (ASP Paths)
  - adding, deleting, or modifying application server (AS)
  - adding, deleting, or modifying application server destination (AS destination)
  - adding, deleting, or modifying application server assignment (AS assignment)

### **OAMP workstation functionality**

The GUI allows multiple sites to be configured on an OAMP workstation at one time. Since the sites are not upgraded at the same time, the following conditions apply:

- The GUI can only be used to access existing USP-Compact capabilities. You cannot access the new capabilities until the USP-Compact is fully upgraded to USPc11.1.
- The GUI allows you to log in to a USPc10 or USPc11 system with or without an upgrade in progress.
- You cannot use a previous version of the GUI to log into a newer version of the USP-Compact software.
- Only one version of the GUI can be installed at a time because the GUI upgrade requires the conversion of local files.

### **Aborting an upgrade**

If you need to abort the USP-Compact upgrade, perform [Downgrading the USP Compact cards.](#)

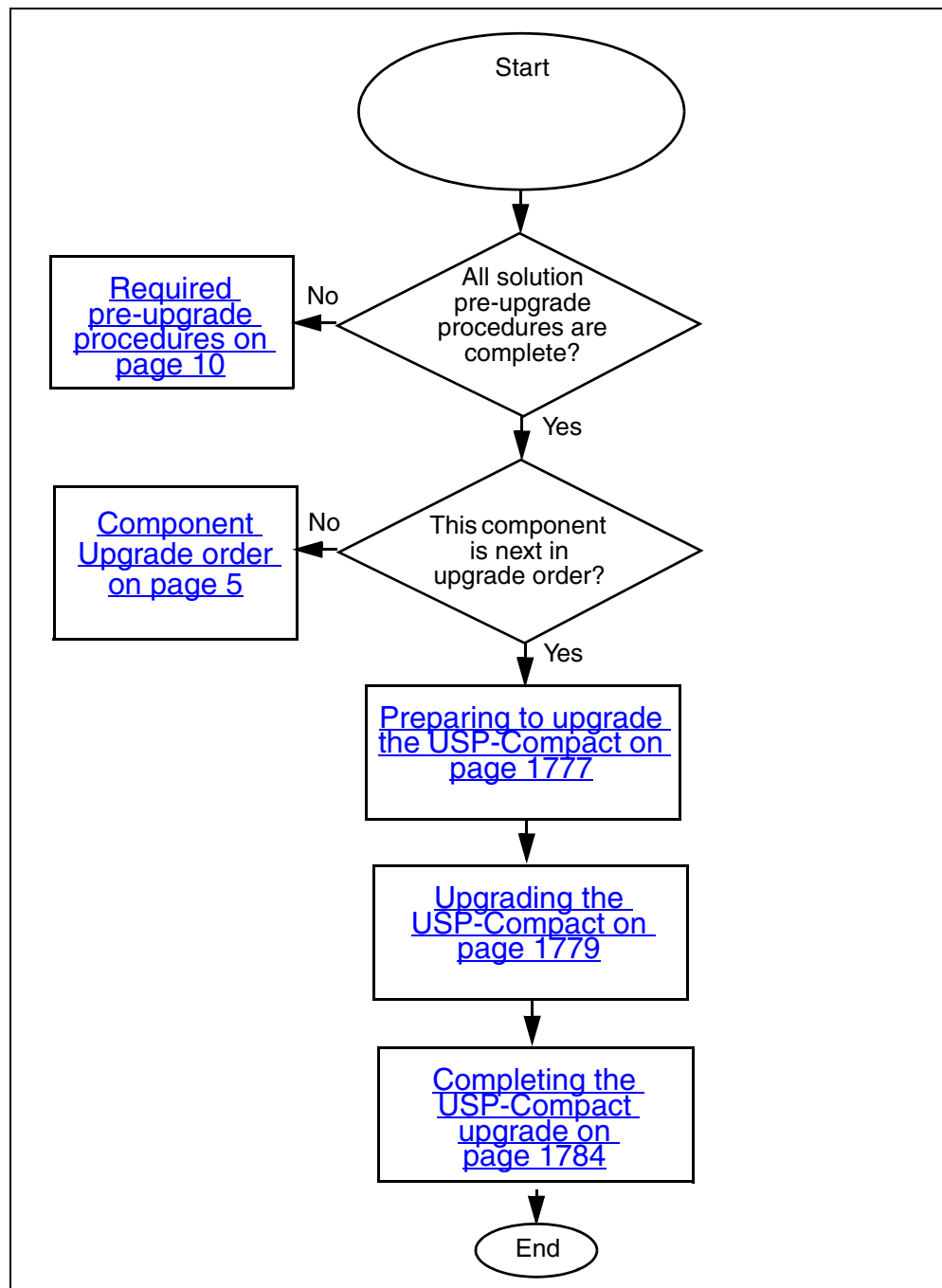
### **Tools and utilities**

This upgrade procedure requires the FTP client application.

## USP-Compact upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

### USP-Compact upgrade tasks



---

## Preparing to upgrade the USP-Compact

---

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

Complete the following tasks:

- Complete any prerequisites identified at the beginning of this document.
- Complete the upgrade of all components that precede the USP-Compact.
- Know how new USP-Compact software is delivered to your office. The following methods are available:
  - compact disk (CD)
  - Electronic Software Delivery (ESD)

### Action

Perform the following procedure to prepare the USP-Compact for a software upgrade.

#### Preparing to upgrade the USP-Compact

##### *At your workstation*

- 1 Log in to the USP-Compact GUI.

##### *At the USP-Compact GUI*

- 2 Determine the release that is running on the USP-Compact, which is indicated in the status bar as “Connected to <lab\_name> <load\_version>”, and ensure the USP-Compact is running the latest point release of the current major release. Check for any RMR bulletins to determine the latest point release.
- 3 Make sure that both USPc cards are in-service. Click **Configuration>platform>node**. Verify that the LED icons for each in-service system node are green.
- 4 Take corrective action to clear all outstanding alarms.
- 5 Virtual linksets are not supported on the USP-Compact. Verify that there are no virtual linksets provisioned on the system. To do this, perform the following steps:
  - a Click **Configuration>mtp>linkset**.



---

## Upgrading the USP-Compact

---

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

Complete the following tasks:

- [Preparing to upgrade the USP-Compact on page 1777](#)
- Know where the USP-Compact GUI resides in your office. The GUI can reside on a windows-based OAMP workstation or the CS 2000 Management Tools-based OAMP workstation.

**Note:** Auto-negotiate capability is supported for the CS LAN and can be enabled during this upgrade.

### Procedure

Perform the following procedure to upgrade the software on the USP-Compact.

#### Upgrading the USP-Compact

|                                                     |
|-----------------------------------------------------|
| <p style="text-align: center;"><b>ATTENTION</b></p> |
|-----------------------------------------------------|

|                                                            |
|------------------------------------------------------------|
| <p>The CLI is not available for use during an upgrade.</p> |
|------------------------------------------------------------|

#### *At your workstation*

- 1 Upgrade the GUI.
  - For Windows-based OAMP workstations see [Upgrading the USP-Compact GUI on a windows-based OAMP workstation on page 1792](#)
  - For CS 2000 Management Tools-based OAMP workstations, see one of the following procedures:
    - Note:** Nortel recommends console mode to upgrade the GUI. GUI mode requires an EXCEED session.
    - To use console mode to upgrade the GUI, see [Upgrading the USP-Compact GUI on a CS 2000 Management Tools OAMP workstation in console mode on page 1796](#)
    - To use GUI mode to upgrade the GUI, see [Upgrading the USP-Compact GUI on a CS 2000 Management](#)



[Tools-based OAMP workstation in GUI mode on page 1799](#)

- 2 Transfer software to the NFS server.
  - a Go to the CD or directory that contains the new USP-Compact software.
  - b Locate the following files in the Program\ntssgusp\load directory:
    - uspc\_11\_01\_XX\_XXX
    - uspc\_11\_01\_XX\_XXX\_base
    - uspc\_11\_01\_XX\_XXX\_t1e1ha

**Note:** XXX is a build version, for example,  
uspc\_11\_01\_00\_05b
  - c Use an FTP client to transfer these files to both of the NFS server cards. The destination directory is:  
/nfsserv/usp/sd0/loads/
  - d Connect to both NFS server cards using SSH, and set the permissions correctly.  
ssh <user\_id>@<IP>  
cd /nfsserv/usp  
chmod -R 777 sd0  
where:  
<user\_id> is ID of the user  
<IP> is the IP address or host name of the server where the application is stored  

**Note:** If a prompt, similar to the following example, displays for accepting the RSA key, enter 'yes.'

### RSA key display example

```
$ ssh nortel@10.247.202.4
The authenticity of host '10.247.202. (10.247.202.4)' can't
be established.
RSA key fingerprint is
99:09:e2:80:57:95:3e:ae:be:26:08:a0:c6:32:ed:48.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.247.202.4' (RSA) to the list
of known hosts.
```

- 3 Transfer the upgrade package to the NFS server.

- a Open the CD or directory that contains the new USP-Compact software.
- b Locate the upgrade package in the USP-Compact zip file:  
upgrade\_pkg.tar.gz
- c Connect to the NFS server using SSH for the Master card.  
ssh <user\_id>@<IP>  
where: <user\_id> is ID of the user  
<IP> is the IP address or host name of the server where the application is stored

**Note:** If a prompt, similar to the following example, displays for accepting the RSA key, enter 'yes.'

### RSA key display example

```
$ ssh nortel@10.247.202.4
The authenticity of host '10.247.202. (10.247.202.4)' can't
be established.
RSA key fingerprint is
99:09:e2:80:57:95:3e:ae:be:26:08:a0:c6:32:ed:48.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.247.202.4' (RSA) to the list
of known hosts.
```

- d Determine which directory the USP-Compact is using for its database. View the /nfsserv/usp/sd0/sysconf file and search for the data\_dir variable. An example data is as follows:

```
data_dir = stp/data/.curr1
```

**Note:** The upgrade.pkg.tar package must be on both NFS servers for the GUI to display the package name to which you are upgrading. If the upgrade.pkg.tar package is not on both servers, the GUI fails to display the package name.

- e Using an FTP client, transfer this file to the following directory on both of the NFS server cards:

```
/nfsserv/usp/sd0/<data_dir>
```

- f Execute the following commands on both the NFS servers:

```
cd /nfsserv/usp/sd0/<data_dir>
```

```
gunzip upgrade_pkg.tar.gz
```

```
tar -xvpf upgrade_pkg.tar
```

```
chmod -R 777 upgrade_pkg
```

- g** Verify the directory owner and group settings by executing the following commands:

```
cd /nfsserv/usps
ls -la
```

For the sd0 directory, the owner and group name will be samss7, as shown in the following example:

```
drwxrwxrwx 7 samss7 samss7 84 Dec 2 01:37 sd0
```
- h** Log in as root and execute the following commands:

```
chown -R samss7 sd0
chgrp -R samss7 sd0
```
- 4** Log in to the USP-Compact GUI.
- 5** Click **Administration>software-upgrade**. Select the software release you are installing in the Target Version text box. Use the notation vn.n.n (for example, v11.0.1).
- 6** Click **Next** when the command is completed.
- 7** Run the precheck to ensure that the upgrade is ready to proceed. The system confirms:

  - Both USP-Compact cards are in-service with an operational state of enabled.
  - The master USP-Compact card is the current active card.
  - Software upgrade packages have been transferred to both the USP-Compact NFS servers.
- 8** Click **Next** when you see the message "upgrade precheck successful."

If any of the checks fail, resolve them before you proceed with the upgrade.
- 9** Restrict user access to the USP-Compact to prevent other users from accidentally modifying provisioning data while the upgrade is in progress. See [Restricting user access to the USP-Compact on page 1803](#)
- 10** Change the alternate boot data snapshot: create a new data snapshot, copy the data snapshot to the OAMP workstation, and change the alternate boot data snapshot for your site

  - a** Click **Administration>backup**.
  - b** Enter a description of the data snapshot in the **snapshot-description** field. You can enter a maximum of 32 characters.



---

## Completing the USP-Compact upgrade

---

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

The cleanup procedure deletes some of the upgrade files that were used during the upgrade. The complete procedure stops the upgrade, shuts down the wizard, creates a data snapshot, and restores access privileges.

### Prerequisites

Complete the following tasks:

- [Upgrading the USP-Compact on page 1779](#)

### Procedure

Perform the following procedure to complete the upgrade of USP-Compact software.

#### Completing the USP-Compact upgrade

**ATTENTION**

Wait 24 hours after you upgrade the USP-Compact before you perform this procedure.

#### *At the OAMP workstation*

- 1 Run the cleanup utility.
  - a Re-launch the upgrade software from the Upgrade Administration window. To do this, perform the following steps:
    - i Click **Administration>software-upgrade**.  
If you have performed the Activate features step, the Deactivate Features panel is displayed.
    - ii Click **Next**.
  - b Click **Run Cleanup**. A confirmation dialog box appears.
  - c Click **Yes**.
  - d Click **Next**.
- 2 Stop the upgrade.
  - a Click **Stop Upgrade**.



**7** In the list of network elements that displays, determine whether the USP-Compact is present.

**8** Use the following table to determine your next step.

| <b>If the USP-Compact is</b> | <b>Do</b>               |
|------------------------------|-------------------------|
| configured in IEMS           | step <a href="#">9</a>  |
| not configured in IEMS       | step <a href="#">10</a> |

**9** Update the software version in the Device Version field by editing the Managed Object Properties in IEMS for the USP-Compact that you just upgraded to reflect the new software version.

Refer to either of the following procedures to update the Device Version field:

- [Editing and viewing object properties using Java Web Start Client on page 2255](#)
- [Editing and viewing object properties using Web Client on page 2261.](#)

**10** You have completed the upgrade of software on the USP-Compact.

---

## Extracting and copying a USP-Compact ESD software file

---

Use this procedure to extract USP-Compact software from an ESD load file and, if necessary, copy the new USP-Compact software to the CS 2000 Management Tools server.

### Prerequisites

Perform the following tasks before you begin this procedure.

- Know the name of the ESD load file with the new USP-Compact software. Check the email from Nortel that announced the availability of the load.
- Know how you will upgrade USP-Compact software. If you upgrade USP-Compact software from the CS 2000 Management Tools server, you must copy the new USP-Compact software to the server.

### Action

Perform the following procedures.

- Extract the new USP-Compact software from the ESD load file. Perform [Extracting USP-Compact software from an ESD load file on page 1787](#).
- If you use the CS 2000 Management Tools server to upgrade USP-Compact software, perform [Copying new USP-Compact software to the CS 2000 Management Tools server on page 1789](#)

### Extracting USP-Compact software from an ESD load file

#### **ATTENTION**

Do not extract or uncompress files on the CS 2000 Management Tools server. The process requires additional disk space that may exceed the capacity of your server.

#### ***At your workstation***

- 1 Create a temporary directory to store the new USP-Compact software.
- 2 Use your FTP client application to copy the USP-Compact ESD load file from your ESD load repository server to your workstation. The actual steps to copy the files will depend on



your FTP client application. Following is an example of typical steps.

*Example*

1. *At your workstation, change directories to the temporary directory.*
  2. *Start an FTP session to the ESD load repository server.*
  3. *Change the session to binary.*
  4. *At the ESD load repository server, change directories to the dropbox with the USP-Compact ESD load file.*
  5. *Use the get command to transfer the USP-Compact ESD load file to the temporary directory on your workstation.*
  6. *Quit the FTP session*
- 3** Use a file archive program such as WinZip to extract a compressed version of new USP-Compact software from the ESD load file to the temporary directory.

*Response*

*The program extracts a compressed file with a .gz extension to a new directory in your temporary directory.*

*Example of name of compressed file*

*USPCM110.110.R.NCL.NAP.VAULT.9.D.tar.gz.tape*

- 4** Locate the compressed USP-Compact software file.
- 5** Rename the compressed USP- Compact software file to remove the .tape extension.

*Example of new file name*

*USPCM110.110.R.NCL.NAP.VAULT.9.D.tar.gz*

- 6** Use your file archive program to extract the new USP-Compact software to the temporary directory.

*Response*

*The program extracts the new software into a new folder in the temporary directory.*

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

| <b>If you install new USP-Compact software</b> | <b>Do</b>                                                                                            |
|------------------------------------------------|------------------------------------------------------------------------------------------------------|
| from your workstation                          | <a href="#">step 8</a>                                                                               |
| from the CS 2000 Management Tools server       | <a href="#">Copying new USP-Compact software to the CS 2000 Management Tools server on page 1789</a> |

- 8 You have completed this procedure. Return to [Preparing to upgrade the USP-Compact on page 1777](#).

### **Copying new USP-Compact software to the CS 2000 Management Tools server**

#### **ATTENTION**

In a two-server configuration, copy the software files to the active server.

#### ***At your workstation***

- Establish a connection to the server through telnet or SSH, and log in using the root user id and password.  
In a two-server configuration, log in to the active server using the physical IP address of the active server. Use the **ubmstat** command to make sure you are on the active server.
- Determine if the server has a /data/esd\_iso directory by typing  
# **ls /data/esd\_iso**  
and pressing the Enter key.
- Use the following table to determine your next step.

| <b>If the response</b>             | <b>Do</b>              |
|------------------------------------|------------------------|
| indicates no such directory exists | <a href="#">step 4</a> |
| displays the name of the directory | <a href="#">step 5</a> |

- Create the directory by typing  
# **mkdir /data/esd\_iso**  
and pressing the Enter key.

- 5 Display the available disk space in the /data directory by typing  
**# df -k /data**  
 and pressing the Enter key.

*Example response*

```
df -k /data
Filesystem kbytes used avail capacity Mounted on
/dev/md/dsk/d2 3082223 144125 2876454 5% /data
```

- 6 Determine the number of megabytes of free space by dividing the number under avail by 1000. The result is the amount of available disk space in Mbytes in the directory.
- 7 Use the following table to determine your next step.

| If the directory                                          | Do                     |
|-----------------------------------------------------------|------------------------|
| does not have at least 200 MBytes of available disk space | <a href="#">step 8</a> |
| has at least 200 MBytes of available disk space           | <a href="#">step 9</a> |

- 8 Clear additional disk space before you continue with this procedure. Follow local office policy. If necessary, contact the next level of support.
- 9 Log off of the CS 2000 Management Tools server.
- 10 Use your FTP client application to copy the uncompressed USP-Compact software from your workstation to the /data/esd\_iso directory on the CS 2000 Management Tools server.
- 11 Confirm all directories and files for new USP-Compact software were copied to the /data/esd\_iso directory of the CS 2000 Management Tools server.

**12****ATTENTION**

The following steps require you to change the permissions on a file on the CS 2000 Management Tools server. Depending on your FTP client application, you may need to quit the FTP client application and establish a telnet or SSH session to the server.

In the directory with new USP-Compact software, locate the file `install.bin`.

**13** Set the file permissions by typing

```
chmod 755 install.bin
```

and pressing the Enter key.

**14** Confirm the file permissions were changed by typing

```
ls -al install.bin
```

and pressing the Enter key.

*Response*

*The file install.bin has the permissions -rwxr-xr-x.*

**15** You have completed this procedure. Return to [Preparing to upgrade the USP-Compact on page 1777](#).

---

## Upgrading the USP-Compact GUI on a windows-based OAMP workstation

---

Perform the following procedures to upgrade the USP-Compact GUI on a windows-based workstation..

### Prerequisites

These procedures have the following prerequisites:

- Close any open applications before you begin this procedure.
- Make sure the OAMP workstation is set to either English or German language character sets. The GUI may not function properly with non-ASCII based character sets.

### Action

Perform the following procedures to upgrade the USP-Compact GUI on a windows-based workstation.

1. [Uninstalling the previous version of the GUI on page 1792](#)
2. [Installing the new version of the GUI on page 1793](#)

#### Uninstalling the previous version of the GUI

##### *At the OAMP workstation*

- 1 Make sure all applications are closed.
- 2 Click the Window's **Start** button on your desktop.
- 3 On the **Settings** menu, click **Control Panel**.
- 4 In the **Control Panel** window, double-click **Add/Remove Programs**.
- 5 In the **Install/Uninstall** tab window of the **Add/Remove Programs Properties** window, select Universal Signaling Point Compact from the alphabetical list of programs.
- 6 Click the **Add/Remove** button. Follow the prompts provided to uninstall the USP software components.
- 7 Click **NEXT**.
- 8 If a pop-up window asks if you want to remove shared files, click **Yes to All**.
- 9 Click **Yes** to confirm your choice. All the files are removed.
- 10 Restart your computer.

- 11 You have uninstalled the previous version of the GUI. Go to [Installing the new version of the GUI on page 1793](#).

### Installing the new version of the GUI

**CAUTION****Application failure on non-approved workstations**

Install USP-Compact software only on a workstation approved by Nortel Networks. If you install USP-Compact software on a workstation not approved by Nortel Networks, you may overwrite system files used by other applications and cause failure of existing applications.

**CAUTION****Certification failure and failure of USP-Compact application**

Install only software approved by Nortel Networks on your USP-Compact OAMP workstation. If you install non-approved software, you may invalidate the certification of the workstation and can cause failure of the USP-Compact application.

**CAUTION****Loss of GUI functionality**

Make sure the OAMP workstation is set to either English or German language character sets. The GUI may not function properly with non-ASCII based character sets.

#### ***At the OAMP workstation***

- 1 Close any open applications.
- 2 Use the following table to determine your next step.

| <b>If new USP-Compact software is located</b> | <b>Do</b>                                                                             |
|-----------------------------------------------|---------------------------------------------------------------------------------------|
| on a CD                                       | <a href="#">step 3</a>                                                                |
| in a directory on your PC                     | Open the directory with the new USP-Compact software and go to <a href="#">step 6</a> |

- 3 Insert the USP-Compact Software CD-ROM disk into the CD-ROM drive.
- 4 Double-click the **My Computer** icon on your desktop.
- 5 Double-click the CD-ROM disk icon.
- 6 Double-click **install.exe**. A pop-up dialog box appears indicating that it is preparing to install. This is followed by a splash screen.
- 7 At the Introduction window for the USP-Compact setup program, click **Next**.
- 8 Select the package(s) that you want to install on this workstation.
  - Select USPc Graphical Interface Client if you want this workstation to be able to log into the USP-Compact site.
  - Select USPc User Manuals and Documentation Suite to install the complete collection of FCAPS documents and Interface Specifications.
  - Select Adobe Acrobat PDF Reader Version 5.1 if you do not have a version of Adobe Acrobat Reader installed on this workstation.

---

**If you select**

---

**Do**

---

the GUI package

[step 9](#)

Acrobat Reader

[step 10](#) to [step 16](#)

---

- 9 Select an Installation Directory and click **Install**. Skip to [step 16](#).
- 10 Select an Installation Directory and click **Install**.
- 11 If you chose to install Acrobat reader, a Welcome window for the Adobe Acrobat Reader Setup Program appears. Adobe Acrobat Reader is required to view the Solution information. If Adobe Acrobat Reader is already installed on this workstation, click **No**.  
Click **Yes** to the Are you sure message. If you do not want to install Adobe Acrobat Reader, skip to [step 16](#).
- 12 Click **Next**. The Acrobat Reader Destination Location window appears.
- 13 Click **Next**.  
**Note:** Do not modify the destination path for Acrobat Reader.
- 14 The Acrobat Reader Setup Complete window appears. Click **OK**.
- 15 Click **Finish**.

- 16 The installation screen will indicate that installation was successful. Click **Done**.
- 17 You have upgraded the GUI. Return to [Upgrading the USP-Compact on page 1779](#).



## Upgrading the USP-Compact GUI on a CS 2000 Management Tools OAMP workstation in console mode

---

Perform the following procedures to use console mode to upgrade the USP-Compact GUI on a CS 2000 Management Tools-based OAMP workstation.

### Prerequisites

None

### Action

Perform the following procedures to upgrade the USP-Compact GUI.

1. [Uninstalling the previous version of the GUI on page 1796](#)
2. [Installing the new version of the GUI on page 1797](#)
3. [Verifying the GUI on page 1798](#)

### Uninstalling the previous version of the GUI

#### *At the OAMP workstation*

- 1 Launch the USP-Compact uninstall procedure.

```
> cd <original install path>/ntssgusp/compact
```

where

#### **original install path**

is /data/usp for offices at USP10 and lower

is /opt/usp for offices at USP11 and higher

```
> ./Uninstall_Universal_Signaling_Point_Compact
-i console
```

**Note:** A space precedes -i in the above command line.

- 2 Press Enter in the Introduction window.
- 3 In the Uninstall Options step.

| If                                             | Do                                                                                                                                                                    |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Completely remove all USPc software components | Press Enter                                                                                                                                                           |
| Choose specific USPc components to uninstall   | Select 2, press Enter; then select component number to be uninstalled (to uninstall multiple components, please use comma to separate the numbers), then press Enter. |

- 4 Press Enter to complete the uninstallation and to exit.
- 5 Clean up the original install directory to save disk space.  

```
>rm -Rf <original install path>/ntssgusp/compact
```

where

**original install path**  
is /data/usp for offices at USP10 and lower  
is /opt/usp for offices at USP11 and higher

**Note:** No space exists between /ntssgusp/compact in the above command line.
- 6 You have uninstalled the previous version of the GUI. Go to [Installing the new version of the GUI on page 1797](#).

## Installing the new version of the GUI

### At the OAMP workstation

- 1 Change directories.  

| If the new USP-Compact software is located | Do                |
|--------------------------------------------|-------------------|
| on a CD                                    | >cd /cdrom/cd0    |
| on the CS 2000 Management Tools server     | >cd /data/esd_iso |
- 2 List the directory and locate the install.bin file.  

```
>ls
```
- 3 Launch the installation program, which can take several minutes to finish launching.  

```
>./install.bin -i console
```
- 4 Press Enter in the Introduction step.
- 5 In the Component Selection step  

| If                                         | Do                                                                                                                                                            |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select all components                      | Press Enter                                                                                                                                                   |
| Choose specific USPc components to install | Input the component number you would NOT install to de-select it, (to input multiple components, please use comma to separate the numbers), then press Enter. |

- 6 In the Pre-Installation Summary step, confirm that USP-Compact Graphical Interface Client is included in Software Components. Press Enter to continue.
- 7 Press Enter in the Installation Directory step to accept the default installation directory.  
**Note:** Executing the Component Installation step can take 20-30 seconds to run.
- 8 When the installation finishes, the following message appears:  

```
PRESS <ENTER> TO EXIT THE INSTALLER
```

  
Press Enter to exit and wait several seconds for completion.
- 9 You have installed the new version of the GUI. Go to [Verifying the GUI on page 1798](#).

## Verifying the GUI

### *From you web browser:*

- 1 Enter the IP of the CMT and press Enter.  
The Application Launch Point window appears.
- 2 Click on the Application Launcher link.  
The Carrier Voice over IP Login screen appears.
- 3 Enter your Login Name and Password.  
The Application Launch Point window appears after a valid login.
- 4 Click the Universal Signaling Point Interface Client item in the displayed list.  
The Java Web Start appears and launches the GUI.
- 5 The USP Interface Client window appears, with either the Session-Login or Site Manager dialog box displayed in the window.
- 6 You have upgraded the GUI. Return to [Upgrading the USP-Compact on page 1779](#)

---

## Upgrading the USP-Compact GUI on a CS 2000 Management Tools-based OAMP workstation in GUI mode

---

Perform the following procedures to use GUI mode to upgrade the USP-Compact GUI on a CS 2000 Management Tools-based OAMP workstation.

### Prerequisites

This procedure has the following prerequisites:

- Close any open applications before you begin this procedure.
- Make sure Exceed is configured to support the upgrade. See [Configuring Exceed for an upgrade on page 1634](#).

### Action

Perform the following procedures to upgrade the USP-Compact GUI

1. [Uninstalling the previous version of the GUI on page 1799](#)
2. [Installing the new version of the GUI on page 1800](#)
3. [Verifying the GUI on page 1802](#)

### Uninstalling the previous version of the GUI

#### *At the OAMP workstation*

- 1 Start an Exceed session. The Exceed application is located in the Exceed folder. The program will be running and minimized to the task bar.
- 2 At the window that is running the telnet session to the CMT, set the DISPLAY back to your Laptop/PC. You should see:  

```
>DISPLAY=<IP address of your PC>:0.0
>export DISPLAY
>echo $DISPLAY
```

- 3 Launch the USP-Compact uninstall procedure:  

```
>cd <original install path>/ntssgusp/compact
```

where  
**original install path**  
is /data/usp for offices at USP10 and lower  
is /opt/usp for offices at USP11 and higher  

```
>./Uninstall_Universal_Signaling_Point_Compact
-i gui
```

**Note:** A new window will appear on your PC (from the Exceed session).
- 4 Click Next in the Introduction window.
- 5 Click Complete Uninstall, then click Next to start the uninstallation.
- 6 Click Done to complete the uninstallation.
- 7 Clean up the original install directory to save disk space:  

```
>rm -Rf <original install
path>/ntssgusp/compact
```

where  
**original install path**  
is /data/usp for offices at USP10 and lower  
is /opt/usp for offices at USP11 and higher
- 8 You have uninstalled the GUI. Go to [Installing the new version of the GUI on page 1800](#).

## Installing the new version of the GUI

### *At the OAMP workstation*

- 1 At the Laptop/PC launch the Exceed Xconfig application. The xconfig.exe application is located in the Exceed folder.
- 2 In the xconfig window, double-click Security.
  - a Ensure that in the Host Access Control List, the Disabled (any host access) radio button is selected.
  - b Click [OK].
- 3 In the xconfig window, double-click Communication.
  - a Ensure the Mode is set to Passive.
  - b Click [OK].

- 4 In the xconfig window, double-click Screen Definition.
  - a Ensure that Window Mode is set to Multiple.
  - b Click [OK].
  - c Exit the xconfig window.
- 5 Start an Exceed session. The Exceed application is located in the Exceed folder. The program will be running and minimized to the task bar.
- 6 At the window that is running telnet session to the CMT, set the DISPLAY back to your Laptop/PC. You will see:
 

```
>DISPLAY=<IP address of your PC>:0.0
>export DISPLAY
>echo $DISPLAY
```

**Note:** To find the IP address of the PC you are using, enter: ipconfig from a DOS window. For Contivity users, use the IP address assigned by Contivity.
- 7 Change directories
 

| If new USP-Compact software is located | Do                          |
|----------------------------------------|-----------------------------|
| on a CD                                | <b>&gt;cd /cdrom/cdrom0</b> |
| on the CS 2000 Management Tools server | <b>cd /data/esd_iso</b>     |
- 8 List the directory and locate the install.bin file:
 

```
>ls
```
- 9 Launch the installation program. It can take several minutes to for the application to launch.
 

```
>./install.bin
```

**Note:** A new window appears on your PC (from the Exceed session).
- 10 Click [Next] in the Introduction window.
- 11 Check USP-Compact Graphical Interface Client to install the USP JAVA GUI on the CMT, then click [Next] in the component selection window.
- 12 If a disk space warning displays, click [OK].
- 13 Click [Install] to start the Installation.
- 14 Click [Done] to complete the Installation.

- 15** You have installed the new version of the GUI. Go to [Verifying the GUI on page 1802](#).

### **Verifying the GUI**

#### ***From you web browser:***

- 1** Enter the IP of the CMT and press Enter.  
The Application Launch Point window appears.
- 2** Click on the Application Launcher link.  
The Carrier Voice over IP Login screen appears.
- 3** Enter your Login Name and Password.  
The Application Launch Point window appears after a valid login.
- 4** Click the Universal Signaling Point Interface Client item in the displayed list.  
The Java Web Start appears and launches the GUI.
- 5** The USP Interface Client window appears, with either the Session-Login or Site Manager dialog box displayed in the window.
- 6** You have upgraded the GUI. Return to [Upgrading the USP-Compact on page 1779](#).

---

## Restricting user access to the USP-Compact

---

To view or restrict user access to the USP-Compact during a software upgrade, perform the following procedure.

### Prerequisites

None

### Action

Perform the following procedure to view or restrict user access to the USP-Compact.

#### Viewing and restricting user access to the USP-Compact

##### *At the OAMP workstation*

- 1 To modify user account information, click **Security>user-account**.
- 2 Click the **Search** tab.
- 3 Select **All** from the **Records** drop-down menu.
- 4 Click **Retrieve**.
- 5

#### **ATTENTION**

Do not include your own user account with the records you have selected. Find your own record in the list and while holding down the Ctrl key, click your record. This will de-select your record, while keeping the others selected

Select all records by clicking on the first one and then hold the shift key down and click on the last record.

- 6 Click on **Post**. An X appears to the left of all the records.
- 7 Create a record showing the currently enabled and disabled users so that you can restore them to their proper status after completion. Do this as follows:
  - a Click the **Export posted records** icon (the second button to the left of the context-sensitive Help button). A message box appears, asking: "Do you want to continue?". Answer **Yes**.



- b** The **Export** dialog box appears. Enter a filename and specify a file type for the exported records file. Click **Save**.

The file you have just created is a list of all user accounts. It shows which users were enabled or disabled before beginning the upgrade procedure. Use this list to restore the correct user account status when directed to do so in [Completing the USP-Compact upgrade on page 1784](#).

- 8** Double-click any posted record. The Administration tab then appears.
- 9** Ensure the **enabled** option is not selected.
- 10** Click **Modify**. A confirmation dialog box appears.
- 11** Click **Posted**. The multi-modify field selection dialog box appears
- 12** Select the **enabled** option field. The letter n" will appear to the right.
- 13** Click **OK**. All posted users are now disabled.
- 14** Return to [Upgrading the USP-Compact on page 1779](#)

---

## Upgrading the inactive USP-Compact card

---

Perform the following procedure to upgrade the inactive USP-Compact card.

### Prerequisites

None

### Action

Perform the following procedure to upgrade the inactive USP-Compact card.

#### Upgrading the inactive USP-Compact card

##### *At the OAMP workstation*

- 1 Inhibit all of the links on the inactive USP-Compact card through **Configuration>mtp>link**.

If there is only one available link on a linkset, you will not be able to inhibit it. If it is a one-link linkset, proceed to step [10](#) without inhibiting the link. If there are other links on the linkset, make at least one of them available before attempting to inhibit the link.

**Note:** The last link in a multi-link linkset cannot be inhibited.

- 2 Click **Search**.
- 3 Click **Retrieve all**.
- 4 Post all links on the inactive card.
- 5 Click **Inhibit**, then click **Yes**.
- 6 Deactivate all the links on the inactive USP-Compact card through **Configuration>mtp>link**.
- 7 Click **Auto refresh**.
- 8 Click **Deactivate**.
- 9 Click **Yes**.
- 10 Deactivate all the paths on the inactive USP-Compact card through **Configuration>ips7>application-server-process-path**.
- 11 Click **Search**.
- 12 Click **Retrieve all**.
- 13 Post all paths on the inactive card.
- 14 Click **Down**.

- 15 Click **Yes**.
- 16 Lock the inactive USP-Compact card on the USP-Compact GUI through **Configuration>platform>node**.
- 17 Click **Graphical view**.
- 18 Double-click the inactive USPc card to open it in the administration panel.
- 19 Click **Lock**, then click **Yes**.

#### ***At the SAM21 Element Manager***

- 20 Lock the inactive USP-Compact card. This will disable the card on the USP-Compact GUI.
- 21 Change the load name of the inactive USP-Compact card to the new boot ROM load name (example: uspc\_11\_01\_00\_05b). From the USPc card view on the SAM21 EM. Select the Provisioning tab.
- 22 Select **Modify**.
- 23 In the Load window, enter the new USPc boot ROM load name (example: uspc\_11\_01\_00\_05b). The boot ROM load is the load that does not have a load type suffix (example: “\_base” or “t1e1ha”). The load name can be found in the following directory: /nfsserv/usp/sd0/loads/. Note that the Get loads file button is greyed out; this functionality is not available for this type of card.
- 24 Click **Save**.
- 25 Unlock the inactive USP-Compact card. The USP-Compact card will start booting. Wait until the card is rebooted before proceeding to the next step. In the SAM21 GUI, ensure the message "Application unlocked successfully" is received. In the USP-Compact GUI, under Configuration, platform, node, double-click the inactive USPc card and ensure the operational state shows enabled. Then proceed to the next step.

#### ***At the OAMP workstation***

- 26 Unlock the USP-Compact card through **Configuration>platform>node**.  
**Note:** The system raises logs and alarms when the loads and images on the USP-Compact cards do not match.
- 27 Click **Graphical view**.
- 28 Double-click the inactive USPc card to open it in the administration panel.
- 29 Click on **Unlock**.

- 30** Verify the USP-Compact 11.1 version is running. If not, double-check that the correct image is selected on the SAM 21 Element Manager. If the right image is selected but the incorrect load is running, contact Nortel Networks technical support.
- 31** Activate all of the paths on the inactive USP-Compact card.
- 32** Activate all of the links on the inactive USP-Compact card.
- 33** Uninhibit any links you inhibited at the start of this procedure.
- 34** Monitor the USP-Compact for 15 minutes to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs. During this period, perform test calls to verify newly loaded USP-Compact card performs. Take steps to make sure test calls are routed through links on this USP-Compact card.
- 35** Return to [Upgrading the USP-Compact on page 1779](#).

---

## Upgrading the master USP-Compact card

---

Perform the following procedure to upgrade the master USP-Compact card.

### Prerequisites

Make sure the inactive card is fully enabled before the master USP-Compact card is locked.

### Action

Perform the following procedure to upgrade the master USP-Compact card.

#### Upgrade the master USP-Compact card

**CAUTION****Service interruption**

Upgrade of the Master USP-Compact card cannot be aborted unless a Complete Office Recovery is performed. This abort action causes an interruption in service.

#### *At the OAMP workstation*

- 1 Perform a SWACT so that the master USP-Compact card becomes inactive through **Configuration>platform>node**.
- 2 Click **Graphical view**.
- 3 Double-click the inactive card.
- 4 Click **swact**.
- 5 Inhibit all of the links on the new inactive USP-Compact card.  
If there is only one available link on a linkset, you will not be able to inhibit it. If there are other links on the linkset, make at least one of them available before attempting to inhibit the link. If it is a one-link linkset, proceed to step [10](#) without inhibiting the link.  
**Note:** The last link in a multi-link linkset cannot be inhibited.
- 6 Click **Search**.
- 7 Click **Retrieve All**.
- 8 Post all links on the inactive card.
- 9 Click **Inhibit**, then click **Yes**.
- 10 Deactivate all of the links on the inactive USP-Compact card.

- 11 Click **Auto Refresh**.
- 12 Click **Search**.
- 13 Click **Retrieve All**.
- 14 Post all links on the inactive card.
- 15 Click **Deactivate**.
- 16 Click **Yes**.
- 17 Deactivate all of the paths on the inactive USP-Compact card through  
**Configuration>ips7>application-server-process-path**.
- 18 Click **Search**.
- 19 Click **Retrieve All**.
- 20 Post all paths on the inactive card.
- 21 Click **Down**.
- 22 Click **Yes**.
- 23 Lock the inactive USP-Compact card through  
**Configuration>platform>node**.
- 24 Click **Graphical view**.
- 25 Double-click the inactive USPc card to open it in the administration panel.
- 26 Click **Lock**, then click **Yes**.
- 27 Click **Yes**.

#### ***At the SAM21 Element Manager***

- 28 Lock the inactive USP-Compact card. This will disable the card on the USP-Compact GUI.
- 29 Click Modify to change the load name of the inactive USP-Compact card to the new boot rom load name (example: uspc\_11\_01\_00\_05b). The boot rom load is the load that does not have a load type suffix (example: "\_base" or "\_t1e1ha"). It is located in directory /nfsserv/usp/sd0/loads/.  
Then, click **Save**.
- 30 Unlock the inactive USP-Compact card. The USP-Compact card will start booting. In the SAM21 GUI, ensure the message "Application unlocked successfully" is received. In the USP GUI, under Configuration, platform, node, double-click the inactive USPc card and ensure the operational state shows enabled. Then proceed to the next step.

***At the OAMP workstation***

- 31** Unlock the USP-Compact card through **Configuration>platform>node**.

**Note:** The system clears logs and alarms when the loads and images on the USP-Compact cards match.

- 32** Click **Graphical view**.

- 33** Double-click the inactive USPc card to open it in the administration panel.

- 34** Click **Unlock**.

- 35** Verify the USP-Compact 11.1 version is running. If not, double-check that the correct image is selected on the SAM 21 Element Manager. If the right image is selected but the incorrect load is running, contact Nortel Networks technical support.

- 36** Activate all the paths on the inactive USP-Compact card.

- 37** Activate all the links on the inactive USP-Compact card.

- 38** Uninhibit any links you inhibited at the start of this procedure.

- 39** Monitor the USP-Compact for 15 minutes to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPS. During this period, perform test calls to verify newly loaded USP-Compact card performs. Take steps to make sure test calls are routed through links on this USP-Compact card.

- 40** Wait 10 minutes and then perform a SWACT.

- 41** Return to [Upgrading the USP-Compact on page 1779](#).

## Downgrading the USP Compact cards

This procedure contains the instructions to abort the upgrade, which consist of one of the following procedures:

- If one USPc card was upgraded, complete procedure [Downgrading a single USP Compact card on page 1811](#) to abort the upgrade.
- If both USPc cards were upgraded, complete procedure [Downgrading both USP Compact cards on page 1813](#) to abort the upgrade.

### Downgrading a single USP Compact card

#### ATTENTION

Perform this procedure only if one blade was upgraded. To downgrade both blades at the same time, perform procedure [Downgrading both USP Compact cards](#).

#### *At the OAMP workstation*

- 1 Ensure that the upgraded card is inactive. Perform a SWACT if it is not. This can be checked by doing the following:
  - a Click **Configuration>platform>node**.
  - b Click **Graphical view**.
  - c Double-click the USPc card to open it in the administration panel.
- 2 Ensure that all links and paths on the master card are inservice.
- 3 Inhibit all of the links on the inactive card.

If there is only one available link on a linkset, you will not be able to inhibit it. If there are other links on the linkset, make at least one of them available before attempting to inhibit the link. If it is a one-link linkset, proceed to [step 5](#) without inhibiting the link.

**Note:** The last link in a multi-link linkset cannot be inhibited.
- 4 Deactivate all of the links on the inactive USP Compact card.
- 5 Deactivate all of the paths on the inactive USP Compact card.
- 6 Lock the inactive USP Compact card. To do this:
  - a Click **Configuration>platform>node**.
  - b Click **Graphical view**.



- c Double-click the inactive USPc card to open it in the administration panel.
- d Click **Lock**.
- e Click **Yes**.

### ***At the SAM21 Element Manager***

- 7 Lock the inactive card. This will disable the card on the USP Compact GUI.
- 8 Change the load name of the inactive card to the ROM load name of the old release (example: uspc\_10\_00\_03\_47c). The boot ROM load is the load that does not have a load type suffix (example: “\_base” or “\_t1e1ha”). It is located in the following directory:

/nfsserv/usp/sd0/loads/

- 9 Unlock the inactive card.

### ***At the OAMP workstation***

- 10 Verify that the load running is the old version. If not, double-check that the correct image is selected on the SAM21 Element Manager. If the right image is selected but the incorrect load is running, contact Nortel Networks technical support.

**Note:** The system clears logs and alarms when the loads and images on the USP Compact cards match.

- 11 Stop the upgrade by doing the following:
  - a Click **Administration>software-upgrade**.
  - b Click **Next** until the Stop Upgrade button is displayed.
  - c Click **Stop Upgrade**.

- 12 Unlock the inactive card. To do this:
  - a Click **Configuration>platform>node**
  - b Click **Graphical view**.
  - c Double-click the inactive USPc card to open it in the administration panel.
  - d Click **Unlock**.
  - e Click **Yes**.

- 13 Activate all of the paths on the inactive USP Compact card.
- 14 Activate all of the links on the inactive USP Compact card.
- 15 Uninhibit any links you inhibited.

- 16 Monitor the USP Compact for 15 minutes to ensure it performs normally and does not report any LOG\_SWERRs or LOG\_TRAPs. During this period, perform test calls to verify that the newly loaded USP Compact card performs. Take steps to make sure test calls are routed through links on this USP Compact card.
- 17 Uninstall the new version of the USP Compact GUI.
- 18 Install the old version of the USP Compact GUI.
- 19 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Downgrading both USP Compact cards

#### ATTENTION

Perform this procedure if both USPc cards have been upgraded and it is necessary to abort the upgrade.

#### ATTENTION

Downgrading both USP Compact cards requires a valid USPc10 or USPc11 snapshot.



#### CAUTION

##### Service interruption

A Complete Office Recovery is required to downgrade both USP Compact cards. This action will cause an interruption in service.

### At the OAMP workstation

- 1 Deactivate all links on both USP Compact cards.
- 2 Deactivate all paths on both USP Compact cards.
- 3 Make the snapshot of the old release the active snapshot for both cards. To do this, perform the following steps:
  - a Select **Configuration>platform>node**.
  - b Double-click the left card and select the snapshot from the drop-down list beside the boot-snapshot field.
  - c Click **Modify** to save the changes.
  - d Repeat this procedure for the right card.

- e Log out of the USP Compact GUI.

***At the SAM21 Element Manager***

- 4 Lock both USP Compact cards on the SAM21 element manager.
- 5 Change the load name of both USP Compact cards to the boot ROM load name of the old release (example: uspc\_10\_00\_03\_47c). The boot ROM load is the load that does not have a load type suffix (example: “\_base” or “\_t1e1ha”). It is located in the following directory:  
/nfsserv/usp/sd0/loads/
- 6 Unlock the left (as seen on the USP Compact GUI System Configuration screen) USP Compact card.

***At the OAMP workstation***

- 7 Log in with the USP Compact GUI.
- 8 Verify that the USP Compact is running the correct snapshot and load. To see the snapshot information:
  - a Click **Configuration>platform>node**.
  - b Click **Graphical view**.
  - c Double-click the USPc card to open it in the administration panel.
- 9 Unlock the other USP Compact card and wait for it to complete booting and verify that it is also running the correct snapshot and load.
- 10 Uninstall the new version of the USP Compact GUI.
- 11 Install the old version of the USP Compact GUI.
- 12 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## USP core bounce to direct messaging cutover

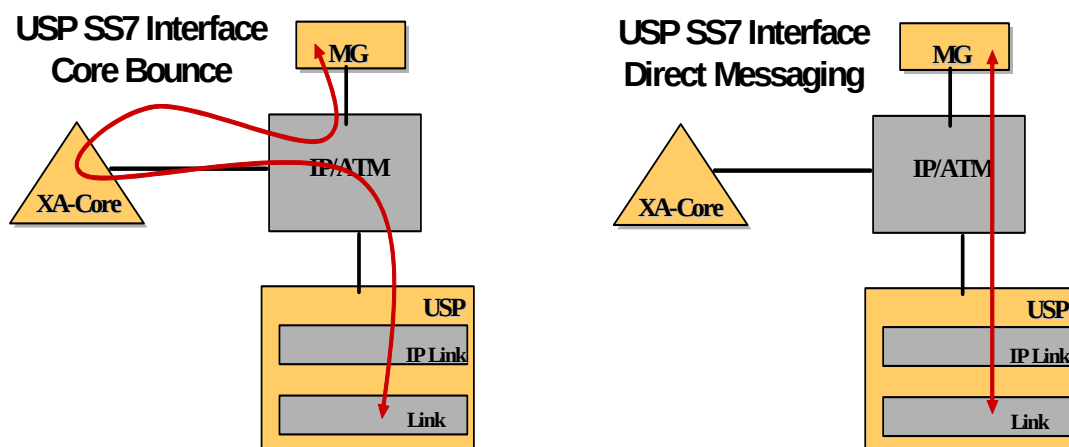
### ATTENTION

This section applies only to IP solutions using the Universal Signalling Point (USP) platform.

Core bounce messaging is messaging between nodes that must first pass or "bounce" through the XA-Core. The USP messaging path to the GWCs is set to core bounce by default. Direct messaging moves directly between nodes. Use this documentation to configure direct messaging between the GWC and USP. For additional information, refer to the engineering guidelines for your solution.

You can perform an abort of the cutover at any time during the cutover procedure until final office cleanup step is completed.

The following figure illustrates the SS7 ISUP message path for Core Bounce compared with Direct Messaging.



This USP core bounce to direct messaging cutover documentation is divided into the following sections:

### GWC IPS7 provisioning

Use [GWC IPS7 provisioning](#) to provision the GWC IPS7 data on the USP. All GWCs setup to handle ISUP traffic must have two IP paths provisioned. GWCs not set up to handle ISUP traffic do not require IP paths.

## GWC cutover from core bounce to direct messaging

Use [GWC cutover from core bounce to direct messaging on page 1819](#) to perform the actual cutover to direct messaging of individual GWCs. All GWCs must be cutover to direct messaging independently, regardless of whether they handle ISUP traffic.

### Prerequisites

Obtain the following from your installation materials before starting this procedure:

- GWC number
- AS Name
- ASP Name (GWC)
- GWC IP address
- USP IPS7 card slot number
- Path ID



#### CAUTION

The core bounce procedures should be used with great care in an office that has working CCS7. Failure to do so can cause degradation to service on existing CCS7 links.

### Standard precautions

Observe all of the following standard precautions prior to and during this procedure.

- Observe all local general safety precautions against personal injury and equipment damage.
- Follow all Electro-Static Discharge prevention practices when handling any hardware. Refer to Method 03-9051, "Event 01 - Planning - DMS Physical Handbook."
- Follow standard troubleshooting procedures, contacting the next level of support for assistance when required.
- At any point during the USP cutover procedure, you may be required to cut back to a previous point in the cutover procedure, or back out of the cutover completely.
- When re-booting the XA-Core with a previously backed-up image, it must be compatible with the image running on the USP.

- Always ensure that the USP and XA-Core datafill are aligned before images are taken on both of these components and only back up to versions taken within context of each other.
- If datafill misalignment is suspected, please contact the next level of support.

### **Preparations**

The following preparations are essential preliminary work to do prior to completing this procedure.

- Nortel Networks strongly recommends that this USP core bounce to direct messaging documentation to be read in its entirety before starting these procedures.
- Prior to starting operations covered by this method, the tools and equipment should be arranged at the work location to minimize fatigue, inconvenience, and maximize productivity.
- The USP must be physically installed and commissioned prior to performing the cutover.
- To ensure proper balance of traffic within your network, Nortel Networks strongly recommends that you enable 8-bit SLS on the CORE.
- Ensure that an office image is taken of the XA-Core and the USP prior to performing this method.
- Determine which Gateway Controllers are setup to handle ISUP traffic. These GWC will require IP paths on the USP. All GWC must be cutover to Direct Messaging but may not require IP paths.

### **Determine the current SLS state**

Also as part of the preparations for this procedure, determine the current SLS state as follows.

***On the XA-Core***

- 1 To enter the SLS8BIT level, enter the following:

**SLS8BIT**

If the SLS8BIT feature is available, the following output displays:

SLS8BIT

If the SLS8BIT feature is unavailable, the following output displays:

TEL00009 must be soc\_on to activate/deactivate  
8 bit SLS.

Contact your Nortel Networks Account Team to purchase the feature.

- 2 To display the current status of 8-bit SLS, enter the following:

**DISPL**

If 8-bit SLS is deactivated, the message "8 bit SLS is  
deactivated" displays.

If 8-bit SLS is active, the message "8-bit SLS is  
activated" displays.

- 3 After successfully entering the SLSBIT level, enter "**ENABLE**"
- 4 To exit the SLS8BIT level, enter the following:  
**QUIT**

## GWC cutover from core bounce to direct messaging

In CS 2000-based solutions, the Universal Signaling Point (USP) messaging path to the CS 2000 GWCs must switch from bouncing through the XA-Core to a direct messaging path.

**Note 1:** It is essential that this procedure is completed to support future upgrades.

**Note 2:** If at any time you need to stop or abort the USP direct messaging cutover procedure, refer to [Aborting the USP direct messaging cutover procedure](#).

### Cutover the USP from core bounce to direct messaging

Use this procedure to perform the core bounce-to-direct-messaging cutover for the USP.



#### CAUTION

You must cutover all GWCs to direct messaging.

Table SERVINV lists all GWCs. Use the **list all** command to display all GWCs.

To cutover each GWC to direct messaging, repeat [step 9](#) through [step 12](#).

#### On the USP GUI

- 1 From the main **USP** menu, click **Network Management**.
- 2 From the **Network Management** window, click **IPS7**.
- 3 From the **IPS7** window, click **ASP Paths**.
- 4 Verify that all IP Paths are up for each GWC and **Close** the **IPS7 Paths** window and **Network Management** window.
- 5 Check the USP and XA-Core for any service affecting conditions.



**On the XA-Core**

- 6** Enter the **USPCUTOVR** level of the **MAP** as follows:

**> USPCUTOVR**

The following warning and cutover output displays:

WARNING: USPCUTOVR already active. Please coordinate activities.

USPCUTOVR: USP cutover utility.

- 7** Start USP cutover to direct messaging as follows:

**STARTCUTAS**

The following output displays:

STARTCUTAS must meet the following criteria before continuing:

- 1) AS Cutover is not already started
- 2) LPP cutover to USP has been completed

STARTCUTAS command will perform the following:

- 1) Update AS Cutover active state

Are you sure you want to continue?

Please confirm ("YES", "Y", "NO", or "N"):

- 8** To confirm the USP cutover to direct messaging enter the following command:

**> Y**

- 9** Perform this step for all GWCs.

- a** Switch the Application Server to perform direct messaging for the first GWC you want to cutover.

**> CUTOVAS GWC <gwc\_number>**

The following output displays:

CUTOVAS must meet the following criteria before continuing:

- 1) Application Server must not be cutover
- 2) STARTCUTAS must have been initiated

CUTOVAS command will perform the following:

- 1) Notifies the specified Application Server (AS) of cutover

2) ISUP MHD data will be re-sent to USP with the IP address of the Application Server to allow for direct messaging.

ATTENTION:

Please ensure all Application Servers are properly provisioned on the Universal Signaling Point (USP) and all IP messaging paths are inservice (UP).

Are you sure you want to continue?

Please confirm ("YES", "Y", "NO", or "N"):

- b** To confirm the switch to direct messaging, enter the following command:

**> Y**

- 10** Display the SS7 message path for the previously cutover GWC, by entering

**> STATAS GWC <gwc\_number>**

The following output displays:

Application Server Messaging Status: Direct

#### ***At the USP GUI***

- 11** Verify that all IP paths to the GWC previously cutover are still up.

#### ***At the GWC***

- 12** Verify that ISUP calls are completing as normal.

**Note:** All GWCs, including those that do not handle ISUP traffic, must be cutover before the **CLEANUPAS** command can be performed.

## Aborting the USP direct messaging cutover procedure

### *At the USP*

- 1 Abort the cutover and switch the SS7 messaging path from direct messaging back to core bounce by entering  
**> ABORTAS GWC <gwc number>**  
The following output displays:  
Starting ISUP MHD data transfer...  
100 tuples transferred.  
200 tuples transferred.  
.  
Application Server cutover completed.
- 2 Repeat [step 1](#) for all GWCs previously cutover.
- 3 Display the SS7 message path for the previously cutover GWC, by entering  
**> STATAS GWC <gwc\_number>**  
The following output displays:  
Application Server Messaging Status: Bounce
- 4 Stop the USP Application Server cutover process by entering  
**> STOPCUTAS**  
The following output displays:  
Are you sure you want to continue?  
Please confirm ("YES", "Y", "NO", or "N"):
- 5 Enter **Y** to complete the **STOPCUTAS** command. The following output displays:  
Stop AS cutover started...  
Stop AS cutover completed successfully

## Setting USP direct messaging as the office default



### CAUTION

Once the cleanup phase has been completed you cannot return to core bounce messaging.

Therefore, you must take an office image of XA-Core and a snapshot of the USP before you do the next procedure ([Setting USP direct messaging as the office default](#)).

### At the USP

- 1 Issue the CLEANUPAS command as follows to set USP direct messaging as the office default:

#### > CLEANUPAS

The following output displays:

CLEANUPAS must meet the following criteria before continuing:

1) All Application Servers are cutover 2) USP direct messaging cutover is NOT already complete

CLEANUP command will perform the following:

1) Set USP Direct Messaging state

Are you sure you want to continue?

Please confirm ("YES", "Y", "NO", or "N"):

- 2 Enter "Y" to confirm the cutover to direct messaging.

> Y

The following output displays:

\*\*\*\*\*

\* WARNING \* WARNING \* WARNING \*

\*\*\*\*\*

Confirmation of this command will permanently set USP direct messaging. There are no procedures to abort this command!

\*\*\*\*\*

Please enter CLEANUPAS to continue, or NO to cancel.

Are you sure you want to continue?

- 3 Confirm USP direct messaging is set as the office default.

**> CLEANUPAS**

The following output displays:

Cleanupas started...

USP Direct messaging is now the office default.

Cleanupas completed successfully.

- 4 Exit the **USPCUTOVR** utility.



Copyright © 2006, Nortel Networks

Nortel Networks Confidential

# Enhanced Network and Message Switch

For details about upgrading the Enhanced Network (ENET) and Message Switch (MS), refer to the *Peripheral Module Release Document*, 297-9051-599 (Intl) or 297-2663-599 (NA) in the DMS Helmsman collection.



## XA-Core upgrade

### ATTENTION

When performing a network upgrade from SN09 to SN09U, the XA-Core does not require an upgrade if it is patch current and at the most recent maintenance release.

The extended architecture core (XA-Core) is the call processing component of the Communication Server 2000 (CS 2000) that controls signaling gateway and media gateway functionality.

Refer to the *XA-Core Maintenance Manual*, 297-8991-510 in the Helmsman DMS collection for any restrictions or limitations.

Stable (answered) 2-port calls are unaffected, but new calls cannot be established during restart SWACT. It is possible to originate calls within one or two minutes after a NoRestartSwact.

In the event you need or want to downgrade the XA-Core, refer to the *XA-Core Maintenance Manual*, 297-8991-510.

### Estimated upgrade times

The following table provides time estimates for an XA-Core SN08 to SN09U ONP.

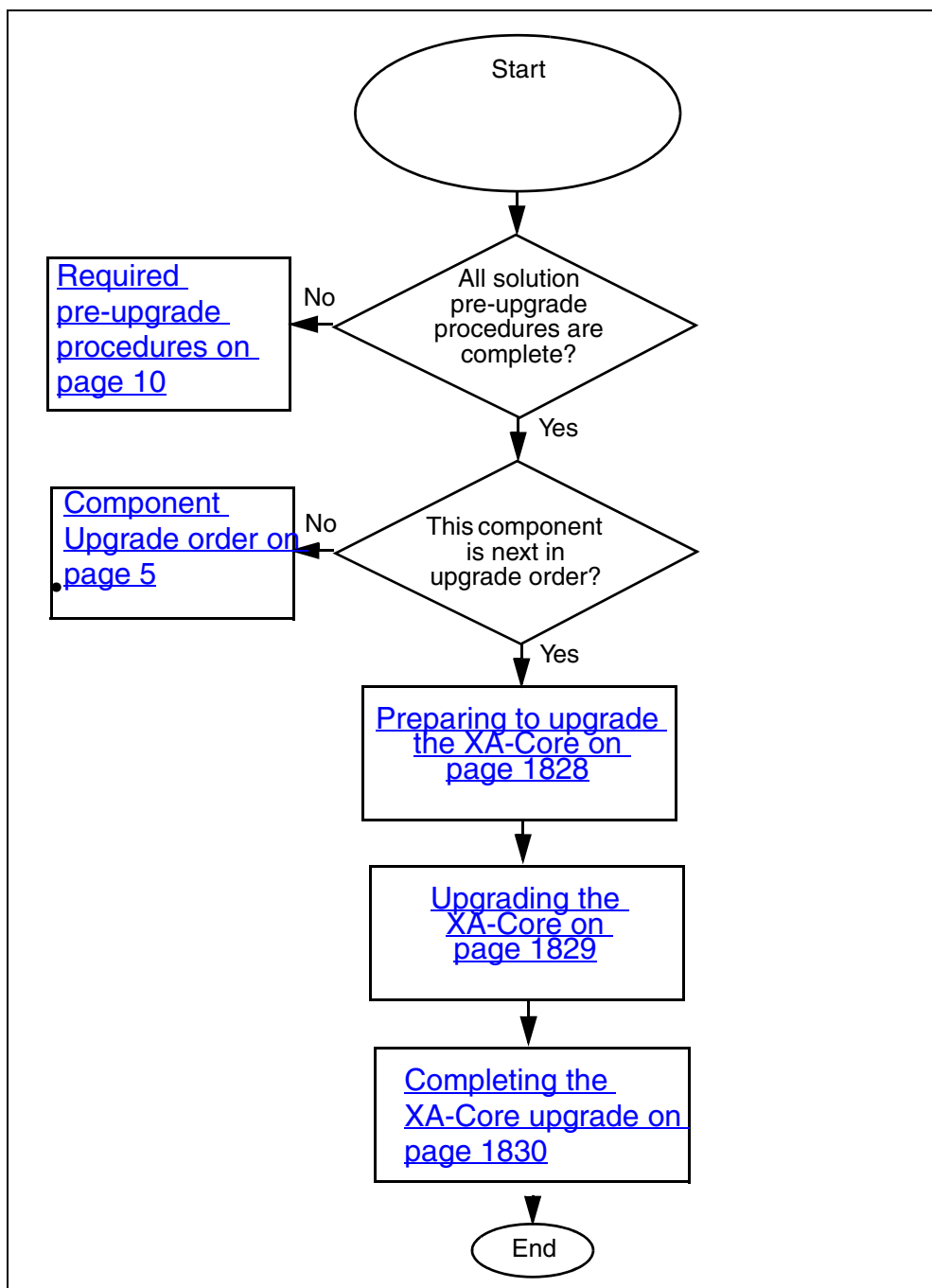
#### Estimated time to complete a software upgrade

| Task                         | Time        |
|------------------------------|-------------|
| Preparing for the upgrade    | 60 minutes  |
| Upgrading the software       | 150 minutes |
| Completing the upgrade       | 60 minutes  |
| Total estimated upgrade time | 270 minutes |

## XA-Core upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

**Figure 1 XA-Core upgrade tasks**





---

## Preparing to upgrade the XA-Core

---

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

### Upgrade paths

This procedure provides the high-level steps to prepare for an upgrade from the SN08 to the SN09 release. SN09U network compatibility is provided through the most recent SN09 maintenance release.

### Action

Refer to *XA-Core Maintenance Manual*, 297-8991-510 in the Helmsman DMS collection.

---

## Upgrading the XA-Core

---

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

### Upgrade paths

This procedure provides the high-level steps to prepare for an upgrade from the SN08 to the SN09 release. SN09U network compatibility is provided through the most recent SN09 maintenance release.

### Prerequisites

Complete [Preparing to upgrade the XA-Core on page 1828](#).

### Action

Refer to *Global Software Delivery One Night Process Software Delivery Procedures*, 297-8991-303 in the Helmsman DMS collection.

---

## Completing the XA-Core upgrade

---

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

Complete [Upgrading the XA-Core on page 1829](#).

### Action

Refer to *XA-Core Maintenance Manual*, 297-8991-510 in the Helmsman DMS collection.



## Compact Call Agent upgrade

### ATTENTION

The Compact Call Agent upgrade consists of two software loads:

- SOS load (SNC00009/CSNWC09)
- NCGL load (CCA00090)

Upgrading from SN08 requires a complete ONP upgrade using the SWUPGRADE platform and application upgrade procedure.

SN09 sites that are SOS patch current and at the most recent NCGL maintenance release (MR) are at SN09U network compatibility and do not require an upgrade.

SN09 sites that are not software current must bring the SOS load to patch currency and perform a platform only MR upgrade to bring the NCGL load to SN09U network compatibility.

Upgrade of the Call Agent is available as an upgrade of platform software, or platform and application software. Patches are available for both software packages. If the CS 2000 - Compact is configured with Message Controller (MC) cards, the software on these cards is upgraded during this procedure.

If a new firmware release is available for the Call Agent or Message Controller cards, the firmware is upgraded during the locking and unlocking of those cards at the CS 2000 SAM21 Manager client. Refer to the *SAM21 Platform Base Release Notes* to determine if firmware software is delivered with the release. To enable the firmware upgrade, the FW Flash Enable checkbox must be checked at provisioning tab of the CS 2000 SAM21 Manager client. For the automated software upgrade (SWUPGRADE), this is during steps [LOAD\\_NEW\\_SIDE\\_BLADE](#) and [LOAD\\_MATE](#), [LOAD\\_MC0\\_BLADE](#), [LOAD\\_MC1\\_BLADE](#), and [LOAD\\_OLD\\_SIDE\\_BLADE](#).

Contact Nortel Global Software Services or your account manager for assistance with a Call Agent upgrade and preparation for the upgrade.

## Estimated upgrade times

The following table provide upgrade time estimates for an ONP upgrade and a Platform Only upgrade:

### Estimated time to complete a software upgrade

| Task                         | Time in minutes |          |
|------------------------------|-----------------|----------|
|                              | ONP             | Platform |
| Preparing for the upgrade    | 60              | 30       |
| Upgrading the software       | 150             | 40       |
| Completing the upgrade       | 60              | 30       |
| Total estimated upgrade time | 270             | 100      |

## Upgrade paths

The supported upgrade paths are:

- SN08 to SN09U network compatibility
- SN09 to SN09U network compatibility

Upgrading from SN08 requires a complete ONP upgrade using the SWUPGRADE platform and application upgrade procedure.

SN09 sites that are SOS patch current and at the most recent NCGL maintenance release (MR) are at SN09U network compatibility and do not require an upgrade.

SN09 sites that are not software current must bring the SOS load to patch currency and perform a platform only MR upgrade to bring the NCGL load to SN09U network compatibility.

## Software upgrade

The following upgrade scenarios are possible:

- upgrade Message Controller software only, where Call Agent platform and call processing software remain the same. This process uses the [Message Controller only upgrade procedure](#).
- upgrade Call Agent platform software, where Message Controller and call processing software remains the same. This is the Call

Agent Maintenance Release upgrade process that uses the [Platform only upgrade procedure](#).

- upgrade Call Agent platform software and Message Controller, where call processing software remains the same. This is the Hybrid Configuration Maintenance Release upgrade process that uses the [Hybrid Configuration upgrade procedure](#).
- upgrade Message Controller, Call Agent platform, and call processing application software. This is the complete upgrade (ONP) from release to release that uses the [SWUPGRADE platform and application upgrade procedure](#).

Different software products are delivered according to the following table.

### Software product and delivery

| Software product                    | Delivery method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Call processing application         | <p>This software is delivered on CDROM or DVDROM.</p> <p>The CDROM or DVDROM is placed in the CDROM tray on the server that provides the CS 2000 Management Tools. Volume management software on that machine mounts the CDROM as <code>/cdrom/cdrom0</code>.</p> <p>From the Call Agent, an FTP session is opened to the CS 2000 Management Tools machine, and the software is pulled from the <code>/cdrom/cdrom0</code> directory with the GET command.</p> <p>The IMPORT command from the DISKUT level of the MAP makes the loads available to the call processing application for booting.</p> |
| Call processing application patches | <p>These patches are delivered through Regional Patch Selector (RPS).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**Software product and delivery**

| Software product                                             | Delivery method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Call Agent platform software and Message Controller software | This software is also delivered on CDROM. Use the platform_load_install.sh tool on the CS 2000 Management Tools machine to extract the ncgl_cca_765_image.x.y.z.zz, ncgl_cca_905_image.x.y.z.zz, and ncgl_mc_image_x.y.z.zz files from CDROM and transfers them to the CS 2000 Core Manager. If the office has a Core and Billing Manager (CBM) instead of a CS 2000 Core Manager, the files are transferred to the CBM instead. For offices without a CS 2000 Core Manager or a CBM, the loads are installed on the CS 2000 Management Tools server. |
| Call Agent platform patches                                  | These patches are delivered through RPS. These files are placed in /swd/3pc/patch on the CS 2000 Core Manager or the CBM.                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Software version**

Software version information for the Call Agent and Message Controller is similar, except that Message Controller software is not patchable.

Prior to SN09, the Call Agent platform load was based on the MCPN765 processor card. With the introduction of new Call Agent processor NTRX51HZ, which is based on the MCPN905-270 card, software loadnames changed for the Call Agent platform for SN09 and newer releases to distinguish between the loads. .

**Call Agent**

Call processing software and patch versions are described in the *Post-Release Software Manager Reference Manual*, 297-8991-540.

Call Agent platform software is managed through the platform\_load\_install.sh tool available on the host that provides the CS 2000 Management Tools.

Call Agent platform software uses the following identification scheme:

- Non-Computing Load (NCL) — ncgl\_cca\_765\_image\_r.w.fc.0, and ncgl\_cca\_905\_image\_r.w.fc.0
  - 765 indicates the platform load based on the MCPN765 processor card.
  - 905 indicates the platform load based on the MCPN905-270 processor card.



- r indicates the release. For example, 7 for SN08, 8 for SN09, and 9 for SN09U.
- w indicates the calendar week number of the load build. For example, 20.
- fc indicates the final compile version. For example, 1 indicates the first compile of week w.

**Example**

ncgl\_cca\_image\_8.20.1.0

- Maintenance NCL (MNCL) — ncgl\_cca\_765\_image\_r.w.fc+i.1, and ncgl\_cca\_905\_image\_r.w.fc+i.1
  - 765 indicates the platform load based on the MCPN765 processor card.
  - 905 indicates the platform load based on the MCPN905-270 processor card.
  - fc+i indicates that this is the ith MNCL for the NCL
  - r, w, and fc values for an MNCL are the same values as for the NCL. This indicates that the MNCL applies to the NCL.

**Note:** Only the latest version of the platform load is supported. If an MNCL exists, only the latest MNCL is supported and is patched. Early MNCL versions and the NCL are not patched to the current release.

- Call Agent platform software patches — ncgl\_cca\_patch\_r.w.c.v
  - r indicates the release. For example, 8 for SN09, and 9 for SN09U.
  - w indicates the calendar week number of the load build. For example, 20.
  - c indicates the compile. This value is equal to the fc value for an NCL or equal to (fc+i) for an MNCL. The patch is only applicable to a load that matches this number.
  - v indicates the patch version. Patch versions begin at 2.

**Load Name Examples**

The following tables provide load name and numbering format examples for NCL and MNCL loads:

**NCL Load name examples**

| Load source                                               | Load name format                                |
|-----------------------------------------------------------|-------------------------------------------------|
| RPM filename on CDROM                                     | ncgl_cca_mc_image-r.w-1.0.noarch.rpm            |
| Load to datafill at CS2K SAM21 Manager Provisioning panel | ncgl_cca_image_r.w.1.0<br>ncgl_mc_image_r.w.1.0 |
| Patch files applied from Call Agent Manager               | ncgl_cca_patch_r.w.1.2<br>ncgl_mc_patch_r.w.1.3 |

**MNCL Load name examples**

| Load source                                               | Load name format                                |
|-----------------------------------------------------------|-------------------------------------------------|
| RPM filename on CDROM                                     | ncgl_cca_mc_image-r.w-2.1.noarch.rpm            |
| Load to datafill at CS2K SAM21 Manager Provisioning panel | ncgl_cca_image_r.w.2.1<br>ncgl_mc_image_r.w.2.1 |
| Patch files applied from Call Agent Manager               | ncgl_cca_patch_r.w.2.2<br>ncgl_mc_patch_r.w.2.3 |

**Message Controller**

Message Controller software is delivered through RPM, and is installed with the CCA load.

Message Controller software uses the following identification scheme:

- Non-Computing Load (NCL) — ncgl\_mc\_image\_r.w.fc.0
  - r indicates the release. For example, 7 for SN08, 8 for SN09, and 9 for SN09U.
  - w indicates the calendar week number of the load build. For example, 20.
  - fc indicates the final compile version. For example, 1 indicates the first compile of week w.

**Example**

ncgl\_mc\_image\_8.20.1.0

- Maintenance NCL (MNCL) - ncgl\_mc\_image\_r.w.fc+i.1
  - fc+i indicates that this is the ith MNCL for the NCL
  - r, w, and fc values for an MNCL are the same values as for the NCL. This indicates that the MNCL applies to the NCL.

**Note:** Message Controller software is not patchable.

## System Capacity

Perform all software upgrade procedures during scheduled maintenance periods, as network capacity is reduced during the software upgrade.

## Patching software

Patching is available during software upgrade and as a maintenance activity for the Call Agent platform and call processing application software. Message Controller software is not patchable. Maintenance releases for the Message Controller are applied by following the Message Controller upgrade procedure in this document.

## Tools and utilities

Preparation activities are performed by operating company personnel. The SWUPGRADE process is typically performed by a Nortel Software Delivery Engineer (SDE). The SDE requires remote connectivity access to the office to perform the SWUPGRADE process and an instance of the CS 2000 SAM21 Manager client. If remote access for the display of the CS 2000 SAM21 Manager client is unavailable, operating company personnel must negotiate an alternative method.

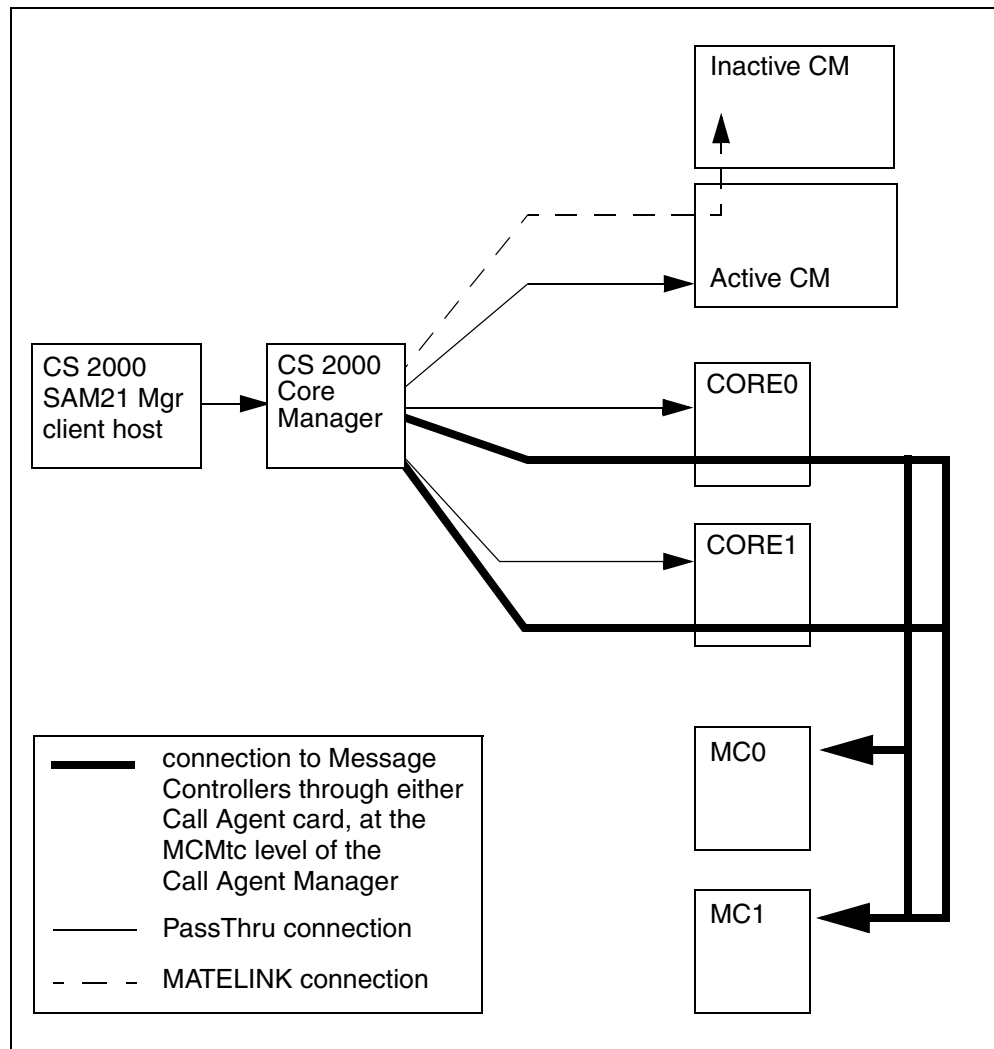
The workstation used for the CS 2000 SAM21 Manager client is the recommended platform from which to perform the software upgrade preparation procedures.

Upgrades require the CS 2000 SAM21 Manager client, the Call Agent Manager, and the MAP. The Call Agent Manager interface is used to maintain the Call Agent cards and the Message Controllers. The MAP is used to control and monitor the SWUPGRADE process and the Switch of Activity (SWACT) for the Call Agent cards.

Patching the application software requires the MAP interface. The Post-Release Software Manager (PRSM) tool is used for patching the call processing application.

For the call processing application upgrade, two MAP connections are required. One connection is to the active call processing application and the other connection is to the inactive call processing application. The connection to the inactive call processing application is made through the active call processing application by using the MATELINK command.

The dashed line in the following figure indicates the relationship between the connections to the active and inactive applications.



**Note:** If the CS 2000 - Compact is equipped with Message Controllers and legacy connectivity equipment exists on the Time Division Multiplex (TDM) network, connectivity may be available from those devices to ACTIVECM. Contact your Nortel account representative for assistance with determining connectivity needs.

## System limitations during upgrade

The following limitations apply:

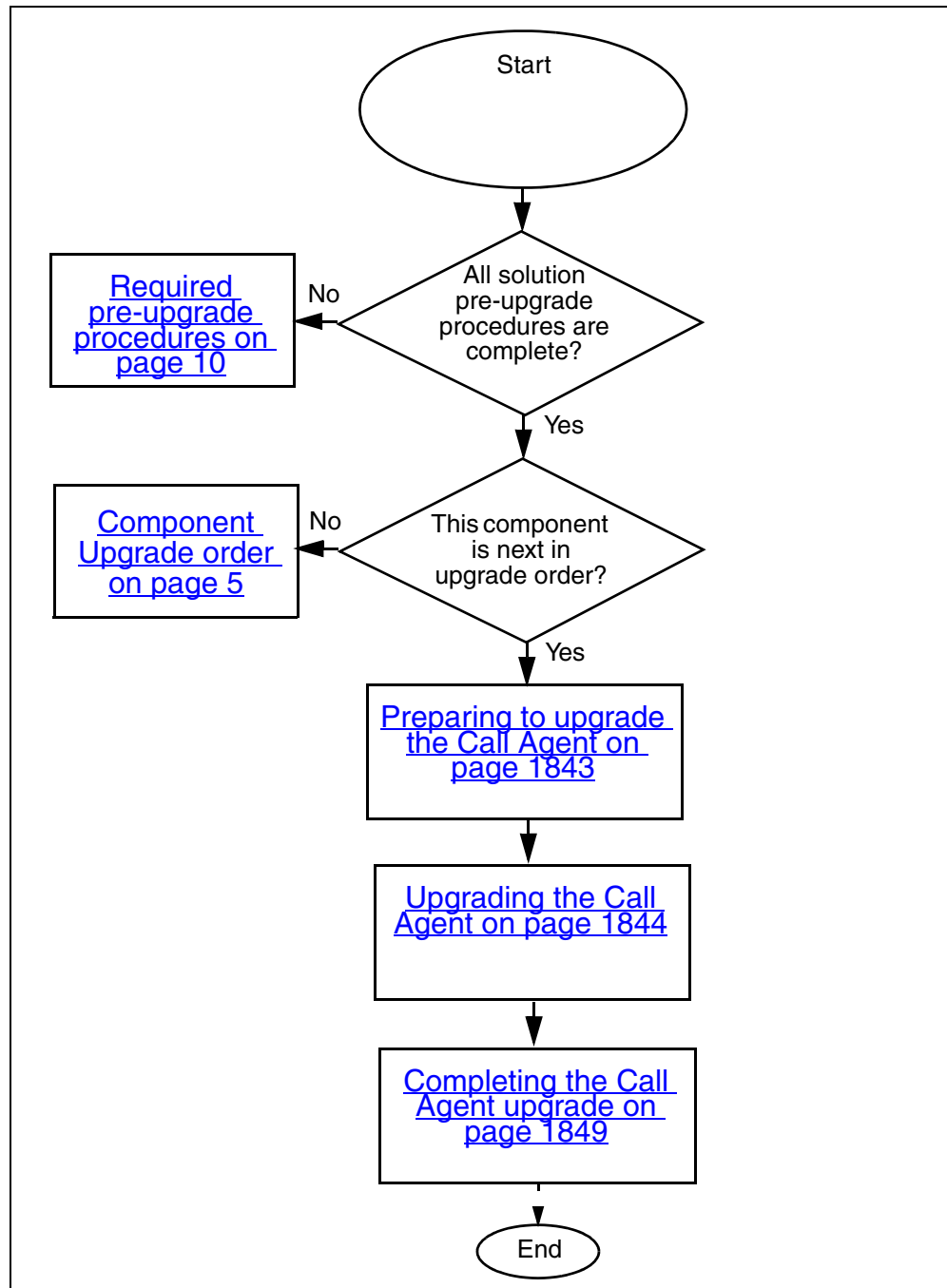
- upgrade Message Controller software only, Call Agent platform and call processing software remain the same.
- upgrade Call Agent platform software, Message Controller and call processing software remains the same. This is the Call Agent Maintenance Release upgrade process that requires use of the Platform only software upgrade procedure.
- upgrade Message Controller, Call Agent platform, and call processing application software. This is the complete upgrade (ONP) from release to release.
- The workstation used for the CS 2000 SAM21 Manager client is the recommended platform from which to perform the software upgrade preparation procedures.
- Upgrades require the CS 2000 SAM21 Manager client, the Call Agent Manager, and the MAP. The Call Agent Manager interface is used to maintain the Call Agent cards and the Message Controllers. The MAP is used to control and monitor the SWUPGRADE process and the Switch of Activity (SWACT) for the Call Agent cards.
- Patching the application software requires the MAP interface. The Post-Release Software Manager (PRSM) tool is used for patching the call processing application.
- For the call processing application upgrade, two MAP connections are required. One connection is to the active call processing application and the other connection is to the inactive call processing application. The connection to the inactive call processing application is made through the active call processing application by using the MATELINK command.

## Service Impacts

Stable (answered) 2-port calls are unaffected, but new calls cannot be established during restart SWACT. It is possible to originate calls within one or two minutes after a NoRestartSwact.

## Call Agent upgrade tasks

The following taskflow provides a high level task sequence to perform this component software upgrade.

**Call Agent upgrade tasks**

---

## Preparing to upgrade the Call Agent

---

The flowcharts found in [Upgrading the Call Agent](#) list the preparation and upgrade procedures to perform an NCL or an MNCL upgrade. Use the process associated with the required upgrade:

- SN08 to SN09U - [Upgrade overview \(SWUPGRADE\)](#)
- MNCL and SN09 or later to SN09U - [Platform only upgrade](#)



---

## Upgrading the Call Agent

---

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

Complete the [Preparing to upgrade the Call Agent](#) required procedures before beginning the upgrade.

### Action

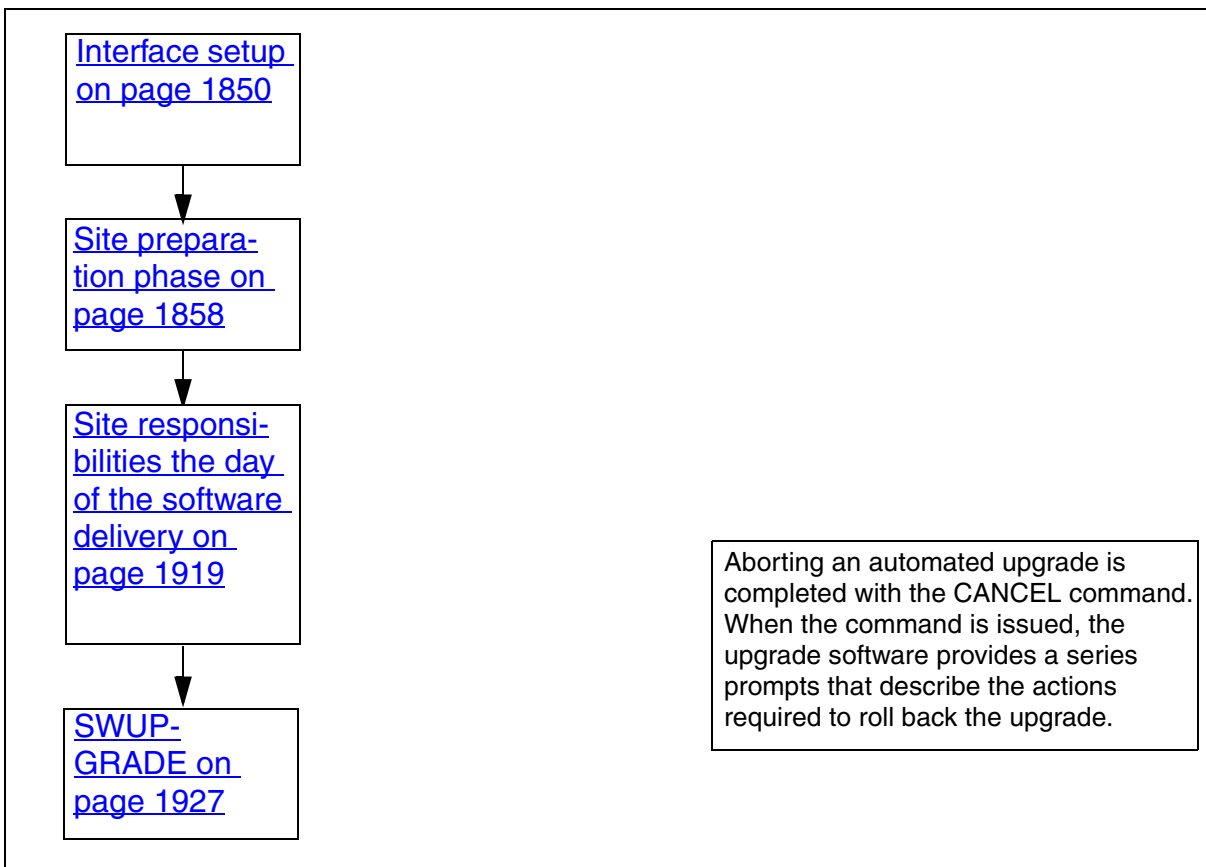
The following flowcharts provide a navigational overview for upgrading to an NCL or an MNCL. Use the process associated with the required upgrade:

- SN08 to SN09U - [SWUPGRADE platform and application upgrade procedure](#)
- MNCL and SN09 or later to SN09U - [Platform only upgrade procedure](#) or [Hybrid Configuration upgrade procedure](#) or [Message Controller only upgrade procedure](#)

## SWUPGRADE platform and application upgrade procedure

The following flowchart provides an overview of the platform and application software upgrade using the automated SWUPGRADE tool.

### Upgrade overview (SWUPGRADE)



### Aborting a SWUPGRADE

The CANCEL command aborts an automated upgrade. The SWUPGRADE process recognizes the command and provides instruction in the form of prompts to roll back the upgrade procedures that were completed. If a rollback is required, choose the appropriate rollback procedure:

- [Revert and Abort on page 1989](#)
- [Revert and Abort for offices with Message Controller cards on page 1998](#)

### Platform only upgrade procedure

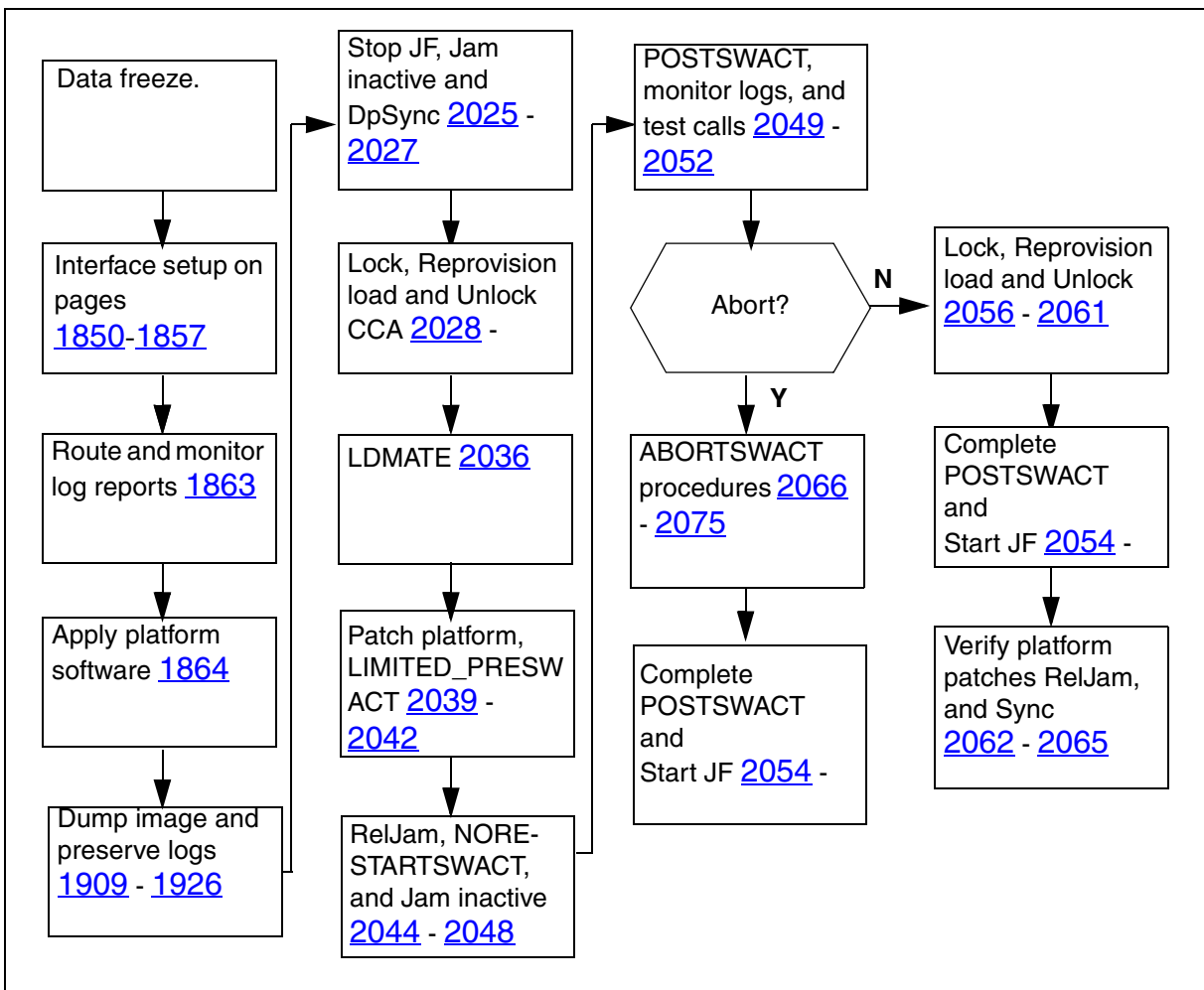
A platform only upgrade shares many of the same steps as an ONP. The Platform only flowchart indicates which procedures apply to a platform upgrade only.

## Requirements

A successful platform only software upgrade requires the following:

- the operating company must set aside a maintenance window during low traffic to perform the platform only upgrade
- an image is taken at the beginning of the maintenance window
- no provisioning is allowed during the maintenance window

## Platform only upgrade



## Aborting a Platform Only upgrade

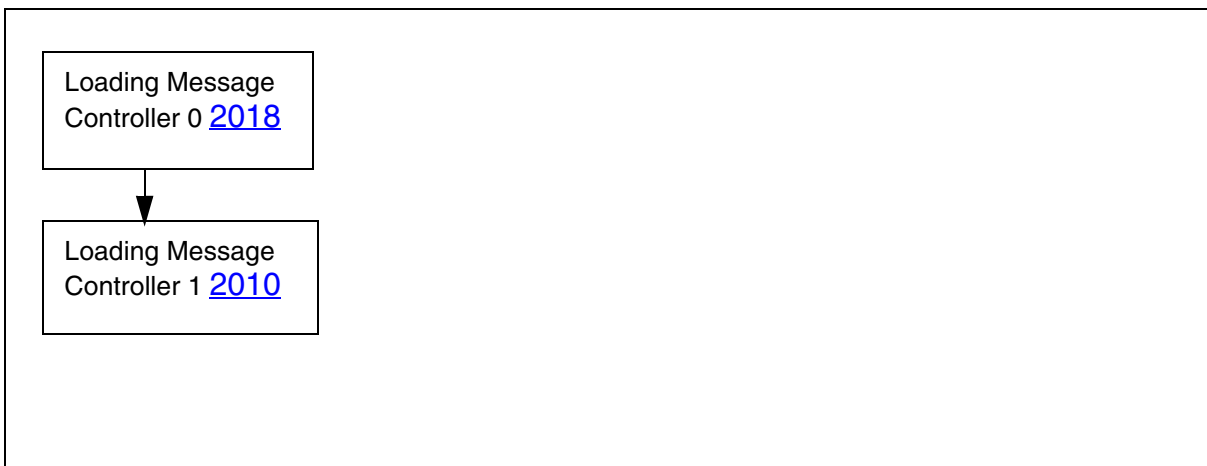
Perform the procedure [ABORTSWACT on page 2066](#) if a Platform Only upgrade fails and only if the inactive Call Agent was not locked during the Start POSTSWACT procedure.

If a Platform Only upgrade fails and the inactive Call Agent was unlocked, contact Nortel support for assistance.

## Message Controller only upgrade procedure

A Message Controller only upgrade consists of upgrading both Message Controller blades (0 and 1). The following flowchart indicates which procedures apply to this upgrade.

### Message Controller only upgrade



## Hybrid Configuration upgrade procedure

Perform a hybrid configuration upgrade by performing the following two upgrades:

- [Message Controller only upgrade procedure](#)
- [Platform only upgrade procedure](#)

The same requirements and restrictions to abort the Platform Only upgrade also apply to the Hybrid Configuration upgrade.

### Requirements

A successful Hybrid Configuration software upgrade requires the following:

- the operating company must set aside a maintenance window during low traffic to perform the upgrade
- an image is taken at the beginning of the maintenance window
- no provisioning is allowed during the maintenance window

### Aborting a Hybrid upgrade

Perform the procedure [ABORTSWACT on page 2066](#) if a Hybrid upgrade fails and only if the inactive Call Agent was not locked during the Start POSTSWACT procedure.

If a Hybrid upgrade fails and the inactive Call Agent was unlocked, contact Nortel support for assistance.

## **Patching Software**

For information on patching software, refer to [Patching Platform and Call Processing software on page 2076](#).

---

## Completing the Call Agent upgrade

---

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

Complete the [Upgrading the Call Agent](#) required procedures before beginning the post upgrade process.

### Action

Perform the following procedures to complete the component upgrade.

- [START\\_POSTSWACT](#)
- [LOAD\\_OLD\\_SIDE\\_BLADE](#)
- [FINISH\\_POSTSWACT](#)
- [DUMP\\_OFFICE\\_IMAGE](#)

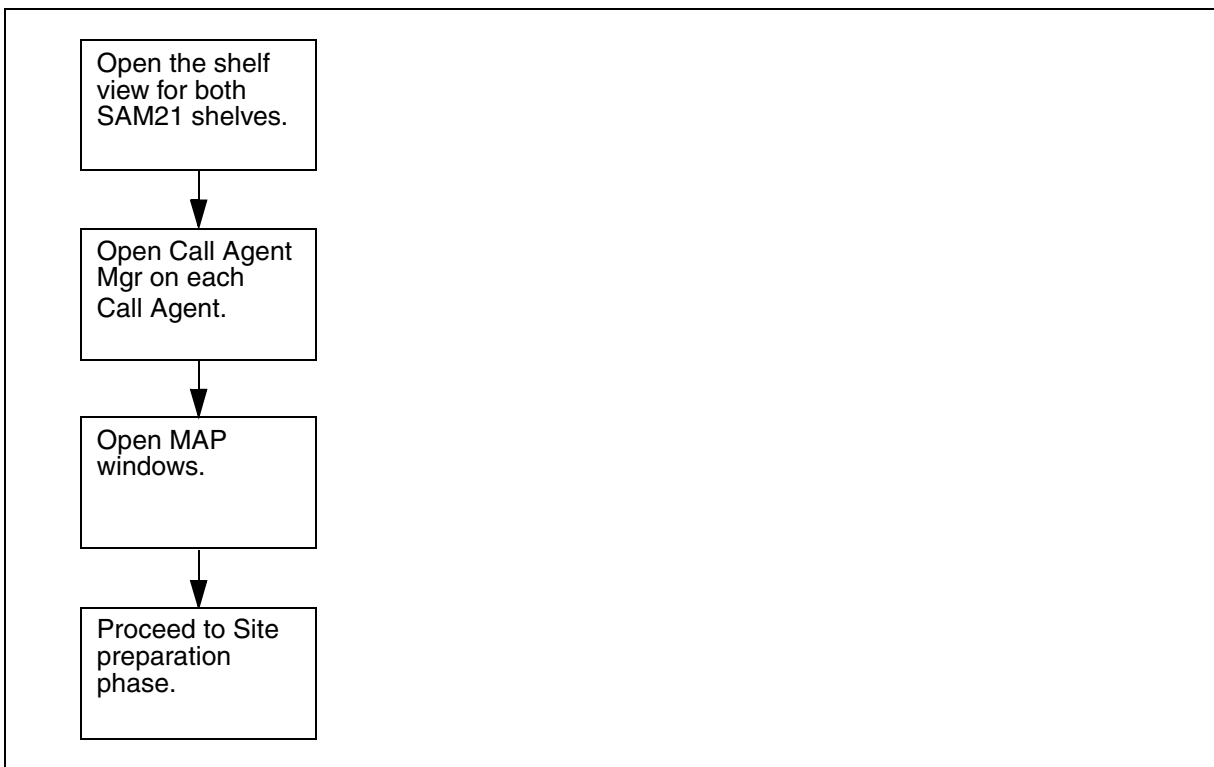
## Interface setup

Procedures in this section use the PassThru feature on the CS 2000 Core Manager or CBM. Refer to “Adding or removing PassThru users” in *CS 2000 Core Manager Security and Administration*, NN10170-611 or *Core Business Manager*, NN10358-611 for more information about the PassThru feature. For offices without a CS 2000 Core Manager or CBM, PassThru is not used, and direct connections to the call processing side of the CS LAN are needed.

If the PassThru usernames are not core0usr, core1usr, and cmusr, then substitute the office’s PassThru usernames for core0usr, core1usr, and cmusr in these procedures.

The procedures provide recommended methods for opening the interfaces required to complete an upgrade, as shown in the following figure.

### Interface setup



Each procedure indicates the interface used to perform the procedure or step. The following table describes the interfaces.

**Interfaces used to perform procedures and steps**

| Interface type                             | Description                                                                                                                                                                                                                                                    |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ACTIVECM                                   | a MAP window connected to the active side session of the call processing application                                                                                                                                                                           |
| INACTIVECM                                 | a MAP window connected to the inactive side session of the call processing application. Actions performed at this interface are also indicated by the command prompt <code>Mate&gt;</code>                                                                     |
| CORE0                                      | a Call Agent Manager window connected to the Call Agent card identified as core0 and provides a maintenance interface. The maintenance interface is started from the <code>ccamtc</code> command.                                                              |
| CORE1                                      | a Call Agent Manager window connected to the Call Agent card identified as core1 and provides a maintenance interface. The maintenance interface is started from the <code>ccamtc</code> command.                                                              |
| Active maintenance window (CORE0 or CORE1) | the active maintenance window (CORE0 or CORE1) that is connected to the active Call Agent. The example in figure <a href="#">Call Agent Manager with Message Controllers in the office: Example on page 1852</a> shows CORE1 as the active maintenance window. |
| SDM                                        | a window connected to the CS 2000 Core Manager. The <code>sdmmtc</code> program and UNIX system activities are completed from this window. SDM is relevant only where it is present.                                                                           |
| CBM                                        | TBD                                                                                                                                                                                                                                                            |
| CMT                                        | TBD                                                                                                                                                                                                                                                            |



**Call Agent Manager with Message Controllers in the office: Example**

|           |       |       |        |        |                    |
|-----------|-------|-------|--------|--------|--------------------|
| CallAgent | SYS   | CON   | APPL   | MC     | Unit: 1            |
| .         | .     | .     | .      | .      |                    |
| CoreMtc   |       | Jam:  | Link0: | Link1: | BLnk: FC: Appl:    |
| 0 Quit    | Unit0 | Inact | no     | . Act  | . Inact . insync . |
| 2 CAMtc   | Unit1 | Act   | no     | . Act  | . Inact . insync . |

The following procedure indicates how to create a shell script that changes the title of an xterm window. This procedure only works on UNIX workstations.

***At an xterm window on the CS 2000 SAM21 Mgr client workstation***

- 1 Use an editor to create the following file. Available editors are vi and dtpad. Save the file with a name of xtermtitle.

```
#!/bin/sh
this script changes the title of an xterm
echo "\033]2;$1\007"
echo "\033]1;$1\007"
```

- 2 Make the file executable.

```
UNIX> chmod +x xtermtitle
```

- 3 To use the script, enter the command and the new name for the window.

```
UNIX> ./xtermtitle <window_title>
```

**window\_title**

is a string like core0, core1, sam21gui, activecm, or inactivecm

- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

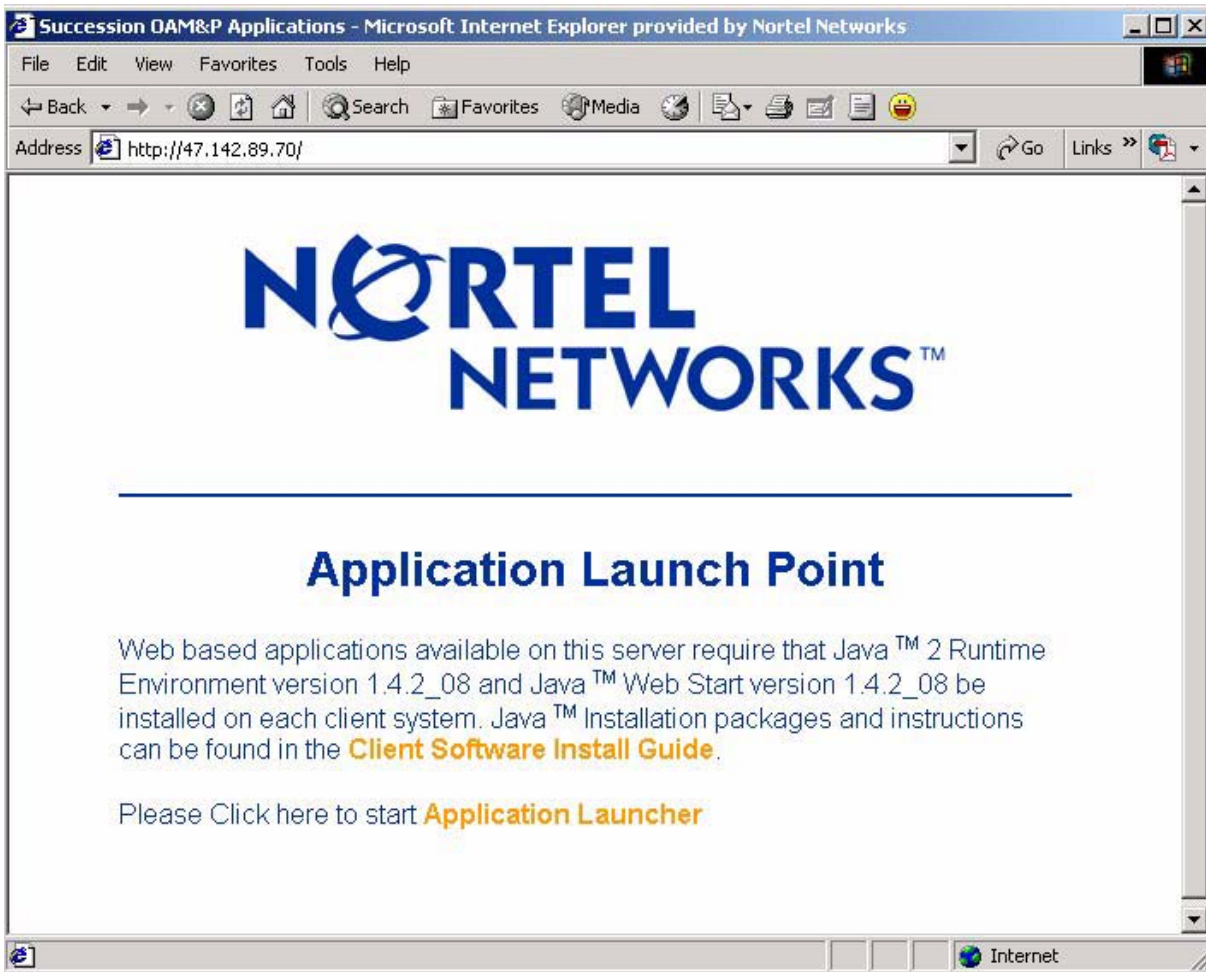
For Microsoft Windows 2000 based workstations, change the title of a command prompt window with the title <window\_name> command.

## Opening SAM21 shelf views

### *At your workstation*

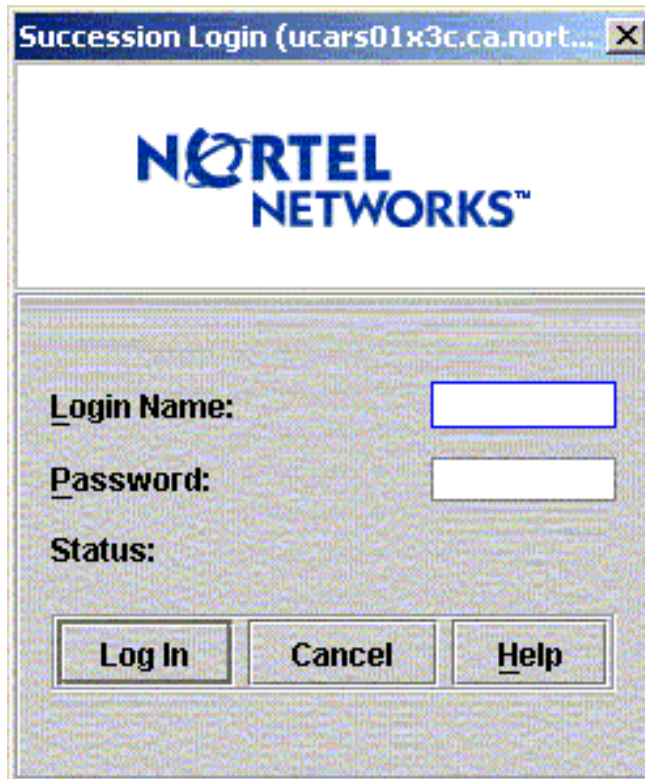
- 1 Open a web browser and enter the IP address or hostname of the server that is hosting the CS 2000 Management Tools.

The Application Launch Point page appears.



**2 Click Application Launcher.**

A login window appears.



The image shows a Windows-style login window titled "Succession Login (ucars01x3c.ca.nort...". The window has a blue header bar with the title and a close button. Below the header is a white area containing the "NORTEL NETWORKS™" logo. The main body of the window has a light gray background and contains the following fields and buttons:

- Login Name:** A text label followed by a white rectangular input field.
- Password:** A text label followed by a white rectangular input field.
- Status:** A text label with no input field.
- Buttons:** Three buttons are located at the bottom: "Log In", "Cancel", and "Help".

- 3 Provide the login name and password and then click **Log In**.

The login account must have mgcrw or mgcadm level permissions.

The Application Launch Point, similar to following, appears.



- 4 Click the link for the Succession SAM21 Element Manager  
The application starts and the Subnet View window opens.
- 5 Identify and open the Shelf View window for shelves that contain call agent cards by double-clicking on the shelf icons from the Subnet View window. (Additional shelves may not contain call agent cards.)
- 6 Position the screens so that alarms and access to locking and unlocking cards are available.
- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Opening Call Agent Manager windows

---

The procedure requires that the PassThru feature and usernames are configured on the CS 2000 Core Manager or CBM. For this procedure and the remainder of the upgrade, the documented usernames are core0usr, core1usr, and cmusr. If the office has different PassThru usernames provisioned, substitute the different usernames. Offices that do not have a CS 2000 Core Manager or CBM require two connections, one to each Call Agent card, but will telnet directly to each Call Agent card.

### ***At your workstation***

- 1 Open two terminal windows and change the title for one window to CORE0 and the other window to CORE1.

### ***SDE — At the CORE0 window***

- 2 Telnet to the CS 2000 Core Manager or CBM and log in as user core0usr.

*The CS 2000 Core Manager or CBM forwards the telnet session to the core0 Call Agent card.*

- 3 Log in to the core0 Call Agent card.

### ***SDE — At the CORE1 window***

- 4 Telnet to the CS 2000 Core Manager or CBM and log in as user core1usr.

*The CS 2000 Core Manager or CBM forwards the telnet session to the core1 Call Agent card.*

- 5 Log in to the core1 Call Agent card.

### ***SDE — At the CORE0 and CORE1 windows***

- 6 Start the maintenance interface.

```
[mtc@core0_ip_address mtc]$ ccamtc
[mtc@core1_ip_address mtc]$ ccamtc
```

- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Opening MAP windows

---

If the office does not have a CS 2000 Core Manager or CBM, create two telnet connections to the IP address of the call processing application instead of following this procedure. The IP address of the call processing application is the activeirm address reported by the QueryIP command at the Call Agent Manager interface.

### ***At your workstation***

- 1 Open two terminal windows and change the title of one to ACTIVECM and the other to INACTIVECM.

### ***SDE — At the ACTIVECM window***

- 2 Telnet to the CS 20000 Core Manager or CBM and log in as user cmusr.

*The CS 2000 Core Manager or CBM forwards the telnet session to the call processing application.*

- 3 Log in to the call processing application.

### ***SDE — At the INACTIVECM window***

- 4 Repeat steps [2](#) and [3](#).
- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

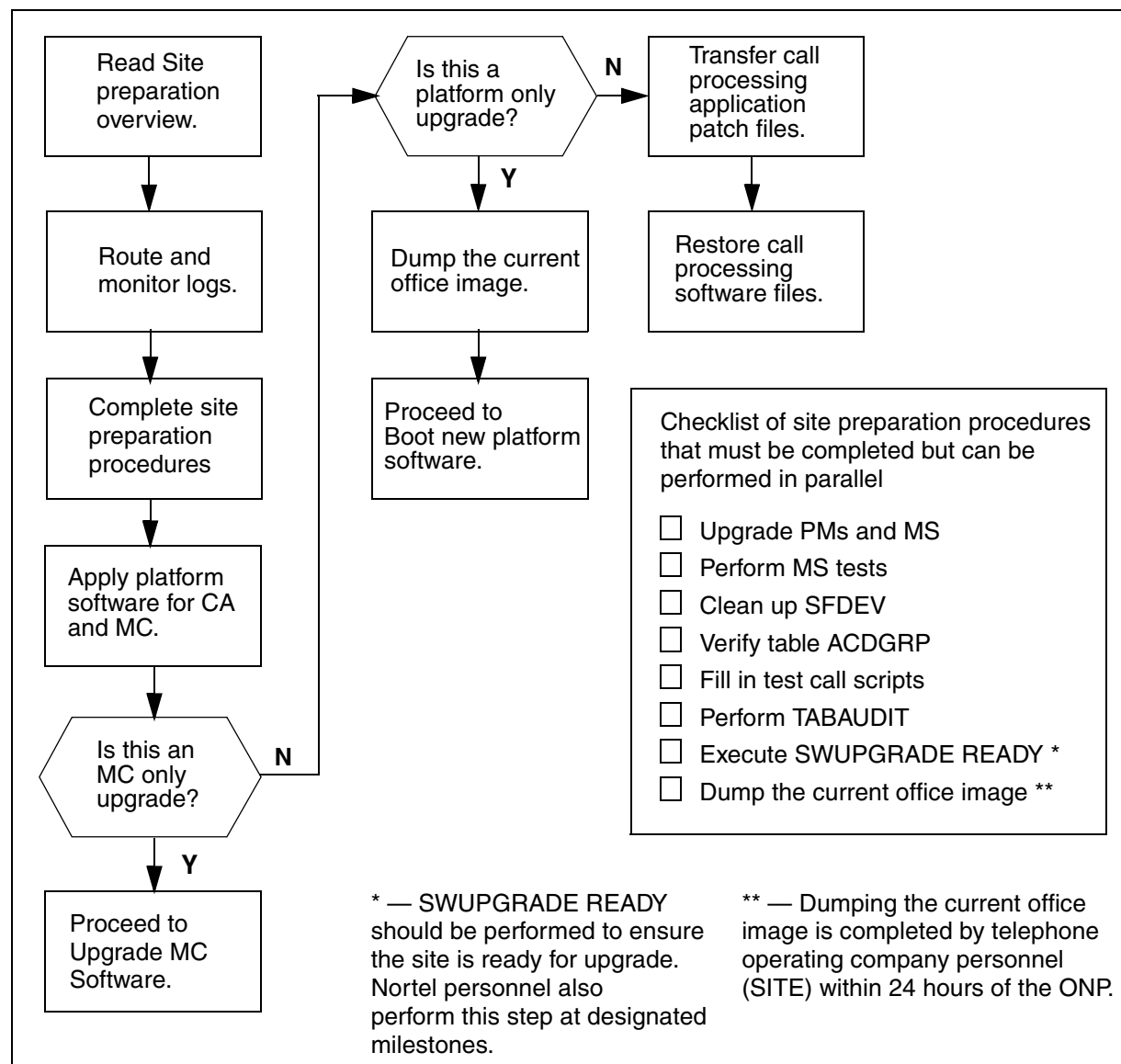
**Note:** The INACTIVECM window does not connect to the inactive call processing application at this time. Later steps indicate when and how to connect to the inactive call processing application, when necessary.

## Site preparation phase

Perform the following procedures when the upgrade software media is delivered, approximately 35 days before the ONP, to verify office stability and prepare the office for an upgrade.

Review [Site preparation overview](#) before performing the procedures in this section. Be sure to understand site preparation responsibilities before the ONP and that a current office image must be taken within 24 hours of the ONP.

### Site preparation phase





The following table indicates the timing of events that need to be completed by telephone operating company personnel for an ONP. This timeline does not apply to platform only MR upgrades or Message Controller only upgrades.

#### Process timeline

| Days before the upgrade | Site preparation activity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 45 days                 | Site delivery checklist and acceptance of schedule arrives at site                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 35 days                 | <ul style="list-style-type: none"> <li>First software media and documentation shipment arrives at site.</li> <li>Site begins checking logs daily. Refer to <a href="#">Monitoring logs on page 1863</a>. Check logs for CCA, SAM21 EM and Ethernet Routing Switch 8600 to be sure links are stable.</li> </ul> <p><b>Note:</b> Continue monitoring logs until the day of SWACT.</p> <ul style="list-style-type: none"> <li>Begin upgrading and verifying PMs and other network components with the latest software loads. Refer to <a href="#">Peripheral Module upgrade on page 999</a>.</li> </ul> |
| 30 days                 | Begin data consistency checks, refer to <a href="#">Performing TABAUDIT on page 1897</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 15 days                 | Ensure that scheduled RExtsts complete successfully                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 7-4 days                | <ul style="list-style-type: none"> <li>Ensure SFDEV is clear. Refer to <a href="#">Cleaning up SFDEV on page 1890</a></li> <li>Continue to monitor logs for CCA, SAM21 EM and Ethernet Routing Switch 8600 until the day of SWACT. Continue to check the logs to be sure links are stable.</li> <li>If office is equipped with PMs, ensure that the latest PM loads and XPM patch files are restored to the proper disk volumes.</li> <li>Site receives final shipment of software media and documentation</li> </ul>                                                                                |



**Process timeline**

| <b>Days before the upgrade</b> | <b>Site preparation activity</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6 days                         | <ul style="list-style-type: none"> <li>• Verify all network nodes are loaded, patched, and working.</li> <li>• Verify dial in connectivity. Refer to <a href="#">Providing remote site access on page 1924</a>.</li> <li>• Ensure all software media are on site.</li> <li>• Verify that site personnel are familiar with the upgrade process.</li> </ul>                                                                                                                                                                                                             |
| 5 days                         | <p>The final site readiness check is performed by Nortel personnel. Nortel Software Delivery Engineer dials in and runs <a href="#">Executing SWUPGRADE READY on page 1902</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                   |
| 3-2 days                       | <ul style="list-style-type: none"> <li>• Verify site personnel has prepared test calls plan.</li> <li>• Obtain name of site personnel representative with the authority to decide in case of an abort with the CANCEL command.</li> <li>• Verify patches for the new software load are downloaded to the site.</li> <li>• Ensure all site preparation checklist items are complete.</li> <li>• Continue monitoring logs for CCA, SAM21 EM and Ethernet Routing Switch 8600 until the day of SWACT. Continue to check the logs to be sure links are stable.</li> </ul> |
| Day of upgrade                 | <p>Refer to <a href="#">Site responsibilities the day of the software delivery on page 1919</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Night of upgrade               | <p>Refer to <a href="#">SWUPGRADE on page 1927</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

---

## Site preparation overview

---

### Planning activities

**CAUTION****Possible service interruption**

Application of the following patch types within 30 days of the ONP must be considered a gating issue to the ONP:

Active (ACT) patch applied and activated

Limited (LTD) status patch

Verification (VO) status patch

If any of the above patches are applied to the office within 30 days of the ONP, immediately contact your Nortel regional customer representative or call the Global Software Delivery Hotline for your market.

A successful software delivery application requires certain activities to be performed before the ONP. Some of these activities depend on factors such as office type and the PCL software being delivered. This section provides a brief overview of the site preparation activities that must take place before the ONP. Other required activities not listed in this section must be approved by and coordinated through the appropriate Nortel customer representatives.

Administrative, warnings, and software delivery data services must be reviewed by office personnel as soon as this document is received.

### Pre-application activities

Pre-application activities include upgrading all peripherals (including remotes) to PM loads compatible with the new PCL software load. In addition, Network (ENET) and Message Switch (MS) software upgrades must be completed before the ONP.

Pre-application activities can include (but are not restricted to) the following:

- first shipment of ONP CD-ROMs and documentation to the site
- site polling by Nortel to obtain specific switch information
- site preparation procedures
- TABAUDIT procedure

- final shipment of ONP CD-ROMs and documentation to site
- pre-loading the message switch
- site-ready checks
- site responsibilities the day of the software delivery application

Some of these activities will be completed by Nortel personnel and some will be completed by the operating company. Site personnel responsible for completing pre-application activities must become familiar with all sections of this document.

## Monitoring logs

**CAUTION****Possible loss of service**

Check the logs for CCA, SAM21 EM and Ethernet Routing Switch 8600 to make sure links are stable. Continue to monitor the logs until the day of SWACT.

Perform this activity according to site operating procedures.

***SITE — At the ACTIVECM window***

1 Enter the BCS update level.

> **BCSUPDATE**

2 Check the logs.

> **LOGCHECK**

3

**ATTENTION**

Do not proceed until all log activity is explained.

This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Module Heading **Applying platform software for Call Agent and Message Controller** Heading

ParaBasic Complete this procedure at least two days before the ONP. ParaBasic

ParaPlus ParaBasic This procedure installs the following software onto the CS 2000 Core Manager of the Core and Billing Manager (CBM): ParaBasic

- List Item ParaBasic Call Agent platform software: ParaBasic
  - List Item ParaBasic ComputerOutputString ncgl\_cca\_765\_image\_<r>.x.y.z ComputerOutputString ParaBasic Item
  - Item ParaBasic ComputerOutputString ncgl\_cca\_905\_image\_<r>.x.y.z ComputerOutputString ParaBasic Item List Item
- Item ParaBasic Message Controller software:
  - ComputerOutputString ncgl\_mc\_image\_<r>.x.y.z
  - ComputerOutputString ParaBasic Item List

**Note:** Note ParaBasic The variable <r> indicates the release. ParaBasic Note ParaPlus

ParaBasic Message Controller software is installed even if the office is not configured with Message Controller cards. If the office is not configured with a CS 2000 Core Manager or a CBM, this procedure installs the software on

ComputerOutputString /data/swd/3pc ComputerOutputString of the CS 2000 Management Tools server. ParaBasic

ParaBasic For offices without a CS 2000 Core Manager or a CBM, manual action is required. Refer to CrossRef [Offices without a CS 2000 Core Manager or CBM on page 1875](#) CrossRef. ParaBasic

**Section** **Heading** **Action** **Heading**

**ParaPlus** **ParaBasic** Perform one of the following procedures (CD or ESD) depending on how you recieved your platform software. **ParaBasic**

- **List** **Item** **ParaBasic** **CrossRef** [Installing software platform using CD ROM](#) **CrossRef** **ParaBasic** **Item** **List**
- **List** **Item** **ParaBasic** **CrossRef** [Electronic Software Delivery \(ESD\) for Call Agent on page 1878](#) **CrossRef** **ParaBasic** **Item** **List** **ParaPlus**

**Procedure** **ProcedureCaption** **Installing software platform using CD ROM** **ProcedureCaption** **Procedure** **Section**

**Procedure** **Context** **Location** **SITE — At the CS 2000 Management Tools server** **Location**

- 1 **Step** **ParaBasic** Insert the CD-ROM in the CD-ROM tray. **ParaBasic** **Step** **Context**

**Context** **Location** **SITE — At a CS 2000 Management Tools terminal** **Location**

- 2 **Step** **ParaBasic** Log in and then use the su command to gain root privilege. **ParaBasic**

**Figure** **Graphic** **Figure** **Step**

```
Trying <hostname>...
Connected to <hostname>.
Escape character is '^]'.
```

```
Authorized use only, activities logged.
login: username
Password: <password>
Last login: Fri Jan 30 12:48:10 from <otherhost>
prompt:>
prompt:> su - root
Password: <root_password>
#
```

- 3 **Step** **ParaBasic** Execute the platform\_load\_install.sh script. **ParaBasic**

**Figure** **Graphic** **Figure**

```
/opt/nortel/sspfs/Scripts/platform_load_install.sh
```

**ParaBasic** The screen clears and a menu is displayed. **ParaBasic**

**Figure** **Graphic** **Figure** **Step**

```
Welcome to the Platform Installation Tool Version 3.2
=====
RPM INSTALLATION/REMOVAL
=====
1) Install RPM from CDROM 2) Install RPM from Disk
3) Uninstall RPM 4) Query all RPMs

OTHER
=====
C) Change Rotation Parameters P) View Rotation Parameters
V) SAM21 Platform Version Installed X) Exit

Please choose one of the following: 1
```

**4** **Step** **ParaBasic** Enter **CommandString** 1 **CommandString** and press the Return key to install the software. **ParaBasic**

**ParaBasic** The screen clears and the contents of the .rpm package are displayed. **ParaBasic**

**Figure** **Graphic** **Figure**

```
Verifying CDROM is mounted
/cdrom/cdrom on /vol/dev/dsk/c0t0d0/cdrom read only/nosuid/mapl-
case/noglobal/rr/traildot/dev=16c0001 on Sat Mar 27 16:34:13 2005
CDROM is mounted.
Listing file names in the rpm on the cd.

/swd/3pc/ncgl_cca_765_image_<r>.x.y.z
/swd/3pc/ncgl_cca_905_image_<r>.x.y.z
/swd/3pc/ncgl_mc_<r>.x.y.z

Do you want to continue (y/n)? y
```

**Note:** **Note** **ParaBasic** If the message **ComputerOutputString** There is no cd in the CDROM drive, please check drive **ComputerOutputString** is displayed, ensure that the CD-ROM is inserted in the tray for this unit. **ParaBasic** **Note** **Step**

- 5 **Step** **ParaBasic** Enter **CommandString** Y **CommandString** to proceed with the software installation. **ParaBasic**

**ParaBasic** The software is extracted from the .rpm package. The .rpm package is transferred to the CS 2000 Core Manager or CBM. **ParaBasic**

**Figure** **Graphic** **Figure** **Step**

Extracting files from the rpm archive on the cd.

```
Installing RPM package ncgl_cca_mc_image-9.x-1.z.noarch.rpm
Sun Microsystems Inc. SunOS 5.8 Generic Patch December 2005
ncgl_cca_mc_image-<r>.x-1.0.noarch.rpm 100% 11MB 750.4KB/s 00:14
root@47.135.214.127's password: <enter root password>
```

- 6 **Step** **ParaBasic** Enter the root password for the CS 2000 Core Manager or CBM. **ParaBasic**

**ParaBasic** The software is installed on the CS 2000 Core Manager or CBM. If a CBM is used, the .rpm package is then copied to the inactive CBM unit and another prompt for the root password appears. If this happens, enter the root password and press Return. After the load file is installed on the CS 2000 Core Manager or CBM, the transferred .rpm package is deleted from the CS 2000 Core Manager or CBM. **ParaBasic**

**Figure** **Graphic** **Figure**

Extracting files from the rpm archive on the cd.

```
Installing RPM package ncgl_cca_mc_image-8.20-1.0
Sun Microsystems Inc. SunOS 5.8 Generic Patch December 2005
ncgl_cca_mc_image-<r>.x-1.y.noarch.rpm 100% 11MB 750.4KB/s 00:14
root@47.135.214.127's password: <enter root password>
Mate IP is 47.135.214.129
Sun Microsystems Inc. SunOS 5.8 Generic Patch July 2006
root@47.135.214.129's password: <enter root password>
```

\*\*\*\*\* Please hit ENTER key to continue \*\*\*\*\*

**ParaBasic** A script is run to verify connectivity to the ACTIVEIRM IP address (the call processing application) and to verify hostname aliases. The output depends on whether the office is configured with a CS 2000 Core Manager or a CBM.



Refer to [CrossRef](#) [Additional information on page 1869](#) [CrossRef](#) for further action. [ParaBasic](#) [Step](#)

7 [Step](#) [ParaBasic](#) Enter X to exit. [ParaBasic](#) [Step](#)

8 [Step](#) [ParaBasic](#) Issue the eject command to open the CD-ROM tray: [ParaBasic](#)

[CommandInstance](#) [CommandName](#) # **eject**  
[CommandName](#) [CommandInstance](#)

[ParaBasic](#) Software on the CS 2000 Management Tools server unmounts the CD-ROM and opens the CD-ROM tray. If the eject command fails and indicates that the device is busy, ensure that the FTP session is ended and no users have changed directory into /cdrom/... directory. Reenter the eject command. [ParaBasic](#) [Step](#) [Context](#)

[Context](#) [Location](#) **SITE — At the CS 2000 Management Tools server** [Location](#)

9 [Step](#) [ParaBasic](#) Remove the CD-ROM from the CD-ROM tray. [ParaBasic](#) [Table](#) [Step](#)

| If                              | Do                                                                                                                                  |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| this is a platform only upgrade | <a href="#">CrossRef</a> <a href="#">Dumping a call processing application image on page 1909</a> <a href="#">CrossRef</a>          |
| otherwise                       | <a href="#">CrossRef</a> <a href="#">Transferring call processing application patch files on page 1882</a> <a href="#">CrossRef</a> |

10 [Step](#) [ParaBasic](#) This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure. [ParaBasic](#) [Step](#) [Context](#) [Procedure](#)

## Section Heading Additional information Heading

ParaPlus ParaBasic After applying the platform software, the installation process invokes the

ComputerOutputString /swd/3pc/bin/user\_config.sh

ComputerOutputString script to verify or set: ParaBasic

- List Item ParaBasic the configuration of the PassThru feature on the CS 2000 Core Manager or CBM ParaBasic Item
- Item ParaBasic hostname aliases core, core0, and core1 ParaBasic Item
- Item ParaBasic NFS sharing of the Call Agent platform software load ParaBasic Item List ParaPlus

ParaBasic The installation process asks if the ncgl\_cca\_image software is for CA (Call Agent) or HMEM (Home Location Registry Memory). ParaBasic

ParaBasic The CS 2000 Core Manager or CBM software provides a prompt to determine if the fileset is for a CA or HMEM application. ParaBasic

ParaPlus ParaBasic Enter CommandString CA CommandString and press the Enter key. ParaBasic

Figure Graphic Figure ParaPlus

Is this a CA or HMEM application? [CA/HMEM] CA: CA

ParaBasic A check is made to determine if aliases core, core0, and core1, as well as PassThru accounts cmusr, core0usr, and core1usr exist. The response is determined by the current configuration. ParaBasic

## Section Heading New installation on Core Business Manager Heading

ParaPlus ParaBasic The software prompts for the ACTIVEIRM IP address, adds the host aliases to the

`ComputerOutputString` /etc/hosts `ComputerOutputString` file, and creates the PassThru users on both CBM units. `ParaBasic`

`Figure` `FigureCaption` **New installation on**  
**CBM** `FigureCaption` `Graphic` `Figure` `ParaPlus` `Section`

```
Is this a CA or HMEM application ? [CA/HMEM] CA : CA
Checking for existing core alias...

hostmtc: Hostname or IP address is not in the hosts database: 'core'.

No existing alias from core found

Cleaning up any alias for core0 core1 and any related passthru accounts,
if found.

Enter the ACTIVEIRM IP ADDRESS (e.g. 172.16.16.72) or q : 10.40.64.72

Adding aliases...

10.40.64.72~core~~
10.40.64.67~core0~~
10.40.64.70~core1~~

Configuring Passthru Users ...

Creating Passthru accounts...
Creating passthru user cmusr
Creating passthru user core0usr
Creating passthru user core1usr

Sharing NFS mount For CCA Access of /swd/3pc ...

NFS mount /swd/3pc successfully shared.
```

`Section` `Heading` **Upgrade on CBM** `Heading`

`ParaPlus` `ParaBasic` In an upgrade on the CBM, the software always prompts to confirm the ACTIVEIRM IP address, always removes the core, core0, and core1 aliases, and always adds them back to the

`ComputerOutputString` /etc/hosts `ComputerOutputString`  
file. `ParaBasic`

`Figure` `FigureCaption` Upgrade on  
CBM `FigureCaption` `Graphic` `Figure` `ParaPlus` `Section`

```
Is this a CA or HMEM application ? [CA/HMEM] CA : CA
Checking for existing core alias...

10.40.64.72~core~~
Please confirm ACTIVE IRM IP address is [10.40.64.72] (yes/no):YES

Temporarily removing alias from /etc/hosts for core core0 core1
and related passthru accounts, while performing network engineering
validation.

Adding aliases...

10.40.64.72~core~~
10.40.64.67~core0~~
10.40.64.70~core1~~

Configuring Passthru Users ...

Creating Passthru accounts...
Creating passthru user cmusr
Creating passthru user core0usr
Creating passthru user core1usr

Sharing NFS mount For CCA Access of /swd/3pc ...

NFS mount /swd/3pc successfully shared.
```

**Section** **Heading** **New installation on CS 2000 Core Manager** **Heading**

**ParaPlus** **ParaBasic** For a new installation, the software prompts for the ACTIVEIRM IP address. This information is available from the Nortel Installation Services engineer, or documentation provided by Nortel Installation Services. **ParaBasic**

**Figure** **FigureCaption** **New installation on CS 2000 Core Manager** **FigureCaption** **Graphic** **Figure** **ParaPlus**

```

Checking for existing aliases...

hostmtc:Hostname or IP address is not in the hosts database:'core'.
hostmtc:Hostname or IP address is not in the hosts database:'core0'.
hostmtc:Hostname or IP address is not in the hosts database:'core1'.

Checking for existing passthru accounts...

passthru:Undefined passthru user cmuser.
passthru:Undefined passthru user core0usr.
passthru:Undefined passthru user core1usr.

Enter the ACTIVEIRM IP ADDRESS (e.g. 172.16.16.72) or q: 10.40.24.80
Do you wish to proceed? [y/n] y: Y

Checking for existing IP in hosts database.

hostmtc:Hostname or IP address is not in the hosts database:'10.40.24.80'
hostmtc:Hostname or IP address is not in the hosts database:'10.40.24.75'
hostmtc:Hostname or IP address is not in the hosts database:'10.40.24.78'

Adding aliases...

10.40.24.80:core::
10.40.24.75:core0::
10.40.24.78:core1::

Adding passthru accounts...

cmuser::221:202,passthru:CA SOS Image:/sdmtools/bin/cm_screener:
/home/cmuser::telnet:core
core0usr::222:202,passthru:CA Unit 0:/sdmtools/bin/cm_screener:
/home/core0usr::telnet:core0
core1usr::223:202,passthru:CA Unit 1:/sdmtools/bin/cm_screener:
/home/core1usr::telnet:core1

exporting NFS mount /swd/3pc...

Mount already exported to core*.

```

**ParaBasic** The aliases and PassThru accounts are created. The status information about installation in the previous figure does not

remain on the screen very long since the installation software clears the screen once the configuration is complete. Please read

[CrossRef](#) [Important password information.](#) [CrossRef](#) [ParaBasic](#) [Section](#)

## [Section](#) [Heading](#) Upgrade configuration on CS 2000 Core Manager [Heading](#)

[ParaPlus](#) [ParaBasic](#) The following figure shows the upgrade configuration on the CS 2000 Core Manager for passthru accounts. Please read [CrossRef](#) [Important password information.](#) [CrossRef](#) [ParaBasic](#)

### [Figure](#) [FigureCaption](#) Upgrade configuration on CS 2000 Core Manager [FigureCaption](#) [Graphic](#) [Figure](#)

```
Checking for existing aliases...

10.40.24.80:core:cm CLLI:Core's IPNETWRK IP Address
10.40.24.75:core0::
10.40.24.78:core1::

Checking for existing passthru accounts...

passthru:Undefined passthru user cmuser.
passthru:Undefined passthru user core0usr.
passthru:Undefined passthru user corelusr.

Adding passthru accounts...

cmuser::221:202,passthru:CA SOS Image:/sdmtools/bin/cm_screener:
/home/cmuser::telnet:core
core0usr::222:202,passthru:CA Unit 0:/sdmtools/bin/cm_screener:
/home/core0usr::telnet:core0
corelusr::223:202,passthru:CA Unit 1:/sdmtools/bin/cm_screener:
/home/corelusr::telnet:core1

exporting NFS mount /swd/3pc...

Mount already exported to core*.
```

**Note:** [Note](#) [ParaBasic](#) Long lines in the display were wrapped. [ParaBasic](#) [Note](#) [ParaPlus](#) [Section](#)

## [Section](#) [Heading](#) Important password information [Heading](#)

[ParaBasic](#) For new installations, new PassThru accounts are created without passwords. Users log in to the CS 2000 Core Manager or CBM

with a username of cmusr, core0usr, or core1usr, and are immediately forwarded to a destination host. The destination host provides a login with password authentication. If password authentication is preferred on the CS 2000 Core Manager or CBM, in addition to the destination host, then reconfigure the accounts at the passthru level of sdmmtc or cbmmtc. [¶ ParaBasic](#) [¶ Section](#)

## Section > Heading > **Offices without a CS 2000 Core Manager or CBM** <Heading

<ParaPlus > ParaBasic > Offices without a CS 2000 Core Manager or a CBM require manual action to ensure that load delivery is complete. Failure to perform these actions may result in a no boot situation. Two tests are available to determine this situation: <ParaBasic

- <List > Item > ParaBasic > The CS 2000 Management Tools server boots the cards in the SAM21 shelf. This is indicated at the CS 2000 SAM21 Manager client if the SAM21 EM Server IP value at the Reprovisioning window is also the value for Server IP on the same window. <ParaBasic > Item
- <Item > ParaBasic > If the command <CommandString > echo \$SDM\_IP <CommandString > returns a blank line from a command prompt at the CS 2000 Management Tools server. <ParaBasic > Item <List > ParaPlus

## Procedure > ProcedureCaption > **Required actions for offices without a CS 2000 Core Manager or CBM** <ProcedureCaption

### Context > Location > **At a CS 2000 Management Tools terminal** <Location

- 1 <Step > ParaBasic > Become the superuser with the <CommandString > su - root <CommandString > command and enter the root password when prompted. <ParaBasic > Step
- 2 <Step > ParaBasic > View the /etc/hosts file: <ParaBasic >
 

<CommandInstance > <CommandName > # cat /etc/hosts  
 <CommandName > <CommandInstance > <Step >
- 3 <Step > ParaBasic > If values for <ComputerOutputString > core <ComputerOutputString >, <ComputerOutputString > core0 <ComputerOutputString >, and <ComputerOutputString > core1 <ComputerOutputString > are not listed, enter them in the file. <ParaBasic >
  - <List > Item > ParaBasic > <ComputerOutputString > core <ComputerOutputString > is the same IP address as the



ACTIVEIRM IP address. For example,  
172.16.16.72. <ParaBasic <Item

- <Item <ParaBasic <ComputerOutputString core0  
<ComputerOutputString is the same as the  
<ComputerOutputString core <ComputerOutputString value, but  
the last octet is 5 less than the last octet of the  
<ComputerOutputString core <ComputerOutputString value. For  
example, 172.16.16.67. <ParaBasic <Item
- <Item <ParaBasic <ComputerOutputString core1  
<ComputerOutputString is the same as the  
<ComputerOutputString core <ComputerOutputString value, but  
the last octet is 2 less than the last octet of the  
<ComputerOutputString core <ComputerOutputString value. For  
example, 172.16.16.70. <ParaBasic <Item <List

<ParaBasic Make a backup copy of the /etc/hosts  
file: <ParaBasic

<CommandInstance <CommandName # **cp /etc/hosts**  
**/etc/hosts.bak** <CommandName <CommandInstance

<ParaBasic Enter the values with the vi editor, the dtpad  
graphical editor, or appending the lines to the end of the  
file: <ParaBasic

<CommandInstance <CommandName # **echo "172.16.16.72**  
**core" >> /etc/hosts**  
**# echo "172.16.16.67 core0" >> /etc/hosts**  
**# echo "172.16.16.70 core1" >> /etc/hosts**  
<CommandName <CommandInstance <Step

- 4 **Step** **ParaBasic** Edit the /etc/dfs/dfstab file to allow the /data/swd/3pc directory to be shared on the network: **ParaBasic**

```

CommandInstance CommandName # echo "#Begin CCA
NFS Configuration" >> /etc/dfs/dfstab

CommandName echo "share -F nfs -o
rw=core0:core1 /data/swd/3pc" >>
/etc/dfs/dfstab

echo "#End CCA NFS Configuration" >>
/etc/dfs/dfstab CommandInstance Step

```
- 5 **Step** **ParaBasic** View the file to ensure the changes are correct: **ParaBasic**

```

CommandInstance CommandName # cat /etc/dfs/dfstab
CommandName CommandInstance

```

**ParaBasic** Ensure that the end of the file resembles the following output. **ParaBasic**

```

ComputerOutputBlock ...
#Begin CCA NFS Configuration
share -F nfs -o rw=core0:core1 /data/swd/3pc
#End CCA NFS Configuration ComputerOutputBlock Step

```
- 6 **Step** **ParaBasic** Enable the sharing: **ParaBasic**

```

CommandInstance CommandName # /usr/sbin/shareall
CommandName CommandInstance Step

```
- 7 **Step** **ParaBasic** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure. **ParaBasic** **Step** **Context** **Procedure** **Section** **Section** **Module**

## Electronic Software Delivery (ESD) for Call Agent

Both the PCL and NCL software loads for the Call Agent are available for electronic transfer from Nortel to a customer dropbox. The PCL name format is CSNNCxx (CSNWCxx for International markets), and the NCL name format is ncgl\_cca\_image\_x.x.x.x.

### ATTENTION

This procedure applies only to the following loads: CM Core, CCA LINUX, and MC.

## Audience

This procedure is intended for telephone operating company personnel who have an ESD agreement with Nortel. When the agreement was established, the operating company furnished Nortel with the location of an electronic dropbox and a username and password pair for delivering software loads. When Nortel delivers a software load to the dropbox, an electronic mail notification is sent to the E-mail address specified by the telephone operating company when the ESD agreement was established.

## Prerequisite

Perform the procedure [Transferring and mounting an ISO image on an SPFS-based server on page 426](#) before you begin this procedure.

## Action

### *At a CS 2000 Management Tools server terminal*

- 1 Use the following table to determine your first step.

| If the ESD file is | Do                      |
|--------------------|-------------------------|
| a PCL              | steps <a href="#">2</a> |
| an NCL             | steps <a href="#">4</a> |

- 2 Record the location of the call processing application files, /data/iso\_esd/<esd\_filename>, such as /data/iso\_esd/SNC0000x.x.R.PCL.PPC3.SDC.2.D.

- 3 Go to procedure [Restoring call processing application files on page 1886](#). At [step 5](#) of the restoration procedure, specify the location recorded in [step 2](#) of this ESD procedure for the call processing application files instead of /cdrom/cdrom0. After you have specified the location, go to [step 11](#).
- 4 Become the root user:  

```
$ su - root
```

*A prompt for the root password is presented. Enter the root password.*
- 5 List the contents of the /tmpmnt/noarch directory (ls /tmpmnt/noarch) and record the name of the .rpm file.
- 6 Enter the platform\_load\_install.sh command.
- 7 Select 2, Install RPM from Disk.
- 8 Enter the .rpm filename when prompted.
- 9 Enter /tmpmnt/noarch when prompted for the location of the .rpm file.
- 10 Unmount the ESD file. Perform procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#)
- 11 The ESD procedure is complete. Return to the "IF DO" [Table on page 1868](#) to continue the install.

## Transferring patch files from optical disk to a Core Manager

Use this procedure to manually transfer Compact Call Agent patches from an optical disk (CD or DVD) to one of the following network supported core managers:

- Core and Billing Manager 850 (CBM)
- CS 2000 Core Manager

### Transferring patch files from optical disk to a Core Manager

#### *At a core manager terminal server*

- 1 Log in to the CS 2000 Core Manager or CBM as the root user if not already logged in.

- 2 Change to the core manager directory designated to store the Compact Call Agent patch files:

```
cd /swd/3pc/patch
```

- 3 Select the appropriate core manager.

| If the core manager is a | Do                     |
|--------------------------|------------------------|
| CBM                      | <a href="#">step 4</a> |
| CS 2000 Core Manager     | <a href="#">step 7</a> |

- 4 Insert the optical disk into the CBM disk drive and access the appropriate directories.

```
cd /cdrom/cdrom0
```

- 5 Copy each of the patch files from the optical disk into the CBM /swd/3pc/patch directory.

```
cp * /swd/3pc/patch/
```

- 6 Eject the optical disk.

```
cd /
```

```
eject cdrom
```

Continue to [step 14](#).

- 7 Insert the optical disk into the SPFS-based server drive that hosts the CS 2000 Management Tools, and access the appropriate optical disk directories.

```
cd /cdrom/cdrom0
```

- 8 Copy the patch files from the optical disk into a temporary location on the server.  
**cp \* /tmp/**
- 9 Eject the optical disk.  
**cd /**  
**eject cdrom**
- 10 Change to the tmp directory.  
**cd /tmp**
- 11 Open an FTP session to the CS 2000 Core Manager and log in with change directory and file transfer privileges:  
**ftp <cs2k\_core\_manager\_ip>**  
**Name:**  
**Password:**
- 12 Change directory, list the file size, change the mode to binary, and get the patch file(s) from the SPFS-based server /tmp directory to the CS 2000 Core Manager /swd/3pc/patch directory:  
**ftp> cd /swd/3pc/patch**  
**ftp> ls**  
**ftp> bin**  
**ftp> prompt**  
**ftp> mget \***
- 13 End the FTP session:  
**ftp> bye**
- 14 Access the directory on the core manager that contains the patch files.  
**cd /swd/3pc/patch**
- 15 Change the access permissions on all the files in the directory.  
**chmod 755 \***
- 16 This procedure is complete.

## Transferring call processing application patch files

Complete this procedure at least two days before the ONP.

### ATTENTION

Do not perform this procedure for a platform only upgrade.

Call processing application patch files are delivered electronically through Regional Patch Selector (RPS). Contact Nortel support personnel for information about RPS and call processing application patch files.

### ***SITE — At a terminal window***

- 1 Log in to the CS 2000 Core Manager or CBM as the root user if not already logged in:

```
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password: <password>
```

- 2 Change directory to the location of the call processing application patch files:  
**# cd <path\_to\_files>**
- 3 Open an FTP session to the call processing application:  
**# ftp cm**
- 4 Log in with a valid username and password.  
**Note:** The user must have FTP privilege and permission to write to SFDEV.
- 5 Change directory to the store file device (SFDEV):  
**ftp> cd /SFDEV**
- 6 Set the transfer options:  
**ftp> bin; site lrecl 128**
- 7 Use the put command to transfer the call processing application patch files:  
**ftp> put <patch\_file\_name>**

**Note:** Optionally use the MPUT and PROMPT commands to transfer multiple files. The MPUT command transfers multiple files. The MPUT command accepts wildcard pattern matching characters. The PROMPT command prevents prompting for each file.

- 8 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Transferring patch files from ESD to a Core Manager

Nortel offers an Electronic Software Delivery (ESD) agreement option whereby the operating company furnishes Nortel with the location of an electronic dropbox and a username and password pair for delivering software loads. When Nortel delivers a software load to the dropbox, an electronic mail notification is sent to the E-mail address specified by the operating company when the ESD agreement was established.

### Transferring patch files from ESD to a Core Manager

#### *At the workstation*

- 1 Select the first step as follows:

| If the core manager is a | Do                     |
|--------------------------|------------------------|
| CS 2000 Core Manager     | <a href="#">step 2</a> |
| CBM                      | <a href="#">step 5</a> |

- 2 Verify that the correct directory path, as shown in the following command, exists on the CS 2000 Core Manager:

```
> cd /swd/3pc/patch/
```

| If the path                                          | Do                     |
|------------------------------------------------------|------------------------|
| does not exist and the response "not found" displays | <a href="#">step 3</a> |
| exists                                               | <a href="#">step 5</a> |

- 3 Create the directory path.

- a Access the storage level from the CS 2000 Core Manager .

```
sdmmtc storage
```

- b Add a logical volume in which to store the ESD file.

```
> esdadd
```

The system prompts you to enter a logical volume to be converted to the /swd/sdm/esd standard.

- 4 Ensure that the correct directory path has been accessed.

```
> cd /swd/3pc/patch/
```

- 5 Use trivial file transfer protocol (TFTP) or file transfer protocol (FTP) to transfer the software load file as a binary file to the directory appropriate to the core manager platform.

- /swd/3pc/patch/ (CS 2000 Core Manager and CBM)

**Note:** Accessing the /swd link using the CBM is equivalent to accessing the /data/swd path.

---

| If your core manager is a | Do                                                                                                          |
|---------------------------|-------------------------------------------------------------------------------------------------------------|
| CS 2000 Core Manager      | <a href="#">Preparing the CS 2000 Core Manager for file transfer from the repository server on page 575</a> |
| a CBM                     | <a href="#">Transferring and mounting an ISO image on an SPFS-based server on page 426</a>                  |

---

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

## Restoring call processing application files

Complete this procedure when the final shipment of software arrives.

### ATTENTION

Do not perform this procedure for a platform only upgrade.

#### ***SITE — At the CS 2000 Management Tools server***

- 1 Insert the DVD in the DVD-ROM tray.

#### ***SITE — At the CORE0 or CORE1 window***

- 2 Exit the Call Agent Manager:

**> 0 all**

*The operating system prompt is returned.*

```
[mtc@hostname mtc]$
```

- 3 Change directory to the destination directory for the upgrade call processing application image:

**> cd /3PC/<sd0x>/<image\_file\_location>**

#### **Example**

**> cd /3PC/sd00/image**

- 4 Open an FTP session to the CS 2000 Management Tools server and log in as a user with privilege to change directory and transfer files with FTP:

**> ftp <cs\_2000\_mgmt\_tools\_ip>**

#### **Example**

```
[mtc@10.40.44.67 image0]$ ftp <cs_2000_mgmt_tools_ip>
Connected to <cs_2000_mgmt_tools_ip>.
220 ProFTPD 1.2.8 Server (Authorized Use Only) [hostname]
Name (hostname:mtc): maint
331 Password required for maint.
Password:
230 User maint logged in.
ftp>
```

- 5 Change directory, list the file size, change the mode to binary, and get the file. Do not transfer a file with a name longer than 32 characters:

```
ftp> cd /cdrom/cdrom0
ftp> ls
ftp> bin
ftp> prompt
ftp> mget *
```

#### Example

```
ftp> cd /cdrom/cdrom0
250 CWD command successful.
ftp> ls
MUC00022810335_MS.img1020
SNC00009810335_CM.img1020
ftp> bin
200 Type set to I.
ftp> prompt
Interactive mode off.
ftp> mget *
local: SNC00009810335_CM.img1020 remote: SNC00009810335_CM.img1020
200 PORT command successful.
150 Opening data connection for SNC00009810335_CM.img1020 (binary mode)
226 Transfer complete.
150 Opening data connection for MUC00022810335_MS.bin1020 (binary mode)
226 Transfer complete.
```

- 6 End the FTP session by typing bye:

```
ftp> bye
```

#### At the ACTIVECM window

- 7 Enter the DISKUT level and import the upgrade call processing application and Message Switch images:

**Note:** Ensure that you have the appropriate file extension to import. The following file extensions are premitted:

```
_cm or .img1020, _ms or .img1020, $ld or
.bin256, $pf or .bin256, $patch or .bin128
```

Otherwise the importing CM load will fail.

```
> DISKUT
> IMPORT <volume_name>
> QUIT
```

**Example of IMPORTing image files**

```
DISKUT:
>IMPORT SD00IMAGE1

Attempting to import 2 files selected on SD00IMAGE1.

Imported MUC00022810335_MS.img1020 as MUC00022810335_MS IMAGE 1020.
Imported SNC00009810335_CM.img1020 as SNC00009810335_CM IMAGE 1020.

Imported 2 files successfully of 2 attempts on SD00IMAGE1.
```

*The call processing application and Message Switch images are imported from the native file system into the call processing application file system. If the disk does not have enough space, a prompt to increase the volume size is presented.*

- 8 Use the set boot file command to enter the image in to the ITOC and make it bootable:

```
> ITOCCI
> SBF CM <filename_cm> 15
```

**Example**

```
> SBF CM SNC00009547159_CM 15
```

```
> QUIT
```

*The complete ITOC is printed to the terminal. If an MS image was loaded too, use the SBF MS <image\_name> <position> command for the MS image too. If there is no free space in the ITOC use the clear boot file command to remove the oldest entry: CBF CM <image\_name>.*

**SITE — At a CS 2000 Management Tools terminal**

- 9 Issue the eject command to open the DVD-ROM tray:

```
eject
```

*Software on the CS 2000 Management Tools server unmounts the DVD and opens the DVD-ROM tray. If the eject command fails and indicates that the device is busy, ensure that the FTP session is ended and no users have changed directory into /cdrom/... directory. Reenter the eject command.*

**SITE — At the CS 2000 Management Tools server**

- 10 Remove the DVD from the DVD-ROM tray.

- 11** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Cleaning up SFDEV

---

Use this procedure to remove files from the Store File Device (SFDEV).

If call processing application patch files were downloaded in SFDEV, do not delete these files.

### ***ACT — At the ACTIVECM window***

- 1 Determine the files in SFDEV:  
**> LISTSF ALL**
- 2 Copy files from SFDEV to storage:  
**> SCANF SFDEV COPY <disk\_vol> NAME <file\_name>**  
**disk\_vol**  
is the destination storage volume like SD00TEMP  
**file\_name**  
is the name of the file to copy
- 3 If required, access the disk administration level to create a disk volume in which to copy the files from SFDEV:  
**> diskadm <disk\_prefix>**  
**disk\_prefix**  
is the disk on which you want to create the volume, either sd00 or sd01
- 4 Create the storage volume:  
**> cv <vol\_name> <size>**  
**vol name**  
is the name you want to give the new volume, for example SD00TEMP  
**size**  
is the size required for the new volume, for example 128 for 128 Megabytes
- 5 Erase files that are not essential from SFDEV:  
**> ERASESF <file\_name>**
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Verifying table ACDGRP

Perform this procedure to prevent the software from incorrectly renumbering tuples in table ACDGRP during the call processing software upgrade.

### **ACT — At the ACTIVECM window**

- 1 Determine if there are non-consecutive keys in table ACDGRP:  
     > **OMSHOW ACDGRP ACTIVE**
- 2 Review the output and note if any keys are missing:

|                                                               |          |          |          |   |
|---------------------------------------------------------------|----------|----------|----------|---|
| ACDGRP                                                        |          |          |          |   |
| CLASS: ACTIVE                                                 |          |          |          |   |
| START:2005/06/20 09:30:00 THU; STOP: 2005/06/20 09:54:27 THU; |          |          |          |   |
| SLOWSAMPLES: 15 ; FASTSAMPLES: 147 ;                          |          |          |          |   |
| KEY (AUTOMATIC_CALL_DISTRIB_GROUP)                            |          |          |          |   |
| ACDOFFR                                                       | ACDANSR  | ACDDFLCT | ACDABNDN |   |
| ACDNS                                                         | ACDPRMPT | ACDBLOCK | ACDTMOFL |   |
| ACDTMINF                                                      | ACDTMANS | ACDCIF   | ACDXFER  |   |
| ACDCPK                                                        | ACDUSAGE | ACDUSAG2 | ACDICQD  |   |
| ACDREQD                                                       | ACDDMCT  | ACDRQABN | ACDRQRTE |   |
| 0 NACDP                                                       | 0        | 0        | 0        | 0 |
|                                                               | 0        | 0        | 0        | 0 |
|                                                               | 0        | 0        | 0        | 0 |
|                                                               | 0        | 0        | 0        | 0 |
|                                                               | 0        | 0        | 0        | 0 |
| 2 NACD2P                                                      | 0        | 0        | 0        | 0 |
|                                                               | 0        | 0        | 0        | 0 |
|                                                               | 0        | 0        | 0        | 0 |
|                                                               | 0        | 0        | 0        | 0 |
|                                                               | 0        | 0        | 0        | 0 |

Index key  
1 is missing.

- 3 If any index keys are missing, have translation personnel provision dummy tuples in the key indexes. Also provide datafill in table DNROUTE for each tuple added to table ACDGRP.
- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



---

## Filling in test call scripts

---

Test calls should be made and verified to work as expected prior to the software upgrade, preferably on the day of the ONP. Identify calling irregularities ahead of time. This will avoid unnecessary investigation of a pre-existing condition after switch of activity (SWACT).

### ATTENTION

Nortel recommends that site personnel complete their test call scripts before continuing with the software release upgrade process. Identifying calling irregularities now avoids unnecessary troubleshooting after SWACT.

This section presents generic guidelines for creating a test call plan to be used both before and after the SWACT to a new load.

The purpose of test calls is to verify the performance of newly installed software for telephone switching systems. Test calls can ensure the smooth operation of thousands of calling situations with different combinations of telephone sets, service features, and traffic conditions on the network. Such testing helps ensure the availability and reliability of features and services for telephone users.

Test call scripts refers to the verification calls as predefined by the telephone/carrier operating company. These are test calls to be performed after activating the new software load in order to confirm acceptability of the new load. In the ONP procedure the test call scripts are put to use as follows:

- As a part of site preparation, this procedure instructs the operating company to fill in and test the test call scripts before beginning the upgrade. This is to provide a thorough test plan exercise for validating the new software load.
- Then, after activating the new software load, the operating company performs the test call scripts again to verify the software load.

The test call scripts provided below are only examples of call types that could be included in the test call scripts. These samples include only basic call processing tests and provide some, but not all, critical test calls. These are provided only as a guideline. Each telephone/carrier

office should determine the best mix of test calls to use based on the office's unique configuration.

**ATTENTION**

The test calls listed in the following procedures will not apply to every office.

The telephone office will have to customize the list according to its own particular configuration.

Nortel recommends including the following items in your post-SWACT testing routine.

Add any other items that are determined to be important.

Post-SWACT call checklist

- ☐ Verify date, time and dialtone
- ☐ Perform Critical Call Tests (for example, 0- and 0+7/10). See the following procedure.
- ☐ Perform International Direct Distance Dialing (IDDD) calls
- ☐ Check Equal Access origination and termination
- ☐ Perform Common Channel Inter-office Signaling (CCIS) calls
- ☐ Verify Automatic Coin Toll Service (ACTS)
- ☐ Verify DRAMS (announcements and SIT tones)
- ☐ Check Wide Area Telephone Service (WATS), INWATS, OUTWATS, 2-way
- ☐ Verify Pay Station Coin Control (Coin Collect and Coin Return)
- ☐ Verify miscellaneous services such as 311, 411, 611, and repair services
- ☐ Check Extended Area Service (EAS) calls
- ☐ Perform Traffic Operator Position System (TOPS) calls
- ☐ Perform Mechanized Calling Card Service (MCCS) calls
- ☐ Perform Direct Inward System Access (DISA) calls
- ☐ Verify Custom Calling Features

**SITE — At the office**

**1** Perform the critical test calls and record the results.

| Test description                                                                                                                                               | From: line type or CLLI | To: call type and digits dialed | Test result |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|---------------------------------|-------------|
| Check for DIALTONE on all line modules                                                                                                                         |                         |                                 |             |
| Verify 0 minus route                                                                                                                                           |                         |                                 |             |
| Verify 0 plus route                                                                                                                                            |                         |                                 |             |
| Verify ONI 1-7, 1-10 digits                                                                                                                                    |                         |                                 |             |
| Verify EAS incoming and outgoing routes                                                                                                                        |                         |                                 |             |
| Verify CAMA routes                                                                                                                                             |                         |                                 |             |
| Verify local Tandem routes                                                                                                                                     |                         |                                 |             |
| Verify DDO routes                                                                                                                                              |                         |                                 |             |
| Verify Directory Assistance                                                                                                                                    |                         |                                 |             |
| Verify critical service routes (911, police, fire, hospitals, and radio stations)                                                                              |                         |                                 |             |
| Verify TOLL COMP (DTS) route                                                                                                                                   |                         |                                 |             |
| Verify 1FR intra-office call                                                                                                                                   |                         |                                 |             |
| Verify Remotes: <ul style="list-style-type: none"> <li>EAS outgoing (one route)</li> <li>0 plus 0 minus</li> <li>CAMA ANI</li> <li>1FR intra-Remote</li> </ul> |                         |                                 |             |
| Verify Operator Intercept route                                                                                                                                |                         |                                 |             |
| Verify all (idle) customer/network trunks                                                                                                                      |                         |                                 |             |

**2** Perform additional test calls sample.

- a** Verify regular POTS calls:
  - line (1FR) -> line (1FR)  
(969-xxxx -> 969-xxxx)
  - line (PPHONE) -> trunk -> line (1FR)  
(969-xxxx -> 9-1-514-970-xxxx)
- b** Verify use of different PM types:
  - line (LM) -> line (RLM)  
(969-xxxx -> 969-xxxx)
  - line (LCM) -> line (RLCM)  
(969-xxxx -> 969-xxxx)
- c** Verify use of different trunk types:
  - line (1FR) -> PTS trunk -> line (1FR)  
(968-xxxx -> 969-xxxx)
  - line (1FR) -> ISUP trunk (all variants supported by office) ->  
line (KSET-Disp M5209T)  
(968-xxxx -> 6-456-xxxx)
- d** Verify ISDN calls:
  - line (KSET-Disp M5317T) -> trunk -> line (KSET-Disp  
M5209T)  
(968-xxxx -> 6-456-xxxx)
  - line (PPHONE-Disp M5317T) -> trunk -> line (1FR-Disp  
Maestro)  
(968-xxxx -> 9-969-xxxx)
  - line (KSET-Disp M5317T) -> trunk -> line  
(PPHONE-Meridan Bus.)  
(968-xxxx -> 9-1-819-456-xxxx)
  - line (KSET-Disp M5317T) -> line (KSET-PSET)  
(968-xxxx -> 968-xxxx)
  - line (BRAMFT set) -> line (BRAFS set)  
(968-xxxx -> 968-xxxx)
  - line (1FR) -> line (BRAKS set)  
(968-xxxx -> 968-xxxx)

**3** Proceed after test call scripts are verified.

- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Performing TABAUDIT

Begin this procedure 30 calendar days before the software delivery application date and complete the TABAUDIT with no errors at least 10 days before the ONP. Nortel Global Software Delivery recommends scheduling automatic TABAUDITs (AUTOTABAUDIT), rather than manual TABAUDITs.

Nortel recommends using TABAUDIT as part of normal maintenance practices for regular ongoing table data integrity checks. This can be done by using the automatic scheduling function. For assistance with TABAUDIT, contact your Nortel regional customer representative.

### Restrictions on AUTOTABAUDIT:

- Only one user at a time is allowed to enter the AUTOTABAUDIT level.
- Before executing AUTOTABAUDIT, a list of session parameters must be defined from within the AUTOTABAUDIT level.
- Only one AUTOTABAUDIT session can execute at a time. However, multiple AUTOTABAUDIT sessions can be scheduled.
- The parameters for the active AUTOTABAUDIT session cannot be changed without terminating the session first.
- AUTOTABAUDIT cannot be executed at the same time as TABXFR or an image dump.
- For wireless applications on HLR offices, AUTOTABAUDIT should be scheduled to execute during off hours to avoid delays with subscriber provisioning.

### ***SITE — At the ACTIVECM window***

1



#### **CAUTION**

##### **Possible service interruption**

Review software delivery bulletins and current warning bulletins about TABAUDIT.

Enter the automated table audit level:

> **TABAUDIT; AUTO**

2

Clear the list of tables to be included in the check:

> **CLEAR INCLUDED**

- 3 Clear the scheduled list of time frames:

> **CLEAR SCHEDULE ALL**

**Note:** This command clears all scheduled TABAUDIT sessions identified in table AUTOTAB.

- 4 Set all tables for verification:

> **INCLUDE ALL**

- 5 Define the scheduled AUTOTABAUDIT session:

> **TIMEFRAME SINGLE** <start\_time> [<start\_date>]  
<stop\_time> [<stop\_date>]

start\_time

is the hour and minute to begin the TABAUDIT and is specified as HH:MM, such as 23:30

start\_date

is an optional parameter and is specified as YYYY:MM:DD, such as 2002:06:21

stop\_time

identifies the latest time by which that the TABAUDIT must complete

**Note:** The timeframe options include single, daily, weekly, and monthly sessions. A timeframe cannot be less than 30 minutes or more than six hours.

For the monthly option, the 31st day of the month cannot be used. Up to eight sessions can be set up. Timeframe definitions must not overlap.

Scheduling a minimum of three hours to complete the AUTOTABAUDIT is recommended. The time can be spread over more than one session, if required.

- 6 Verify the parameters:

> **STATUS**

AUTOTABAUDIT is scheduled to execute during the start and stop period between the start and stop dates.

| AUTOTABAUDIT STATUS |            |                     |           |                   |                   |
|---------------------|------------|---------------------|-----------|-------------------|-------------------|
| Active Timeframe    |            | Executing Timeframe |           |                   |                   |
| Start Date          | Stop Date  | Start Time          | Stop Time | Scheduling Option | REGULAR or SUBSET |
| 2005/06/24          | 2005/06/24 | 18:30               | 20:00     | SINGLE            | REGULAR           |

Current time : 2005/06/24 07:16:07

AUTOTABAUDIT : Inactive

The following events were logged while verifying tables:

1 TABAUDIT aborted. All included tables not verified. Out of time.

The following tables are included for the REGULAR AUTOTABAUDIT:

From table VERSIONS (0) to table INWATNPA (1408).

No tables have been excluded for the REGULAR AUTOTABAUDIT.

No tables have been included for the SUBSET AUTOTABAUDIT.

The following tables are excluded for the SUBSET AUTOTABAUDIT:

From table VERSIONS (0) to table INWATNPA (1408).

## 7 Execute the scheduled AUTOTABAUDIT session:

### > EXECUTE

The system displays a STATUS. If the status is correct, enter YES at the prompt.

**Note:** The scheduler starts AUTOTABAUDIT at the specified start time(s), and stops testing at the specified stop time(s). Only the included tables are tested in the order they are listed in table DART.

## 8 Check the status of AUTOTABAUDIT after the scheduled stop time:

### > STATUS



Determine if AUTOTABAUDIT has completed verifying all tables.

| If AUTOTABAUDIT                                                                              | Do                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| has completed verifying all tables                                                           | step <a href="#">9</a>                                                                                                                                                                                                    |
| has not completed verifying all tables (process failed, insufficient time, or other reasons) | determine what steps are necessary to complete the process. It may be necessary either to repeat steps <a href="#">1</a> through <a href="#">3</a> , or to schedule multiple sessions to verify all tables in the office. |

**9** After AUTOTABAUDIT completes, obtain an error report:

**> REPORT ERRORS**

| If                     | Do                                                                                                                                   |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| no errors are reported | step <a href="#">11</a>                                                                                                              |
| errors are reported    | Correct the errors using the table editor and repeat from step <a href="#">4</a> . Refer to <a href="#">Additional information</a> . |

**10** If any tables failed, perform the following steps for each table.

**a** Quit to the TABAUDIT level:

**> QUIT**

**b** Include the failed table:

**> INCLUDE <table\_name>**

**c** Execute the TABAUDIT:

**> EXECUTE**

**d** View the results:

**> REPORT <table\_name>**

**e** Repeat from [step b](#) for each failed table.

**11** Quit to the CI level:

**> QUIT ALL**

**12** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Additional information

Use the following procedure to assist in repairing tables.

### ***SITE — At the ACTIVECM window***

- 1 Enter the table that has an error:  
**> TABLE <table\_name>**  
tab\_name  
is a table name like TRKMEM
- 2 Position on the failed tuple:  
**> POS <tuple>**  
tuple  
is the failed tuple such as AL7ITICS7 2
- 3 Check the tuple:  
**> CHECK**
- 4 Note the error message and make corrections.
- 5 Repeat this procedure for all failed tables. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Executing SWUPGRADE READY

Nortel Global Software Delivery personnel complete this procedure at scheduled milestones before the ONP.

At any time during this procedure, to determine the status, use the DISP STEPS command. Help for steps is available with the HELP command. A step can be re-run with the RUNSTEP <step\_name> command. Ensure that all steps complete successfully, but a step can be overridden with the OVERRIDE command. To cancel the procedure, use the CANCEL command.

The steps are determined by the CS 2000 - Compact configuration. If the CS 2000 - Compact is configured with Message Controller cards, more steps are provided.

### SWUPGRADE READY steps

| without Message Controllers | with Message Controllers      |
|-----------------------------|-------------------------------|
| SETUP_ENV_VARS              | SETUP_ENV_VARS                |
|                             | VERIFY_SN_PECES_INFO          |
| VERIFY_LOGS_INFO            | VERIFY_LOGS_INFO              |
| DEVICE_CHECK                | DEVICE_CHECK                  |
| TABAUDIT_VERIFY_TABLES      | TABAUDIT_VERIFY_TABLES        |
|                             | DISPLAY_PERIPHERAL_LOAD_NAMES |
|                             | DISPLAY_SPM_LOADNAMES         |
|                             | DISPLAY_PRL_LOADS             |
|                             | CHECK_ISN_PMS                 |
|                             | DISPLAY_MS_FW_LOADS           |
|                             | VERIFY_PM_LOAD_NAMES          |
|                             | LIUINV_CHECK                  |
|                             | C7LINK_CHECK                  |
|                             | CHECK_LTCINV                  |

**SWUPGRADE READY steps**

| without Message Controllers | with Message Controllers |
|-----------------------------|--------------------------|
| DISPLAY_NOP_USERS           | DISPLAY_NOP_USERS        |
| DISPLAY_DPP_VERSION         | DISPLAY_DPP_VERSION      |
|                             | CHECK_LCMINV             |
| SBA_CHECK                   | SBA_CHECK                |
| SBA_VOLSIZE_CHECK           | SBA_VOLSIZE_CHECK        |
| READY_STATUS                | READY_STATUS             |
| READY_COMPLETE              | READY_COMPLETE           |

**SDE — At the ACTIVECM window**

1 Enter the SWUPGRADE level:

> **SWUPGRADE READY**

2 Begin the process:

> **START**

*Step SETUP\_ENV\_VARS begins. This step sets the environment variables that will be used during the READY session. Default values appear in square brackets and variables without brackets have no default. To accept the default value press the Return key without entering a value.*

*Values consisting of more than one word must not be enclosed in quotes. If they are, the quotes will be considered as part of the word and the variable will be either set to an incorrect value or not set at all.*

**a** Set the TRACE\_USER variable.

TRACE\_USER (no default)

Holds the USER name on whose console output messages are printed. Changing the value of this variable, also changes the value of the TRACE\_DEVICE variable, and causes the output to be redirected to the new USER device.

Value: <user name> or ME - a user name, such as ADMIN, or ME which indicates the current user

**Note:** For clarity purposes, it is recommended to set this variable to a user other than the current user.

The user must be logged in when this variable is set. The current setting is: <none>

> **ME**

- b** Do not change the TRACE\_DEVICE variable, press the Enter key.

**TRACE\_DEVICE**

Holds the device name on which output messages are printed. Changing the value of this variable causes the output to be redirected to the new device.

Value: <trace device name> - a string, such as MAP

**Note:** For clarity purposes, it is recommended to set this variable to a device other than the terminal currently logged onto.

The current setting is: <none>

>

- c** Set LOGS variable.

**LOGS**

Holds the names of the logs that are checked by the LOGS step. More than one log can be specified by entering log names separated by a blank.

**Example**

CM — Check CM logs and display a message if CM logs are recorded.

**Example**

SWERR TRAP — Check traps and swerrs. Display a message if traps or swerrs are recorded.

The current setting is: TRAP SWERR

> **TRAP SWERR**

- d** Set TO\_CSP\_CM\_LOAD variable. Enter the value of the CSP load number.

**TO\_CSP\_LOAD**

The TO\_CSP\_LOAD variable allows the user to set the CSP load to which the site plans to upgrade. This variable is then used to check the PMs for a software load which equals this value.

The current setting is: 0

> **22**

- e** Set the PM\_VERIFY\_FILE variable, and press the Enter key.

**PM\_VERIFY\_FILE**

The PM\_VERIFY\_FILE variable allows the user to set which verification file will be used to validate if the queried peripheral module loads are valid.

The default setting is: NONE

>

- f** Do not change the PRINTER variable, press the Enter key.

**PRINTER**

The PRINTER variable holds the name of the printer on which output messages are recorded. The printer echoes all output sent to the trace device. Changing the value of this variable causes the recording to be directed to the new device.

Value: <printer name> or SINK

where <printer name> is a device datafilled in table TERMDEV. SINK indicates not to record to a printer device.

The current setting is: SINK

>

- g** Do not change the PAUSE\_ENABLED variable, press the Enter key.

**PAUSE\_ENABLED**

PAUSE\_ENABLED is used to determine if the READY steps will run continuously or be paused out after executing. A NO setting allows the READY platform to run until completion of all the steps. A YES setting prompts the process to pause after each step is run. This pause allows time for the user to review the results and set a step COMPLETED/NEEDED before proceeding.

**Note:** Type HELP STEP\_STATUS for more information on setting the step status.

The current setting is: YES

>

SWUPGRADE variables for target READY:

| Variable Name  |   | Value        |
|----------------|---|--------------|
| -----          |   |              |
| TRACE_USER     | = | ME           |
| TRACE_DEVICE   | = | TELNSVR00033 |
| LOGS           | = | TRAP SWERR   |
| TO_CSP_LOAD    | = | 22           |
| PM_VERIFY_FILE | = | NONE         |
| PRINTER        | = | SINK         |
| PAUSE_ENABLED  | = | YES          |

Setup completed.

Enter GO to begin execution of steps.

**h** Commit the variable changes:

**> GO**

*Step SETUP\_ENV\_VARS completes.*

*If the CS 2000 - Compact is configured with Message Controller cards, step VERIFY\_SN\_PECs\_INFO runs. This step checks and prints the Message Switch software load and all the hardware in the Message Switch.*

*Step VERIFY\_LOGS\_INFO runs and completes. This step displays any log reports provided in environment variable LOGS. These logs should be checked periodically for front-end stability. Include or exclude any log(s) the user would like displayed.*

*Step DEVICE\_CHECK runs. This step verifies that all devices on the active CPU are in an OK, OFFLINE, or UNEQUIPPED status. These are acceptable states for SWACT. Any devices found in any other state are displayed.*

*Step TABAUDIT\_VERIFY\_TABLES runs. This step verifies that TABAUDIT has been executed and tables to be dumped and restored have been audited in the last thirty days.*

*If the CS 2000 - Compact is configured with Message Controller cards, steps DISPLAY\_PERIPHERAL\_LOAD\_NAMES, DISPLAY\_SPM\_LOADNAMES, DISPLAY\_PRL\_LOADNAMES, CHECK\_ISN\_PMS, and DISPLAY\_MS\_FW\_LOADS run. These steps print all the PM names, locations, and software load names for the PMs in the office, as well as the firmware loads in the Message Switch.*

- 3** If the CS 2000 - Compact is configured with Message Controller cards, step VERIFY\_PM\_LOAD\_NAMES runs. This step queries all the PMs with downloadable software and verifies that each PM is loaded with the load specified in PM\_VERIFY\_FILE. PM\_VERIFY\_FILE was set during step SETUP\_ENV\_VARS. This file is a PM to PM load cross reference. If the file is not available, or a PM is running a different load, the process stops. Correct the problem, type GO and press the Enter key.

*Step VERIFY\_PM\_LOAD\_NAMES completes.*

*If the CS 2000 - Compact is configured with Message Controller cards, steps LIUINV\_CHECK, C7LINK\_CHECK, CHECK\_LTCINV, and CHECK\_LCMINV run. These steps ensure that no LIU name has a LIUNO greater than 512, that all MSB7 and LIU7 PMs have field LINKNAME datafilled, that all DTCs datafilled in table LTCINV for CCS7 are datafilled correctly, and that LCMs have the amount of memory datafilled in table LCMINV and that the LCMs are in service.*
- 4** Step DISPLAY\_NOP\_USERS runs and completes.

*This step displays all NOP/MPC users and their status.*
- 5** Step DISPLAY\_DPP\_VERSION runs and completes.

*This steps displays DPP hardware and software information and DPP status.*
- 6** Steps SBA\_CHECK runs and completes.

*This step verifies that on an XA-Core machine if an upgrade is being performed to CSP16 and beyond, then all the backup volumes are configured only on IOP disks. No older disk types are supported as backup for the SBA streams on an XA-Core platform from CSP16 onwards.*
- 7** Step SBA\_VOLSIZE\_CHECK runs and completes.

*This step verifies that the size of the volumes that are configured as backup for SBA satisfy the minimal size requirements. This check will print out those stream-volume pairs whose backup volume sizes are below the minimal criterion that have been set.*
- 8** Step READY\_STATUS runs and completes.

*This step displays step state and status.*



- 9 Step READY\_COMPLETE runs and completes. Ensure that step READY\_STATUS indicates all steps are complete.  
**> QUIT**  
*This step reminds the user to quit the SWUPGRADE increment and QUIT from the switch after the READY program is completed.*
- 10 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Dumping a call processing application image

Complete this procedure the day of the ONP.

### **SITE — At the ACTIVECM window**

- 1 Enter the disk utilities level:
  - > **DISKUT**
- 2 Verify that there are at least 500 000 free blocks for an office image:
  - > **LV SD00IMAGE; LV SD01IMAGE**

```
> LV SD00IMAGE; LV SD01IMAGE
Volumes found matching the prefix SD00IMAGE:

NAME TYPE TOTAL FREE TOTAL OPEN ITOC LARGEST
 BLOCKS BLOCKS FILES FILES FILES FREE SEGMENT

SD00IMAGE STD 1638400 822665 0 0 0 822665
Total number of volumes matching prefix SD00IMAGE : 1.
Volumes found matching the prefix SD01IMAGE:

NAME TYPE TOTAL FREE TOTAL OPEN ITOC LARGEST
 BLOCKS BLOCKS FILES FILES FILES FREE SEGMENT

SD01IMAGE STD 1638400 814430 3 0 1 814430
Total number of volumes matching prefix SD01IMAGE : 1.
>
```

**Note:** If there is not enough space, determine if old images can be deleted. Use the DDF command to delete files. Refer to [DDF Example](#) for more information.

- 3 Dump the image to a disk volume using one of the following commands:  
If AUTODUMP is active for the office, enter  
**AUTODUMP MANUAL**  
or  
If AUTODUMP is not active for the office, enter  
**DUMP <image\_name> <disk\_vol> ACTIVE UPDATE  
VERBOSE NODE CM**  
where  
**image\_name**  
is the name of the file to create  
**disk\_vol**  
is sd00image or sd01image  
The dump can require two hours to complete. If you used the AUTODUMP MANUAL command, use the AUTODUMP STATUS command to view the new image name and the location of where the new image is stored.
- 4 Record the name of the image on a sheet of paper. If this upgrade is an ONP, it is important to have a current image as a backup in the event that the ONP fails. If this is a platform only MR upgrade, it is necessary to know the name of the image so it can be loaded during [Completing LDMATE \(Load inactive\) on page 2036](#).
- 5 Nortel recommends backing up the image. The backup procedure is documented in *Call Agent Fault Management*, NN10087-911 and is reproduced here for convenience under heading [Backing up an image](#).
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## DDF Example

The following figure shows an example of using the DDF command.

```
>diskut
```

```
Disk utility now active.
```

```
DISKUT:
```

```
>lf sd00image0
```

```
File information for volume SD00IMAGE0:
```

```
{NOTE: 1 BLOCK = 512 BYTES }
```

```

```

| FILE NAME          | O R I O O V FILE<br>R E T P L L CODE<br>G C O E D D<br>C N | MAX<br>REC<br>LEN | NUM OF<br>RECORDS<br>IN<br>FILE | FILE<br>SIZE<br>IN<br>BLOCKS |
|--------------------|------------------------------------------------------------|-------------------|---------------------------------|------------------------------|
| CSNW08BA           | I F                                                        | 0 1020            | 208457                          | 415286                       |
| .ITOC              | O F                                                        | 0 1024            | 1                               | 2                            |
| SCS08BA_WC_0131_CM | I F Y                                                      | 0 1020            | 213073                          | 424482                       |
| SCS07BK_WC_0131_CM | I F                                                        | 0 1020            | 196563                          | 391591                       |
| SCS07BK_WC_0128_CM | I F                                                        | 0 1020            | 196563                          | 391591                       |

```

```

```
>ddf CSNW08BA
```

```
Delete CSNW08BA from volume SD00IMAGE0?
```

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

```
>Y
```

```
File CSNW08BA has been deleted from volume SD00IMAGE0.
```

## Backing up an image

Use the following procedure to back up a call processing application image.

### ***At the active Call Agent Manager window (CORE0 or CORE1)***

- 1 Quit the Call Agent Manager interface:  

```
> QUIT ALL
```
- 2 Change directory to the location of the image. If the image was dumped to disk SD01, substitute sd01 for sd00 in the following figure.

```
[mtc@hostname mtc]$ cd /3PC/sd00/image0
[mtc@hostname image0]$ ls -lrt <IMG_TO_BACKUP>
-rw-r--r-- 1 root root 225820860 Feb 27 11:37 IMG_TO_
[mtc@hostname image0]$
```

- 3 Use the mount command to determine the IP addresses of the STORM units.

```
[mtc@ip_address mtc]$ mount
```

Determine which STORM unit provides sd00 and which provides sd01. This information is needed in [step 7](#).

```
[mtc@10.40.44.67 mtc]$ mount
/dev/ram0 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0622)
10.40.44.238:/nfsserv/3pc/mtc/tape0 on /TAPE type nfs (rw,rsiz=4096...
10.40.44.239:/nfsserv/3pc/mtc/tape1 on /TAPE1 type nfs (rw,rsiz=409...
10.40.44.238:/nfsserv/3pc/cs/sd00 on /3PC/sd00 type nfs (rw,rsiz=409...
10.40.44.239:/nfsserv/3pc/cs/sd01 on /3PC/sd01 type nfs (rw,rsiz=409...
10.40.44.238:/nfsserv/3pc/mtc/log0 on /var/log_mate type nfs (rw,rsi...
10.40.44.239:/nfsserv/3pc/mtc/log1 on /var/log type nfs (rw,rsiz=409...
```

#### ***At the CS 2000 Management Tools frame***

- 4 Insert a DVD-RW (write once DVD) in the CD-ROM tray. A rewritable DVD (DVD+RW) will not work. If the CS 2000 Management Tools server uses two Sun Microsystems Netra 240 machines, insert the DVD-RW into the active unit. The active unit is identified by a lit USER LED.

#### ***At a CS 2000 Management Tools terminal***

- 5 Log in as a maintenance level user such as the maint user. Root permissions are needed later in this procedure to write the DVD.
- 6 Change directory to /data and create a temporary directory to store the files:

```
$ cd /data
```

```
$ mkdir tmp
```

**Note:** Do not change directory into tmp now. The tmp directory will hold the data to backup.

- 7 Secure copy the files from the STORM unit to the /data/tmp directory created in [step 6](#). Enter the root password for the STORM unit when prompted.

```
$ scp "root@<stormip>:</path_to_files>"
/data/tmp
```

**Note:** There is a space before the /data/tmp argument.

**stormip**

is the IP Address of the STORM unit such as 10.40.44.238. Use the value determined in [step 3](#).

**/path\_to\_file**

is the absolute path to the files on the STORM unit to copy such as

/nfsserv/3pc/cs/sd00/image0/IMG\_TO\_BACKUP

**Example**

Copy an office image named S040210135002\_CM from SD00ADUMP0:

**\$ scp**

“root@<stormip>:/nfsserv/3pc/cs/sd00/adump0/S040210135002\_CM” /data/tmp

**Note:** The first time this command is issued, the secure copy program provides a prompt to exchange keys. Confirm the exchange with a “yes.” The root password for the STORM unit is needed.

*The secure copy program provides a progress indicator during the copy. Wait for the copy to complete and the \$ prompt to return.*

- 8 Rename the image file to end in .img1020:

```
$ cd /data/tmp
```

```
$ mv <IMG_TO_BACKUP> <IMG_TO_BACKUP>.img1020
```

- 9 Change directory to /data and make an ISO9660 image named dvdimage.iso with Rock Ridge extensions from the image:

```
$ cd /data
```

```
$ mkisofs -R -o /data/dvdimage.iso
/data/tmp/<IMG_TO_BACKUP>.img1020
```

**Note:** There is a space after /data/dvdimage.iso and before /data/tmp/<IMG\_TO\_BACKUP>.img1020

*Status is printed to the terminal:*

## Creating dvdimage.iso with mkisofs command

```
$ mkisofs -R -o /data/dvdimage.iso /data/tmp/<IMG_TO_BACKUP>.img1020
4.56% done, estimate finish Tue Feb 10 14:52:00 2005
9.11% done, estimate finish Tue Feb 10 14:52:00 2005
13.67% done, estimate finish Tue Feb 10 14:52:00 2005
...
95.67% done, estimate finish Tue Feb 10 14:52:05 2005
Total extents actually written = 109764
Total translation table size: 0
Total rockridge attributes bytes: 421
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 8000
109764 extents written (214 Mb)
$
```

### 10 Become the root user:

```
$ su - root
```

Provide the root password at the prompt.

### 11 Optionally verify the ISO9660 image:

```
lofiadm -a /data/dvdimage.iso /dev/lofi/1
mount -F hsfs /dev/lofi/1 /mnt
ls -asl /mnt
```

*The contents of the ISO 9660 image are displayed. These files will be written to the DVD-RW. Ensure the display looks similar to the following image.*

**Note 1:** If the `lofiadm` command reports the error `lofiadm: could not map file /data/dvdimage.iso to /dev/lofi/1: Device busy`, then the first loopback file driver is already in use. Re-enter the command and substitute `/dev/lofi/2` for `/dev/lofi/1`. Continue incrementing the number until the command succeeds and then use the successful value in the `mount` command.

**Note 2:** If the `mount` command reports the error `mount: /dev/lofi/1 is already mounted, /mnt is busy, or allowable number of mount points exceeded`, unmount the `/mnt` directory with the `umount /mnt` command and reenter the `mount` command.

**Listing contents of the ISO 9660 image**

```
lofiadm -a /data/dvdimage.iso /dev/lofi/1
mount -F hsfs /dev/lofi/1 /mnt
ls -asl /mnt
total 431996
 4 dr-xr-xr-x 2 root sys 2048 Apr 20 09:48 .
 2 drwxr-xr-x 33 root root 1024 Apr 20 11:16 ..
431990 -rw-r--r-- 1 maint maint 221178840 Apr 20 09:47 IMG_TO_BACKUP.img1
```

**12 Determine the name of the DVD-RW device:**

```
cdrw -l
```

*All optical disk devices are printed.*

**Determining the DVD-RW device name**

```
cdrw -l
Looking for CD devices...
 Node Connected Device Device type
-----+-----+-----
cdrom0 | TOSHIBA DVD-ROM SD-R6012 1033 | CD Reader/Writer
```

**Note:** If the command responds with “o CD writers found or no media in the drive, and the CS 2000 Management Tools server is a cluster then verify that the DVD-RW is placed in the active unit. The active unit is identified by a lit USER LED on the face of the unit.

**13** Optionally simulate (-S flag) recording the image to verify that the ISO 9660 image can be recorded on the DVD-RW. This step requires approximately 10 minutes:

```
cdrw -d <dvd_dev> -S -i /data/dvdimage.iso
```

**Example**

```
cdrw -d cdrom0 -S -i /data/dvdimage.iso
```

*The CD-ROM tray ejects after this simulation.*

Close the CD-ROM tray and continue this procedure to write the DVD-RW.

**14** Record the image. This step requires approximately 10 minutes:

```
cdrw -d <dvd_dev> -i /data/dvdimage.iso
```

**Example**

```
cdrw -d cdrom0 -i /data/dvdimage.iso
```



*If the error response Media in the device is not writable is returned, verify that the CD-ROM tray is closed.*

*Approximately two minutes pass before progress is printed to the screen. After the first one percent is written, each additional percent requires about two seconds.*

#### CDRW command progress

```
cdrw -d cdrom0 -i /data/dvdimage.iso
Initializing device...done.
Preparing to write DVD
Writing track 1 ... 99 %
```

*Approximately nine minutes pass before the command completes.*

```
done.
done.
Finalizing (Can take up to 4 minutes)...done.
$
```

*The CD-ROM tray on the CS 2000 Management Tools server ejects.*

Close the CDROM tray and continue this procedure to verify the contents of the DVD-RW.

- 15** Check that ISO 9660 image recorded correctly:

```
ls -asl /cdrom/cdrom0
```

*The contents of the DVD-ROM are printed.*

- 16** Unmount the DVD-RW, eject it, and exit from root privilege:

```
eject cdrom
```

If the ISO 9660 image was verified with the lofiadm command, remove the loopback file driver device:

```
umount /mnt
```

```
lofiadm -d /dev/lofi/1
```

**Note:** If /dev/lofi/2 was used above, substitute /dev/lofi/2 in this command.

Exit from root privilege:

```
exit
```

```
$
```

*The dollar sign command prompt returns.*

- 17** Use the rm command to erase the image so the volume does not fill up:

```
$ rm /data/tmp/<IMG_TO_BACKUP>.img1020
$ rm /data/dvdimage.iso
```

***At the CS 2000 Management Tools server***

- 18** Remove the DVD-RW from the tray and close the tray. Label the DVD-RW.
- 19** Store the DVD-RW for each office procedure.
- 20** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Listing FTP users

---

Complete this procedure at least two days before the ONP.

After the ONP (or a norestartswact or restartswact) all FTP user definitions, except 'admin', are lost. Use this procedure to list and print the FTP users prior to the ONP and reinstate those users after the upgrade using [Restoring FTP users on page 2064](#).

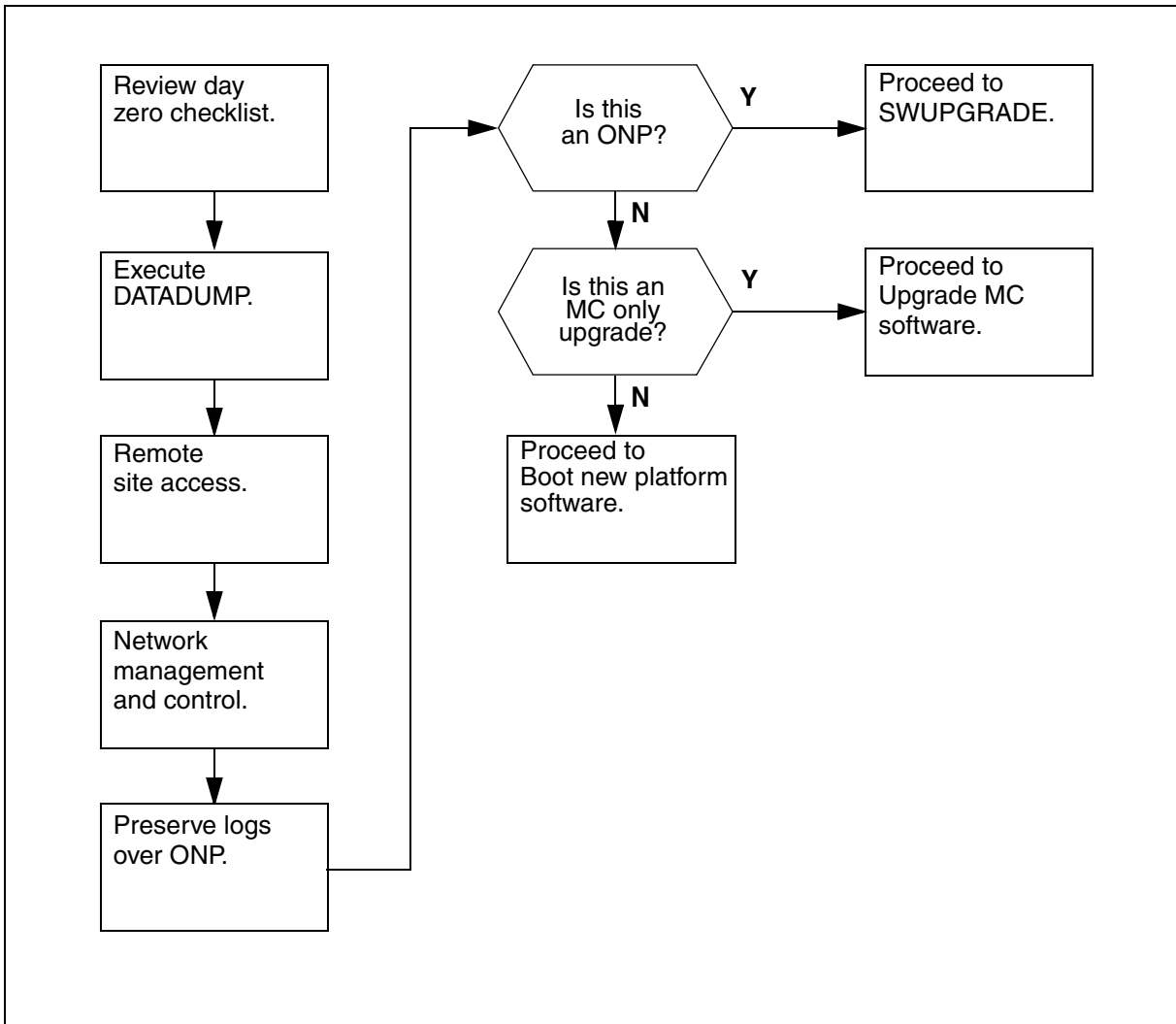
### ***ACT — At the ACTIVECM window***

- 1 Go to the FTP level and type:  
**FTP**
- 2 List the FTP users by typing:  
**SHOWSVUSERS**
- 3 Print the user list and restore the user identities after the ONP.
- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Site responsibilities the day of the software delivery

Complete this section on the day of the ONP. Complete the following procedures before the Software Delivery Applicator contacts the site to begin the scheduled ONP.

### Site responsibilities the day of the software delivery



---

## Using the day zero checklist

---

### ***SITE — At the ACTIVECM window***

- 1 Verify that all pre-application activities are complete. This includes the [Site preparation overview on page 1861](#), [Performing TABAUDIT on page 1897](#), and [Restoring call processing application files on page 1886](#).
- 2 Verify the ONP start time. Either Nortel or the operating company established this start time during the site preparation phase. To verify this time, refer to the software delivery site-ready reports or contact your next level of support. If requesting a change to the start time contact your Nortel regional customer representative.
- 3 Verify front-end stability by ensuring the last REx test passed.
- 4 Take an office IMAGE and back it up. Refer to [Dumping a call processing application image on page 1909](#). Store the copy of the office IMAGE for at least 30 days following the ONP.
- 5 Ensure you have defined and tested the Test Call Scripts. The test call plan must be ready before activation of the new software load.
- 6 Patches and process files downloaded for the ONP must remain where they are. Do not erase these files.
- 7 Check for a SOC file <cli>\_SCF or <cli>\$SCF in SFDEV (or download device). If a SOC file is present, copy the file to a disk drive.

**Note:** For information on installing the right-to-use (RTU) SOC password file, refer to the *Software Optionality Control User's Manual*, 297-8991-900.

- 8 Verify that SFDEV is clear of unnecessary files. (This is to clear store file device space for ONP work.)
- 9 Ensure that no peripheral hardware or software changes, including retrofits, extensions, or maintenance activities, are scheduled to take place during the ONP. Any affected hardware must be made installation busy (INB), in both the host and remote offices.

**Note:** Recently removed hardware must have all associated software removed as well. Peripheral hardware that is not in the in-service or offline state may jeopardize the ONP.

- 10** For offices equipped with a CS 2000 Core Manager or Core and Billing Manager (CBM), ensure the SuperNode Billing Application (SBA) is not undergoing backup or recovery. The SBA system must be operating in normal mode during the ONP. If necessary, refer to *CS 2000 Core Manager Fault Management*, NN10082-911 or *Core and Billing Manager 850 Fault Management*, NN10351-911 for alarm clearing procedures.
- 11** Set up user interfaces and ensure they are available.
- 12** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Executing DATADUMP

### ATTENTION

Allow sufficient time to run the DATADUMP. Depending on the office, DATADUMP can require eight hours or more. Failure to allow sufficient time may impact the application start time.

### **SITE — At the ACTIVECM window**

- 1 Record the datadump on disk or in the storefile device (SFDEV):

> **RECORD START ONTO <device>**

#### **device**

is a disk device such as SD00TEMP or is the storefile device, SFDEV

**Note:** The name of the created file is RECORDFILE.

- 2 Execute the DATADUMP:

> **BCSUPDATE;DATADUMP**

*Several confirmation prompts are presented. Confirm each prompt with yes.*

```
Data Dump for CO: OFC_CLLI Date: MAY 11, 2005 13:36:34
=====
Do you want to display INB, MB and RES trunks?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display 1MR registers?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display INB lines?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display tables?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
Do you want to display hardware?
Please confirm ("YES", "Y", "NO", or "N"):
>YES
```

*The datadump runs and completes.*

- 3 When the DATADUMP completes, quit to the CI level:  
**> QUIT ALL**
- 4 Stop the recording:  
**>RECORD STOP ONTO <device>**
- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Providing remote site access

At the established ONP start time, the telephone operating company is responsible for providing remote site access to the Nortel Applicator. If not provided to Nortel in advance, be prepared to furnish all the necessary information for this task.

### **SITE**

- 1 Ensure there will be uninterrupted communication with the Applicator during the ONP. Nortel recommends using Foreign Exchange (FX) voice and data lines for this purpose.
  - Two site connections — One connection is used for the active terminal (controlling the ONP procedure) and the second is used for tracing. If IOC or IOM equipment is available, Nortel recommends that one site connection reside on one unit of the device, and the other connection on the second unit.
  - One reliable voice number is required.

**Note 1:** If these services are unavailable, contact Nortel support personnel to determine if the available services are sufficient.

**Note 2:** Foreign Exchange (FX) numbers are recommended for both voice and data lines for Applicator remote site access.

- 2 Ensure two usernames and passwords with at least the following settings are provided for the ONP:
  - COMCLASS — ALL
  - PRIVCLASS — ALL
  - STACKSIZE — 10000
  - PRIORITY — 4

3



#### **DANGER**

Prolonged software upgrade time

Failure to provide working and reliable remote access can cause problems during the software upgrade.

---

## Network management control

---

**ATTENTION**

If necessary, contact your network maintenance support for assistance with these steps.

If network management code blocking is active before the ONP, the code blocking must be restored after the ONP is complete.

***SITE — At the ACTIVECM window***

- 1 Make a list of all active code controls before the ONP to aid in restoration of code blocking.  
**> MASSCALL LIST CGAP ACODE ALL**
- 2 Code blocking must be restored after the ONP. Make arrangements with network maintenance personnel for assistance.
- 3 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Preserving logs over ONP

---

Logs that are suppressed or have a threshold set are configured for each site. Unless these logs are datafilled in table LOGCLASS, the settings will not be restored in the new call processing software load. Follow this procedure to determine which log reports are specially configured and how to provision table LOGCLASS.

### ***SITE — At the ACTIVECM window***

- 1 Determine which log reports are specially configured:
  - > **LOGUTIL**
  - > **LISTREPS SPECIAL**
  - > **QUIT**
- 2 Access table LOGCLASS:
  - > **TABLE LOGCLASS**
- 3 Determine if the log reports are already datafilled in table LOGCLASS:

The field for threshold is spelled THRESHLD. The first command lists all tuples with a threshold that does not equal zero.

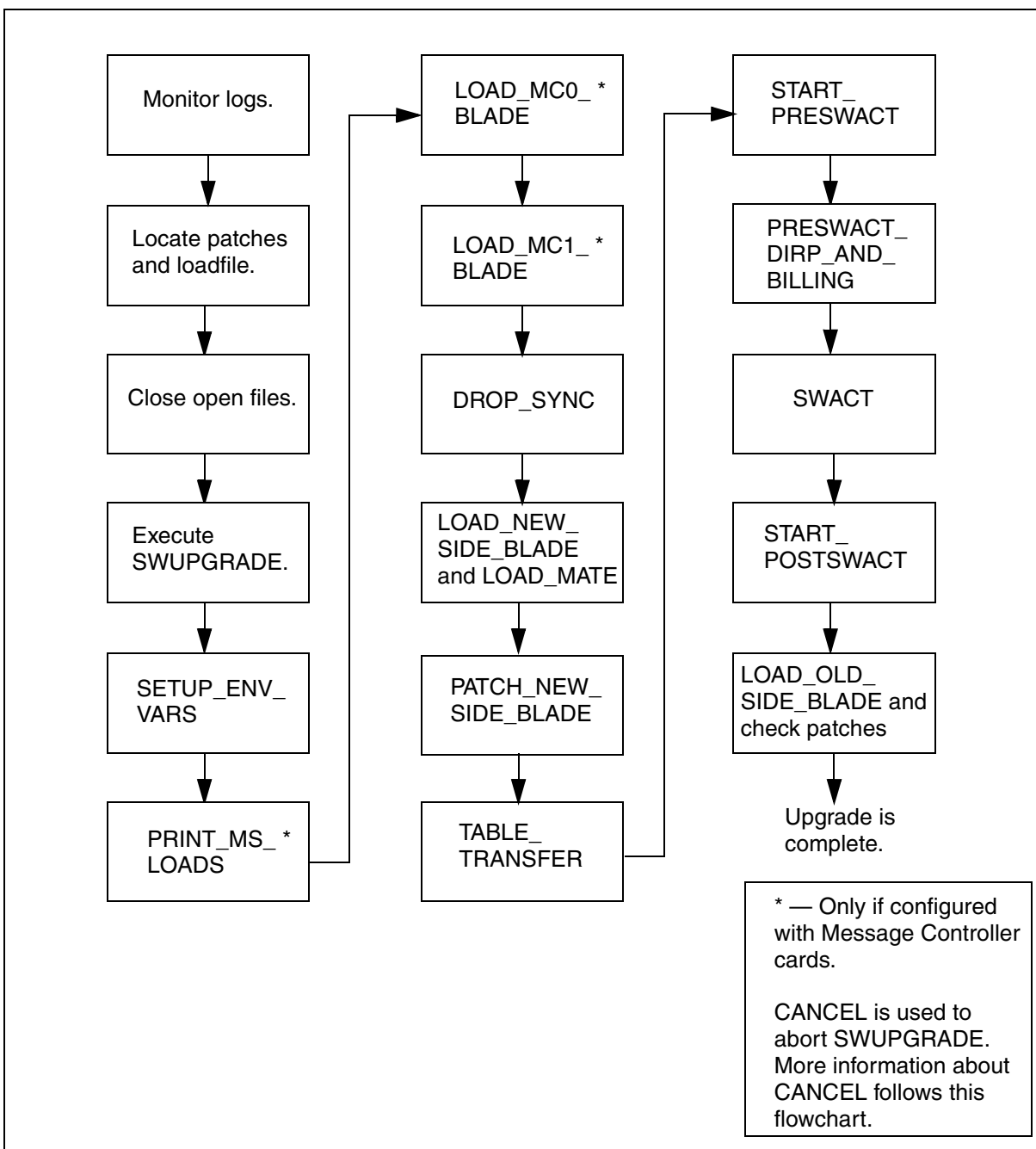
  - > **LIS ALL (THRESHLD NE '0')**
  - > **LIS ALL (SUPPRESS NE N)**
- 4 If the output from [step 3](#) does not equal the output from [step 1](#), change as necessary to match the output from the LISTREPS output:
  - > **RWOK ON**
  - > **POS <log\_name>**
  - > **CHA <THRESHLD or SUPPRESS> <value or Y>**
  - > **YES**

**log\_name**  
is the log report name such as TRKMEM listed in the LISTREPS output

**value**  
is an integer value listed in the LISTREPS output
- 5 Repeat [step 4](#) for each required change and then exit the LOGUTIL level:
  - > **QUIT**
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## SWUPGRADE

This section contains procedures that automate many of the upgrade tasks. Please read the important information following this flowchart.



Before proceeding with the procedures in this SWUPGRADE section of this document, complete the procedures in sections [Interface setup on page 1850](#), [Site preparation phase on page 1858](#), and [Site responsibilities the day of the software delivery on page 1919](#).

## Software

The CS 2000 Management Tool reads CD-ROMS and DVDs.

Software for the Call Agent platform is available on CD-ROM as a package for the CS 2000 Management Tools server. The software package is installed with the platform\_load\_install.sh tool on the CS 2000 Management Tools server. Software for the Message Controller cards is automatically installed in all offices even though not all offices have Message Controller cards. If the software is not installed, refer to [Applying platform software for Call Agent and Message Controller on page 1864](#).

The software image for the call processing application is taken from DVD on the CS 2000 Management Tools server, and then transferred to the Call Agent card file system. It is then imported with the IMPORT command at the MAP to make the new image available for booting. If the upgrade software load is not available on one of the disk volumes, refer to [Restoring call processing application files on page 1886](#).

If the office is configured with Message Controller cards, then a Message Switch software image is required for the Message Switch. This software image is taken from DVD on the CS 2000 Management Tools server at the same time as the upgrade call processing application image. Once the Message Switch software is transferred, it is imported to one of the disk volumes. If the Message Switch software load is not available on one of the disk volumes, refer to [Peripheral Module upgrade on page 999](#).

## CANCEL command

The CANCEL command is issued on the active terminal to abort SWUPGRADE. Instructions for the rollback are printed to the device that is selected as the TRACE\_DEVICE.

To ensure that the TRACE\_DEVICE is prepared to receive messages, enter command TRACECI TEST 'TESTMESSAGE' at the active terminal. The TRACE\_DEVICE is still connected if TESTMESSAGE is printed to it.

---

## Locating patches and loadfile

---

Call processing application patch files were loaded into the first device listed in table PADNDEV during the preparation phase. Use this procedure to verify the location of the patch files. The location is a required parameter during the SETUP\_ENV\_VARIABLES step of the software upgrade.

The call processing application image was retrieved from DVD, transferred, and stored during the preparation phase. Verify the location of the image.

### ***SDE — At the ACTIVECM window***

- 1 Determine the default call processing application patch file location provisioned in table PADNDEV:  
  
    > **TABLE PADNDEV; LIS ALL; QUIT**
- 2 Make a note of the location. This value is a required parameter for the software upgrade.
- 3 Enter the disk utilities level and list the disk volumes:  
  
    > **DISKUT; LV**
- 4 List the contents of the volume with the upgrade call processing software image:  
  
    > **LF <volume\_name>**  
        **volume\_name**  
        is a string like SD00IMAGE
- 5 Make a note of the image file name. This value is a required parameter for environment variable LDMATE\_IMAGE.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

If the CS 2000 - Compact is configured with Message Controller cards, check the Message Switch software loads and ensure that both Message Switches are running the same load and the load is specified in the *Peripheral Module Software Release Document*.

### ***SDE — At the ACTIVECM window***

- 1 Remote login to Message Switch 0:  
  
    > **REMLOGIN MS 0**  
  
    *The terminal is now active on Message Switch 0.*

**2** Issue the IMAGENAME command:

**MS0> IMAGENAME**

*The software load running in the Message Switch is displayed.*

```
MS-U BCS 57 AV built on 2005-MAR-28 at 12:23:00
using mux22av
LOAD: NIL.000
LAYER: BAS.23.0.AV
LAYER: TL.22.0.AV
```

**3** Logout of the Message Switch:

**MS0> REMLOGOUT**

**4** Ensure that the software load displayed (mux222av in the example) is the correct Message Switch load for this release.

Use the REMLOGIN command to log into Message Switch 1, issue the IMAGENAME command, and REMLOGOUT. Ensure that the two Message Switches are running the same software load.

**5**



**CAUTION**

**Possible service interruption**

If the Message Switch is not loaded correctly, escalate immediately. Incorrect MS loads will cause subsequent AutoONP processes to fail and will jeopardize the software delivery application.

This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Closing open files

Open files can have data in cache rather than written to storage. Follow this procedure to ensure that data is written to storage.

### **SDE — At the ACTIVECM window**

- 1 Determine if there are any open files:

**> DISKUT; LV**

DISKUT:

Volumes found:

| NAME       | TYPE | TOTAL<br>BLOCKS | FREE<br>BLOCKS | TOTAL<br>FILES | OPEN<br>FILES |
|------------|------|-----------------|----------------|----------------|---------------|
| SD00IMAGE  | STD  | 1638400         | 269821         | 4              | 0             |
| SD00IMAGE1 | STD  | 1638400         | 718476         | 3              | 0             |
| SD00TEMP   | STD  | 409600          | 409498         | 4              | 0             |

- 2 For billing and Device Independent Recording Package (DIRP) files, rotate the volumes:

**> MAPCI;MTC;IOD;DIRP**

**> ROTATE <subsystem>**

**> QUIT ALL**

#### **subsystem**

is a billing or DIRP subsystem such as AMA

- 3 For regular files, determine the name of the open file and close the file:

**> LF <volume\_name>**

**> FILECLOSE <file\_name> <volume\_name>**

#### **volume\_name**

is the name of the volume with open files from [step 1](#)

#### **file\_name**

is the name of the file to close returned by the LF command

- 4 For assistance with closing open files, contact Nortel support personnel.

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Executing SWUPGRADE

The Automated One Night Process (AutoONP) maintains a list of steps to execute. When a step fails or requires user input, the process stops, the user responds to the problem and types GO to continue until all steps are executed.

Help for the SWUPGRADE level commands is available by typing HELP while in the SWUPGRADE level.

Step DOWNLOAD\_FILES reminds the Software Delivery Engineer to retrieve the bulletins file. If the bulletins file is not available in SFDEV, the software upgrade will fail.

The number of steps in the AutoONP process is determined by the CS 2000 - Compact configuration. If the CS 2000 - Compact is configured with Message Controller cards, there are more steps.

### SWUPGRADE CA steps

| without Message Controllers | with Message Controllers |
|-----------------------------|--------------------------|
| SETUP_ENV_VARS              | SETUP_ENV_VARS           |
| NOTIFY_USERS                | NOTIFY_USERS             |
| SET_LOGIN_BANNER            | SET_LOGIN_BANNER         |
| DOWNLOAD_FILES              | DOWNLOAD_FILES           |
| READ_BULLETINS              | READ_BULLETINS           |
| VERIFY_DEVICES              | VERIFY_DEVICES           |
| PRINT_PARMs_AND_SAVE        | PRINT_PARMs_AND_SAVE     |
| CHECK_LOGS_1                | CHECK_LOGS_1             |
| STOP_JOURNAL_FILE           | STOP_JOURNAL_FILE        |
|                             | PRINT_MS_LOADS           |
| DISABLE_PRSM_AUDIT_ACT      | DISABLE_PRSM_AUDIT_ACT   |
|                             | LOAD_MC0_BLADE           |
|                             | LOAD_MC1_BLADE           |

**SWUPGRADE CA steps**

| <b>without Message Controllers</b> | <b>with Message Controllers</b> |
|------------------------------------|---------------------------------|
| DROP_SYNC                          | DROP_SYNC                       |
| LOAD_NEW_SIDE_BLADE                | LOAD_NEW_SIDE_BLADE             |
| LOAD_MATE                          | LOAD_MATE                       |
| PATCH_NEW_SIDE_BLADE               | PATCH_NEW_SIDE_BLADE            |
| MATELINK_RTS                       | MATELINK_RTS                    |
| UPDATE_STEPS_AND_VARS              | UPDATE_STEPS_AND_VARS           |
| CHECK_NEW_LOAD                     | CHECK_NEW_LOAD                  |
| SET_DATE_AND_LOGMSG                | SET_DATE_AND_LOGMSG             |
| CHECK_LOGS_2                       | CHECK_LOGS_2                    |
| CLEAR_TRAPINFO                     | CLEAR_TRAPINFO                  |
| TRANSFER_DEVICES_INFO              | TRANSFER_DEVICES_INFO           |
| TRANSFER_PARM_VALUES               | TRANSFER_PARM_VALUES            |
|                                    | MS_CHECK                        |
| DISABLE_AUTOIMAGE                  | DISABLE_AUTOIMAGE               |
| SET_OFFICE_TUPLES                  | SET_OFFICE_TUPLES               |
| SET_PADNDEV                        | SET_PADNDEV                     |
| SEND_PATCHES                       | SEND_PATCHES                    |
| APPLY_PATCHES                      | APPLY_PATCHES                   |
| CHECK_LOGS_3                       | CHECK_LOGS_3                    |
| RESTORE_PADNDEV                    | RESTORE_PADNDEV                 |
| TABLE_TRANSFER                     | TABLE_TRANSFER                  |
| TABXFR_REPORT                      | TABXFR_REPORT                   |
| CHECK_LOGS_4                       | CHECK_LOGS_4                    |
| START_PRESWACT                     | START_PRESWACT                  |

**SWUPGRADE CA steps**

| <b>without Message Controllers</b> | <b>with Message Controllers</b> |
|------------------------------------|---------------------------------|
| PRESWACT_DIRP_AND_BILLING          | PRESWACT_DIRP_AND_BILLING       |
| PRINT_SPMS_INDICES                 | PRINT_SPMS_INDICES              |
| GET_FIRST_SWACT_AGREEMENT          | GET_FIRST_SWACT_AGREEMENT       |
| PREPARE_FOR_SWACT                  | PREPARE_FOR_SWACT               |
| STATUSCHECK                        | STATUSCHECK                     |
| CHECK_LOGS_5                       | CHECK_LOGS_5                    |
| TRANSFER_TIMINGS                   | TRANSFER_TIMINGS                |
| SWACT                              | SWACT                           |
| DISPLAY_DATE                       | DISPLAY_DATE                    |
| RECOVER_DIRP_AND_BILLING           | RECOVER_DIRP_AND_BILLING        |
| PERFORM_TEST_CALLS_1               | PERFORM_TEST_CALLS_1            |
| START_POSTSWACT                    | START_POSTSWACT                 |
| RESTART_OLD_LOAD                   | RESTART_OLD_LOAD                |
| DRTIME_PRINT                       | DRTIME_PRINT                    |
| PERFORM_TEST_CALLS_2               | PERFORM_TEST_CALLS_2            |
| LOAD_OLD_SIDE_BLADE                | LOAD_OLD_SIDE_BLADE             |
| SYNC_SWITCH                        | SYNC_SWITCH                     |
| FINISH_POSTSWACT                   | FINISH_POSTSWACT                |
| RESTORE_PARMS                      | RESTORE_PARMS                   |
| RESET_DEVICES                      | RESET_DEVICES                   |
| COMPLETE_NEW_LOAD_INIT             | COMPLETE_NEW_LOAD_INIT          |
| RESET_LOGIN_BANNER                 | RESET_LOGIN_BANNER              |
| DUMP_NEW_LOAD                      | DUMP_NEW_LOAD                   |

**SWUPGRADE CA steps**

| without Message Controllers | with Message Controllers |
|-----------------------------|--------------------------|
| RESUME_REX_TEST             | RESUME_REX_TEST          |
| START_JOURNAL_FILE          | START_JOURNAL_FILE       |
| PRINT_SWUPGRADE_REPORT      | PRINT_SWUPGRADE_REPORT   |
| STOP_RECORD                 | STOP_RECORD              |
| UPGRADE_COMPLETE            | UPGRADE_COMPLETE         |

***SDE — At the ACTIVECM window***

- 1 Enter the software upgrade level:  
> **SWUPGRADE CA**
- 2 Press return twice to display the current office header message.  
Note the office header message for environment variable  
INACT\_LOGMSG.
- 3 Begin the upgrade:  
> **START**
- 4 Proceed to [SETUP\\_ENV\\_VARS](#).

**Additional information****Inserting, deleting, or modifying steps**

To allow customization of the AutoONP, SWUPGRADE allows the user to change the steps that are normally performed. Commands are available to insert, delete, or modify the AutoONP steps as follows.

- INSERT adds a new step or copies an existing step into another location in the step list.
- DISP STEPS prints the step list.
- REMOVE removes any step or pause that was added.
- OVERRIDE disables the execution of a step.
- PAUSE halts the AutoONP process before or after a step.
- RESUME resumes the process after pausing.

**Using the BULLETINS file**

The BULLETINS file is maintained by Nortel Global Software Delivery and is used to provide as much automation as possible when performing the application bulletins and workarounds. Since

application bulletins and workarounds vary depending on the from and to software loads, it is recommended that the BULLETINS file and all bulletins and workarounds be reviewed before starting the AutoONP. When required, follow and manually execute bulletins and workarounds during the AutoONP.

#### **ATTENTION**

The BULLETINS file is a critical file that must be located in SFDEV for execution during the AutoONP.

If this file is missing from SFDEV or if it is named incorrectly, the AutoONP will fail. For assistance with the BULLETINS file contact the Global Software Delivery hotline for your market.

Step DOWNLOAD\_FILES, towards the beginning of the AutoONP process, will remind the user to download the BULLETINS file (along with other required files). If desired, print a hard copy of the BULLETINS file and review the file contents.

Step READ\_BULLETINS will read (that is, execute) the BULLETINS file during the AutoONP.

### **Using the CANCEL command**

The CANCEL command is used to terminate or abort the software upgrade and halt the execution of the SWUPGRADE process at any time during the AutoONP. This command reverts all SWUPGRADE steps and returns the switch to its original state.

### **Getting help on AutoONP steps**

The SWUPGRADE increment is used to perform the AutoONP. At any time within this increment you may type HELP for a list of the commands available. Also, the HELP command has options to obtain information about a command syntax, specific step, or variable as follows.

- HELP displays a brief description of the SWUPGRADE increment and a list of the available CI commands.
- HELP <swupgrade command> displays a brief description and syntax of the command.
- HELP STEP <step> displays a brief description of a step's functionality.
- HELP VAR <variable> displays a brief description and the current value of the variable.

For additional information about SWUPGRADE commands, refer to section "SWUPGRADE summary" of Appendix A in *Software Delivery One Night Process Software Delivery Procedures*, 297-8991-303.

---

## SETUP\_ENV\_VARS

---

### **SDE — At the ACTIVECM window**

- 1 Set variable TRACE\_USER to the user name logged in for TRACE\_DEVICE:

#### **TRACE\_USER (no default)**

Holds the USER name on whose console output messages are printed. Changing the value of this variable changes the value of the TRACE\_DEVICE variable, and causes the output to be redirected to the new USER device.

Value: <user\_name> where <user\_name> is the username of the trace user

**Note:** For clarity, it is recommended that you set this variable to the user logged in to the TRACE\_DEVICE.

The user must be logged in when this variable is set. The current setting is: <none>

- 2 It is recommended that you do not change the TRACE\_DEVICE variable. Press the Enter key.

#### **TRACE\_DEVICE**

Holds the device name on which output messages are printed. Changing the value of this variable causes the output to be redirected to the new device.

Value: <trace\_device\_name> - a string, such as MAP

**Note:** For clarity, it is recommended to set this variable to a device other than the currently logged on terminal.

The current setting is: <none>

*The selected device indicates "This device is selected for TRACing."*

- 3 Do not change the PRINTER variable. Press the Enter key.

#### **PRINTER**

Holds the name of the printer on which output messages are recorded. The printer echoes all output sent to the trace device. Changing the value of this variable causes the recording to be directed to the new device.

Value: <printer name> or SINK where <printer name> is a device datafilled in table TERMDEV. Choosing SINK means choosing no printer output.

> **SINK**

- 4 Do not change the LOGS variable. Press the Enter key.

**LOGS**

Holds the names of the logs that are checked by the LOGS step. More than one log can be specified by entering log names separated by a blank.

**Example**

SWERR TRAP — Check traps and swerrs. Display a message if traps or swerrs are recorded.

The current setting is: TRAP SWERR

- 5 Enter the INACT\_LOGMSG variable. Use the existing office header except update the new job order number, software level, and current date.

**INACT\_LOGMSG**

Holds the log message that will be displayed on the inactive side of the switch.

**Example**

\*\*\* H1234 Office\_Name SN000xxx 17/MAR/2005 \*\*\*

- 6 Enter the LDMATE\_IMAGE variable:

**LDMATE\_IMAGE**

Holds the volume name and filename used to load the inactive unit.

**Example**

SD00IMAGE0 CSN00xxBG

**Note:** The software checks to verify that a file with the specified name exists on the volume.

- 7 Enter the PADNDEVS variable. The default value is SFDEV. If the call processing application files were loaded into SFDEV, press the Enter key. Otherwise, enter up to three device names if the patches were loaded into a location other than SFDEV during procedure [Transferring call processing application patch files](#).

- 8 Do not change the TABXFR\_STOPIF variable. Press the Enter key.

**TABXFR\_STOPIF**

Determines the threshold for the maximum number of failed tables allowed before halting TABXFR.



- 9 Do not change the TABXFR\_LIMIT variable. Press the Enter key.
- TABXFR\_LIMIT**  
Determines the threshold for the maximum number of tuple failures allowed before halting TABXFR.
- 10 Do not change the TABXFR\_INITIAL\_PRINT variable. Press the Enter key.
- TABXFR\_INITIAL\_PRINT**  
Determines the time interval for printing a single message containing the current table name.
- 11 Set the TABXFR\_INTERVAL\_PRINT variable to 30 seconds:
- TABXFR\_INTERVAL\_PRINT**  
Determines the time interval for printing regular table transfer status messages. This is particularly useful for large tables.
- > 30 SECS
- 12 Do not change the SPMS\_OPTION variable. Press the Enter key.
- SPMS\_OPTION**  
Holds the date, or number of days, to generate the SPMS (Switch Performance Monitoring System) indices.
- 13 Do not change the DRTIME\_REPORT variable. Press the Enter key.
- DRTIME\_REPORT**  
Determines if the DRTIME report should be printed before SYNC. DRTIME provides statistics on the TABXFR process. Normally this information is not used unless this information is requested.
- 14 Set the DUMP\_NEW\_LOAD variable:
- DUMP\_NEW\_LOAD**  
Determines if an image dump of the new load should be taken.
- > NO
- Note:** If the value of this variable is set to NO, the Site is responsible for manually taking an image of the new software load immediately after the AutoONP is complete.

*The variables are printed to the terminal.*

WARNING: An ACTIVE VOLUME must be datafilled in table  
IMAGEDEV to use AUTODUMP.

SWUPGRADE variables for target CA:

| Variable Name         | Value                  |
|-----------------------|------------------------|
| TRACE_USER            | = USERNAME             |
| TRACE_DEVICE          | = TELNSVR00019         |
| PRINTER               | = SINK                 |
| LOGS                  | = TRAP SWERR           |
| INACT_LOGMSG          | = INACT_LOGIN_MESSAGE  |
| LDMATE_IMAGE          | = SD00IMAGE0 CSN00xxBG |
| PADNDEVS              | = SFDEV                |
| TABXFR_STOPIF         | = 1                    |
| TABXFR_LIMIT          | = 25                   |
| TABXFR_INITIAL_PRINT  | = 30 SECS              |
| TABXFR_INTERVAL_PRINT | = 30 SECS              |
| SPMS_OPTION           | = NONE                 |
| DRTIME_REPORT         | = NO                   |
| DUMP_NEW_LOAD         | = NO                   |

**15** To proceed with the upgrade, enter

**> GO**

Monitor messages on the TRACE\_DEVICE.

*Response:*

*Step NOTIFY\_USERS automatically runs. The notified usernames and environment variables print to the terminal.*

*Step SET\_LOGIN\_BANNER automatically runs.*

*Step DOWNLOAD\_FILES begins, reminds the SDE to download optional application and BULLETINS file and then waits for the SDE to enter the GO command.*

- 16** After downloading any required files, type

> **GO**

and press the enter key.

| <b>If a BULLETINS file</b> | <b>Do</b>                                          |
|----------------------------|----------------------------------------------------|
| is located in SFDEV        | it is read and executed during step READ_BULLETINS |
| is not located in SFDEV    | the step fails                                     |
| is not needed              | <a href="#">step 17</a>                            |

- 17** To override step READ\_BULLETINS, type

> **OVERRIDE READ\_BULLETINS**

and press the Enter key.

| <b>If</b>                               | <b>Do</b>                                                                    |
|-----------------------------------------|------------------------------------------------------------------------------|
| you want to confirm the override        | type <b>Y</b> and press the Enter key. Continue to <a href="#">step 19</a> . |
| you do not want to confirm the override | type <b>N</b> and press the Enter key. Continue to <a href="#">step 18</a> . |

- 18** Refer to the following table to determine your next action.

| <b>If</b>                                 | <b>Do</b>                                                                                                                                                                                                                   |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you want to continue the procedure        | <a href="#">step 19</a>                                                                                                                                                                                                     |
| you do not want to continue the procedure | cancel the upgrade by performing procedure <a href="#">Revert and Abort</a> or <a href="#">Revert and Abort for offices with Message Controller cards</a> . After the upgrade is cancelled, go to <a href="#">step 20</a> . |

- 19** To continue the procedure, enter

> **GO**

*Response:*

*The following steps automatically run:*

- **VERIFY\_DEVICES**
- **PRINT\_PARDS\_AND\_SAVE**
- **CHECK\_LOGS1**

**Note:** Display the contents of all logs listed. Use the **DISPLAY LOG <log\_name> ALL <ACT or INACT>** command.

- *STOP\_JOURNAL\_FILE*

---

**If the CS 2000 - Compact****Do**

is equipped with Message  
Controller cards

step [PRINT\\_MS\\_LOADS](#)  
automatically runs after step  
STOP\_JOURNAL\_FILE

is not equipped with Message  
Controller cards

step DISABLE\_PRSM\_  
AUDIT\_ACT automatically runs  
after step STOP\_JOURNAL\_FILE  
This step has several substeps.  
When step DISABLE\_PRSM\_  
AUDIT\_ACT completes, proceed  
to step [DROP\\_SYNC](#)

---

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

## Additional information

If any variables require correction, use the SET command to change the variable. If the variable consists of two or more words such as SD00PATCH and SD01PATCH, use quotation marks to enclose the words.

**Example**

```
SET PADNDEVS 'SFDEV SD00PATCH SD01PATCH'
```

Variables can be displayed at any time with the DISP VAR command.

**Example**

```
DISP VAR PADNDEVS
```

## PRINT\_MS\_LOADS

### ATTENTION

Steps PRINT\_MS\_LOADS, [LOAD\\_MC0\\_BLADE](#) and [LOAD\\_MC1\\_BLADE](#) run only if the CS 2000 - Compact is configured with Message Controller cards. If the CS 2000 - Compact is not configured with Message Controller cards, continue to step [DROP\\_SYNC](#).

### **SDE — At the ACTIVECM window**

- 1 Step PRINT\_MS\_LOADS runs.

Starting step PRINT\_MS\_LOADS.  
Please note that the displayed information corresponds to the BASE layer of the MS load.  
Load in MS 0 = MS-U23BC  
Load in MS 1 = MS-U23BC

Please check the above MS loads for correctness.  
Step PRINT\_MS\_LOADS is complete.

The SWUPGRADE process has paused. Enter GO.

- 2 If the value reported is not correct, do not proceed. Contact Nortel support personnel immediately.
- 3 Type GO and press the Enter key.  
*Step PRINT\_MS\_LOADS completes.*  
*Step DISABLE\_PRSM\_AUDIT\_ACT runs and completes.*
- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## LOAD\_MC0\_BLADE

### ATTENTION

Steps [PRINT\\_MS\\_LOADS](#), [LOAD\\_MC0\\_BLADE](#) and [LOAD\\_MC1\\_BLADE](#) only run if the CS 2000 - Compact is configured with Message Controller cards. If the CS 2000 - Compact is not configured with Message Controller cards, continue to step [DROP\\_SYNC](#).

### **SDE — At the ACTIVECM window**

#### **1 Step LOAD\_MC0\_BLADE runs.**

Starting step LOAD\_MC0\_BLADE.

Upgrade load of MC 0 at the SAM21 EM GUI by using the following manual procedure:

- 1) At the MAPCI;MTC;MS map level, verify that MS 1 is the master MS.
- 2) If MS 1 is not the master, perform a SWMAST. If performed, soak 10 minutes.
- 3) At SAM21 EM GUI, open Card View for MC 0
  - a) Under Provisioning Tab, determine IP address of the card.
  - b) Ensure IP address in GUI matches IP address of MC 0.
- 4) Under the States Tab, Lock the card.
  - a) Wait for the lock icon to appear.
- 5) Under the Provisioning Tab, change the boot file:
  - a) Click Modify.
  - b) Change boot file name to new load.
  - c) Click Save.
- 6) Under the States Tab, Unlock the card
  - a) Wait for the lock icon to disappear.
- 7) At Active CCAMTC MAP; MC level, Validate newly booted load.
  - a) QryLd command for MC0 must indicate new MC load version.
- 8) Soak for 10 minutes, monitoring logs.

Type GO to continue SWUPGRADE when above steps are successfully completed.

Step LOAD\_MC0\_BLADE is not complete.  
The SWUPGRADE process has paused. Enter GO.

- 2** At the MAPCI;MTC;MS level, ensure that MS 1 is the master MS.

|            | MS             | IOD | Net   | PM     | CCS   | Lns | Trks              | Ext | APPL |
|------------|----------------|-----|-------|--------|-------|-----|-------------------|-----|------|
|            | .              | .   | .     | .      | .     | .   | ...               | .   | .    |
| MS         | Message Switch |     | Clock |        | Shelf | 0   | Inter-MS Link 0 1 |     |      |
| 0 Quit     | MS 0           | .   | .     | Slave  | .     | F   | .                 | .   | .    |
| 2          | MS 1           | .   | .     | M Free | .     | F   | .                 | .   | .    |
| 3          |                |     |       |        |       |     |                   |     |      |
| 4          |                |     |       |        |       |     |                   |     |      |
| 5          |                |     |       |        |       |     |                   |     |      |
| 6 Tst_     |                |     |       |        |       |     |                   |     |      |
| 7 Bsy_     |                |     |       |        |       |     |                   |     |      |
| 8 RTS_     |                |     |       |        |       |     |                   |     |      |
| 9          |                |     |       |        |       |     |                   |     |      |
| 10 LoadMS_ |                |     |       |        |       |     |                   |     |      |

- 3** If MS 1 is not the master MS, perform a SWMAST. If SWMAST is performed, then soak 10 minutes before continuing.

***At the active Call Agent Manager interface (CORE0 or CORE1)***

- 4** At the MCMtc level, verify that both Message Controllers are in service (.) prior to Locking Message Controller 0 in the next step.

| CallAgent | SYS    | CON | APPL  | MC      | Unit: 0     |
|-----------|--------|-----|-------|---------|-------------|
| .         | .      | .   | .     | .       | .           |
| MCMtc     | Blade: |     | Eth0: | Eth1:   | Atm0: Atm1: |
| 0 Quit    | MC0    | .   | . Act | . Inact | open open   |
| 2         | MC1    | .   | . Act | . Inact | open open   |
| 3         |        |     |       |         |             |

- 5** Exit the Call Agent Manager interface and determine the IP address of Message Controller 0:

**>0 ALL**

**[mtc@hostname mtc]\$ grep mc0 /etc/hosts**

*The grep command returns the address of Message Controller 0.*

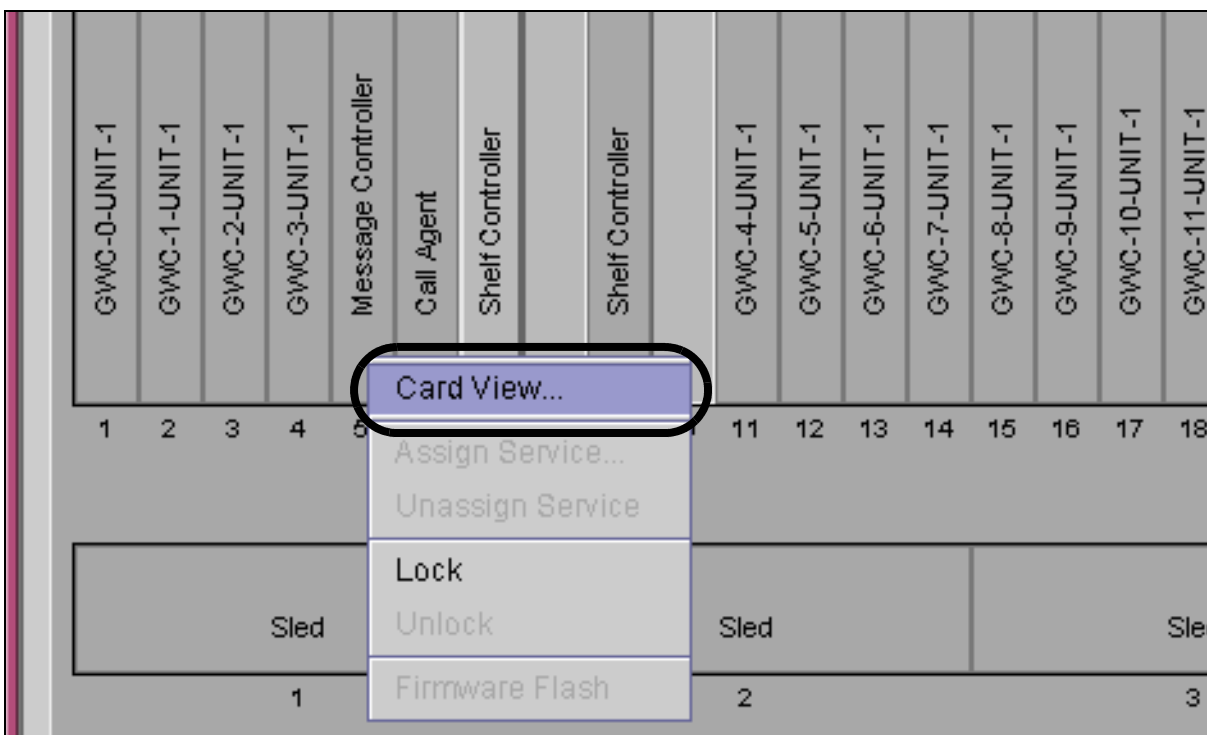
10.40.54.60 mc0

- 6** Start the Call Agent Manager interface again:

**[mtc@hostname mtc]\$ ccamtc mcmtc**

**At the CS 2000 SAM21 Manager client**

- 7 From the Shelf View, right-click the card and select Card View.



**Note:** The Shelf View window will reflect office provisioning and the hardware configuration of the SAM21 shelf.

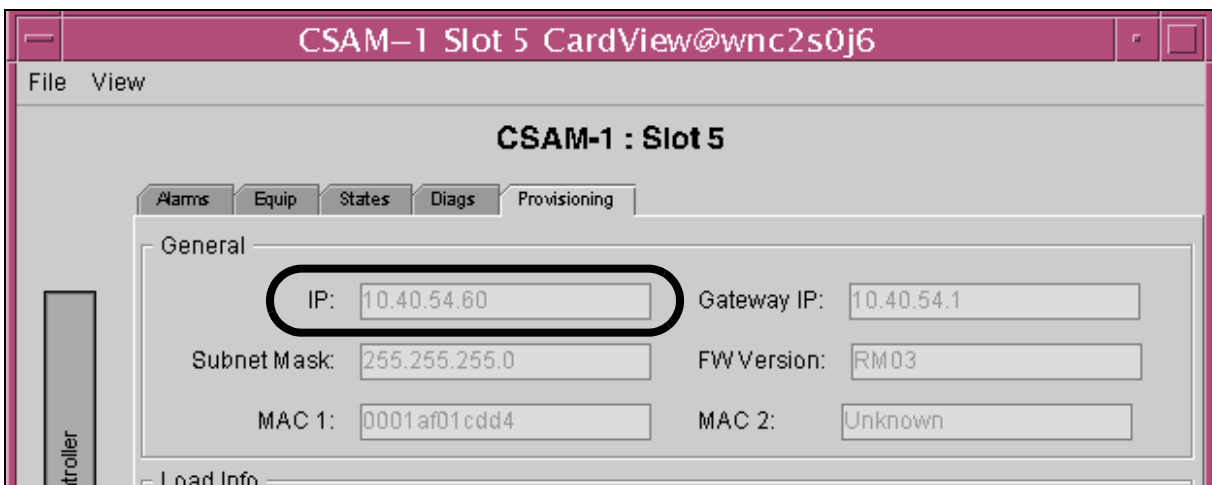
*The Card View window opens.*

- 8 Select the Provisioning tab on the Card View window.

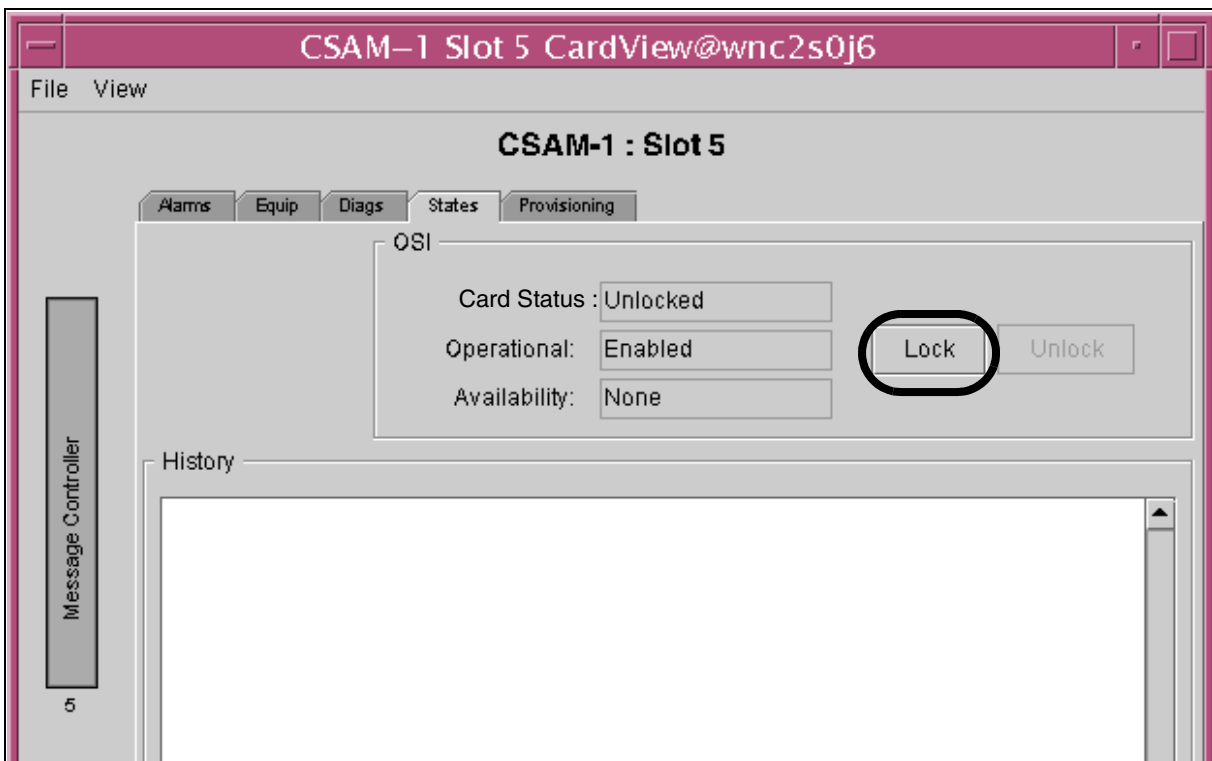
Ensure that the IP address specified in the IP field matches the IP address of Message Controller 0 from [step 5](#). If the values do not match, open the other Shelf View from the CS 2000 SAM21



Manager and check the Message Controller provisioning for that shelf.

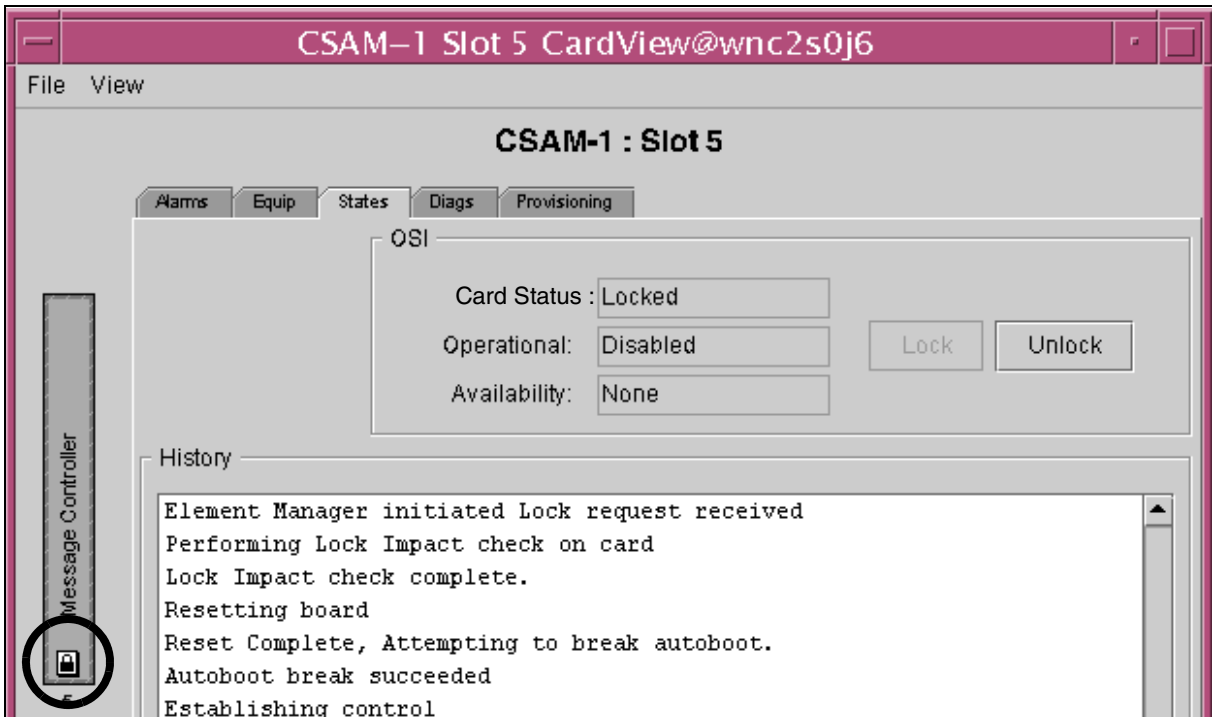


- 9 Click the States tab.  
Click the Lock button.



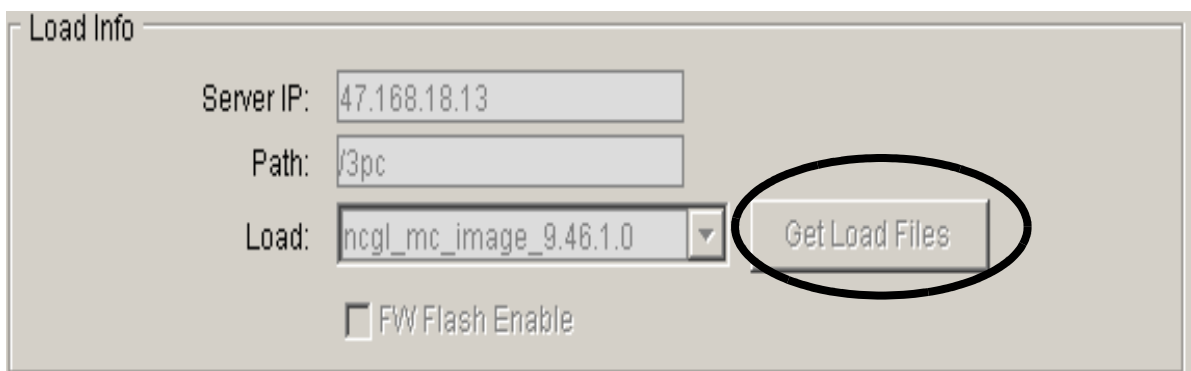
*A lock warning dialog window opens. Confirm the lock warning.*

- 10 Wait for the lock icon to appear on the card icon.



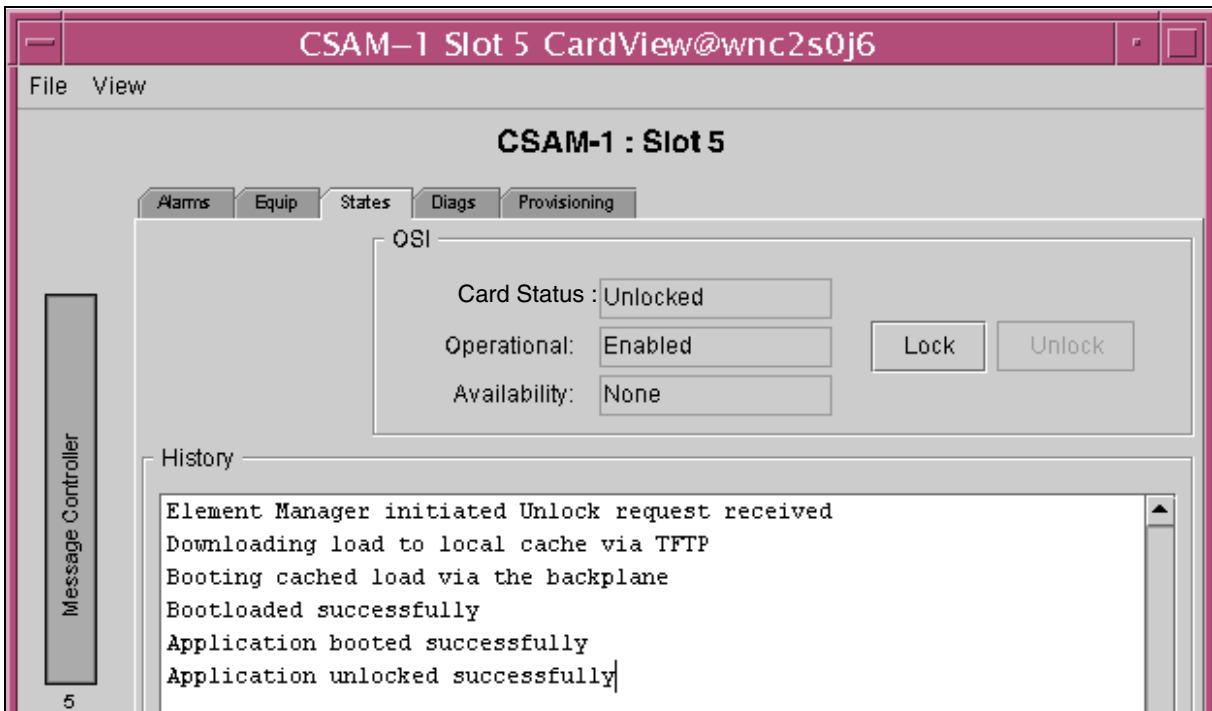
*At the Call Agent Manager, a major ATM alarm is raised. The Message Controller enters the Remote Busy (R) state and is reported as out of service.*

- 11 Click the *Provisioning* tab in the upper window.  
12 Click the *Modify* button at screen bottom.  
13 Click the *Get Load Files* button.



- 14 Select the load from the *Load:* drop-down list.  
**Note:** The format is: ncgl\_mc\_image\_<r>.x.y.zz

- 15 Click the *Save* button at screen bottom.  
*A warning dialog generates indicating a load mismatch between the provisioning for the two Message Controller cards. Confirm the warning dialog by clicking OK.*
- 16 Click the *States* tab and click the *Unlock* button.  
Wait for the lock icon to disappear.



*At the Call Agent Manager, the card enters the in service state (.), and the major ATM alarm clears. The Message Controller may raise a major MCTbl alarm while the Message Controller synchronizes to the NTP server.*

**At the active Call Agent Manager interface (CORE0 or CORE1)**

- 17 Query the software load for Message Controller 0 and ensure that the new load is reported:
  - > **MCMtc**
  - > **QryLd 0**

```
CallAgent SYS CON APPL MC Unit: 0
.

MCMtc Blade: Eth0: Eth1: Atm0: Atm1:
0 Quit MC0 . . Act . Inact open open
2 MC1 . . Act . Inact open open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trnsl
9
10
11
12
13 LogQuery
14 Alarm
15
16 MC Load report retrieved on Thu Mar 19 13:48:45 2005:
17 Help
18 Refresh Ramdisk: ncgl_mc_image_8.20.1.0
 mtc
Time 13:48 >
```

*Soak the load for 10 minutes while monitoring log reports.*

**SDE — At the ACTIVECM window**

- 18** Type GO and press the Enter key to continue.
- 19** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## LOAD\_MC1\_BLADE

### ATTENTION

Steps [PRINT\\_MS\\_LOADS](#), [LOAD\\_MC0\\_BLADE](#) and [LOAD\\_MC1\\_BLADE](#) only run if the CS 2000 - Compact is configured with Message Controller cards. If the CS 2000 - Compact is not configured with Message Controller Cards, continue to step [DROP\\_SYNC](#).

### **SDE — At the ACTIVECM window**

#### **1 Step LOAD\_MC1\_BLADE runs.**

Starting step LOAD\_MC1\_BLADE.

Upgrade load of MC 1 at the SAM21 EM GUI by using the following manual procedure:

- 1) At the MAPCI;MTC;MS map level, verify that MS 0 is the master MS.
- 2) If MS 0 is not the master, perform a SWMAST. If performed, soak 10 minutes.
- 3) At SAM21 EM GUI, open Card View for MC 1
  - a) Under Provisioning Tab, determine IP address of the card.
  - b) Ensure IP address in GUI matches IP address of MC 1.
- 4) Under the States Tab, Lock the card.
  - a) Wait for the lock icon to appear.
- 5) Under the Provisioning Tab, change the boot file:
  - a) Click Modify.
  - b) Change boot file name to new load.
  - c) Click Save.
- 6) Under the States Tab, Unlock the card
  - a) Wait for the lock icon to disappear.
- 7) At Active CCAMTC MAP; MC level, Validate newly booted load.
  - a) QryLd command for MC 1 must indicate new MC load version.
- 8) Soak for 10 minutes, monitoring logs.

Type GO to continue SWUPGRADE when above steps are successfully completed.

Step LOAD\_MC1\_BLADE is not complete.  
The SWUPGRADE process has paused. Enter GO.

- 2** At the MAPCI;MTC;MS level, ensure that MS 0 is the master MS.

|            | MS                           | IOD | Net | PM     | CCS | Lns | Trks | Ext | APPL              |
|------------|------------------------------|-----|-----|--------|-----|-----|------|-----|-------------------|
|            | .                            | .   | .   | .      | .   | .   | ...  | .   | .                 |
| MS         | Message Switch Clock Shelf 0 |     |     |        |     |     |      |     | Inter-MS Link 0 1 |
| 0 Quit     | MS 0                         | .   |     | M Free |     | F   |      |     | .                 |
| 2          | MS 1                         | .   |     | Slave  |     | F   |      |     | .                 |
| 3          |                              |     |     |        |     |     |      |     |                   |
| 4          |                              |     |     |        |     |     |      |     |                   |
| 5          |                              |     |     |        |     |     |      |     |                   |
| 6 Tst_     |                              |     |     |        |     |     |      |     |                   |
| 7 Bsy_     |                              |     |     |        |     |     |      |     |                   |
| 8 RTS_     |                              |     |     |        |     |     |      |     |                   |
| 9          |                              |     |     |        |     |     |      |     |                   |
| 10 LoadMS_ |                              |     |     |        |     |     |      |     |                   |

- 3** If MS 1 is not the master MS, perform a SWMAST . If SWMAST is performed, then soak 10 minutes before continuing.

**At the active Call Agent Manager interface (CORE0 or CORE1)**

- 4** At the MCMtc level, verify that both Message Controllers are in service (.) prior to Locking Message Controller 1 in the next step.

| CallAgent | SYS    | CON | APPL | MC | Unit: 0 |
|-----------|--------|-----|------|----|---------|
| .         | .      | .   | .    | .  |         |
| MCMtc     | Blade: |     |      |    |         |
| 0 Quit    | MC0    | .   | Act  | .  | Inact   |
| 2         | MC1    | .   | Act  | .  | Inact   |
| 3         |        |     |      |    |         |

- 5** Exit the Call Agent Manager interface and determine the IP address of Message Controller 0:

**>0 ALL**

**[mtc@hostname mtc]\$ grep mc1 /etc/hosts**

*The grep command returns the address of Message Controller 1.*

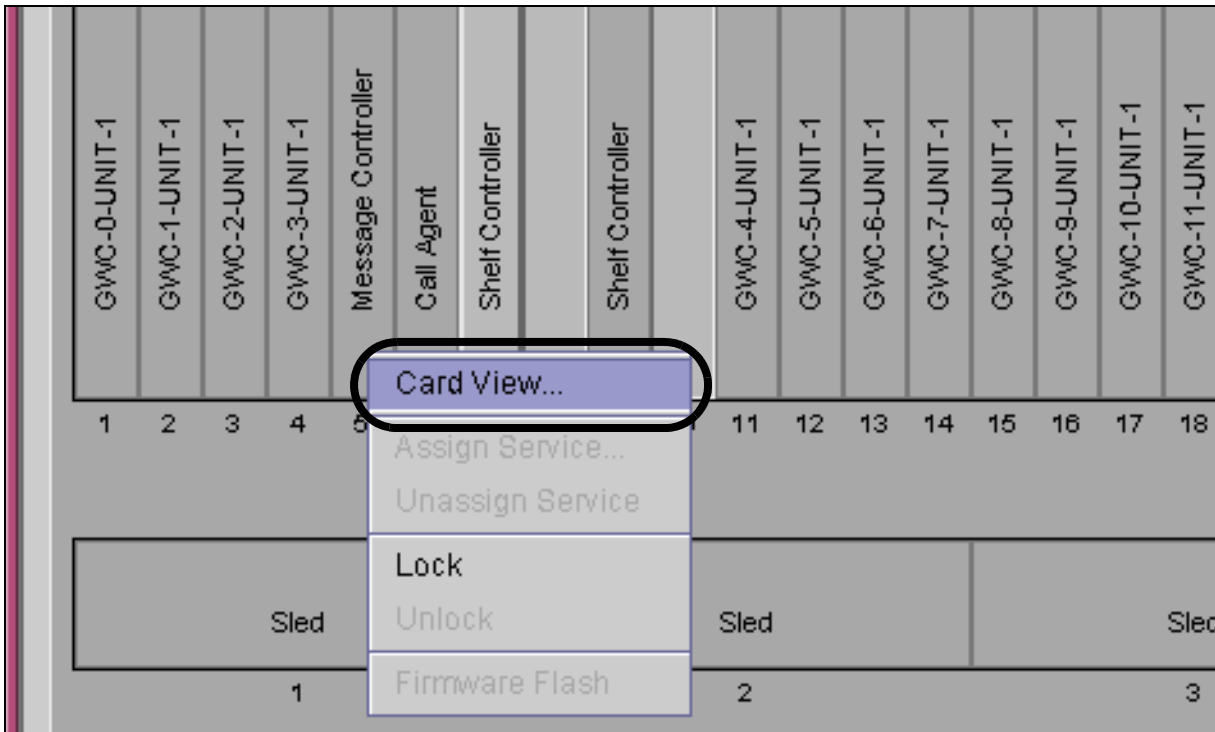
10.40.54.61 mc1

- 6** Start the Call Agent Manager interface again:

**[mtc@hostname mtc]\$ ccamtc mcmtc**

***At the CS 2000 SAM21 Manager client***

- 7 From the Shelf View, right-click the card and select Card View.



**Note:** Message Controller 1 is located in slot 12 for some markets.

*The Card View window opens.*

**8** Select the Provisioning tab on the Card View window.

Ensure that the IP address specified in the IP field matches the IP address of Message Controller 1. If the values do not match, open the other Shelf View from the CS 2000 SAM21 Manager and check the Message Controller provisioning for that shelf.

The screenshot shows a web-based interface for configuring a Message Controller. The window title is "CSAM-1 Slot 5 CardView@wnc2s0j6". The main heading is "CSAM-1 : Slot 5". Below this are tabs for "Alarms", "Equip", "States", "Diags", and "Provisioning". The "Provisioning" tab is selected. On the left, a vertical bar labeled "Message Controller" has a "5" at the bottom. The "General" section contains the following fields:

|              |               |             |            |
|--------------|---------------|-------------|------------|
| IP:          | 10.40.54.61   | Gateway IP: | 10.40.54.1 |
| Subnet Mask: | 255.255.255.0 | FW Version: | N          |
| MAC 1:       | 0001af01cdd4  | MAC 2:      | Unknown    |

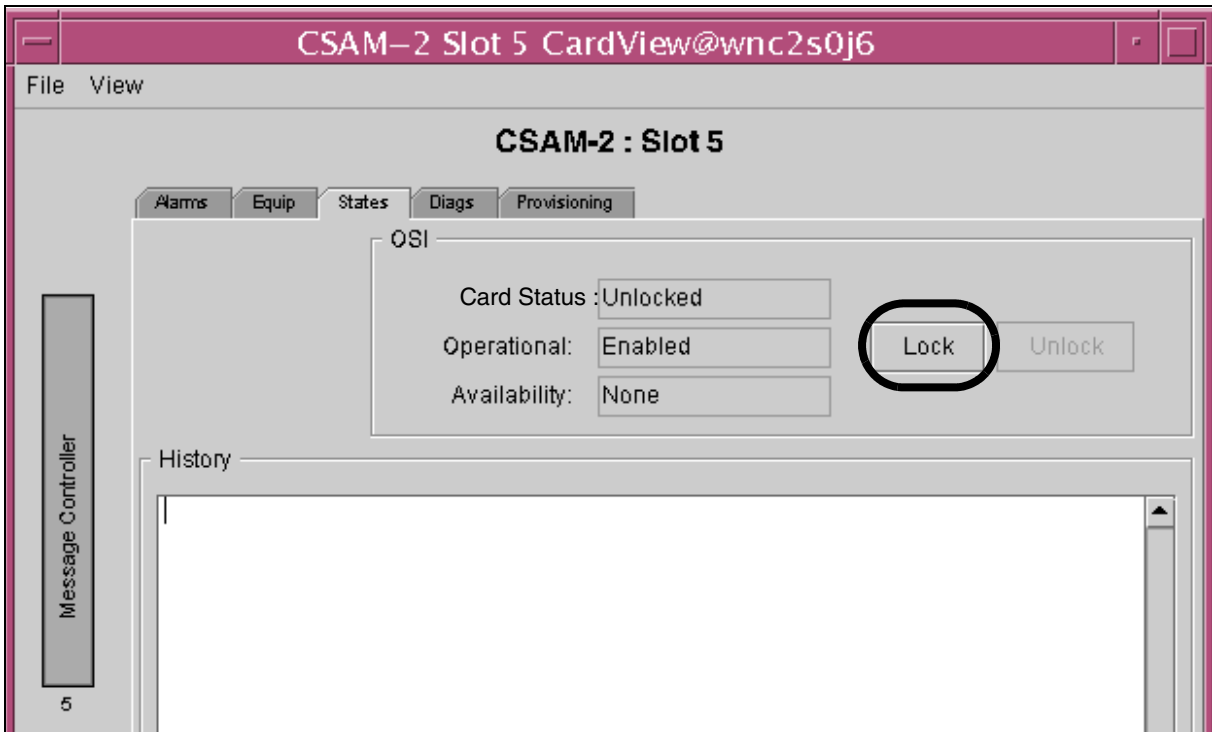
The "Load Info" section contains the following fields:

|            |                        |
|------------|------------------------|
| Server IP: | 10.40.54.1             |
| Path:      | /swd/3pc               |
| Load:      | ncgl_mc_image_7.15.1.0 |

There is an unchecked checkbox labeled "FW Flash Enable" at the bottom of the "Load Info" section.

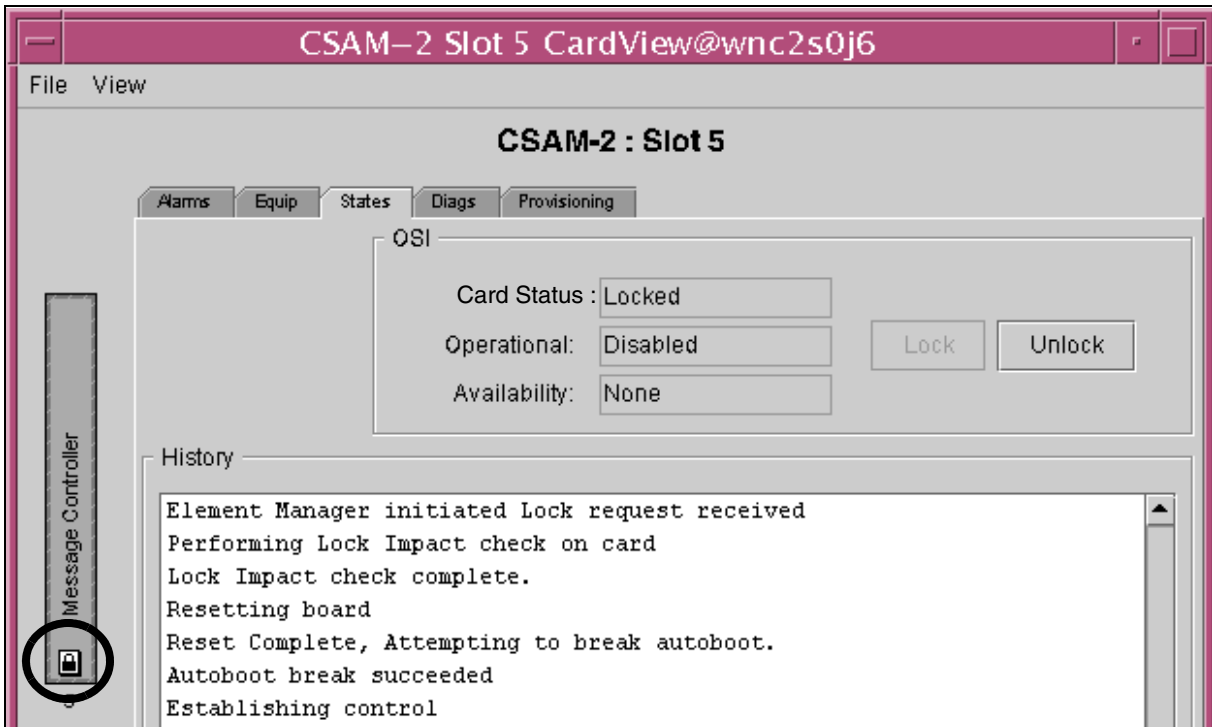


- 9 Click the States tab.  
Click the Lock button.



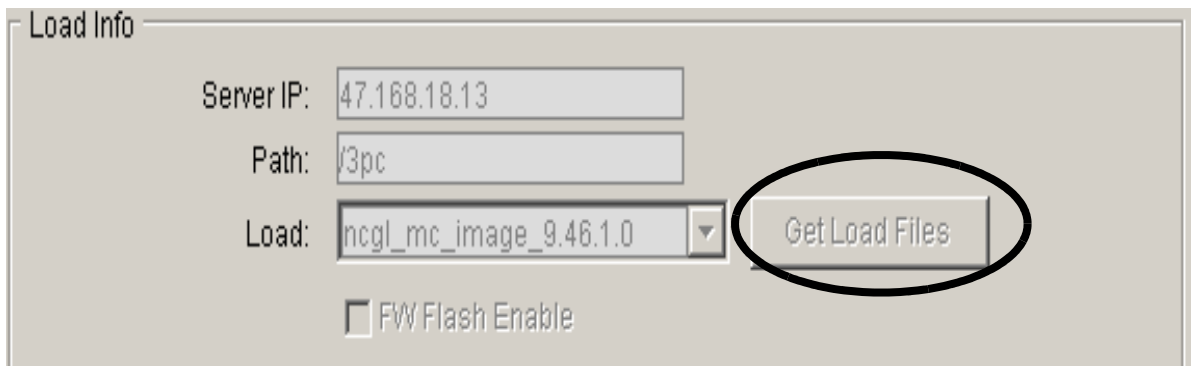
*A lock warning dialog window opens. Confirm the lock warning.*

- 10 Wait for the lock icon to appear on the card icon.



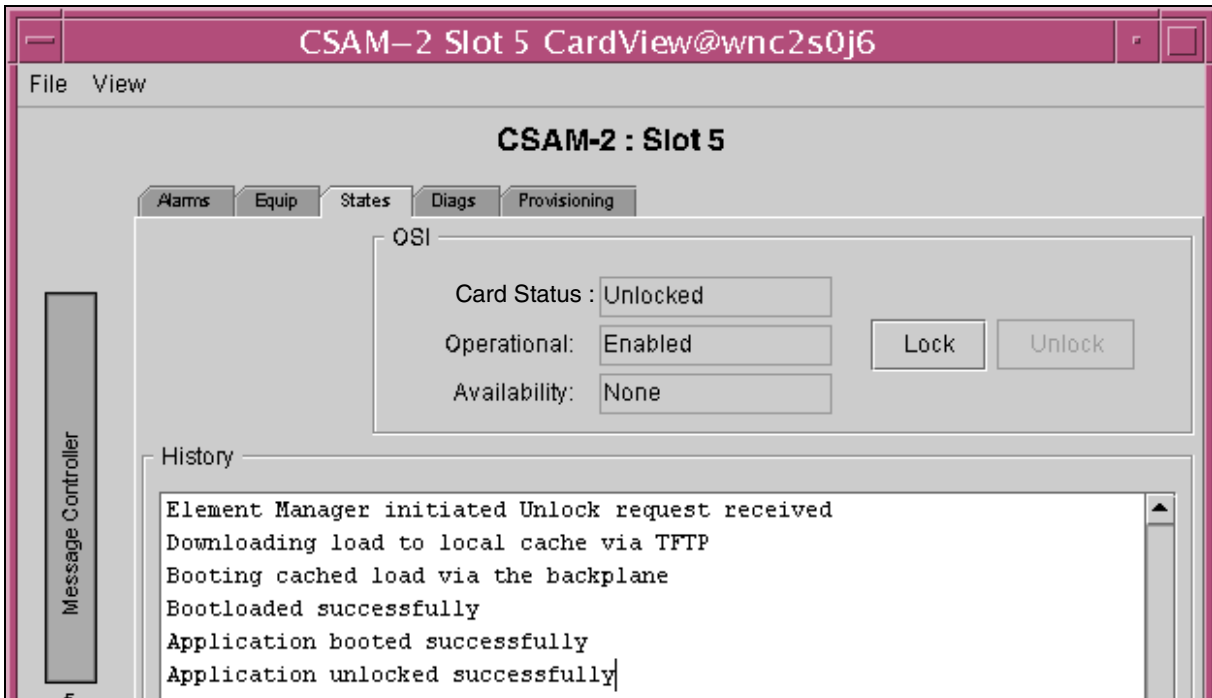
*At the Call Agent Manager, a major ATM alarm is raised, the Message Controller enters the Remote Busy (R) state and is reported as out of service.*

- 11 Click the *Provisioning* tab in the upper window.  
12 Click the *Modify* button at screen bottom.  
13 Click the *Get Load Files* button.



- 14 Select the load from the *Load:* drop-down list.  
**Note:** The format is: ncgl\_mc\_image\_<r>.x.y.zz

- 15 Click the *Save* button at screen bottom.
- 16 Click the *States* tab and click the *Unlock* button.  
Wait for the lock icon to disappear.



*At the Call Agent Manager, the card enters the in service state (.), and the major ATM alarm clears. The Message Controller can raise a major MCTbl alarm while the Message Controller synchronizes to the NTP server.*

**At the active Call Agent Manager interface (CORE0 or CORE1)**

- 17 Query the software load for Message Controller 1 and ensure that the new load is reported:
  - > **MCMtc**
  - > **QryLd 1**

```
CallAgent SYS CON APPL MC Unit: 0
.
MCMtc Blade: Eth0: Eth1: Atm0: Atm1:
0 Quit MC0 . . Act . Inact open open
2 MC1 . . Act . Inact open open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 Trnsl
9
10
11
12
13 LogQuery
14 Alarm
15
16 MC Load report retrieved on Thu Jun 19 14:15:54 2004:
17 Help
18 Refresh Ramdisk: ncgl_mc_image_8.20.1.0
 mtc
Time 13:48 >
```

*Soak the load for 10 minutes while monitoring log reports.*

**SDE — At the ACTIVECM window**

- 18** Type GO and press the Enter key to continue.
- 19** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## DROP\_SYNC

Step DROP\_SYNC requires jamming the inactive Call Agent from the active Call Agent Manager.

### ***SDE — At the ACTIVECM window***

- 1 Obtain approval to drop synchronization of the call processing application.
- 2 Type GO and press the Enter key to continue.

Starting step DROP\_SYNC.

Please JAM the Inactive CA Application and confirm when complete:

At the Active COREMTC MAP (ccamtc coremtc); CAMtc Level:

1) JAM - Jam the Inactive application

Type GO to continue the SWUPGRADE when JAM is completed

Step DROP\_SYNC is not complete.

The SWUPGRADE process has paused. Enter GO.

### ***SDE — At the CORE0 or CORE1 window***

- 3 Jam the inactive Call Agent from the active Call Agent Manager window.  
**> CoreMtc;CAMtc;Jam**
- 4 Monitor the jam and verify that a Jlnact alarm is raised.

### ***SDE — At the ACTIVECM window***

- 5 Type GO and press the Enter key to continue.
- 6 This procedure is complete. Proceed to [LOAD\\_NEW\\_SIDE\\_BLADE and LOAD\\_MATE.](#)

## LOAD\_NEW\_SIDE\_BLADE and LOAD\_MATE

This procedure requires the SDE to perform the following actions:

- lock the inactive Call Agent card
- reprovision the platform software load
- unlock the inactive Call Agent

### ***SDE — At the ACTIVECM window***

- 1 Review the message printed to the terminal.

Starting step LOAD\_NEW\_SIDE\_BLADE.

Upgrade the New Side Call Agent load at the SAM21 EM GUI by using the following manual procedure:

- 1) At Active COREMTC MAP (ccamtc coremtc), query the Inact blade IP addr
  - a) Use QueryIP command to determine the IP address of mate blade.
- 2) At SAM21 EM GUI, open Card View for Inact Call Agent Card:
  - a) Under the Provisioning Tab, determine IP address of the card.
  - b) Ensure IP address in GUI matches inactive card IP address.
- 3) Under the States Tab, Lock the card.
- 4) Under the Provisioning Tab, change the boot file:
  - a) Click Modify.
  - b) Change boot file name to new load.
  - c) Click Save.
- 5) Under the States Tab, Unlock the card.
  - a) Monitor the boot progress in the History pane.
- 6) At Active COREMTC MAP, monitor Inact load initialization:
  - a) Inact status begins with "/booting"
  - b) Wait until the status becomes "/waiting"
- 7) At Inactive COREMTC map (ccamtc coremtc), Validate newly booted load:
  - a) Telnet/Login to the Inact Blade
  - b) Under the Sys level, QryLd must indicate the new load version

Type GO to continue the SWUPGRADE when above steps are successfully completed. Step LOAD\_NEW\_SIDE\_BLADE is not complete.

The SWUPGRADE process has paused. Enter GO.

- 2 Perform the instructions listed in the output. Refer to the following procedures for assistance:
  - Lock the inactive Call Agent — [Locking the Call Agent on page 2028](#)
  - Change the boot file — [Reprovisioning the Call Agent platform load on page 2030](#)
  - Unlock the inactive Call Agent — [Unlocking the Call Agent on page 2034](#)
- 3 Type GO and press the Enter key.

*Step LOAD\_NEW\_SIDE\_BLADE completes.*

*Step LOAD\_MATE begins, loads the new call processing application on the inactive Call Agent, and completes. The image specified in variable LDMATE\_IMAGE is loaded. Progress is displayed at the ACTIVECM window and the CORE0 and CORE1 windows.*
- 4 This procedure is complete. Proceed to [PATCH\\_NEW\\_SIDE\\_BLADE](#).

---

## PATCH\_NEW\_SIDE\_BLADE

---

This step provides a prompt for the SDE to apply patches to the upgraded Call Agent platform software load. Patches for the call processing application are applied later in the upgrade. The patches must reside in the `/swd/3pc/patch` directory on the CS 2000 Core Manager or CBM.

**Note:** The steps printed to the terminal may not be accurate. Perform the following steps to patch the new side blade.

1. At the inactive maintenance window (CORE0 or CORE1) verify that this is the inactive Call Agent.
2. Enter the Admin level and then the SWIM level.
3. At the TRANSFER level a list of available patches is displayed
  - a. SELECT the patch by number
  - b. FETCH INA the patch to the INACTIVE unit
4. At the PATCH level, for each patch to be applied and committed:
  - a. SELECT the patch by number
  - b. APPLY INA FORCE the patch to the INACTIVE unit
  - c. SELECT the patch by number
  - d. COMMIT INA the patch to the INACTIVE unit

Each patch is applied and committed to the inactive Call Agent unit. The Status for each patch changes from NEW to COMMITTED. The COMMIT command commits the patch to the load so that the patch is reapplied the next time the card is reset. If the patch is not committed, it will not be reapplied the next time the card is reset.



**SDE — At the ACTIVECM window****1 Review the message printed to the terminal.**

Starting step PATCH\_NEW\_SIDE\_BLADE.

If patches for the New Side Call Agent Load are available, upgrade the load to the current patch level using the following manual procedure:

1) At the Inact COREMTC map (ccamtc corematc):

a) Verify that this card is the Inact unit.

2) At the TRANSFER map level:

a list of available patches is displayed.

For each patch to be transferred:

a) SELECT the patch by number

b) FETCH the patch to BOTH units

3) At the PATCH map level:

For each patch to be applied and committed:

a) SELECT the patch by number

b) APPLY INA - apply the patch on Inactive only

c) SELECT the patch by number

d) COMMIT INA - commit the patch on Inactive only

Type GO to continue the SWUPGRADE when above steps are successfully complete. Step PATCH\_NEW\_SIDE\_BLADE is not complete.

The SWUPGRADE process has paused. Enter GO.

**2** Refer to [Patching Platform and Call Processing software on page 2076](#) for assistance with the platform software patching procedure.

**3** After patching is complete, or if no patches are available, type GO and press the Enter key.

*Step PATCH\_NEW\_SIDE\_BLADE completes.*

*Step MATELINK\_RTS runs and completes. This step verifies the communication path between the active call processing application and the upgraded, inactive call processing application.*

*Step UPDATE\_STEPS\_AND\_VARS runs and completes. This step automatically provisions environment variables and updates the list of steps on the inactive call processing application. The active and inactive call processing application data for the ONP is synchronized.*

*Step CHECK\_NEW\_LOAD runs and completes. This step verifies that the inactive call processing application on the inactive Call Agent has no datafill. The software verifies that this load has no datafill by checking that table TERMDEV has a single tuple.*

*Step SET\_DATE\_AND\_LOGMSG runs and completes. This step sets the inactive side time and date from the active side. The login message is set from variable INACT\_LOGMSG.*

*Step CHECK\_LOGS\_2 runs and completes. This step displays the count of logs in the LOGUTIL buffer since the start of the process. The log report types displayed are determined by the variable LOGS.*

*Step CLEAR\_TRAPINFO runs and completes. This step clears all traps on the upgraded inactive call processing application. By clearing the traps now, it is easier to differentiate between old and new traps that are caused by subsequent steps.*

*Step TRANSFER\_DEVICES\_INFO runs and completes. This step copies data from variable VERIFY\_DEVICES on the active call processing application to the inactive call processing application.*

*If the CS 2000 - Compact is configured with Message Controllers, step MS\_CHECK runs. This step checks that the software load in the Message Switch is the correct load for the upgraded call processing application load.*

*Step DISABLE\_AUTOIMAGE runs and completes. This step disables the automatic image dump process since the automatic image dump process could interfere with the ONP.*

*Step SET\_OFFICE\_TUPLES runs and completes. This step retains the current state of office parameters NODEREXCONTROL, LCDREX\_CONTROL, and GUARANTEED\_TERMINAL\_CPU\_SHARE and then sets both NODEREXCONTROL and LCDREX\_CONTROL to OFF. GUARANTEED\_TERMINAL\_CPU\_SHARE is set to its maximum value.*

*Step SET\_PADNDEV runs and completes. This step saves the tuples in table PADNDEV, deletes all the tuples, and then adds tuples according to variable PADNDEV.*

*Step SEND\_PATCHES runs and completes. This step copies the patch files for the upgraded inactive call processing application from the location specified by variable PADNDEV to the inactive call processing application.*

*Step APPLY\_PATCHES runs and completes. The patches that were copied in step SEND\_PATCHES are applied.*

*Step CHECK\_LOGS\_3 runs and completes. This step displays the count of log reports stored in the LOGUTIL buffer.*

*Step RESTORE\_PADNDEV runs and completes. This step restores table PADNDEV to contain the exact tuples it contained before step SET\_PADNDEV.*

- 4 This procedure is complete. Proceed to [TABLE\\_TRANSFER](#).

---

## TABLE\_TRANSFER

---

This step copies table provisioning data from the active call processing application to the undatafilled, inactive call processing application.

Step TABLE\_TRANSFER is automated. Manual intervention is needed only if some of the table data fails to transfer. The table transfer stops according to variables STOPIF and LIMIT.

For any failed tables, compare the old, active side data to the new, inactive side data to identify and correct any tuples. If necessary, contact your translations engineer or Nortel support personnel for assistance.

For some offices, it is necessary or preferred to change office variables and parameters on the inactive side after this step completes. One possible parameter to change is field LOG\_OFFICE\_ID in table OFCVAR. Change this parameter after TABLE\_TRANSFER completes and before step START\_PRESWACT. Use the procedure below for logging into the inactive call processing application.

### ATTENTION

If it is necessary to access the inactive call processing application to correct a problem, use the following procedure.

If it is necessary to abort the upgrade at this point, issue the CANCEL command at the ACTIVECM window.

### *At the INACTIVECM window*

- 1 Log in to the active call processing application by telnetting to the CS 2000 Core Manager as user cmusr.
- 2 Enter the mate input/output level and log in to the inactive call processing application:

**>MATEIO;MATELOG ME;SLEEP 60 MINS**

**Note 1:** The `Mate>` prompt indicates that the command is sent to the inactive call processing application.

**Note 2:** If the MATELOG ME command fails, enter MATELINK RTS and retry the MATELOG ME command.

```
>mateio
MATEIO -- MATECOM link not available. Attempt RTS.
>matelink rts
RTS PASSED
```

- 3 At the Mate> prompt, log in to the inactive call processing application:

**Mate> username password**

- 4 Use the table editor to correct any datafill problems.
- 5 Use the LOGOUT command at the Mate> prompt to exit the inactive call processing application:

**Mate> LOGOUT**

**Note:** Do not log out of the active call processing application. Verify that the prompt is the Mate> prompt.

- 6 Wake up the active side terminal. Enter:

**> <Ctrl+B> HX**

**At the ACTIVECM window**

- 7 Type GO and press the Enter key to continue.

*Step TABXFR\_REPORT runs and completes. This step prints a report of all table failures to the trace device.*

*Step CHECK\_LOGS\_4 runs and completes.*

- 8 This procedure is complete. Proceed to [START\\_PRESWACT](#).

---

## START\_PRESWACT

---

Step START\_PRESWACT has several substeps. If any substep fails to complete, make corrections according to the error message and continue the START\_PRESWACT step by typing GO and pressing the Enter key. START\_PRESWACT re-executes the failed step and continues.

Read the following notes while step START\_PRESWACT executes:

START\_PRESWACT sub step TABLE\_DELTA displays the changes, additions, and deletions between the old and new call processing application software loads for the following tables:

- OFCENG
- OFCSTD
- OFCVAR
- OFCOPT
- DATASIZE
- TCAPTRID
- OPTCTL

For any tables with differences, compare the OLD/NEW and ADDED tuples to identify and correct any errors.

**Note:** Errors stop sub step TABLE\_DELTA from completing with the message `TABLE_DELTA not complete`. The software also provides informative messages such as “Table ATTCONS Checksum incorrect, keys match.” The informative messages do not stop the step from completing and do not require any manual action. At a convenient point during the upgrade, compare the old and new loads to understand and validate the differences.

If office parameter changes were made after step TABLE\_TRANSFER on the inactive call processing application, then TABLE\_DELTA displays the change.

Proceed to [PRESWACT DIRP AND BILLING](#).

## PRESWACT\_DIRP\_AND\_BILLING

### ***SDE — At the ACTIVECM window***

- 1 Step PRESWACT\_DIRP\_AND\_BILLING runs and completes, but pauses the process. The CS 2000 - Compact requires no manual action for DIRP and billing.

Starting step PRESWACT\_DIRP\_AND\_BILLING.

AMA and SMDR Billing subsystem information

-----

MAPCI:

MTC:

IOD:

DIRP:

| SSNAME | SSNO | SEQNO | ROTATES | POOLNO | PARLPOOL | EMERGENCY |
|--------|------|-------|---------|--------|----------|-----------|
| AMA    | 3    | 1     | 4       | 1      | NONE     | NO        |

REGULAR

| FILE(S)  | STATE | VOLUME   | RECCOUNT | BLOCK | E | V  | V_B | VLID | FNUM | FRN# |
|----------|-------|----------|----------|-------|---|----|-----|------|------|------|
| ACTIVE   | AVAIL | SD00AMA0 | 181941   | 9098  | 0 | 71 | NO  | 8402 | 0000 | 718F |
| STANDBY1 | AVAIL | SD01AMA0 | 0        | 0     | 0 | 69 | NO  | 8442 | 0001 | 5191 |

PARALLEL

| FILE | STATE | VOLUME | BLOCK | E | V | V_B | VLID | FNUM | FRN# |
|------|-------|--------|-------|---|---|-----|------|------|------|
|      | NONE  |        |       |   |   |     |      |      |      |

MAPCI:

MTC:

IOD:

DIRP:

| SSNAME | SSNO | SEQNO | ROTATES | POOLNO | PARLPOOL | EMERGENCY |
|--------|------|-------|---------|--------|----------|-----------|
| SMDR   | 7    | 1     | 2       | 5      | NONE     | NO        |

REGULAR

| FILE(S) | STATE | VOLUME   | RECCOUNT | BLOCK | E | V  | V_B | VLID | FNUM | FRN# |
|---------|-------|----------|----------|-------|---|----|-----|------|------|------|
| ACTIVE  | AVAIL | SD00SMDR | 1        | 1     | 0 | 71 | NO  | 8407 | 0058 | 6190 |

PARALLEL

| FILE | STATE | VOLUME | BLOCK | E | V | V_B | VLID | FNUM | FRN# |
|------|-------|--------|-------|---|---|-----|------|------|------|
|      | NONE  |        |       |   |   |     |      |      |      |

.....

TRANSFERRING table DIRPPPOOL to inactive side.  
-----

ACT-WARNING: If any DIRP actions other than those described in this step occur between now and SWACT, the user may need to manually correct any discrepancies in table DIRPPPOOL.

D/R DART# 719-> DIRPPPOOL: Restored 13, Failed 0

To prepare DIRP billing subsystems for the SWACT, please follow instructions in the NTP 'One Night Process Software Delivery Procedures.'

This verifies that all DIRP billing subsystems have been properly prepared for the upcoming SWACT and DIRP information is readily available for timely restoration to minimize the loss of existing data, should DIRP file storage devices become corrupted during the transition.

These measures may include, but are not limited to:

- DIRP rotation of disk primary billing.
- DIRP rotation of tape primary billing.
- close existing billing file and open a new one.
- prepare tape billing standby volumes.
- prepare tape parallel standby volumes.
- copy unprocessed disk billing file to backup tape.
- copy disk parallel files to backup.
- match DIRPPPOOL volumes between active and inactive.

Step PRESWACT\_DIRP\_AND\_BILLING is complete.  
The SWUPGRADE process has paused. Enter GO.

- 2 Type GO and press the Enter key to confirm PRESWACT\_DIRP\_AND\_BILLING.

*Step PRINT\_SPMS\_INDICES runs and completes.*

- 3 Step GET\_FIRST\_SWACT\_AGREEMENT begins and pauses the process. The SDE must receive agreement from the customer to proceed with the SWACT.

**Note:** If a delay of longer than 15 minutes is expected before the SWACT, the SDE will wait until all preparations are made before continuing.



*System response:*

Starting step GET\_FIRST\_SWACT\_AGREEMENT.  
NORESTARTSWACT will be used for initiating a CC Warm SWACT.  
Do you wish to proceed with the preparation for the CC warm swact?  
Step GET\_FIRST\_SWACT\_AGREEMENT is complete.  
The SWUPGRADE process has paused. Enter GO.

- 4 Type GO and press the Enter key to confirm GET\_FIRST\_SWACT\_AGREEMENT.
- 5 Step PREPARE\_FOR\_SWACT begins.

Starting step PREPARE\_FOR\_SWACT.

DISPLAY\_NOP\_USERS executing

| SESSION | STATE | APPL. | ID | NODE |
|---------|-------|-------|----|------|
|---------|-------|-------|----|------|

|   |      |  |  |  |
|---|------|--|--|--|
| 0 | IDLE |  |  |  |
|---|------|--|--|--|

|   |      |  |  |  |
|---|------|--|--|--|
| 1 | IDLE |  |  |  |
|---|------|--|--|--|

|   |      |  |  |  |
|---|------|--|--|--|
| 2 | IDLE |  |  |  |
|---|------|--|--|--|

|   |      |  |  |  |
|---|------|--|--|--|
| 3 | IDLE |  |  |  |
|---|------|--|--|--|

|   |      |  |  |  |
|---|------|--|--|--|
| 4 | IDLE |  |  |  |
|---|------|--|--|--|

|   |      |  |  |  |
|---|------|--|--|--|
| 5 | IDLE |  |  |  |
|---|------|--|--|--|

|   |      |  |  |  |
|---|------|--|--|--|
| 6 | IDLE |  |  |  |
|---|------|--|--|--|

|   |      |  |  |  |
|---|------|--|--|--|
| 7 | IDLE |  |  |  |
|---|------|--|--|--|

|   |      |  |  |  |
|---|------|--|--|--|
| 8 | IDLE |  |  |  |
|---|------|--|--|--|

|   |      |  |  |  |
|---|------|--|--|--|
| 9 | IDLE |  |  |  |
|---|------|--|--|--|

|    |      |  |  |  |
|----|------|--|--|--|
| 10 | IDLE |  |  |  |
|----|------|--|--|--|

|    |      |  |  |  |
|----|------|--|--|--|
| 11 | IDLE |  |  |  |
|----|------|--|--|--|

|    |      |  |  |  |
|----|------|--|--|--|
| 12 | IDLE |  |  |  |
|----|------|--|--|--|

|    |      |  |  |  |
|----|------|--|--|--|
| 13 | IDLE |  |  |  |
|----|------|--|--|--|

|    |      |  |  |  |
|----|------|--|--|--|
| 14 | IDLE |  |  |  |
|----|------|--|--|--|

DISPLAY\_NOP\_USERS complete

Please perform the following:

- Remind the Telco personnel to inform 'active' NOP users listed above (if any) to log out of their session(s) before the S/W upgrade can continue.
- Remind the Telco personnel to contact the high profile customers to ensure that they are not in emergency call processing mode and inform them of the approximate SWACT time.
- Disable all polling and periodic testing. There is to be no activity on the Core, MS and CLOCK until cleared by the software delivery engineer.

WARNING: FAILURE TO COMPLY MAY RESULT IN A SYSTEM RESTART.

- Ensure no further activity is performed on the DPP, including DPP polling or disk backup, and inform the downstream processing center.
- Dump all special logs so they can be restored onto the new load after postswact has completed.

Step PREPARE\_FOR\_SWACT is complete.

The SWUPGRADE process has paused. Enter GO.

- 6 Type GO and press the Enter key to confirm PREPARE\_FOR\_SWACT.  
*Step STATUSCHECK runs and completes.*  
*Step CHECK\_LOGS\_5 runs and completes.*  
*Step TRANSFER\_TIMINGS runs and completes.*
- 7 This procedure is complete. Proceed to [SWACT](#).

## SWACT

**CAUTION****Possible loss of service**

Before proceeding with SWACT, check the GUIs for CCA, SAM21 EM and Ethernet Routing Switch 8600. Check the logs for those devices to be sure that the links are stable and clear and any alarms for those devices.

***SDE — At the ACTIVECM window***

- 1 Review the instructions for step SWACT.

Starting step SWACT.

Confirm that the Inactive CA Application is NOT JAMmed,

-or- RELEASE the JAM and confirm when complete:

At the Active TPCMTC MAP; CAMtc Level:

- 1) RELJAM - Release the Jam on the Inactive application

Type GO to confirm, and to continue the SWUPGRADE

Step SWACT is not complete.

The SWUPGRADE process has paused. Enter GO.

***SDE — At the CORE0 or CORE1 window***

- 2 Confirm that inactive Call Agent is not jammed or release the jam.

***SDE — At the ACTIVECM window***

- 3 Type GO and press the Enter key to continue with the SWACT.  
*The process performs final checks and pauses for a final NORESTARTSWACT confirmation.*

Beginning SWACT checks:

All the SWACT checks have finished successfully.

The VR\_PRESWACT\_TRANSFER step completed successfully.

All INSV and ISTB series 1 PMs will have execs loaded after the SWACT.

\*\*\*\*\* FINAL SWACT CONFIRMATION \*\*\*\*\*

Do you wish to proceed with the NORESTARTSWACT CC warm swact?

Step SWACT is not complete.

The SWUPGRADE process has paused. Enter GO.

- 4** Receive final agreement from the telephone operating company personnel to proceed with the SWACT. Type GO and press the Enter key once confirmation is received.

**5** Monitor the messages printed to the terminal and verify that activity does switch at the CORE0 or CORE1 windows.

Starting step SWACT.

After the completion of the CC warm swact, please log both the TRACE user and the ACT user onto the new active side and enter SWUPGRADE;GO.

All Pre-SWACT checks completed. Starting Warm SWACT now.

\*\*\*\*\* The cursor will not be returned \*\*\*\*\*

\*\*\*\*\* unless a critical failure occurs. \*\*\*\*\*

\*\*\*\*\* Now monitoring Warm SWACT messages.\*\*\*\*\*

Pre-initialization done

Communication established

Exchange of data with the mate done

Transfer of data done (FASPECT)

Data estimation done

Store allocated on active CC

Store allocated on inactive CC

AMA processing completed

SWACT Inactive Procs running, this may take a few minutes

Before\_callp\_stopped procs completed

Call processing in PM stopped

Call processing I/O in CC stopped

Call data extracted

Data transfer completed

*Activity switches to the upgrade call processing application. The connection at the ACTIVECM window is dropped.*

**6** Log in to the upgraded call processing application by telnetting to the CS 2000 Core Manager or CBM as user cmusr from the ACTIVECM and INACTIVECM windows.

**Note:** The switch provides a prompt to perform test calls after step RECOVER\_DIRP\_AND\_BILLING.

7 Continue the software upgrade.

> **SWUPGRADE ; GO**

8

**ATTENTION**

Instruct the operating company to perform a 911 test call. If the test call fails to complete, contact Nortel Emergency Recovery immediately. **Do not continue.** If the test call is successful, continue with the software upgrade and ensure the following actions take place:

- system recovery of all DIRP and billing subsystems
- system recovery of any critical alarms
- operating company begins test calls
- system logs are monitored for office stability

*Tracing begins and the software upgrade continues.*

*Step DISPLAY\_DATE completes.*

*Step RECOVER\_DIRP\_AND\_BILLING begins.*

2005/07/08 09:52 INACT\_LOGMSG

>**SWUPGRADE;GO**

SWUPGRADE:

This device is selected for TRACEing

Variable TRACE\_DEVICE has been set to TELNSVR00001.

Starting step DISPLAY\_DATE.

Date: 2005/07/08, Time: 10:18:17

Finished step DISPLAY\_DATE.

Starting step RECOVER\_DIRP\_AND\_BILLING.

To recover DIRP billing subsystems after the SWACT, please follow instructions in the NTP 'One Night Process Software Delivery Procedures'.

This verifies that all DIRP billing subsystems have properly recovered from the SWACT.

Check these devices for proper operation.

The DIRP increment of the IOD MAPCI level provides a QUERY command to verify the resulting disposition of these subsystems (i.e. QUERY AMA) and the DPP increment of the IOD MAP level allows the applicator to display the alarm status for the DPP active and standby units (command ERRMAP ALARMS) and also provides the ability to list DPP active files (command LSTACT).

Step RECOVER\_DIRP\_AND\_BILLING is complete.

The SWUPGRADE process has paused. Enter GO.

### Determine the next action.

|           | If                                                                                                                                                                                              | Do                                                                                             |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
|           | reversion to the old call processing application load is required                                                                                                                               | Type CANCEL, press the Enter key, and refer to <a href="#">Revert and Abort on page 1989</a> . |
|           | reversion is not required                                                                                                                                                                       | <a href="#">step 9</a>                                                                         |
| <b>9</b>  | No manual action is required for step RECOVER_DIRP_AND_BILLING. Type GO and press the Enter key.<br><i>Step RECOVER_DIRP_AND_BILLING completes.</i><br><i>Step PERFORM_TEST_CALLS_1 begins.</i> |                                                                                                |
| <b>10</b> | Have telephone operating company personnel perform test calls while the software upgrade process pauses 20 seconds.                                                                             |                                                                                                |



Starting step PERFORM\_TEST\_CALLS\_1.

AMAB has been added to the LOGS variable for automatic monitoring during the execution of the test calls for possible AMA test call failures.

Please perform the test calls that were identified ahead of time and documented in the test file scripts.

WARNING: If an abort becomes necessary due to critical test failures, refer to the 'Revert to the old load' procedure described in the ONP MOP.

The AutoONP process will continue in 20 seconds.

Finished step PERFORM\_TEST\_CALLS\_1.

**11** This procedure is complete. Determine the next action.

| If                                                                | Do                                                                                           |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| reversion to the old call processing application load is required | Type CANCEL, press the Enter key, and refer to <a href="#">Revert and Abort on page 1989</a> |
| reversion is not required                                         | proceed to <a href="#">START POSTSWACT on page 1981</a>                                      |

## START\_POSTSWACT

Step START\_POSTSWACT is automated and runs many substeps. The automated process stops at step PERFORM\_TEST\_CALLS\_2.

### **SDE — At the ACTIVECM window**

- 1 Monitor the progress of step START\_POSTSWACT.

*Step START\_POSTSWACT completes.*

*Step RESTART\_OLD\_LOAD runs and completes. This step performs a restart on the old call processing application software to verify that the old call processing software can accept activity in the event of software reversion.*

*Step PERFORM\_TEST\_CALLS\_2 begins.*

Finished step START\_POSTSWACT.

Starting step RESTART\_OLD\_LOAD.

Finished step RESTART\_OLD\_LOAD.

Starting step DRTIME\_PRINT.

A DRTIME PRINT was not requested.

Finished step DRTIME\_PRINT.

Starting step PERFORM\_TEST\_CALLS\_2.

If not already done, please perform test calls.

WARNING: If an abort becomes necessary due to critical test failures, refer to the 'Revert to the old load' procedure described in the ONP MOP.

Step PERFORM\_TEST\_CALLS\_2 is not complete.

The SWUPGRADE process has paused. Enter GO.

### **2**

#### **ATTENTION**

Do not proceed to step LOAD\_OLD\_SIDE\_BLADE until the test calls complete successfully. Once the old side Call Agent card is locked, normal abort is not supported.

Receive confirmation from the telephone operating company to proceed with the software upgrade.

Have operating company personnel perform test calls.

| If                        | Do                                                                                           |
|---------------------------|----------------------------------------------------------------------------------------------|
| reversion is required     | Type CANCEL, press the Enter key, and refer to <a href="#">Revert and Abort on page 1989</a> |
| reversion is not required | <a href="#">step 3</a>                                                                       |

**3** Type GO and press the Enter key to continue the upgrade.

**4** This procedure is complete. Proceed to [LOAD\\_OLD\\_SIDE\\_BLADE.](#)

## LOAD\_OLD\_SIDE\_BLADE

### ***SDE — At the ACTIVECM window***

- 1 Review the instructions printed to the terminal.

Starting step LOAD\_OLD\_SIDE\_BLADE.  
ACT - WARNING: The revert to the old load is not possible after the  
ACT - WARNING: Old Side Call Agent card has been Locked.  
Are you ready to continue?.  
Type GO to continue the SWUPGRADE.  
Step LOAD\_OLD\_SIDE\_BLADE is not complete.  
The SWUPGRADE process has paused. Enter GO.

Type GO and press the Enter key.

- 2 Review the instructions printed to the terminal.

Starting step LOAD\_OLD\_SIDE\_BLADE.  
Upgrade the Old Side Call Agent load at the SAM21 EM GUI  
by using the following manual procedure:

- 1) At Active COREMTC MAP (ccamtc coremtc), query the Inact blade IP addr
  - a) Use QueryIP command to determine IP address of mate blade.
- 2) At SAM21 EM GUI, open Card View for Inact Call Agent Card:
  - a) Under the Provisioning Tab, determine IP address of the card.
  - b) Ensure IP address in GUI matches inactive card IP address.
- 3) Under the States Tab, Lock the card
- 4) Under the Provisioning Tab, change the boot file:
  - a) Click Modify.
  - b) Change boot file name to new load.
  - c) Click Save.
- 5) Under the States Tab, Unlock the card
  - a) Monitor the boot progress in the History pane.
- 6) At Active COREMTC MAP, monitor Inact load initialization:
  - a) Inact status begins with "/booting"
  - b) Wait until the status becomes "/waiting"
- 7) At Inact COREMTC map (ccamtc coremtc), Validate newly booted load
  - a) Telnet/Login to the Inact Blade
  - b) Under the Sys level, QryLD must indicate the new load version

Type GO to continue the SWUPGRADE when above steps are successfully completed  
Step LOAD\_OLD\_SIDE\_BLADE is not complete.  
The SWUPGRADE process has paused. Enter GO.

For assistance, refer to the following procedures:

- [Locking the Call Agent on page 2028](#)
- [Reprovisioning the Call Agent platform load on page 2030](#)
- [Unlocking the Call Agent on page 2034](#)

**Note:** If CallAgent C\_MisM alarm is active at the CORE0 or CORE1 window, patch the platform software:

1. At the inactive maintenance window (CORE0 or CORE1) verify that this is the inactive Call Agent.
  2. Enter the Admin level and then the SWIM level.
  3. At the TRANSFER level a list of available patches is displayed
    - a. SELECT the patch by number
    - b. FETCH INA the patch to the INACTIVE unit
  4. At the PATCH level, for each patch to be applied and committed:
    - a. SELECT the patch by number
    - b. DISADMIN the patch and follow any special instructions
    - c. APPLY INA the patch to the INACTIVE unit
    - d. SELECT the patch by number
    - e. COMMIT INA the patch to the INACTIVE unit
- 3** Type GO and press the Enter key to complete step LOAD\_OLD\_SIDE\_BLADE.
- Step LOAD\_OLD\_SIDE\_BLADE completes.*
- 4** This procedure is complete. Continue to procedure [FINISH\\_POSTSWACT](#).

## FINISH\_POSTSWACT

*The events in the following procedure occur after Step LOAD OLD SIDE BLADE completes.*

### **SDE — At the ACTIVECM window**

#### **1 Step SYNC\_SWITCH begins.**

Starting step SYNC\_SWITCH.

Confirm that the Inactive CA Application is NOT JAMmed,  
-or- RELEASE the JAM and confirm when complete:

At the Active COREMTC MAP (ccamtc coremtc); CAMtc Level:

1)RELJAM - Release the Jam on the Inactive application

Type GO to confirm, and to continue the SWUPGRADE

Step SYNC\_SWITCH is not complete.

The SWUPGRADE process has paused. Enter GO.

Starting step SYNC\_SWITCH step.

SWUPGRADE has now reached the SYNC\_SWITCH step.

Are you ready to SYNC the switch?

Step SYNC\_SWITCH is not complete.

The SWUPGRADE process has paused. Enter GO.

Starting step SYNC\_SWITCH.

Step Footprint transfer is 0 % complete.

Step Footprint transfer is 10 % complete.

Step Footprint transfer is 20 % complete.

Step Footprint transfer is 30 % complete.

Step Footprint transfer is 40 % complete.

Step Footprint transfer is 50 % complete.

Step Footprint transfer is 60 % complete.

Step Footprint transfer is 70 % complete.

Step Footprint transfer is 80 % complete.

Step Footprint transfer is 90 % complete.

Step Footprint transfer is 100 % complete.

Step Memory Sync is 0 % complete.

Step Memory Sync is 10 % complete.

Step Memory Sync is 20 % complete.

Step Memory Sync is 30 % complete.

Step Memory Sync is 40 % complete.

Step Memory Sync is 50 % complete.

Step Memory Sync is 60 % complete.

Step Memory Sync is 70 % complete.

Step Memory Sync is 80 % complete.

Step Memory Sync is 90 % complete.

Step Memory Sync is 100 % complete.

Finished step SYNC\_SWITCH.

## 2 Type GO and press the Enter key.

*Step SYNC\_SWITCH completes. Optionally, monitor the synchronization from the CORE0 or CORE1 windows.*

*Step FINISH\_POSTSWACT runs and completes. This step executes any remaining POSTSWACT steps. Several reports about the software upgrade are printed to the terminal. If a step fails to complete, follow the instructions given; type GO and press the enter key to continue.*

*Step RESTORE\_PARMs runs and completes. This step restores the office parameters NODEREXCONTROL, LCDREX\_CONTROL, GUARANTEED\_TERMINAL\_CPU\_SHARE, and DUMP\_RESTORE\_IN\_PROGRESS that were saved in step PRINT\_PARMs\_AND\_SAVE.*

*Step RESET\_DEVICES runs and completes. This step verifies that all devices used during the software upgrade are set to their original values.*

*Step COMPLETE\_NEW\_LOAD\_INIT runs and completes. This step prints messages as a reminder to SITE that need to be performed after POSTSWACT is complete.*

Starting step COMPLETE\_NEW\_LOAD\_INIT.

- 1) Re-input any data changes made prior to the software update but not captured on journal file, if any.
- 2) Notify NOP end users to log back in.
- 3) Reassign all current PROFILE information (LOGIN or RESTART) in SFDEV.
- 4) Restore any special logs (listreps special).
- 5) Reassign any temporary log ROUTING setup via LOGUTIL.
- 6) Reassign any changes in the INTEG level of the MAP (for example, UPTH, BUFFSEL, FILTER and others).
- 7) If Network Management code blocking was removed earlier, have Network Maintenance personnel restore code blocking active.

Step COMPLETE\_NEW\_LOAD\_INIT is complete.  
The SWUPGRADE process has paused. Enter GO.

**SITE — At the ACTIVECM window**

- 3 Perform any actions specified in step COMPLETE\_NEW\_LOAD\_INIT.

**SDE — At the ACTIVECM window**

- 4 Type GO and press the Enter key to complete step COMPLETE\_NEW\_LOAD\_INIT.

*Step COMPLETE\_NEW\_LOAD\_INIT completes.*

*Step RESET\_LOGIN\_BANNER runs and completes. This step erases the software upgrade banner.*

*Step DUMP\_NEW\_LOAD runs and completes.*

*Step RESUME\_REX\_TEST runs and completes.*

*Step START\_JOURNAL\_FILE runs and completes.*

*Step PRINT\_SWUPGRADE\_REPORT runs and completes. This step prints the start and stop time for each step in the software upgrade.*

*Step STOP\_RECORD runs and completes.*

*Step UPGRADE\_COMPLETE begins.*

Starting step UPGRADE\_COMPLETE.

Process complete. You may now QUIT out of the SWUPGRADE increment.  
Finished step UPGRADE\_COMPLETE.

SWUPGRADE Process complete - all steps have been executed.

>**QUIT**

CI:

- 5 Type QUIT and press the Enter key.
- 6 The Call Agent software upgrade is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



---

## DUMP\_OFFICE\_IMAGE

---

### ***SITE — At the ACTIVECM window***

- 1      Nortel recommends making a backup of the new load.  
If the AUTODUMP MANUAL command is used, the ITOC is updated to reference the newly dumped load. Otherwise, use the SBF command within ITOCCI to set the boot file to the new load.  
  
Once the dump is complete, use the ITOCCI;LBF CM to verify that the boot file is set to the new load.  
  
The procedure for backing up a call processing application image is listed in procedure [Dumping a call processing application image](#) under heading [Backing up an image on page 1911](#).

---

## Revert and Abort

---

Perform this procedure only if it is necessary to abort (CANCEL) the SWUPGRADE.

### ***SDE — At the ACTIVECM window***

1 Type the following commands to abort the upgrade:

> **SWUPGRADE**

> **CANCEL**

*Two confirmations are required to continue.*

> **Y** (enter twice)

#### **Example**

The following is an example of the messages generated when the CANCEL command is entered at the ACTIVECM window and confirmed twice.

```

** **
** WARNING!! **
** **
** The CANCEL command cancels all work done **
** by SWUPGRADE so far. Once cancelled **
** SWUPGRADE has to be re-started. **
** To halt temporarily, use the PAUSE **
** command. Type: **
** HELP PAUSE **
** for more information. **
** **
** Do you wish to CANCEL the SWUPGRADE? **

Please confirm ("YES", "Y", "NO", or "N"):
>YES
```

```

** **
** WARNING!! **
** **
** CANCEL will rollback all completed steps. **
** The switch is not in sync. **
** Do you want to sync the switch during **
** the rollback? **

Please confirm ("YES", "Y", "NO", or "N"):
> YES
```

*End of example.*

**2****ATTENTION**

Watch the output messages on the TRACE DEVICE!

The TRACE DEVICE displays messages indicating what steps are being rolled back (see below). Upon getting the messages:

*The SWUPGRADE process has paused. Enter GO or type GO to resume CANCEL.*

The operator must follow the instructions printed to the TRACE DEVICE and type GO and press return on the ACTIVECM window until the following message appears:

*SWUPGRADE CANCEL is completed.  
You may now QUIT out of the SWUPGRADE increment.*

**3** After the SWACT, log in to the old load by typing the following in the ACTIVECM window. If using a terminal window as the trace device, repeat this step at a second terminal window.

> **telnet <cs\_2000\_core\_mgr\_ip\_addr>**

and logging in as cmuser. This action forwards the connection to the login prompt on the call processing application. Log in with a username and password:

> **<username> <password>**

or

> **<username>**

> **<password>**

Important: Immediately after logging in to the old load and before continuing the CANCEL, type the following:

> **TABXFR;CANCEL**

**\*\*WARNING:** This command cancels the data move. Once cancelled it cannot be restarted without rebooting the new BCS image. If a temporary halt is desired please use the HALT or STOPXFR commands. Do you wish to CANCEL the data move?

Please confirm ("YES", "Y", "NO", or "N"):

> **Y**

> **QUIT**

**4** Ensure the trace device is still set:

> **SWUPGRADE;DISP VAR TRACE\_DEVICE**

If the tracing is not set to a device, or if it is set to the wrong device, set the trace device as follows:

> **SET TRACE\_DEVICE <device\_name>**

**device\_name**

is a value like TELNSVR00445. Use the QUSER command to determine the correct device to use.

5 Continue the CANCEL to conclusion:

> **SWUPGRADE;GO**

6 Enter the following when SWUPGRADE CANCEL is complete:

> **QUIT ALL**

7 This procedure is complete. If applicable , return to the task flow or procedure that directed you to this procedure.

### Example session of SWUPGRADE CANCEL

WARNING: The rollback of software upgrade steps is about to start.  
Messages sent to 1 user.

Executing the step RESTART\_OLD\_LOAD.  
The step RESTART\_OLD\_LOAD is completed.

Executing the step STATUSCHECK.  
Checking Nodes Status  
Checking DS1 Carriers Status  
Checking MS Interface Cards Status  
Checking LIU Status  
Checking MS FBUS Status  
Checking Integrated Node Maintenance  
STATUSCHECK successful.  
The step STATUSCHECK is completed.

Executing the roll back for step recover\_dirp\_and\_billing.

Configure the DIRP billing subsystems for revert SWACT to the old load.

Note: For details for completing the following refer to "PRESWACT DIRP and billing" procedure.

- a. ACT Take down billing tapes and format new standby volumes in DIRP. Leave these demounted, they will become the active volumes after SWACT.  
Disk volumes will rotate and recover automatically after SWACT.



**Example session of SWUPGRADE CANCEL**

```
***** FINAL SWACT CONFIRMATION *****
Do you wish to proceed with the ABORTSWACT CC warm swact?
Execution is not complete.
The SWUPGRADE process has paused. Enter GO.

Executing the step SWACT.
After the completion of the CC warm swact, please log
both the TRACE user and the ACT user
onto the new active side and enter SWUPGRADE;GO.
All Pre-SWACT checks completed. Starting Warm SWACT now.
***** The cursor will not be returned *****
***** unless a critical failure occurs. *****
***** Now monitoring Warm SWACT messages.*****

Pre-initialization done

Communication established

Exchange of data with the mate done

Transfer of data done (FASPECT)

Data estimation done

Store allocated on active CC

Store allocated on inactive CC

AMA processing completed

 SWACT Inactive Procs running, this may take a few minutes
Before_callp_stopped procs completed

Call processing in PM stopped

Call processing I/O in CC stopped

Call data extracted

Data transfer completed

>
Connection closed by foreign host.
username@host:~$
%%
%% Telnet to the CS 2000 Core Manager and log in as user cmusr %%
%% The CS 2000 Core Manager forwards the connection to the %%
%% old PCL. Log in with <username> <password> %%
%%
```

**Example session of SWUPGRADE CANCEL**

```

** **
** WARNING...WARNING...WARNING...WARNING. **
** **
** In LINEMODE,To Enter into BREAK..... **
** **
** Press ^B, Type the Command and Press <Enter> **
** **
** Example: ^Bhx <Enter> **
** **
** **

Telnet LINEMODE.

Enter username and password
MIB variable CharOptionAllowed must be set first to allow CHAR MODE.
><username> <password>
MIKEM Logged in on 2005/10/21 at 11:11:14.

** **
** This is a private database. **
** All activity is subject to monitoring. **
** Any UNAUTHORIZED access or use is PROHIBITED, and **
** may result in PROSECUTION. **
** **

** **
** WARNING: SOFTWARE UPGRADE IS IN PROGRESS **
** ----- **
** **
** Please refrain from using SERVORD or TABLE EDITOR or **
** CI commands that may interfere with the process. **
** **
** Under no circumstances is SYNC to be done !!! **
** **

2005/10/06 14:32 swupgrade rollback doc
This device is selected for TRACEing

Executing the step DISPLAY_DATE
This device is selected for TRACEing
Variable TRACE_DEVICE has been set to TELNSVR00002.

Starting step DISPLAY_DATE.
Date: 2005/10/21, Time: 11:11:33
The step DISPLAY_DATE is completed
```

**Example session of SWUPGRADE CANCEL**

Resetting the default tabxfr platform.  
Tabxfr platform has been reset to XACORE.

Executing the step START\_POSTSWACT

|                     |           |
|---------------------|-----------|
| REACTIVATE_TRIGASGN | executing |
| REACTIVATE_TRIGASGN | complete  |

|               |           |
|---------------|-----------|
| DIRP_RECOVERY | executing |
| DIRP_RECOVERY | complete  |

|            |           |
|------------|-----------|
| DIRP_AUDIT | executing |
| DIRP_AUDIT | complete  |

|                |           |
|----------------|-----------|
| HARDWARE_CHECK | executing |
| HARDWARE_CHECK | complete  |

...

|               |           |
|---------------|-----------|
| BEGIN_TESTING | executing |
| BEGIN_TESTING | complete  |

Enter Postswact after office testing has been completed  
The step START\_POSTSWACT is completed

Executing the step CHECK\_LOGS\_1

New logs on ACTIVE unit since 2005/10/21 11:00:04:

|       |     |
|-------|-----|
| TRAP  | : 0 |
| SWERR | : 1 |

Use command DISPLAY LOG <log name> <n or ALL> [Act or Inact]  
to see the content of a log.

Execution completed.

The SWUPGRADE process has paused. Enter GO.

Executing the rollback for step PRESWACT\_DIRP\_AND\_BILLING.

Please follow the step Recover billing from the ONP MOP  
procedure Revert to old load to perform the rollback  
of the step PRESWACT\_DIRP\_AND\_BILLING.

Execution completed.

The SWUPGRADE process has paused. Enter GO.

Executing the step RESTORE\_PARMS

The step RESTORE\_PARMS is completed.

Executing the step PERFORM\_TEST\_CALLS.

AMAB has been added to the LOGS variable for  
automatic monitoring during the execution of the  
test calls for possible AMA test call failures.



**Example session of SWUPGRADE CANCEL**

```
If not already done, please perform test calls.
Execution is not complete.
The SWUPGRADE process has paused. Enter GO.

Executing the step PERFORM_TEST_CALLS.
AMAB has been removed from the LOGS variable.
The step PERFORM_TEST_CALLS is completed.
Reload the original New Side Call Agent load at the SAM21 EM GUI
by using the following manual procedure:
 1) At Active COREMTC MAP (ccamtc coremtc), query the Inact blade IP
address:
 a) Use QueryIP command to determine IP address of mate blade.
 2) At SAM21 EM GUI, open Card View for Inact Call Agent Card:
 a) Under the Provisioning Tab, determine IP address of the card.
 b) Ensure IP address in GUI matches inactive card IP address.
 3) Under the States Tab, Lock the card
 4) Under the Provisioning Tab, change the boot file:
 a) Click Modify.
 b) Restore the boot file name to the original load file.
 c) Click Save.
 5) Under the States Tab, Unlock the card
 a) Monitor the boot progress in the History pane.
 6) At Active COREMTC MAP, monitor Inact load initialization:
 a) Inact status begins with "/booting"
 b) Wait until the status becomes "/waiting"
 7) At Inactive COREMTC map (ccamtc coremtc), Validate newly booted load:
 a) Telnet/Login to the Inact Blade
 b) Under the Sys level, QryLD must indicate the original load version
Type GO to continue the SWUPGRADE when complete
Execution is not complete.
The SWUPGRADE process has paused. Enter GO.

Executing the step SYNC_SWITCH.
SWUPGRADE has now reached the SYNC_SWITCH step.
Are you ready to SYNC the switch?
Execution is not complete.
The SWUPGRADE process has paused. Enter GO.

Executing the step SYNC_SWITCH.
The step SYNC_SWITCH is completed.

Executing the step FINISH_POSTSWACT

XA_UNSPPLIT executing
XA_UNSPPLIT complete
...
Executing the step RESET_DEVICES
The step RESET_DEVICES is completed.
```

**Example session of SWUPGRADE CANCEL**

If any abort actions are required for step READ\_BULLETINS, please perform them now.

Execution completed.

The SWUPGRADE process has paused. Enter GO.

Executing the ABORT\_PRESWACT.

|                |           |
|----------------|-----------|
| REACTIVATE_DCT | executing |
|----------------|-----------|

|                |          |
|----------------|----------|
| REACTIVATE_DCT | complete |
|----------------|----------|

|                     |           |
|---------------------|-----------|
| REACTIVATE_TRIGASGN | executing |
|---------------------|-----------|

|                     |          |
|---------------------|----------|
| REACTIVATE_TRIGASGN | complete |
|---------------------|----------|

|                    |           |
|--------------------|-----------|
| NBD_ABORT_PRESWACT | executing |
|--------------------|-----------|

|                    |          |
|--------------------|----------|
| NBD_ABORT_PRESWACT | complete |
|--------------------|----------|

|                     |           |
|---------------------|-----------|
| RESET_OFFICE_TUPLES | executing |
|---------------------|-----------|

WARNING: Guaranteed\_Terminal\_CPU\_Share already restored.

WARNING: Auxcp\_Cpu\_Share already restored.

|                     |          |
|---------------------|----------|
| RESET_OFFICE_TUPLES | complete |
|---------------------|----------|

|                  |           |
|------------------|-----------|
| ENABLE_AUTOIMAGE | executing |
|------------------|-----------|

|                  |          |
|------------------|----------|
| ENABLE_AUTOIMAGE | complete |
|------------------|----------|

|                  |           |
|------------------|-----------|
| ENABLE_PES_AUDIT | executing |
|------------------|-----------|

|                  |          |
|------------------|----------|
| ENABLE_PES_AUDIT | complete |
|------------------|----------|

|            |           |
|------------|-----------|
| RESUME_ATT | executing |
|------------|-----------|

|            |          |
|------------|----------|
| RESUME_ATT | complete |
|------------|----------|

|                        |           |
|------------------------|-----------|
| RESET_SIS_ROUTING_DATA | executing |
|------------------------|-----------|

|                        |          |
|------------------------|----------|
| RESET_SIS_ROUTING_DATA | complete |
|------------------------|----------|

|                      |           |
|----------------------|-----------|
| CLEANUP_VR_MATE_DATA | executing |
|----------------------|-----------|

|                      |          |
|----------------------|----------|
| CLEANUP_VR_MATE_DATA | complete |
|----------------------|----------|

ABORT\_PRESWACT has completed.

Execution completed.

Executing the step STOP\_RECORD

The step STOP\_RECORD is completed.

The rollback of SWUPGRADE steps is completed.

SWUPGRADE CANCEL is completed.

You may now QUIT out of the SWUPGRADE increment.

>

%%%%%%%%%%%%%%%%%%%%%%%%

%% > QUIT ALL %%

%%%%%%%%%%%%%%%%%%%%%%%%

*End of example.*

---

## Revert and Abort for offices with Message Controller cards

---

This procedure is only for offices configured with Message Controller (MC) cards. Perform the procedure only if it is necessary to abort (CANCEL) the SWUPGRADE.

### ***SDE — At the ACTIVECM window***

- 1 Type the following commands to abort the upgrade:

```
> SWUPGRADE
> CANCEL
```

*Two confirmations are required to continue.*

```
> Y (enter twice)
```

#### ***Example:***

The following is an example of the messages generated when the CANCEL command is entered at the ACTIVECM window and confirmed twice.

```

** **
** WARNING!! **
** **
** The CANCEL command cancels all work done
** by SWUPGRADE so far. Once cancelled
** SWUPGRADE has to be re-started.
** To halt temporarily, use the PAUSE
** command. Type:
** HELP PAUSE
** for more information.
**
** Do you wish to CANCEL the SWUPGRADE?

Please confirm ("YES", "Y", "NO", or "N"):
>YES

** **
** WARNING!! **
** **
** CANCEL will rollback all completed steps.
** The switch is not in sync.
** Do you want to sync the switch during
** the rollback?

Please confirm ("YES", "Y", "NO", or "N"):
> YES
```

*End of example*

**2****ATTENTION**

Watch the output messages on the TRACE DEVICE!

The TRACE DEVICE displays messages informing the operator what steps are being rolled back (see below). Upon getting the messages:

```
The SWUPGRADE process has paused. Enter GO or
type GO to resume CANCEL
```

The operator must follow the instructions printed to the TRACE DEVICE and type GO and press return on the ACTIVECM window until the following message appears:

```
SWUPGRADE CANCEL is completed.
You may now QUIT out of the SWUPGRADE
increment.
```

- 3** After the SWACT, log in to the old load by typing the following in the ACTIVECM window. If using a terminal window as the trace device, repeat this step at a second terminal window.

```
> telnet <cs_2000_core_mgr_ip_addr>
```

and logging in as cmusr. This action forwards the connection to the login prompt on the call processing application. Log in with a username and password.

Important: Immediately after logging in to the old load and before continuing the CANCEL, type the following:

```
> TABXFR;CANCEL
```

```
**WARNING: This command cancels the data move.
Once cancelled it cannot be restarted without
rebooting the new BCS image. If a temporary halt
is desired please use the HALT or STOPXFR
commands. Do you wish to CANCEL the data move?
```

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

```
> Y
```

```
> QUIT
```

- 4** Continue the CANCEL to conclusion:

```
> SWUPGRADE;GO
```

- 5** Enter the following when SWUPGRADE CANCEL is complete:

```
> QUIT ALL
```

- 6** This procedure is complete. If applicable, return to the task flow or procedure that directed you this procedure.

#### Example session of SWUPGRADE CANCEL

Messages sent to 1 user.

Executing the step RESTART\_OLD\_LOAD.  
The step RESTART\_OLD\_LOAD is completed.

Executing the step STATUSCHECK.  
Checking Nodes Status  
Checking DSL Carriers Status  
Checking MS Interface Cards Status  
Checking LIU Status  
Checking MS FBUS Status  
Checking Integrated Node Maintenance  
STATUSCHECK successful.  
The step STATUSCHECK is completed.

Executing the roll back for step recover\_dirp\_and\_billing.

Configure the DIRP billing subsystems for revert SWACT to the old load.

Note: For details for completing the following refer to "PRESWACT DIRP and billing" procedure.

- a. ACT Take down billing tapes and format new standby volumes in DIRP. Leave these demounted, they will become the active volumes after SWACT.  
Disk volumes will rotate and recover automatically after SWACT.  
Parallel volumes on tape (or DPP/BMC) can be recovered manually after SWACT.
- b. INACT Ensure datafill is correct on the inactive side for table DIRPPPOOL.
- c. INACT if DIRP\_REC file is present on the inactive SFDEV, ensure each entry in DIRP\_REC is correct for the revert SWACT.  
Note: In DIRP\_REC the parallel volume assignments for DIRPPPOOL should be set to nil (\$) for all pools.

Execution completed.

The SWUPGRADE process has paused. Enter GO.

>go

**Example session of SWUPGRADE CANCEL**

WARNING: SWUPGRADE is about to execute the ABORTSWACT step.  
Do you wish to proceed?

Execution completed.  
The SWUPGRADE process has paused. Enter GO.  
>go

Executing the step PRELOAD\_EXECS.  
Successfully fetched: KSETEX  
Successfully fetched: DTCEX  
Successfully fetched: POTSEX  
PRELOAD\_EXECS complete

Executing the step SWACT.  
Confirm that the Inactive CA Application is NOT JAMmed,  
-or- RELEASE the JAM and confirm when complete:  
At the Active COREMTC MAP (ccamtc coremtc); CAMtc Level:  
1) RELJAM - Release the Jam on the Inactive application  
Type GO to confirm, and to continue the SWUPGRADE  
Execution is not complete.  
The SWUPGRADE process has paused. Enter GO.  
>go

Executing the step SWACT.  
Beginning SWACT checks:  
All the SWACT checks have finished successfully.

\*\*\*\*\* FINAL SWACT CONFIRMATION \*\*\*\*\*  
Do you wish to proceed with the ABORTSWACT CC warm swact?  
Execution is not complete.  
The SWUPGRADE process has paused. Enter GO.  
>go

Executing the step SWACT.  
After the completion of the CC warm swact, please log  
both the TRACE user and the ACT user  
onto the new active side and enter SWUPGRADE;GO.  
All Pre-SWACT checks completed. Starting Warm SWACT now.  
\*\*\*\*\* The cursor will not be returned \*\*\*\*\*  
\*\*\*\*\* unless a critical failure occurs. \*\*\*\*\*  
\*\*\*\*\* Now monitoring Warm SWACT messages.\*\*\*\*\*

Pre-initialization done

Communication established

Exchange of data with the mate done

**Example session of SWUPGRADE CANCEL**

```
Transfer of data done (FASPECT)

Data estimation done

Store allocated on active CC

Store allocated on inactive CC

AMA processing completed

 SWACT Inactive Procs running, this may take a few minutes

Before_callp_stopped procs completed

Call processing in PM stopped

Call processing I/O in CC stopped

Call data extracted

Data transfer completed

>
Connection closed by foreign host.

**** telnet to Core
telnet 10.40.54.72
Telnet escape character is '^G'.
Trying 10.40.54.72...
Connected to 10.40.54.72.
Escape character is '^G'.
Trying to complete connection. Please wait...

** **
** WARNING...WARNING...WARNING...WARNING. **
** **
** **
** In LINEMODE, To Enter into BREAK..... **
** **
** Press ^B, Type the Command and Press <Enter> **
** **
** Example: ^Bhx <Enter> **
** **
** **

Telnet LINEMODE.
```

**Example session of SWUPGRADE CANCEL**

```

Enter username and password
>mikem admin (<--example username and password)
MIKEM Logged in on 2005/03/16 at 18:56:49.

** **
** This is a private database. **
** All activity is subject to monitoring. **
** Any UNAUTHORIZED access or use is PROHIBITED, and **
** may result in PROSECUTION. **
** **

** **
** WARNING: SOFTWARE UPGRADE IS IN PROGRESS **
** ----- **
** **
** Please refrain from using SERVORD or TABLE EDITOR or **
** CI commands that may interfere with the process. **
** **
** Under no circumstances is SYNC to be done !!! **
** **

2005/03/16 12:45 psnncsh08bb 3pc_tdm
>TABXFR;CANCEL

** **
** WARNING!! **
** **
** This command cancels the data move. Once cancelled it **
** cannot be restarted without rebooting the new BCS image. **
** If a temporary halt is desired, please use the HALT **
** or STOPXFR command. **
** **
** Do you wish to cancel the data move? **
** **

Please confirm ("YES", "Y", "NO", or "N"):
>Y
>QUIT

>swupgrade
SWUPGRADE:
>go

This device is selected for TRACEing
Variable TRACE_DEVICE has been set to TELNSVR00001.
It is recommended that this value NOT be changed.
Variable TRACE_USER has been reset to the SWUPGRADE user: MIKEM

```



**Example session of SWUPGRADE CANCEL**

```
Starting DISPLAY_DATE.
Date: 2005/03/16, Time: 18:56:53
The step DISPLAY_DATE is completed.

Resetting the default tabxfer platform.
Tabxfr platform has been reset to STANDARD.

Executing the step START_POSTSWACT

REACTIVATE_TRIGASGN executing
REACTIVATE_TRIGASGN complete

DIRPOOL2_CONSOLE executing
DIRPOOL2_CONSOLE complete

DIRP_RECOVERY executing
DIRP_RECOVERY complete

DIRP_AUDIT executing
DIRP_AUDIT complete

.....

BEGIN_TESTING executing
BEGIN_TESTING complete

Enter Postswact after office testing has been completed
The step START_POSTSWACT is completed

Executing the step CHECK_LOGS_1
New logs on ACTIVE unit since 2005/03/16 18:22:47:
 TRAP : 0
 SWERR : 0
Use command DISPLAY LOG <log name> <n or ALL> [Act or Inact]
to see the content of a log.
The step CHECK_LOGS_1 is completed.
Executing the rollback for step PRESWACT_DIRP_AND_BILLING.

Please follow the step Recover billing from the ONP MOP
procedure Revert to old load to perform the rollback
of the step PRESWACT_DIRP_AND_BILLING.
Execution completed.
The SWUPGRADE process has paused. Enter GO.
>go

Executing the step RESTORE_PARMS
The step RESTORE_PARMS is completed.
```

**Example session of SWUPGRADE CANCEL**

Executing the step PERFORM-TEST\_CALLS.

AMAB has been added to the LOGS variable for automatic monitoring during the execution of the test calls for possible AMA test call failures.

If not already done, please perform test calls.

Execution is not complete.

The SWUPGRADE process has paused. Enter GO.

>go

Executing the step PERFORM\_TEST\_CALLS.

AMAB has been removed from the LOGS variable.

The step PERFORM\_TEST\_CALLS is completed.

Reload the original New Side Call Agent load at the SAM21 EM GUI by using the following manual procedure:

- 1) At Active COREMTC MAP (ccamtc coremtc), query the Inact blade IP address:
  - a) Use QueryIP command to determine IP address of mate blade.
- 2) At SAM21 EM GUI, open Card View for Inact Call Agent Card:
  - a) Under the Provisioning Tab, determine IP address of the card.
  - b) Ensure IP address in GUI matches inactive card IP address.
- 3) Under the States Tab, Lock the card.
- 4) Under the Provisioning Tab, change the boot file:
  - a) Click Modify.
  - b) Restore the boot file name to the original load file.
  - c) Click Save.
- 5) Under the States Tab, Unlock the card.
  - a) Monitor the boot progress in the History pane.
- 6) At Active COREMTC MAP, monitor Inact load initialization:
  - a) Inact status begins with "/booting"
  - b) Wait until the status becomes "/waiting"
- 7) At Inactive COREMTC map (ccamtc coremtc), Validate newly booted load:
  - a) Telnet/Login to the Inact Blade.
  - b) Under the Sys level, QryLD must indicate the original load version.

Type GO to continue the SWUPGRADE when complete.

Execution is not complete.

The SWUPGRADE process has paused. Enter GO.

>go

Executing the step SYNC\_SWITCH.

Confirm that the Inactive CA Application is NOT JAMmed,

-or- RELEASE the JAM and confirm when complete:

At the Active COREMTC MAP (ccamtc coremtc); CAMtc Level:

- 1) RELJAM - Release the Jam on the Inactive application.

Type GO to confirm, and to continue the SWUPGRADE.

Execution is not complete.

The SWUPGRADE process has paused. Enter GO.

>go

**Example session of SWUPGRADE CANCEL**

Executing the step SYNC\_SWITCH.  
SWUPGRADE has now reached the SYNC\_SWITCH step.  
Are you ready to SYNC the switch?  
Execution is not complete.  
The SWUPGRADE process has paused. Enter GO.  
>go

Executing the step SYNC\_SWITCH.  
Step Footprint transfer is 0% complete.  
Step Footprint transfer is 10% complete.  
Step Footprint transfer is 20% complete.  
Step Footprint transfer is 30% complete.  
.....  
Step Footprint transfer is 100% complete.  
Step Memory Sync is 0% complete.  
Step Memory Sync is 10% complete.  
Step Memory Sync is 20% complete.  
Step Memory Sync is 30% complete.  
.....  
Step Memory Sync is 100% complete.  
The step SYNC\_SWITCH is completed.

Starting step RELOAD\_MC1\_BLADE.  
Reload the original MC load on MC 1 at the SAM21 EM GUI.  
by using the following manual procedure:

- 1) At the MAPCI;MTC;MS map level, verify that MS 0 is the master MS.
- 2) If MS 0 is not the master, perform a SWMAST. If performed, soak 10 minutes.
- 3) At SAM21 EM GUI, open Card View for MC 1.
  - a) Under the Provisioning Tab, determine IP address of the card.
  - b) Ensure IP address in GUI matches IP address of MC 1.
- 4) Under the States Tab, Lock the card.
  - a) Wait for the lock icon to appear.
- 5) Under the Provisioning Tab, change the boot file:
  - a) Click Modify.
  - b) Restore the boot file name to the original MC load file.
  - c) Click Save.
- 6) Under the States Tab, Unlock the card.
  - a) Wait for the lock icon to disappear.
- 7) At Active CCAMTC Map; MC Level, Validate newly booted load.
  - a) QryLd command for MC must indicate original MC load version.
- 8) Soak for 10 minutes, monitoring logs.

Type GO to continue the SWUPGRADE when above steps are successfully completed.  
Execution is not complete.  
The SWUPGRADE process has paused. Enter GO.  
>go

**Example session of SWUPGRADE CANCEL**

Starting step RELOAD\_MC0\_BLADE.

Reload the original MC load on MC 0 at the SAM21 EM GUI.

by using the following manual procedure:

- 1) At the MAPCI;MTC;MS map level, verify that MS 1 is the master MS.
- 2) If MS 1 is not the master, perform a SWMAST. If performed, soak 10 minutes.
- 3) At SAM21 EM GUI, open Card View for MC 0.
  - a) Under the Provisioning Tab, determine IP address of the card.
  - b) Ensure IP address in GUI matches IP address of MC 0.
- 4) Under the States Tab, Lock the card.
  - a) Wait for the lock icon to appear.
- 5) Under the Provisioning Tab, change the boot file:
  - a) Click Modify.
  - b) Restore the boot file name to the original MC load file.
  - c) Click Save.
- 6) Under the States Tab, Unlock the card.
  - a) Wait for the lock icon to disappear.
- 7) At Active CCAMTC Map; MC Level, Validate newly booted load.
  - a) QryLd command for MC must indicate original MC load version.
- 8) Soak for 10 minutes, monitoring logs.

Type GO to continue the SWUPGRADE when above steps are successfully completed.

Execution is not complete.

The SWUPGRADE process has paused. Enter GO.

>go

Executing the step FINISH\_POSTSWACT

|          |           |
|----------|-----------|
| CCA_SYNC | executing |
| CCA_SYNC | complete  |

|                              |           |
|------------------------------|-----------|
| ENABLE_PATCH_AUDIT_POSTSWACT | executing |
| ENABLE_PATCH_AUDIT_POSTSWACT | complete  |

|                                               |           |
|-----------------------------------------------|-----------|
| POST_MS_CHECK                                 | executing |
| Load in MS 0 = MS-U23BD                       |           |
| Load in MS 1 = MS-U23BD                       |           |
| Passed POST_MS_CHECK for active CM load: 23BB |           |
| POST_MS_CHECK                                 | complete  |

|                                                          |           |
|----------------------------------------------------------|-----------|
| RESET_OFFICE_TUPLES                                      | executing |
| WARNING: Guaranteed_Terminal_CPU_Share already restored. |           |
| RESET_OFFICE_TUPLES                                      | complete  |

.....

|                      |          |                                |
|----------------------|----------|--------------------------------|
| DELETE_DPT_LNODES    | complete | 03/16/05 19:00:01 00:00:00:000 |
| CLEANUP_VR_MATE_DATE | complete | 03/16/05 19:00:01 00:00:00:004 |

## Example session of SWUPGRADE CANCEL

Total execution time for all complete procedures is 00:00:25.057.

```
All POSTSWACT steps completed successfully.
```

|               |          |          |          |           |
|---------------|----------|----------|----------|-----------|
| ONP Steps     | Start    | Stop     | Elapsed  | Operative |
| Drop Sync     | N/A      | N/A      | N/A      | N/A       |
| Loadmate Prep | N/A      | N/A      | N/A      | N/A       |
| .....         | ...      | ...      | ...      | ...       |
| Postswact     | 18:56:48 | 19:00:01 | 00:03:03 | 00:00:25  |
| TOTALS        | 12:25:20 | 19:00:01 | 06:34:41 | 00:09:27  |

The step FINISH\_POSTSWACT is completed.

### Executing the step DUMP\_NEW\_LOAD

No Automatic Image Dump was requested. If needed, please dump the image manually as soon as possible.

The step DUMP\_NEW\_LOAD is completed.

The journal file was not originally on.

It will not be restarted automatically.

```
Executing the step RESET_DEVICES.
```

The step RESET\_DEVICES is completed.

```
If any abort actions are required for step READ_BULLETINS,
please perform them now.
```

```
Execution completed.
```

The SWUPGRADE process has paused. Enter GO.

>go

Executing the ABORT\_PRESWACT.

```
REACTIVATE_DCT executing
```

```
REACTIVATE_DCT complete
```

```
REACTIVATE_TRIGASGN executing
```

```
REACTIVATE_TRIGASGN complete
```

```
NBD_ABORT_PRESWACT executing
```

```
NBD_ABORT_PRESWACT complete
```

```
RESET_OFFICE_TUPLES executing
```

WARNING: Guaranteed\_Terminal\_CPU\_Share already restored.

WARNING: Auxcp\_Cpu\_Share already restored.

```
RESET_OFFICE_TUPLES complete
```

```
ENABLE_AUTOIMAGE executing
```

```
ENABLE_AUTOIMAGE complete
```

```
ENABLE PES AUDIT executing
```

```
ENABLE_PES_AUDIT complete
```

```
RESUME ATT executing
```

```
RESUME ATT complete
```

```
RESET SIS ROUTING DATA executing
```

```
RESET SIS ROUTING DATA complete
```

**Example session of SWUPGRADE CANCEL**

```
CLEANUP_VR_MATE_DATA executing
CLEANUP_VR_MATE_DATA complete
ABORT_PRESWACT has completed.
Execution completed.

Executing the step STOP_RECORD
The step STOP_RECORD is completed.

The rollback of SWUPGRADE steps is completed.

SWUPGRADE CANCEL is completed.
You may now QUIT out of the SWUPGRADE increment.
>quit
CI:
>
```

*End of example*

## Loading Message Controller 1

### ATTENTION

Perform this step only if the CS 2000 - Compact is configured with Message Controller cards.

### At the MAP

- 1 At the MAPCI;MTC;MS level, ensure that MS 0 is the master MS.

|            | MS             | IOD | Net | PM     | CCS   | Lns   | Trks | Ext               | APPL |
|------------|----------------|-----|-----|--------|-------|-------|------|-------------------|------|
|            | .              | .   | .   | .      | .     | .     | ...  | .                 | .    |
| MS         | Message Switch |     |     |        | Clock | Shelf | 0    | Inter-MS Link 0 1 |      |
| 0 Quit     | MS 0           | .   |     | M Free |       | F     |      |                   | ..   |
| 2          | MS 1           | .   |     | Slave  |       | F     |      |                   | ..   |
| 3          |                |     |     |        |       |       |      |                   |      |
| 4          |                |     |     |        |       |       |      |                   |      |
| 5          |                |     |     |        |       |       |      |                   |      |
| 6 Tst_     |                |     |     |        |       |       |      |                   |      |
| 7 Bsy_     |                |     |     |        |       |       |      |                   |      |
| 8 RTS_     |                |     |     |        |       |       |      |                   |      |
| 9          |                |     |     |        |       |       |      |                   |      |
| 10 LoadMS_ |                |     |     |        |       |       |      |                   |      |

- 2 If MS 0 is not the master MS, perform an SWMAST . If SWMAST is performed, then soak 10 minutes before continuing.

### At the active Call Agent Manager

- 3 At the MCMtc level, verify that both Message Controllers are in service (.) prior to Locking Message Controller 1 in the next step.

|        | CallAgent | SYS | CON   | APPL    | MC    | Unit: 0 |
|--------|-----------|-----|-------|---------|-------|---------|
|        | .         | .   | .     | .       | .     |         |
| MCMtc  | Blade:    |     | Eth0: | Eth1:   | Atm0: | Atm1:   |
| 0 Quit | MC0       | .   | . Act | . Inact | open  | open    |
| 2      | MC1       | .   | . Act | . Inact | open  | open    |
| 3      |           |     |       |         |       |         |

- 4 Exit the Call Agent Manager interface and determine the IP address of Message Controller 1:

```
>0 ALL
[mtc@hostname mtc]$ grep mc1 /etc/hosts

The grep command returns the address of Message
Controller 1.

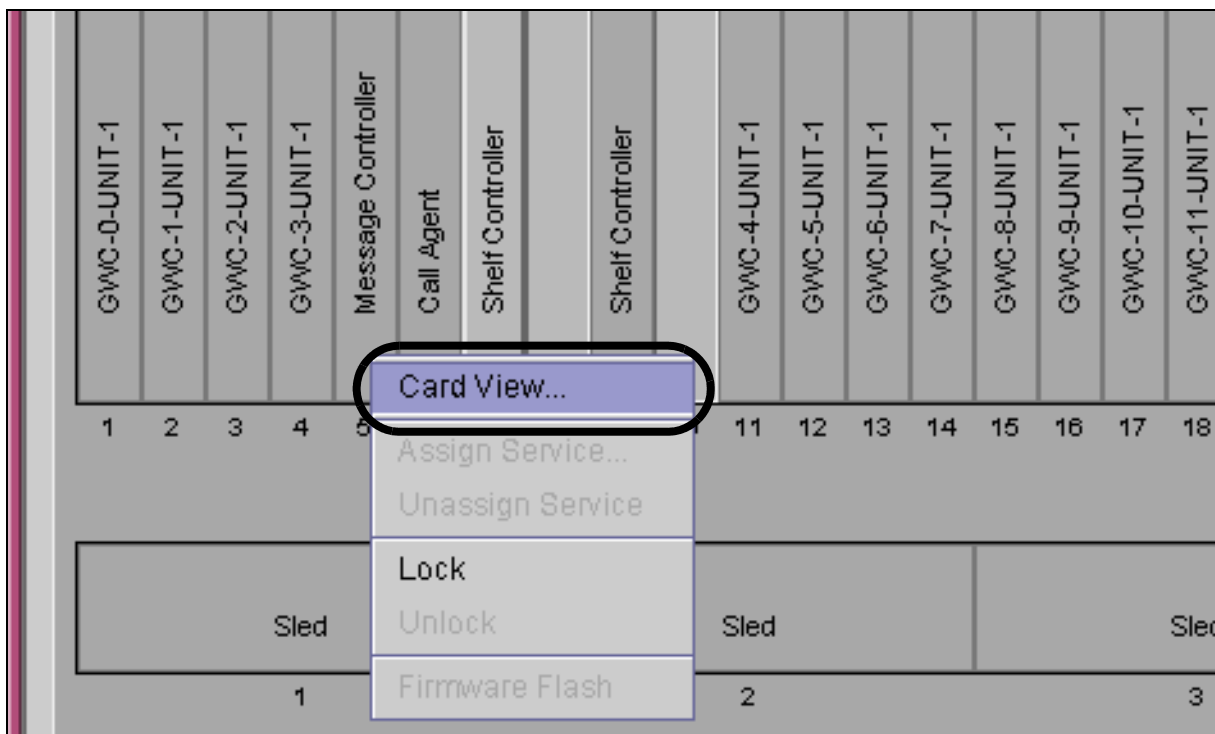
10.40.54.61 mc1
```

- 5 Start the Call Agent Manager interface again:

```
[mtc@hostname mtc]$ ccamtc mcmtc
```

***At the CS 2000 SAM21 Manager client***

- 6 From the Shelf View, right-click the card and select Card View.



*The Card View window opens.*

- 7 Select the Provisioning tab on the Card View window.  
Ensure that the IP address specified in the IP field matches the IP address of Message Controller 1. If the values do not match,



open a different Shelf View from the CS 2000 SAM21 Manager and check the Message Controller provisioning for that shelf.

The screenshot shows a web-based interface for a Nortel CSAM-1 Slot 5. The title bar reads "CSAM-1 Slot 5 CardView@wnc2s0j6". Below the title bar is a menu bar with "File" and "View". The main content area is titled "CSAM-1 : Slot 5" and contains several tabs: "Alarms", "Equip", "States", "Diags", and "Provisioning". The "Provisioning" tab is selected. On the left side of the interface is a vertical sidebar labeled "Message Controller" with a "5" at the bottom. The "Provisioning" tab is divided into two sections: "General" and "Load Info". The "General" section contains fields for "IP:" (10.40.54.61), "Gateway IP:" (10.40.54.1), "Subnet Mask:" (255.255.255.0), "FW Version:" (N), "MAC 1:" (0001af01cdd4), and "MAC 2:" (Unknown). The "Load Info" section contains fields for "Server IP:" (10.40.54.1), "Path:" (/swd/3pc), and "Load:" (ncgl\_mc\_image\_7.15.1.0). There is also a checkbox labeled "FW Flash Enable" which is currently unchecked.

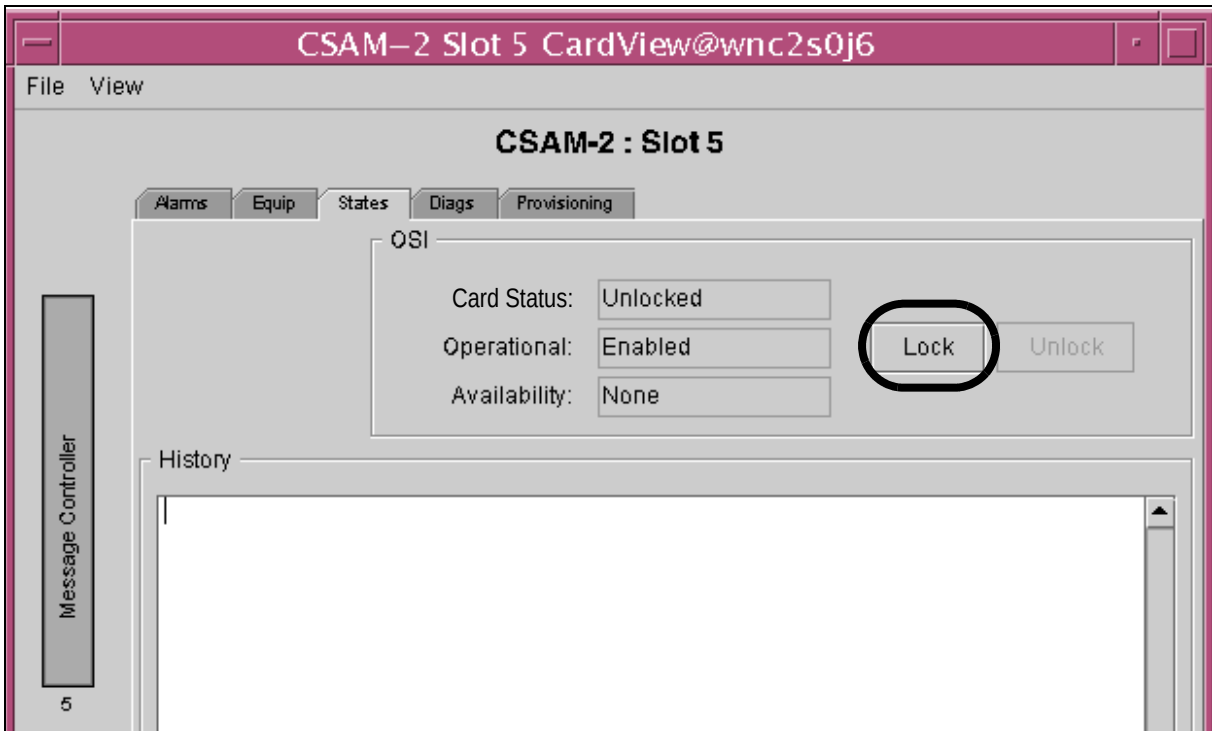
| General      |               |
|--------------|---------------|
| IP:          | 10.40.54.61   |
| Gateway IP:  | 10.40.54.1    |
| Subnet Mask: | 255.255.255.0 |
| FW Version:  | N             |
| MAC 1:       | 0001af01cdd4  |
| MAC 2:       | Unknown       |

| Load Info                                |                        |
|------------------------------------------|------------------------|
| Server IP:                               | 10.40.54.1             |
| Path:                                    | /swd/3pc               |
| Load:                                    | ncgl_mc_image_7.15.1.0 |
| <input type="checkbox"/> FW Flash Enable |                        |

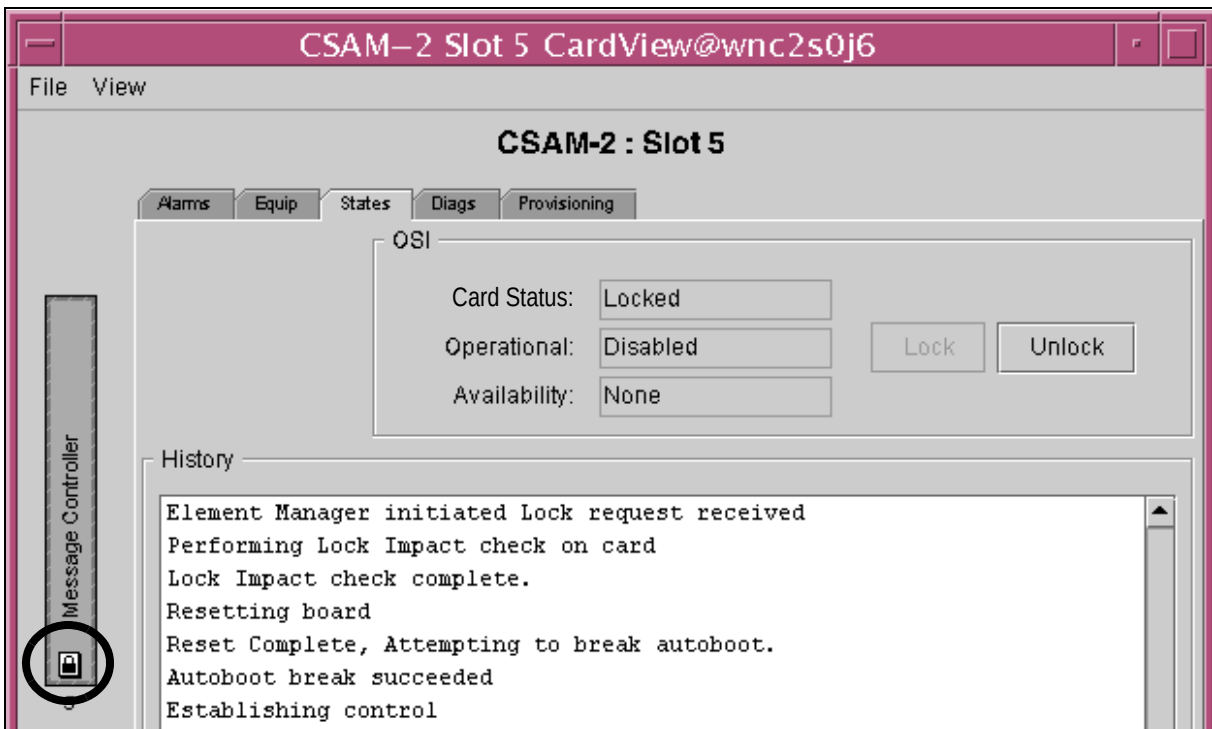
8 Click the States tab.

Click the Lock button.



*A lock warning dialog window opens. Confirm the lock warning.*

9 Wait for the lock icon to appear on the card icon.

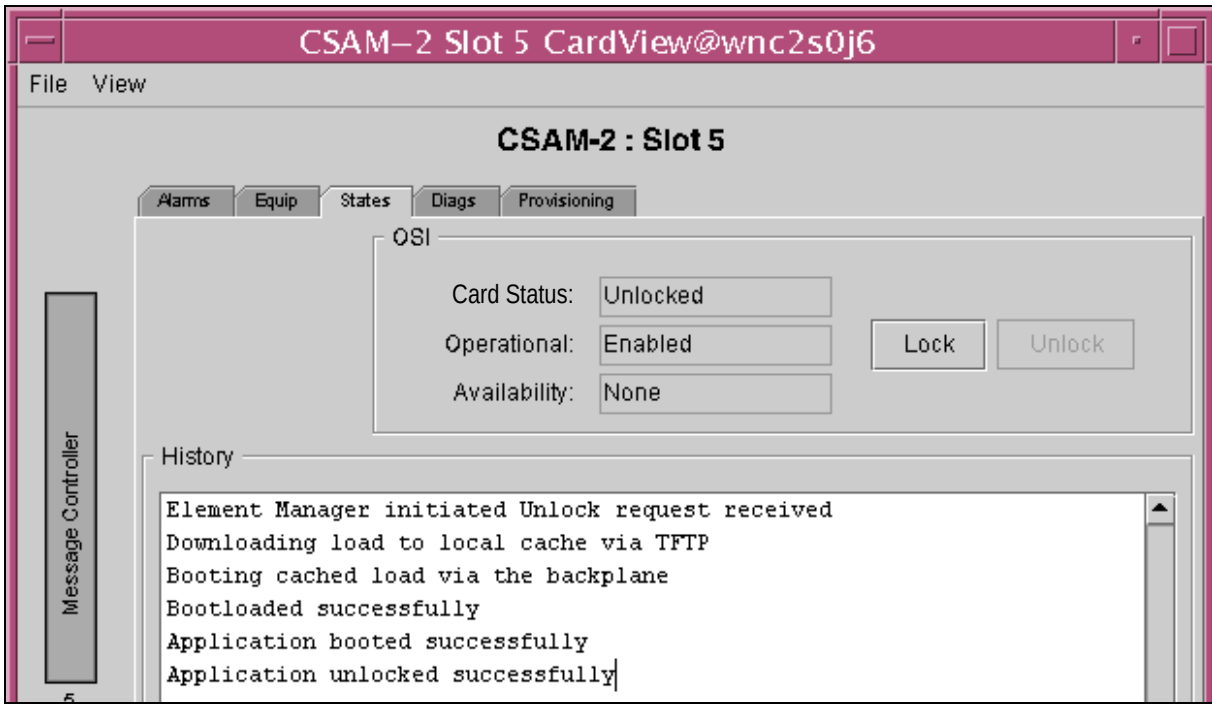


*At the Call Agent Manager, a major ATM alarm is raised, the Message Controller enters the Remote Busy (R) state and is reported as out of service.*

- 10 Click the Provisioning tab, click on Modify, change the Load value to the new software load name, and click Save.

The screenshot shows a web-based configuration interface for a Nortel device. The title bar reads "CSAM-2 Slot 5 CardView@wnc2s0j6". The interface has a "File View" menu and a "Message Controller" sidebar. The main content area is titled "CSAM-2 : Slot 5" and contains several tabs: "Alarms", "Equip", "States", "Diags", and "Provisioning". The "Provisioning" tab is selected, showing a "General" section with fields for IP (10.40.54.61), Gateway IP (10.40.54.1), Subnet Mask (255.255.255.0), FW Version (N), MAC 1 (0001af01cdd4), and MAC 2 (Unknown). Below this is the "Load Info" section, which includes fields for Server IP (10.40.54.1), Path (/swd/3pc), and Load (ncgl\_mc\_image\_8.20.1.0). The "Load" field is highlighted with a red circle. There is also a checkbox for "FWFlash Enable". Below the "Load Info" section is the "Message Controller Data" section with radio buttons for "Unit 0" and "Unit 1" (selected). The "Call Agent Links" section has fields for "Call Agent 0 IP" (10.40.54.67) and "Call Agent 1 IP" (10.40.54.70). At the bottom, there are buttons for "Modify", "Save", "Clear", "Cancel", and "Details...". The "Save" button is highlighted with a red circle.

- 11 Click the States tab and click the Unlock button.  
Wait for the lock icon to disappear.



*At the Call Agent Manager, the card enters the in service state (.), and the major ATM alarm clears. The Message Controller can raise a major MCTbl alarm while the Message Controller synchronizes to the NTP server.*

**At the active Call Agent Manager**

- 12 Query the software load for Message Controller 1 and ensure that the new load is reported:

**>QryLd 1**

```
CallAgent SYS CON APPL MC Unit: 0
.
MCMtc Blade: Eth0: Eth1: Atm0: Atm1:
0 Quit MC0 . . Act . Inact open open
2 MC1 . . Act . Inact open open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 TrnsL
9
10
11
12
13 LogQuery
14 Alarm
15
16 MC Load report retrieved on Thu Jun 19 14:15:54 2004:
17 Help
18 Refresh Ramdisk: ncgl_mc_image_8.20.1.0
 mtc
Time 13:48 >
```

*Soak the load for 10 minutes while monitoring log reports.*

- 13** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Loading Message Controller 0

### ATTENTION

Perform this step only if the CS 2000 - Compact is configured with Message Controller cards.

### At the MAP

- 1 At the MAPCI;MTC;MS level, ensure that MS 1 is the master MS.

|            | MS             | IOD | Net    | PM | CCS   | Lns | Trks              | Ext | APPL |
|------------|----------------|-----|--------|----|-------|-----|-------------------|-----|------|
|            | .              | .   | .      | .  | .     | .   | ...               | .   | .    |
| MS         | Message Switch |     | Clock  |    | Shelf | 0   | Inter-MS Link 0 1 |     |      |
| 0 Quit     | MS 0           | .   | Slave  |    |       | F   | ..                |     |      |
| 2          | MS 1           | .   | M Free |    |       | F   | ..                |     |      |
| 3          |                |     |        |    |       |     |                   |     |      |
| 4          |                |     |        |    |       |     |                   |     |      |
| 5          |                |     |        |    |       |     |                   |     |      |
| 6 Tst_     |                |     |        |    |       |     |                   |     |      |
| 7 Bsy_     |                |     |        |    |       |     |                   |     |      |
| 8 RTS_     |                |     |        |    |       |     |                   |     |      |
| 9          |                |     |        |    |       |     |                   |     |      |
| 10 LoadMS_ |                |     |        |    |       |     |                   |     |      |

- 2 If MS 1 is not the master MS, perform an SWMAST. If SWMAST is performed, then soak 10 minutes before continuing.

### At the active Call Agent Manager

- 3 At the MCMtc level, verify that both Message Controllers are in service (.) prior to Locking Message Controller 0 in the next step.

|        | CallAgent | SYS | CON   | APPL    | MC    | Unit: 0 |
|--------|-----------|-----|-------|---------|-------|---------|
|        | .         | .   | .     | .       | .     |         |
| MCMtc  | Blade:    |     | Eth0: | Eth1:   | Atm0: | Atm1:   |
| 0 Quit | MC0       | .   | . Act | . Inact | open  | open    |
| 2      | MC1       | .   | . Act | . Inact | open  | open    |
| 3      |           |     |       |         |       |         |

- 4 Exit the Call Agent Manager interface and determine the IP address of Message Controller 0:

```
>0 ALL
```

```
[mtc@hostname mtc]$ grep mc0 /etc/hosts
```

*The grep command returns the address of Message Controller 0.*

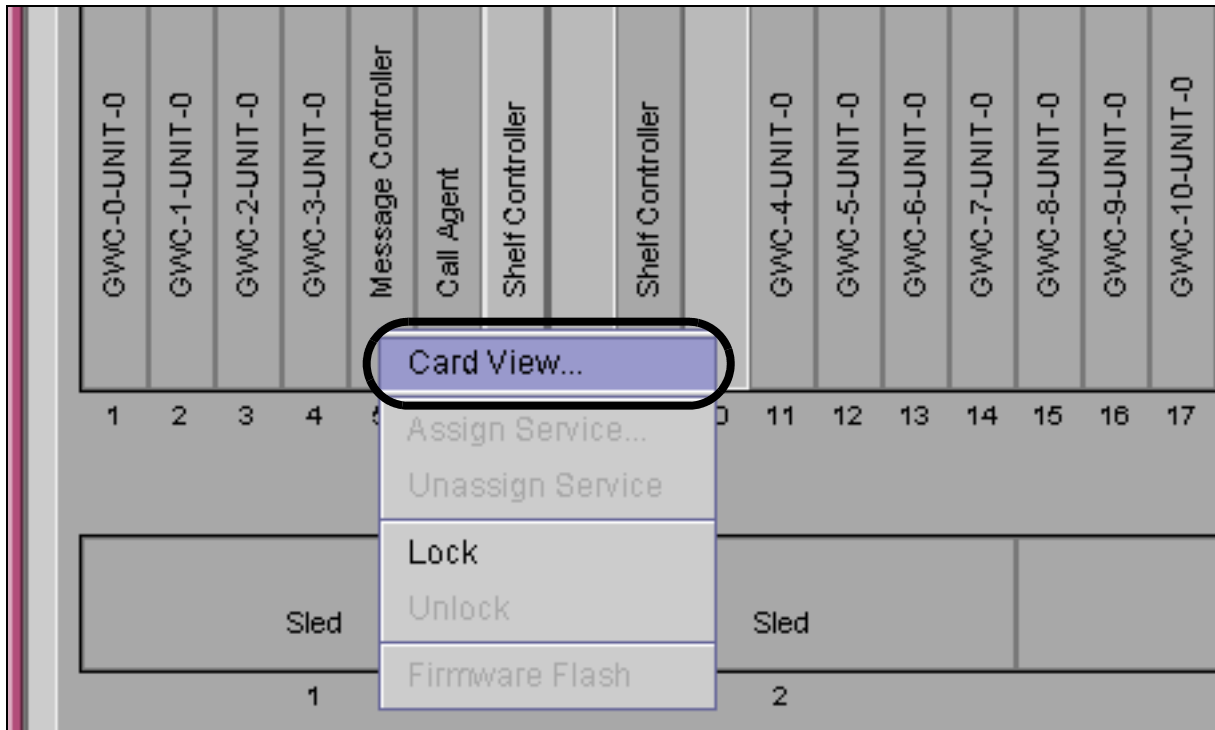
```
10.40.54.60 mc0
```

- 5 Start the Call Agent Manager interface again:

```
[mtc@hostname mtc]$ ccamtc mcmtc
```

***At the CS 2000 SAM21 Manager client***

- 6 From the Shelf View, right-click the card and select Card View.

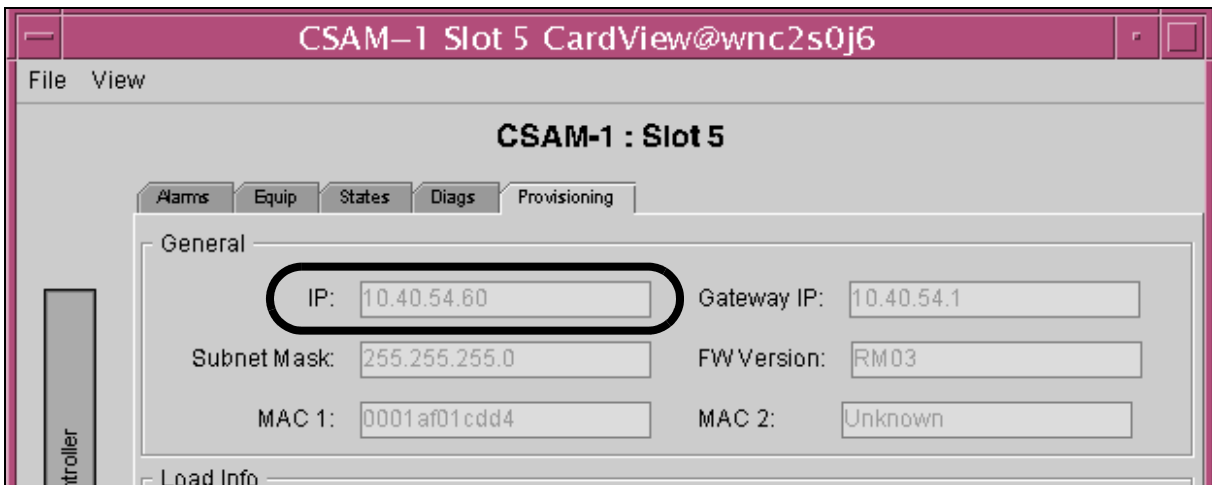


*The Card View window opens.*

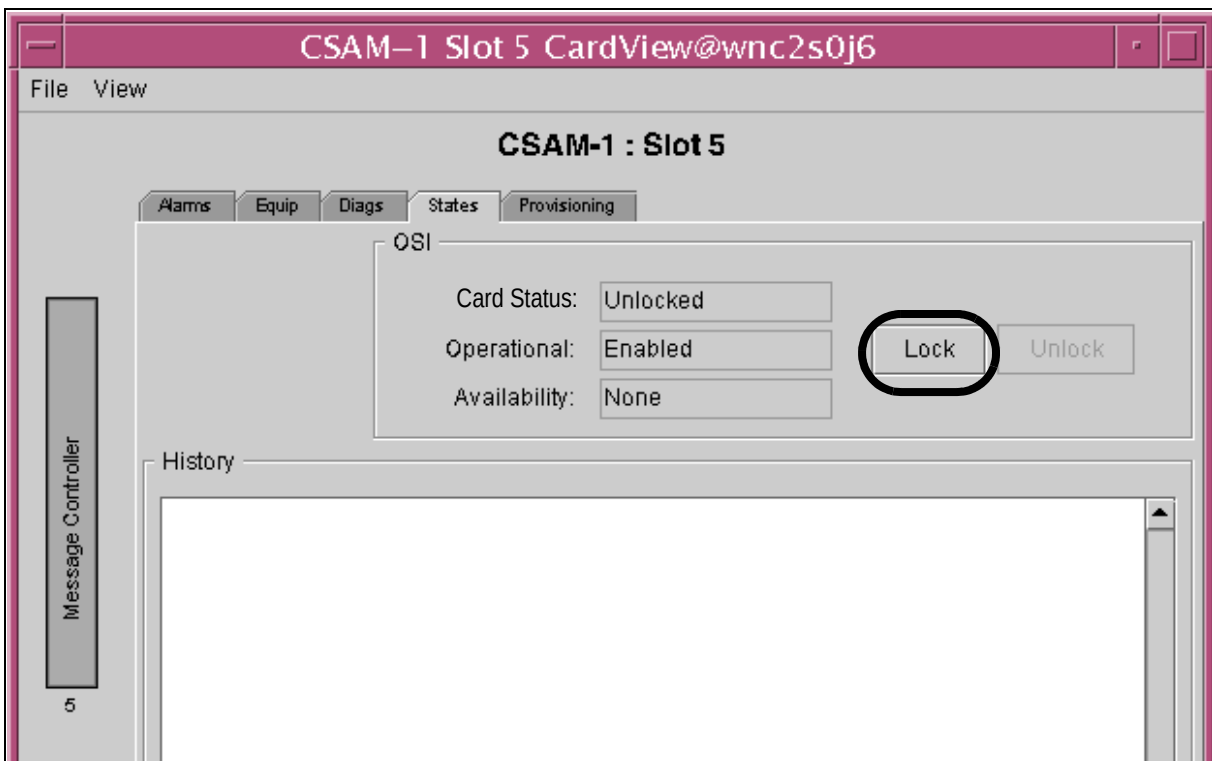
- 7 Select the Provisioning tab on the Card View window.  
Ensure that the IP address specified in the IP field matches the IP address of Message Controller 0. If the values do not match,



open a different Shelf View from the CS 2000 SAM21 Manager and check the Message Controller provisioning for that shelf.

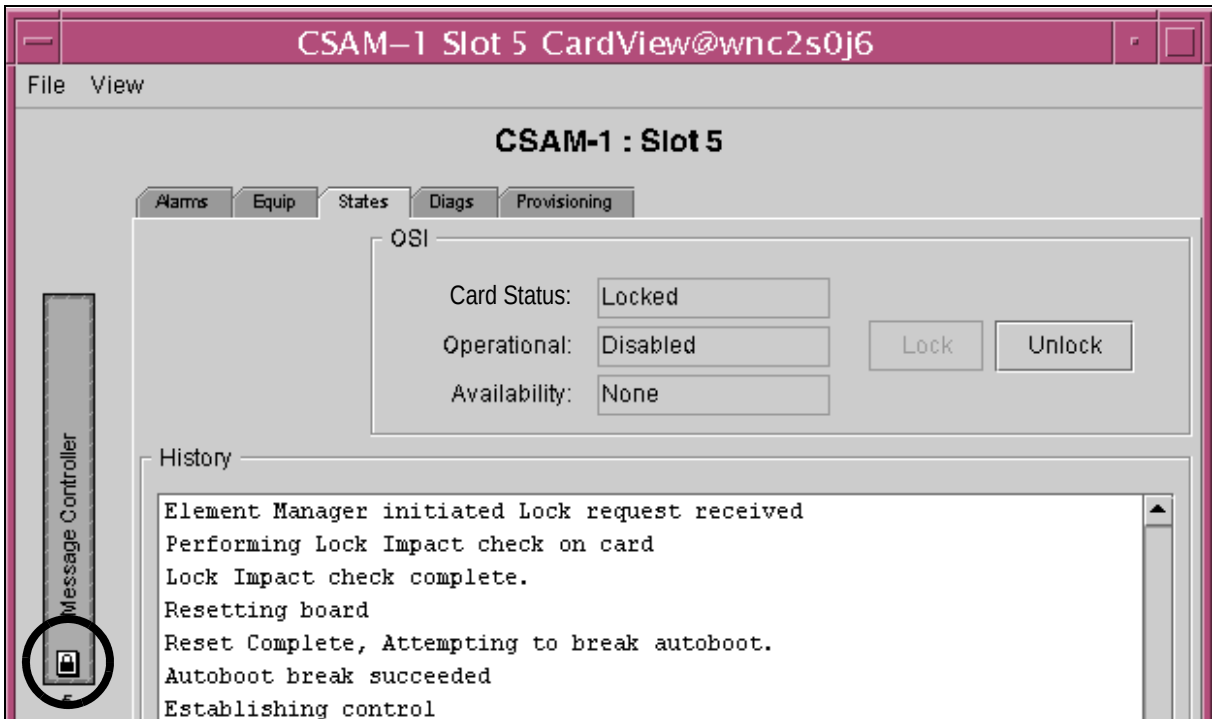


- 8 Click on the States tab.  
Click on the Lock button.



*A lock warning dialog window opens. Confirm the lock warning.*

9 Wait for the lock icon to appear on the card icon.



*At the Call Agent Manager, a major ATM alarm is raised, the Message Controller enters the Remote Busy (R) state and is reported as out of service.*

- 10 Click the Provisioning tab, change the Load value to the new software load name, and click Save.

CSAM-1 Slot 5 CardView@wnc2s0j6

File View

CSAM-1 : Slot 5

Alarms Equip Diags States **Provisioning**

General

IP: 10.40.54.60 Gateway IP: 10.40.54.1

Subnet Mask: 255.255.255.0 FW Version: RM03

MAC 1: 0001af01cdd4 MAC 2: Unknown

Load Info

Server IP: 10.40.54.1

Path: /swd/3pc

Load: ncgl\_mc\_image\_8.20.1.0

☐ FW Flash Enable

Message Controller Data

☒ Unit 0 ☐ Unit 1

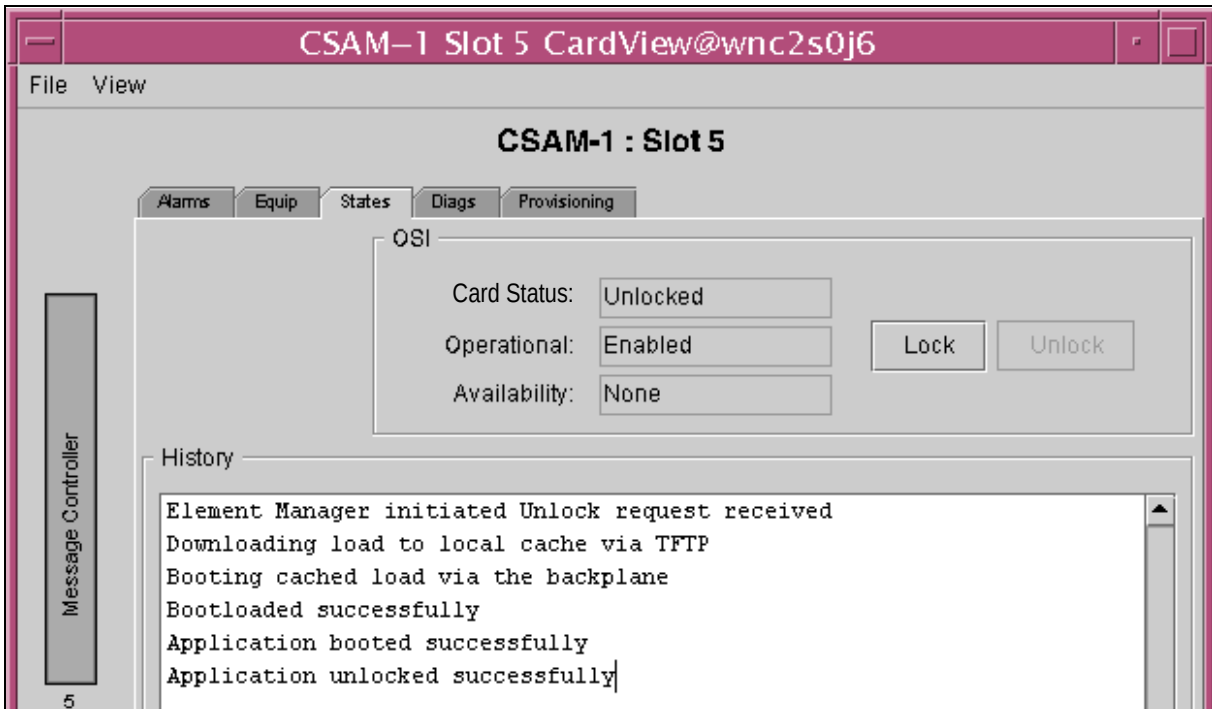
Call Agent Links

Call Agent 0 IP: 10.40.54.67

Call Agent 1 IP: 10.40.54.70

Modify **Save** Clear Cancel Details...

- 11 Click the States tab and click the Unlock button.  
Wait for the lock icon to disappear.



*At the Call Agent Manager, the card enters the in service state (.), and the major ATM alarm clears. The Message Controller can raise a major MCTbl alarm while the Message Controller synchronizes to the NTP server.*

**At the active Call Agent Manager**

- 12 Query the software load for Message Controller 0 and ensure that the new load is reported:

**>QryLd 0**

```
CallAgent SYS CON APPL MC Unit: 0
.
MCMtc Blade: Eth0: Eth1: Atm0: Atm1:
0 Quit MC0 . . Act . Inact open open
2 MC1 . . Act . Inact open open
3
4
5 QryLd
6 QryHits
7 ClrHits
8 TrnsL
9
10
11
12
13 LogQuery
14 Alarm
15
16 MC Load report retrieved on Thu Jun 19 13:48:45 2005:
17 Help
18 Refresh Ramdisk: ncgl_mc_image_8.20.1.0
 mtc
Time 13:48 >
```

*Soak the load for 10 minutes while monitoring log reports.*

- 13** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Stopping the journal file

---

### ***SITE —At the ACTIVECM window***

- 1 Enter the device independent recording package (DIRP) level and query journal file activity:  
**> MAPCI;MTC;IOD;DIRP;QUERY JF ALL**
- 2 Stop all journal file activity:  
**> JF STOP**
- 3 Close the active journal file and confirm the prompt:  
**> CLOSE JF ACTIVE**  
**> YES**
- 4 Query the journal file again to verify rotation of the storage:  
**> QUERY JF ALL**
- 5

#### **ATTENTION**

SERVORD activity, OSSgate activity, and table changes are not permitted.

Inform all operating company personnel that data changes such as SERVORD, OSSgate, and table changes must be halted until after the upgrade is completed. Data changes made during the software upgrade can cause ONP process problems and can result in lost data on the restored side.

This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Jamming the inactive Call Agent

### *At the active Call Agent Manager*

**1** Issue the Jam command:

```
> ccamtC
> CoreMtc
> CAMtc
> Jam
```

```
CallAgent SYS CON APPL Unit: 0
JInact . . .

CAMtc
0 Quit Unit0 Act no . Inact . Act . . insync .
2 Jam Unit1 Inact yes . Inact . Act . . insync .
3 RelJam
4 RExTst
5 SwAct
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 Jam: Jam the inactive unit, to prevent it taking activity.
17 Help Pams: [FORCE]
18 Refresh FORCE - bypass system stability checks
 mtc
Time 10:38 >
```

*A JInact alarm appears in the alarm banner under CallAgent.*

**2** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Dropping application image synchronization

### *At the active Call Agent Manager*

1 Enter the DpSync command:

```
> CoreMtc
> Appl
> DpSync
```

```
CallAgent SYS CON APPL Unit: 0
JInact . . simplex
M
Appl
0 Quit Unit0 Act no . Inact . Act . NA nosync .
2 ImgTst Unit1 Inact yes . Act . Inact . NA nosync /restart
3 Sync
4 DpSync
5
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP DpSync: Drop application synchronization.
16 Parms: [RestartType]
17 Help Restart - (WARM | COLD | RELOAD | NORESTART)
18 Refresh (default) - COLD
 mtc
Time 12:25
```

2 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Locking the Call Agent



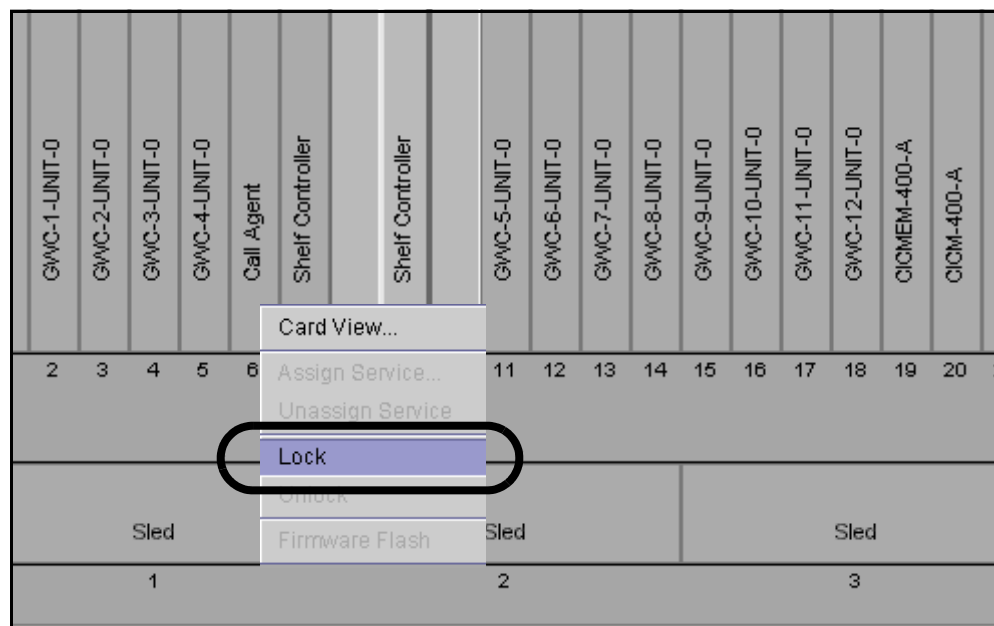
### CAUTION

#### Possible service interruption

Do not lock the active Call Agent. The CS 2000 SAM21 Manager client responds to an active Call Agent lock with a warning. Click **No**. Do not click Yes. The inactive Call Agent is located in the other CS 2000 SAM21 Manager shelf and a lock request does not provide a warning when the Call Agent is inactive.

### At the CS 2000 SAM21 Manager client

- 1 From the Shelf View, right click on the card and select Lock from the context menu.



**Note:** Lock is also available from the States tab of the Card View window.

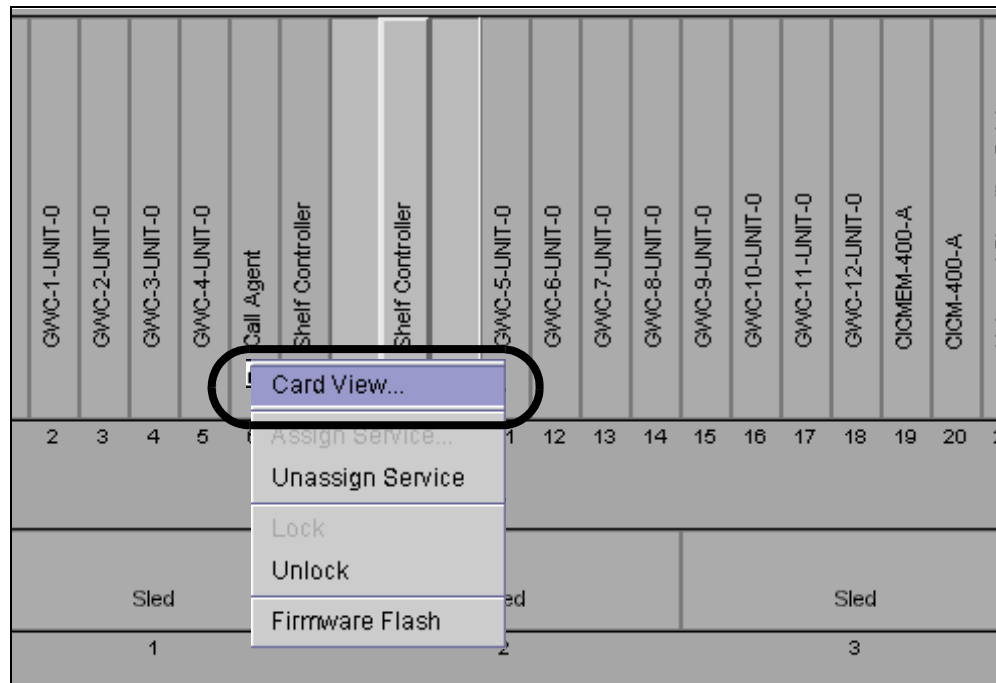
- 2 Do not confirm a lock warning. The warning is only available for the active Call Agent. Wait for the lock icon to appear on the selected card.
- 3 This procedure is complete.



## Reprovisioning the Call Agent platform load

### *At the CS 2000 SAM21 Manager client*

- 1 From the Shelf View, right-click the card and select Card View from the context menu to open the Card View window.



- 2 Click the Provisioning tab from the Card View window.

The screenshot shows the 'OTT4 CA-1 Slot 6 CardView@ucars01x3c.ca.nortel.com (CM CLI: BNR\_LAB\_LOAD)' window. The 'Provisioning' tab is selected and circled. The window contains several sections: 'General' with fields for IP (10.72.17.22), Gateway IP (10.72.16.1), Subnet Mask (255.255.240.0), FW Version (RM03-2.4), MAC Address (0001AF12AFA0), and MAC 2 (0001AF12AF9F); 'NTP' with Primary NTP (47.135.43.193) and Secondary NTP (47.135.43.196); 'Load Info' with Server IP (47.135.43.193), Path (/3pc), Load (ncgl\_cca\_image\_7.02.1.0), and a 'Get Load Files' button; and 'Geographical CS 2000 Compact' with an 'Enable' checkbox and a 'Backup Path' section containing GEO UNIT 0 IP (10.72.0.12) and GEO UNIT 1 IP (10.72.0.20). The 'Modify' button at the bottom is also circled.

- 3 Click the Modify button.
- 4 Click the Get Load Files button.

5 Select the load from the drop-down list.

- ncgl\_cca\_765\_image.8.20.1.0 (765 is added for loads based on the MCPN765 processor card)
- ncgl\_cca\_905\_image.8.20.1.0 (905 is added for loads based on the MCPN905-270 processor card, introduced in SN09)

The following example display assumes a software load based on the MCPN765 processor card.

OTT4 CA-1 Slot 6 CardView@ucars01x3c.ca.nortel.com (CM CLI: BNR\_LAB\_LOAD)

File View

**OTT4 CA-1 : Slot 6**

Alarms Equip States Diags Provisioning

General

IP: 10.72.17.22 Gateway IP: 10.72.16.1

Subnet Mask: 255.255.240.0 FW Version: RM03-2.4

MAC Address: 0001AF12AFA0 MAC 2: 0001AF12AF9F

NTP

Primary NTP: 47.135.43.193 Secondary NTP: 47.135.43.196

Load Info

Server IP: 47.135.43.193

Path: /3pc

Load: ncgl\_cca\_image\_7.02.1.0 Get Load Files

☒ FW Flash Enable

Network File System Message Controller Geographical Survivable

Geographical CS 2000 Compact

☒ Enable

Backup Path:

GEO UNIT 0 IP: 10.72.0.12 Mask: 255.255.255.248

GEO UNIT 1 IP: 10.72.0.20 Mask: 255.255.255.248

Modify Save Clear Cancel Details... Help

**Note 1:** To verify the card type, click the Equip tab. The panel displays the appropriate card (MCPN765 or MCPN905-270) and memory size.

**Note 2:** Click the firmware flash enable (FW Flash Enable) checkbox if the *SAM21 Platform Base Release Notes* indicate a firmware upgrade is available.

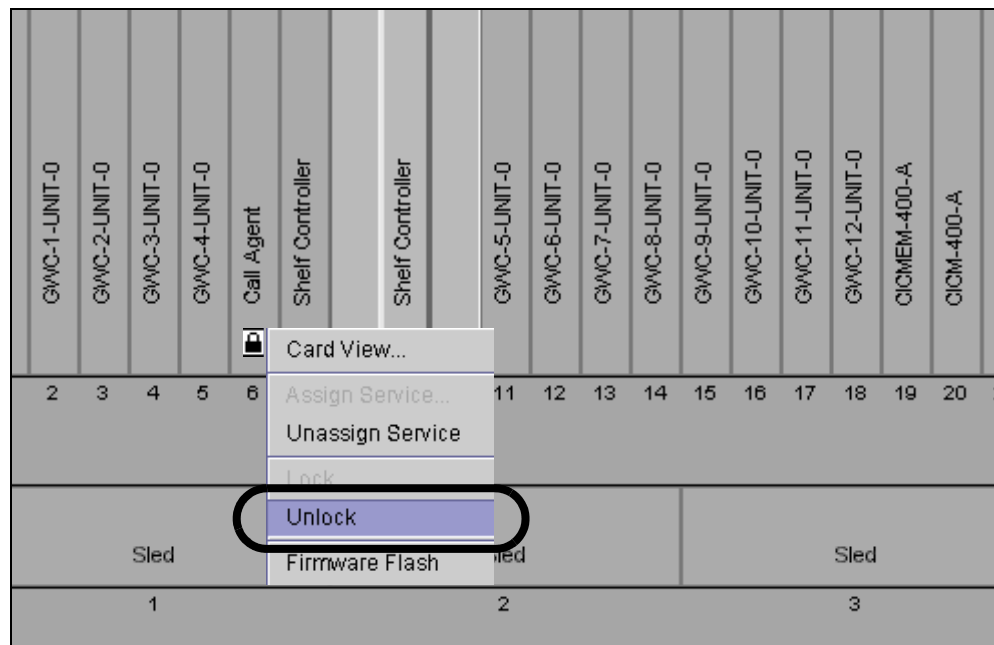
There is no consequence if the checkbox is enabled and firmware is not available. If a firmware flash upgrade is available, verify that Firmware flash: succeeded is reported in the History area of the States tab during the Unlock.

- 6 Click the Save button.
- 7 Click *OK* to proceed on the Warning Window.
- 8 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Unlocking the Call Agent

### *At the CS 2000 SAM21 Manager client*

- 1 From the Shelf View, right click on the card and select Unlock from the context menu.



**Note:** Unlock is also available from the States tab of the Card View window.

The card resets, downloads software, and reboots.

- 2 Wait for the lock icon to disappear.

**Note:** Do not perform any patching activities on the Call Agent until ten minutes have passed.

### *At the INACTIVECM window*

- 3 Enter the ccamtc level to verify the current load is the new load.
  - > **ccamtc**
  - > **sys**

**> qryld**

**Note:** If CallAgent C\_MisM alarm is active at the CORE0 or CORE1 window, patch the platform software:

1. At the inactive maintenance window (CORE0 or CORE1) verify that this is the inactive Call Agent.
  2. Enter the Admin level and then the SWIM level.
  3. At the TRANSFER level a list of available patches is displayed
    - a. SELECT the patch by number
    - b. FETCH INA the patch to the INACTIVE unit
  4. At the PATCH level, for each patch to be applied and committed:
    - a. SELECT the patch by number
    - b. DISADMIN the patch and follow any special instructions
    - c. APPLY INA the patch to the INACTIVE unit
    - d. SELECT the patch by number
    - e. COMMIT INA the patch to the INACTIVE unit
- 4** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



**Module** **Heading** **Completing LDMATE (Load inactive)** **Heading**

**ParaBasic** This procedure is used for a platform only MR upgrade. Use the LDMATE command to load the currently running and active call processing application onto the inactive Call Agent. **ParaBasic**

**Procedure** **Context** **Location** **At the active Call Agent Manager** **Location**

**1** **Step** **Precaution** **Precaution**

**PrecautionLabel** **ATTENTION** **PrecautionLabel**  
**PrecautionBody** Wait for the synchronization flag to change to **SpecialText** /waiting **SpecialText** before proceeding. **PrecautionBody**



**PrecautionLabel** **CAUTION** **PrecautionLabel**  
**Possible data loss** **PrecautionLabel**  
**PrecautionBody** When performing the LDMATE command, ensure that the image dump taken during procedure **CrossRef** [Dumping a call processing application image on page 1909](#) **CrossRef** is the image that is loaded. **PrecautionBody**  
**PrecautionBody** Loading any other image may result in a data loss. **PrecautionBody**

**ParaBasic** Verify that the call processing application is set to **ComputerOutputString** /waiting **ComputerOutputString**:  
**ParaBasic**

**Figure** **Graphic** **Figure** **Step** **Context**

| CoreMtc | Unit0 | Inact | Jam: | Link0: | Link1:  | Blnk: | FC: | Appl:  |          |
|---------|-------|-------|------|--------|---------|-------|-----|--------|----------|
| 0 Quit  | Unit0 | Inact | yes  | . Act  | . Inact | .     | S   | nosync | /waiting |
| 2 CAMtc | Unit1 | Act   | no   | . Act  | . Inact | .     | S   | nosync |          |

**Context** **Location** **SDE — At the ACTIVECM window** **Location**

- 2 **Step** **ParaBasic** Make the call processing application file available by listing the image volume: **ParaBasic**

**CommandInstance** **CommandName** > **SCANF** <volume\_name>  
**CommandName** **CommandInstance**

**Definition** **Term** **volume\_name** **Term**

**Description** **ParaBasic** is the name of the volume that contains the image dump. For example,

SD00IMAGE. **ParaBasic** **Description** **Definition** **Step**

- 3 **Step** **ParaBasic** Load the image that was dumped during **CrossRef** [step 3](#) **CrossRef**, page **CrossRef** [1910](#) **CrossRef** onto the inactive Call Agent: **ParaBasic**
- CommandInstance** **CommandName** > **LDMATE** <**filename**>  
**CommandName** **CommandInstance**
- Definition** **Term** **filename** **Term**  
**Description** **ParaBasic** is the name of the call processing application image that was dumped earlier **ParaBasic** **Description** **Definition**
- Example** **ParaBasic** **Example**  
**CommandString** **CommandName** > **LDMATE**  
**S040210210503\_CM**  
**CommandName** **CommandString** **ParaBasic** **Example**  
**Step**
- 4 **Step** **ParaBasic** Monitor the progress at the MAP and Call Agent Manager windows. At the Call Agent Manager, the synchronization flag for the inactive Call Agent will change from **SpecialText** /booting **SpecialText** to **SpecialText** /restart **SpecialText**.  
When ldmate is completed successfully, the inactive Call Agent will change from **SpecialText** /restart **SpecialText** to **SpecialText** . (dot) **SpecialText** like the following: **ParaBasic**  
**Figure** **Graphic** **Figure** **Step**
- |         |       |       |        |        |         |     |          |
|---------|-------|-------|--------|--------|---------|-----|----------|
| CoreMtc |       | Jam:  | Link0: | Link1: | BLnk:   | FC: | Appl:    |
| 0 Quit  | Unit0 | Act   | no     | . Act  | . Inact | .   | . nosync |
| 2 CAMtc | Unit1 | Inact | yes    | . Act  | . Inact | .   | . nosync |
- 5 **Step** **ParaBasic** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure. **ParaBasic** **Step** **Context** **Procedure** **Module**

## Patching platform software

### *At the inactive Call Agent Manager*

- 1 At the CoreMtc level, ensure that this unit is the inactive unit.

|           |       |       |        |               |
|-----------|-------|-------|--------|---------------|
| CallAgent | SYS   | CON   | APPL   |               |
| JInact    | .     | .     | simplx | Unit: 1       |
|           |       |       | M      |               |
| CoreMtc   |       | Jam:  | Link0: | Link1:        |
| 0 Quit    | Unit0 | Act   | no     | . Inact . Act |
| 2 CAMtc   | Unit1 | Inact | no     | . Inact . Act |
|           |       |       | BLnk:  | FC: Appl:     |
|           |       |       | .      | . nosync .    |
|           |       |       | .      | . nosync .    |

Unit 1 is the unit number, and Unit 1 is Inactive. For this example, patch from Unit 0.

- 2 Enter the Transfer level and display the list of available patches.  
> **Transfer**

*The Call Agent Manager enters the Transfer level and the list of available patches is retrieved and displayed.*

```

CallAgent SYS CON APPL Unit: 0
JInact . . simplx
 M
Transfer Current Load : 8.20.1.0
0 Quit Source : /3pc/patch
2 Select
3 Fetch # Patch Description Version
4 Source 1 ncgl_cca_patch 8.20.1.2
5 2 ncgl_cca_patch 8.20.1.3
6
7
8
9
10
11 Up
12 Down
13 LogQuery
14 Alarm
15
16
17 Help
18 Refresh
 mtc
Time 10:52 >

```

- 3** If no patches are listed, verify that the selected source, /3pc/patch in the example, is correct. If the source is correct and no patches are available, go to [step 7](#).

If new patch files are available but have not been transferred to the CS 2000 Core Manager or CBM, refer to either [Transferring patch files from optical disk to a Core Manager on page 1880](#) or [Transferring patch files from ESD to a Core Manager on page 1884](#) (depending on the transfer media applicable to the office).

- 4** For each patch to be transferred, select the patch by number and transfer the patch to the inactive unit.

```

> Select <num>
> Fetch INA

```

**5** Enter the Patch level.**> Patch**

*The Call Agent Manager enters the **Patch** level and the patches are listed as NEW.*

```

CallAgent SYS CON APPL Unit: 0
JInact . . simplx
 M
Patch Current Load : 8.20.1.0
0 Quit Filter : ALL
2 Select
3 Apply # Patch Description Version Status
4 Delete 1 Patch description 8.20.1.2 NEW
5 Commit 2 Patch description 8.20.1.3 NEW

```

**6** For each patch file, select the patch, apply the patch to the inactive unit, select it again, and commit it.

```

> Select <num>
> Apply INA FORCE
> Select <num>
> Commit INA

```

*Each patch is applied and committed to the inactive Call Agent unit. The Status for each patch changes from NEW to COMMITTED.*

**7** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Performing LIMITED\_PRESWACT

---

This procedure is used for a platform only MR upgrade. For an ONP, Nortel supports the SWUPGRADE process.

LIMITED\_PRESWACT executes a series of steps required before the office switch of activity (SWACT). If a step fails to complete, LIMITED\_PRESWACT stops and gives additional information. Whenever LIMITED\_PRESWACT stops, use the information given to investigate and correct the problem. All LIMITED\_PRESWACT steps must be completed before SWACT.

### **SITE —At the ACTIVECM window**

- 1 Execute LIMITED\_PRESWACT:

```
> BCSUPDATE; LIMITED_PRESWACT
```

*The LIMITED\_PRESWACT command presents a warning:*

```
Limited_Preswact should not be used for
BCSUPGRADE SWACTs. Do you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
```

- 2 Confirm the warning with a Y.

*A series of steps execute and complete. LIMITED\_PRESWACT stops at step MATE\_RESTART\_RELOAD:*

```
MATE_RESTART_RELOAD executing
There are users still logged on the Inactive. Do
you wish to continue?
MATE_RESTART_RELOAD not complete
ACT - Error: Restart aborted. Type
LIMITED_PRESWACT to continue
Investigate and correct if needed.
```

- 3 Reenter LIMITED\_PRESWACT to continue:

```
> LIMITED_PRESWACT
```

*Another warning is printed:*

```
MATE_RESTART_RELOAD executing
There are users still logged on the Inactive. Do
you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
```

- 4 Confirm the warning with a Y.

*The inactive unit indicates /restart at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated as follows:*

Total execution time for all complete procedures  
00:07:31.362

All LIMITED\_PRESWACT steps completed  
successfully.

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Releasing jam on the inactive Call Agent

### *At the active Call Agent Manager*

1 Enter the RelJam command:

```
> CoreMtc
> CAMtc
> RelJam
```

```
CallAgent SYS CON APPL Unit: 0
. . . simplx
 M
CAMtc Jam: Link0: Link1: BLnk: FC: Appl:
0 Quit Unit0 Act no . Inact . Act . . nosync .
2 Jam Unit1 Inact no . Inact . Act . . nosync .
3 RelJam
4 RExtTst
5 SwAct
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh RelJam: Release jam on the inactive unit.
 mtc
Time 10:38 >
```

2 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Executing NORESTARTSWACT

**CAUTION****Possible loss of service**

NORESTARTSWACT does not check if the inactive Call Agent is unjammed. If the inactive Call Agent is jammed and a NORESTARTSWACT is requested, service is affected. Verify that the inactive Call Agent is not jammed.

**CAUTION****Possible loss of service**

Use the Call Agent Manager to verify that the inactive Call Agent does not have any critical alarms. A critical alarm causes the NORESTARTSWACT to fail. Check the GUIs for CCA, SAM21 EM and Ethernet Routing Switch 8600, and clear any alarms for those devices before proceeding with NORESTARTSWACT.

**SITE —At the ACTIVECM window**

- 1 Check status:

> **BCSUPDATE; SWACTCI; STATUSCHECK**

*Success is indicated as follows:*

SWACTCI:

Checking Nodes Status

STATUSCHECK successful

- 2 Execute the NORESTARTSWACT:

> **NORESTARTSWACT**

**Note 1:** Only simple two-port and echo calls that are in a stable talking state (that is, not in a transition state such as dialing) survive a CC WarmSWACT. Survival means that the call is kept up until the next signaling message is received (usually, for example, a terminate message, but on any other message as well, such as an attempt to use the conference feature).

**Note 2:** Attendant Consoles will be in night service after the SWACT if the INSV field is set to Y in table ATTCONS (Attendant Consoles).

*Progress is printed and the process stops to verify that the inactive Call Agent is not jammed:*

```
Beginning SWACT checks:
All the SWACT checks have finished successfully.
The VR_PRESWACT_TRANSFER step completed
successfully.
All INSV and ISTB series 1 PMs will have execs
loaded after the SWACT.
Device Checking Status:
NOMATCH option is set to OFF <default setting>.
Device matching during CC WARM SWACT Enabled.
Do you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
>
```

**3** Confirm the warning with a Y if the only alarm is an APPL simplx.

*The final progress follows. Activity also switches at the Call Agent Manager.*

```
Please confirm ("YES", "Y", "NO", or "N"):
>Y
All Pre-SWACT checks completed. Starting Warm
SWACT now.
***** The cursor will not be returned *****
***** unless a critical failure occurs. *****
***** Now monitoring Warm SWACT messages.*****

Pre-initialization done
Communication established
Exchange of data with the mate done
Transfer of data done (FASPECT)
Data estimation done
```

**4** The telnet sessions to the active and inactive call processing applications are lost. Reestablish the connection. Refer to the [Interface setup](#) in this Upgrades document for procedures.

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

**ATTENTION****ABORT PROCEDURE**

Reversion to the previous software release is possible until procedure [Locking the inactive Call Agent](#). If this is a PCL upgrade with the SWUPGRADE tool, reversion is started with the CANCEL command. If this is a platform only MR upgrade, refer to [ABORTSWACT on page 2066](#).

## Jamming the inactive Call Agent

### *At the active Call Agent Manager*

1 Enter the Jam command:

```
> CoreMtc
> CAMtc
> Jam
```

```
CallAgent SYS CON APPL Unit: 1
JInact . . simplx
M
CAMtc
0 Quit Unit0 Inact yes . Inact . Act . . nosync .
2 Jam Unit1 Act no . Inact . Act . . nosync .
3 RelJam
4 RExtTst
5 SwAct
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 Jam: Jam the inactive unit, to prevent it taking activity.
17 Help Params: [FORCE]
18 Refresh FORCE - bypass system stability checks
 mtc
Time 10:38 >
```

2 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Executing POSTSWACT

---

### ***SITE —At the ACTIVECM window***

- 1 Execute POSTSWACT:

**> BCSUPDATE;POSTSWACT**

*POSTSWACT begins, steps execute, and complete.*

*POSTSWACT stops at step BEGIN\_TESTING:*

|                     |           |
|---------------------|-----------|
| REACTIVATE_TRIGASGN | executing |
| REACTIVATE_TRIGASGN | complete  |
|                     |           |
| DIRP_RECOVERY       | executing |
| DIRP_RECOVERY       | complete  |
|                     |           |
| ...                 |           |
| BEGIN_TESTING       | executing |
| BEGIN_TESTING       | complete  |

Enter Postswact after office testing has been completed

- 2 Proceed to [Monitoring logs on page 2050](#) and [Testing calls and acceptance on page 2052](#) before reentering the POSTSWACT command on page [2054](#).

---

## Monitoring logs

---

### ***SITE —At the INACTIVECM window***

- 1 Log in to the mate image. Refer to [Logging in to the mate image.](#)
- 2 Review previous log reports:  
  - > **LOGUTIL;OPEN SWCT;BACK ALL**
- 3 Set the terminal to receive logs:  
  - > **LOGUTIL;START;QUIT**or  
  - > **STARTDEV <device>**  
**device**  
is a different terminal device
- 4 Let logs run for 30 minutes and then run LOGCHECK:  
  - > **LOGUTIL;STOP;QUIT**
  - > **BCSUPDATE;LOGCHECK;QUIT**
- 5 When LOGCHECK completes. Set the terminal to receive logs again.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Logging in to the mate image

### ***SITE —At the ACTIVECM window***

- 1 Use MATELINK, MATEIO, and MATELOG to log in.  
  - > **MATELINK RTS**
  - > **MATEIO**
  - > **MATELOG ME; SLEEP <nn> MINS**  
**nn**  
is the number of minutes to sleep. Allow at least 30 minutes.

2

#### **ATTENTION**

While logged into the inactive call processing application, the system prompt changes to `Mate>`.

Log in to the inactive call processing application with a username and password.

- 3** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Testing calls and acceptance

### ***SITE —At the ACTIVECM window***

- 1 Make sure all emergency services are functioning.
- 2 Refer to the Test Call Scripts and perform the required test calls.
- 3 Confirm that the customer accepts the new load.
- 4 Use the following table to determine your next step.

| If                    | Do                                                 |
|-----------------------|----------------------------------------------------|
| abort is required     | proceed to <a href="#">ABORTSWACT on page 2066</a> |
| abort is not required | <a href="#">step 5</a>                             |

- 5 Dump the new call processing application image using one of the following commands:

If AUTODUMP is active for the office, enter

**AUTODUMP MANUAL**

or

If AUTODUMP is not active for the office, enter

**DUMP <image\_name> <disk\_vol> ACTIVE UPDATE**

where

**image\_name**

is the name of the file to create

**disk\_vol**

is sd00image or sd01image

If you used the AUTODUMP MANUAL command, use the AUTODUMP STATUS command to view the new image name and the location of where the new image is stored.

- 6 Enter the ITOCCI level.

**> ITOCCI**

- 7 Set the boot file pointer to the new software load if this was not done when the software was transferred to storage.  

```
> diskut
> lf <disk_vol>
> SA CM <image_name>
```

**disk\_vol**  
is the disk volume name where the image was taken

**image\_name**  
is the name of the new call processing application image from [step 5](#)
- 8 Go to procedure [Locking the inactive Call Agent on page 2056](#).
- 9 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Executing POSTSWACT again

---

### ***SITE —At the ACTIVECM window***

- 1     Execute POSTSWACT:  
      > **BCSUPDATE;POSTSWACT**
- 2     Confirm the prompt to sync the Call Agent:  
      > **Y**
- 3     Clean up SFDEV by erasing any application-related files, such as FEATDATA, SITEINFO, and DIRP\_INAC.

### ***For operating personnel to perform at the ACTIVECM window***

- 4     Verify password for user ADMIN.
- 5     Reassign all current PROFILE information (LOGIN or RESTART) in SFDEV.
- 6     Reassign any temporary log ROUTING setup using LOGUTIL.
- 7     If table PADNDEV was altered, restore the original values.
- 8     This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Restarting the journal file

---

***SITE —At the ACTIVECM window***

- 1 Access the DIRP level of the MAP:  
    > **MAPCI;MTC;IOD;DIRP**
- 2 Verify whether the journal file is running:  
    > **QUERY JF**
- 3 Use the following table to determine your next step.

| If the journal file is | Do                     |
|------------------------|------------------------|
| running                | <a href="#">step 5</a> |
| not running            | <a href="#">step 4</a> |
- 4 Start the journal file:  
    > **JF START**
- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Locking the inactive Call Agent

---

**ATTENTION**

Verify that the customer accepts the new load.

ABORTSWACT is no longer available after this procedure. ABORTSWACT is the preferred method to revert a platform only upgrade. Reversion is still possible after this procedure, but requires assistance from Nortel support personnel.

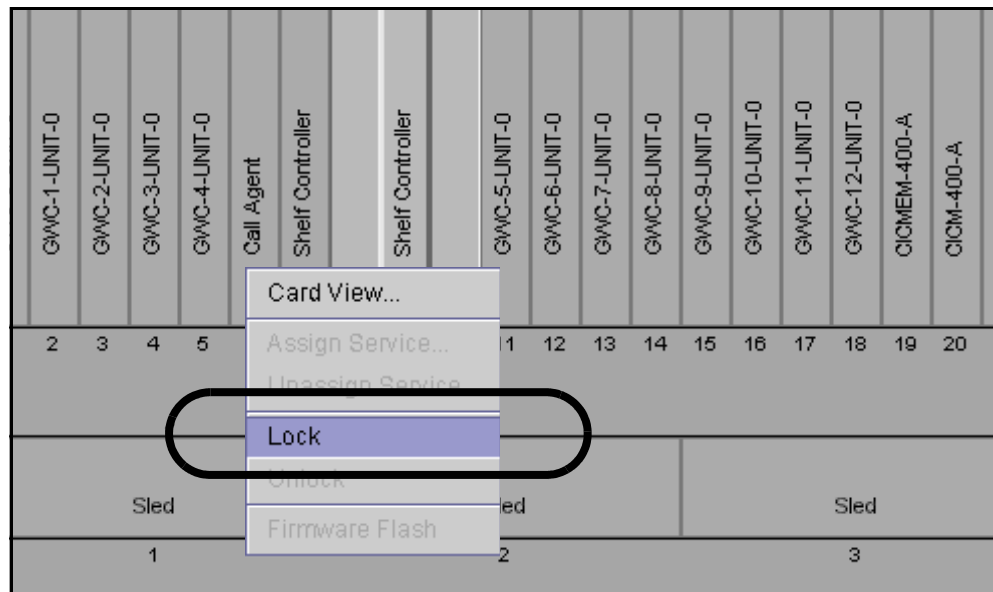
**CAUTION****Possible service interruption**

Do not lock the active Call Agent.

The CS 2000 SAM21 Manager client responds to an active Call Agent lock with the prompt shown in figure Call Agent lock warning. Do not click Yes. The inactive Call Agent is located in the other CS 2000 SAM21 Manager shelf and a lock request does not provide a prompt when the Call Agent is inactive.

***At the CS 2000 SAM21 Manager client***

- 1 From the Shelf View, right-click the card and select Lock from the context menu.



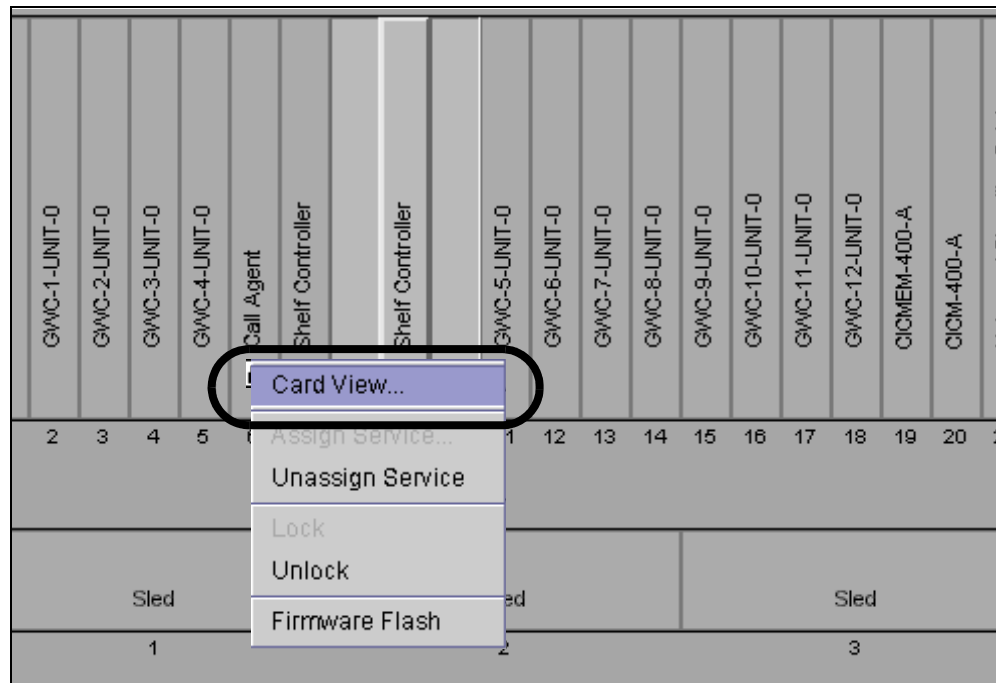
**Note:** Lock is also available from the States tab of the Card View window.

- 2 Wait for the lock icon to appear on the selected card.
- 3 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Provisioning a new software load

### *At the CS 2000 SAM21 Manager client*

- 1 From the Shelf View, right-click the card and select Card View from the context menu to open the Card View window.



- 2 Click the Provisioning tab from the Card View window.
- 3 Click the Modify button.
- 4 Click the Get Load Files button.
- 5 Select load from the drop-down list.
  - ncgl\_cca\_765\_image.8.20.1.0 (765 is added for loads based on the MCPN765 processor card)
  - ncgl\_cca\_905\_image.8.20.1.0 (905 is added for loads based on the MCPN905-270 processor card, introduced in SN09)

The following example display assumes a software load based on the MCPN765 processor card.

OTT4 CA-1 Slot 6 CardView@ucars01x3c.ca.nortel.com (CM CLI: BNR\_LAB\_LOAD)

File View

OTT4 CA-1 : Slot 6

Alarms Equip States Diags Provisioning

General

IP: 10.72.17.22 Gateway IP: 10.72.16.1

Subnet Mask: 255.255.240.0 FW Version: RM03-2.4

MAC Address: 0001AF12AFA0 MAC 2: 0001AF12AF9F

NTP

Primary NTP: 47.135.43.193 Secondary NTP: 47.135.43.196

Load Info

Server IP: 47.135.43.193

Path: /3pc

Load: ncgl\_cca\_765\_image\_8.20.1.0 Get Load Files

☒ FW Flash Enable

Network File System Message Controller Geographical Survivable

Geographical CS 2000 Compact

☒ Enable

Backup Path:

GEO UNIT 0 IP: 10.72.0.12 Mask: 255.255.255.248

GEO UNIT 1 IP: 10.72.0.20 Mask: 255.255.255.248

Modify Save Clear Cancel Details... Help

**Note 1:** To verify the card type, click the Equip tab. The panel displays the appropriate card (MCPN765 or MCPN905-270) and memory size.

**Note 2:** Click the firmware flash enable (FW Flash Enable) checkbox if the *SAM21 Platform Base Release Notes*, SAM2006 indicate a firmware upgrade is available. However, there is no consequence if the checkbox is enabled and firmware is not available. If a firmware flash upgrade is available, verify that Firmware flash: succeeded is reported in the History area of the States tab.

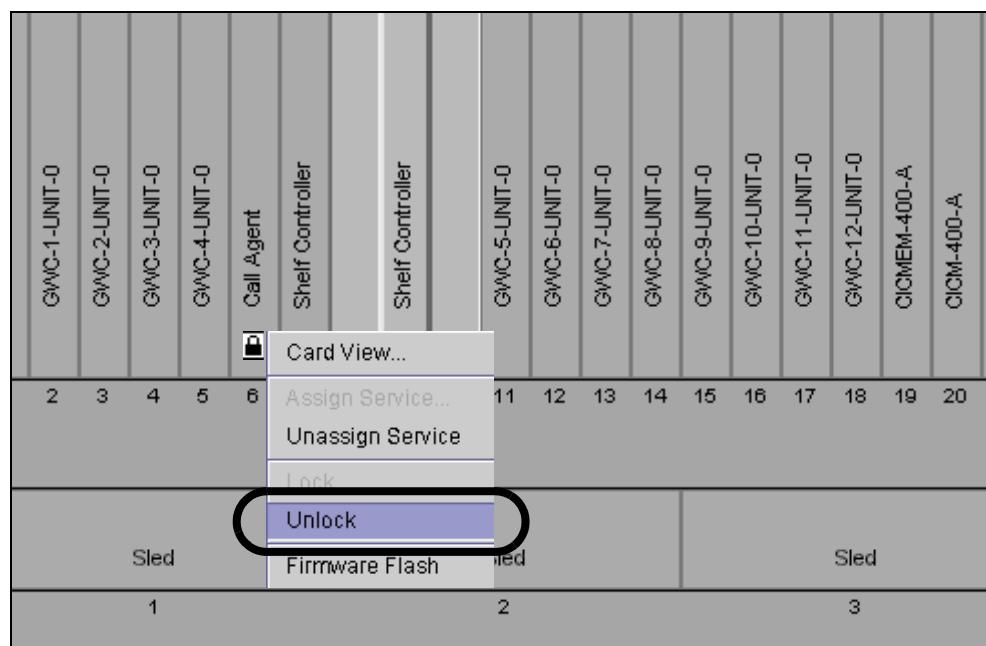


- 6** Click the Save button.
- 7** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Unlocking the inactive Call Agent

### At the CS 2000 SAM21 Manager client

- 1 From the Shelf View, right-click the card and select Unlock from the context menu.



**Note:** Unlock is also available from the States tab of the Card View window.

The card resets, downloads software, and reboots.

- 2 Wait for the lock icon to disappear.

### At the active Call Agent Manager

- 3 Verify that the call processing application loads successfully and waits for synchronization.

|         |             |      |        |         |       |     |        |          |
|---------|-------------|------|--------|---------|-------|-----|--------|----------|
| CoreMtc |             | Jam: | Link0: | Link1:  | BLnk: | FC: | Appl:  | /waiting |
| 0 Quit  | Unit0 Inact | yes  | . Act  | . Inact | S     | S   | nosync |          |
| 2 CAMtc | Unit1 Act   | no   | . Act  | . Inact | S     | S   | nosync |          |

**Note:** The previous figure is used only to show the waiting flag. Disregard the values for activity and jam state.

- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Verifying platform patches

---

Perform this procedure only if platform patches were applied earlier to the first Call Agent.

***At the active Call Agent Manager***

- 1 If platform patches are available, platform patches may need to be applied to this Call Agent unit:
- 2 At the TRANSFER level (ccamtc transfer) a list of available patches is displayed.

***At the TRANSFER level, for each patch***

- 3 SELECT the patch by number
- 4 FETCH INA the patch to the INACTIVE unit

***At the PATCH level, for each patch to be applied and committed***

- 5 SELECT the patch by number
- 6 DISADMIN the patch and follow any special instructions
- 7 APPLY INA the patch to the INACTIVE unit
- 8 SELECT the patch by number
- 9 COMMIT INA the patch to the INACTIVE unit

***For the Call Agent***

- 10 Verify that the reported load information is the same for both Call Agents.
- 11 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Releasing jam on the inactive Call Agent

### *At the active Call Agent Manager*

**1** Enter the RelJam command:

```
> CoreMtc
> CAMtc
> RelJam
```

```
CallAgent SYS CON APPL Unit: 1
. . . .

CAMtc
0 Quit Unit0 Inact no . Inact . Act . . insync .
2 Jam Unit1 Act no . Inact . Act . . insync .
3 RelJam
4 RExtTst
5 SwAct
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh RelJam: Release jam on the inactive unit.
 mtc
Time 10:38 >
```

**2** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

The upgrade is complete. Backup the image taken during procedure [Testing calls and acceptance on page 2052](#). For the details of how to make the backup, refer to section [Backing up an image on page 1911](#).

---

## Restoring FTP users

---

Complete this procedure after the ONP using the listing acquired before the ONP described in [Listing FTP users on page 1918](#).

After the ONP (or a norestartswact or restartswact) all FTP user definitions except 'admin' are lost. Use this procedure to restore the FTP users after the upgrade.

### ***ACT — At the ACTIVECM window***

- 1 Go to the FTP level and type:  
**FTP**
- 2 Add each FTP user, using single quotation marks where indicated, by typing:  
**ADDUSERINFO '<user\_1>' '<user\_1>' '/SFDEV' 'Y'**
- 3 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

**Module** **Heading** **Synchronizing the Application Image** **Heading**


---

**Procedure** **Context** **Location** **At the active Call Agent Manager** **Location**

1 **Step** **ParaBasic** Enter the Sync command: **ParaBasic**

**CommandInstance** > **CommandName** **CoreMtc**

> **Appl**

> **Sync** **CommandName** **CommandInstance**

**Figure** **Graphic** **Figure** **Step**

```

CallAgent SYS CON APPL Unit: 0
JInact . . simplx
M
Appl
0 Quit Unit0 Inact no . Act . inact . NA nosync .
2 ImgTst Unit1 Act no . Act . Act . NA nosync .
3 Sync
4 DpSync
5
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh Sync: Synchronize application.
 mtc
Time 00:24 >

```

2 **Step** **ParaBasic** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure. **ParaBasic** **Step** **Context** **Procedure** **Module**

## ABORTSWACT

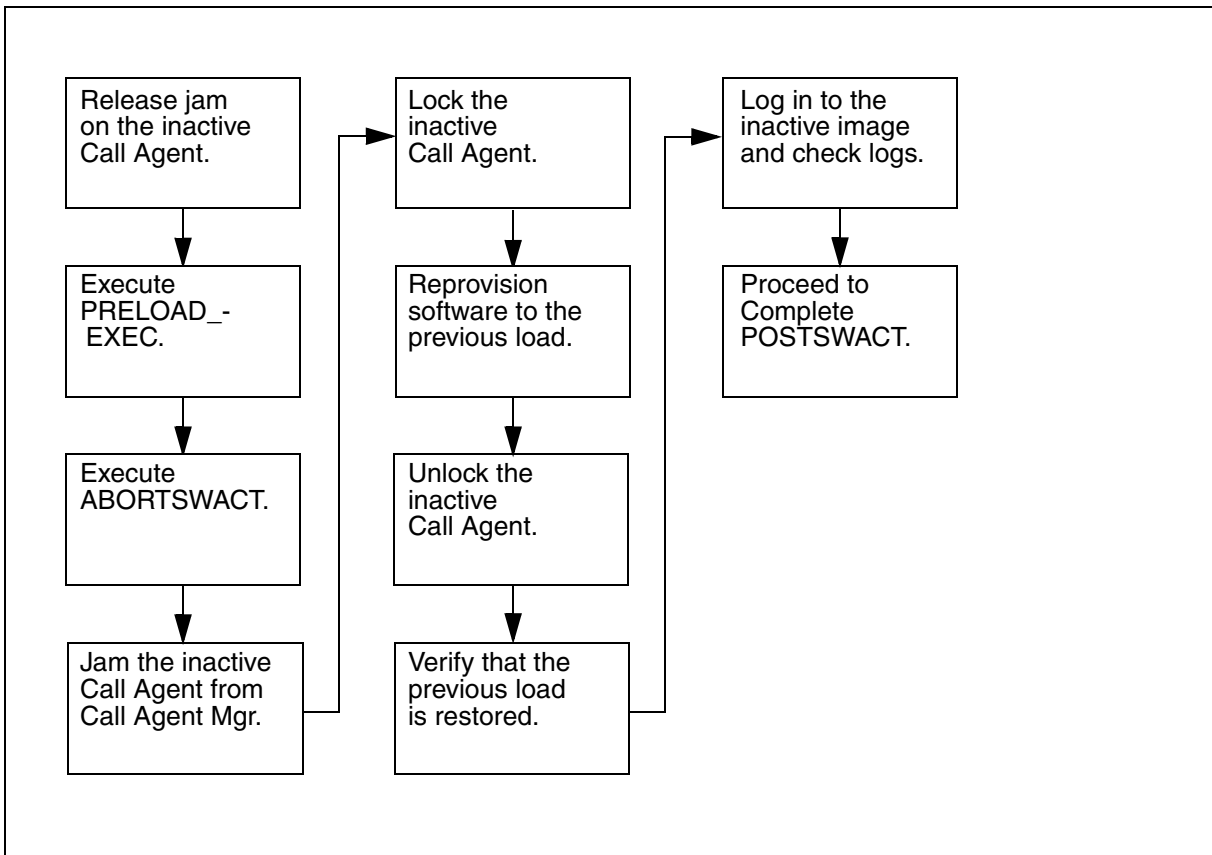
**CAUTION****Possible loss of service**

Reversion with ABORTSWACT is available only if the inactive Call Agent was not locked during the Start POSTSWACT procedure.

If the inactive Call Agent was unlocked, contact Nortel support personnel for assistance.

Perform the procedures in this section only if the software upgrade fails.

### ABORTSWACT procedure



## ABORT: Releasing jam on the inactive Call Agent

### *At the active Call Agent Manager*

1 Enter the RelJam command:

```
> CoreMtc
> CAMtc
> RelJam
```

```
CallAgent SYS CON APPL Unit: 0
. . . simplex
M
CAMtc Jam: Link0: Link1: BLnk: FC: Appl:
0 Quit Unit0 Act no . Inact . Act . . nosync .
2 Jam Unit1 Inact no . Inact . Act . . nosync .
3 RelJam
4 RExtTst
5 SwAct
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16
17 Help
18 Refresh RelJam: Release jam on the inactive unit.
 mtc
Time 10:38 >
```

2 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## ABORT: Executing PRELOAD\_EXECS and ABORTSWACT

### **SITE —At the ACTIVECM window**

- 1 Preload the PM executables:  
     > **BCSUPDATE;RUNSTEP PRELOAD\_EXECS**
- 2 Confirm the command:  
     > **Y**
- 3 Abort swact:  
     > **SWACTCI;ABORTSWACT**
- 4 Confirm the command:  
     > **Y**

### **At the active Call Agent Manager**

- 5 Monitor the SWACT.  
     Verify that the synchronization flags begin with /restart,  
     proceed to /loading, and then /waiting.  
     Verify that activity switches from active to inactive.

#### **Before ABORTSWACT**

|         |             |      |         |         |       |     |          |
|---------|-------------|------|---------|---------|-------|-----|----------|
| CoreMtc |             | Jam: | Link0:  | Link1:  | BLnk: | FC: | Appl:    |
| 0 Quit  | Unit0 Act   | no   | . Inact | . Act   | .     | .   | insync . |
| 2 CAMtc | Unit1 Inact | no   | . Act   | . Inact | .     | .   | insync . |

#### **After ABORTSWACT**

|         |             |      |         |         |       |     |          |
|---------|-------------|------|---------|---------|-------|-----|----------|
| CoreMtc |             | Jam: | Link0:  | Link1:  | BLnk: | FC: | Appl:    |
| 0 Quit  | Unit0 Inact | no   | . Inact | . Act   | .     | .   | insync . |
| 2 CAMtc | Unit1 Act   | no   | . Act   | . Inact | .     | .   | insync . |

- 6 The telnet sessions to the active and inactive call processing applications are lost. Re-establish the connection. Refer to the [Interface setup](#) in this Upgrades document for procedures.
- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## ABORT: Jamming the inactive Call Agent

### ***SDE — At the active maintenance window (CORE0 or CORE1)***

- 1** Enter the CoreMtc level:  
     > **CoreMtc**
- 2** Enter the CAMtc level:  
     > **CAMtc**
- 3** Enter the Jam command:  
     > **Jam**

```

CallAgent SYS CON APPL Unit: 0
JInact . . .

CAMtc
0 Quit Unit0 Act no . Inact . Act . . insync .
2 Jam Unit1 Inact yes . Inact . Act . . insync .
3 RelJam
4 RExTst
5 SwAct
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 Jam: Jam the inactive unit, to prevent it taking activity.
17 Help Pams: [FORCE]
18 Refresh FORCE - bypass system stability checks
 mtc
Time 10:38 >

```

- 4** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

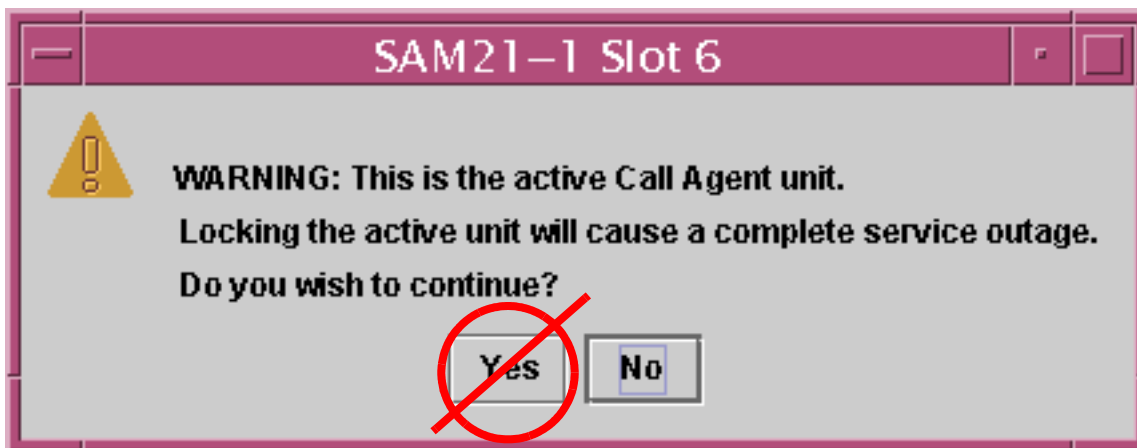
## ABORT: Locking the inactive Call Agent

**CAUTION****Possible service interruption**

Do not lock the active Call Agent.

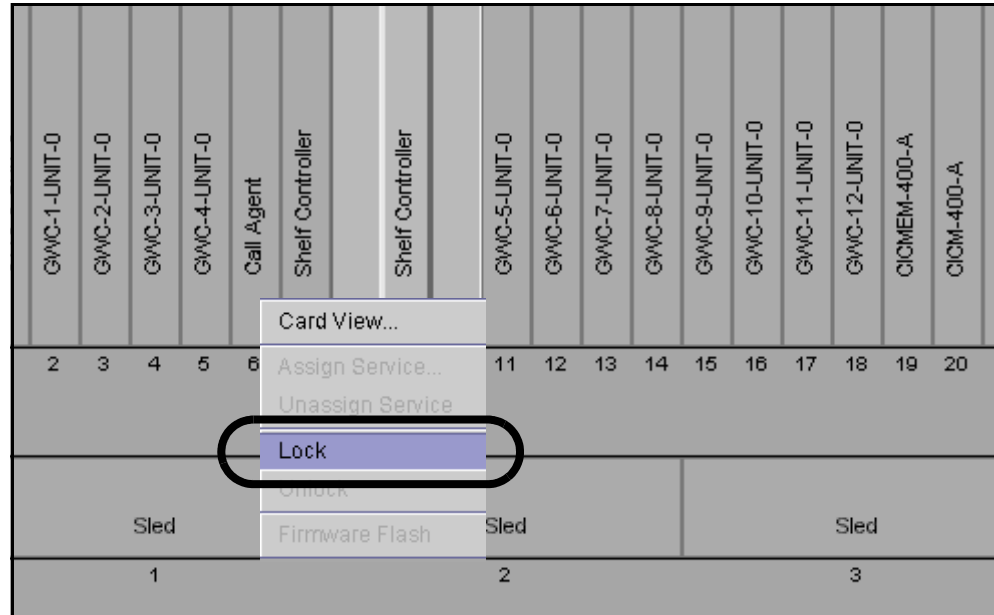
The CS 2000 SAM21 Manager client responds to an active Call Agent lock with the prompt shown in figure [Call Agent lock warning](#). Do not click Yes. The inactive Call Agent is located in the other SAM21 shelf and a lock request does not provide a prompt when the Call Agent is inactive.

**Call Agent lock warning**



**At the CS 2000 SAM21 Manager client**

- 1 From the Shelf View, right-click the card and select Lock from the context menu.



**Note:** Lock is also available from the State tab of the Card View window.

- 2 Wait for the lock icon to appear on the selected card.
- 3 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

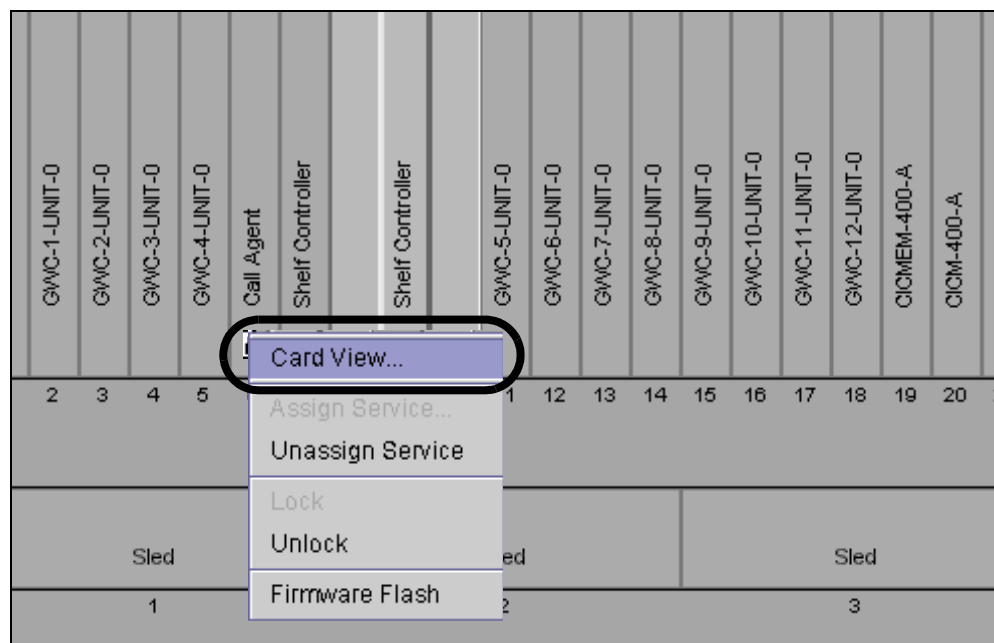
## ABORT: Provisioning previous software load

### ATTENTION

Enter the software load from the previous release.

#### *At the CS 2000 SAM21 Manager client*

- 1 From the Shelf View, right-click the card and select Card View from the context menu to open the Card View window.



- 2 Click the Provisioning tab from the Card View window.
- 3 Click the Modify button.
- 4 Click the Get Load Files button.
- 5 Select the load from the drop-down list.
- 6 Select Save.

**7** Enter the previous load file name in the load field.

**Note:** The loadname format in the example display assumes the previous load is prior to SN09. The following examples show loadname formats for previous SN09 loads.

- ncgl\_cca\_765\_image.8.20.1.0 (for loads based on the MCPN765 card processor)
- ncgl\_cca\_905\_image.8.20.1.0 (for loads based on the MCPN905-270 card processor, introduced in SN09)

OTT4 CA-1 Slot 6 CardView@ucars01x3c.ca.nortel.com (CM CLI: BNR\_LAB\_LOAD)

File View

OTT4 CA-1 : Slot 6

Alarms Equip States Diags Provisioning

General

IP: 10.72.17.22 Gateway IP: 10.72.16.1

Subnet Mask: 255.255.240.0 FW Version: RM03-2.4

MAC Address: 0001AF12AFA0 MAC 2: 0001AF12AF9F

NTP

Primary NTP: 47.135.43.193 Secondary NTP: 47.135.43.196

Load Info

Server IP: 47.135.43.193

Path: /3pc

Load: ncgl\_cca\_image\_7.02.1.0 Get Load Files

☒ FW Flash Enable

Network File System Message Controller Geographical Survivable

Geographical CS 2000 Compact

☒ Enable

Backup Path:

GEO UNIT 0 IP: 10.72.0.12 Mask: 255.255.255.248

GEO UNIT 1 IP: 10.72.0.20 Mask: 255.255.255.248

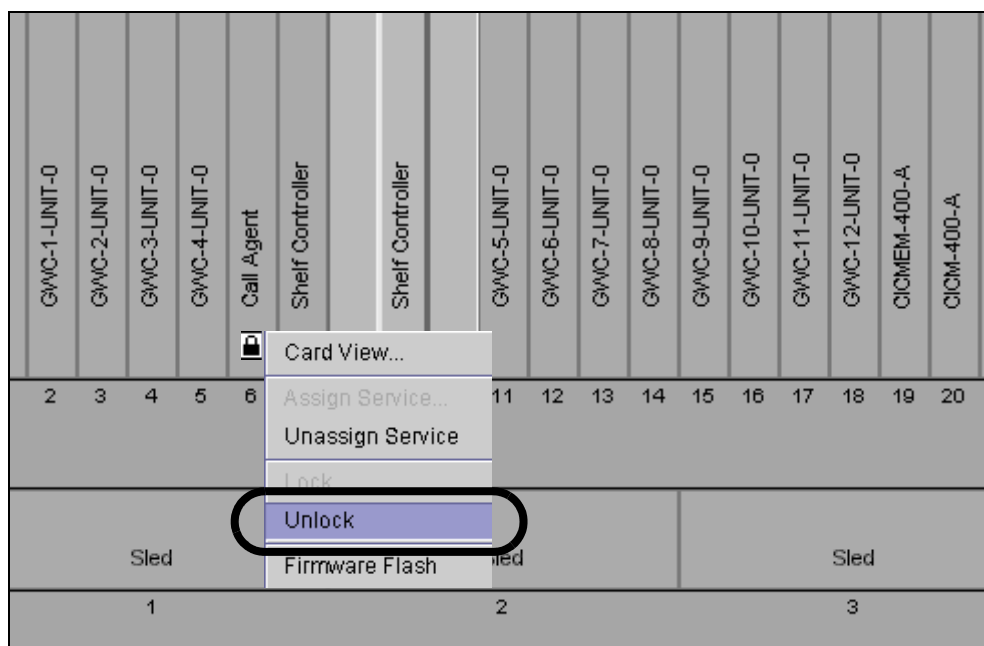
Modify Save Clear Cancel Details... Help

- 8** Click the Save button.
- 9** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## ABORT: Unlocking the inactive Call Agent

### At the CS 2000 SAM21 Manager client

- 1 From the Shelf View, right-click the card and select Unlock from the context menu.



**Note:** Unlock is also available from the States tab of the Card View window.

*The card resets, downloads software, and reboots. If platform patches were applied to the inactive Call Agent earlier in this upgrade, then the same patches are applied and automatically committed on this Call Agent unit as the card boots. No action is required for platform patching.*

- 2 Wait for the lock icon to disappear.
- 3 This procedure is complete. Proceed to [Executing POSTSWACT on page 2049](#).



## Patching Platform and Call Processing software

Platform and call processing application software is patchable. Platform patching does not patch the Linux kernel.

### What's new in platform software patching

To download patching software, go to [www.nortel.com](http://www.nortel.com) and select Products (under Products & Services)-> Software-> Families-> Succession-> Succession Communication Server 2000 - Compact-> Software.

### Platform patching

Patch files have the following identification scheme:

ncgl\_cc\_patch\_r.w.c.v

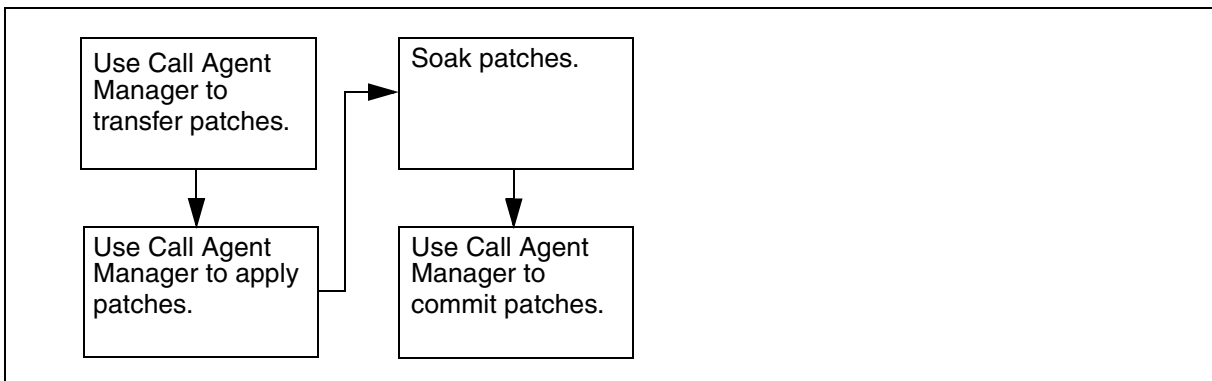
- **r** indicates the release.
- **w** indicates the week number of the load build. For example, 20.
- **c** indicates the compile. This value is equal to the fc value for an NCL or equal to (fc+i) for an MNCL. The patch is only applicable to a load that matches this number.
- **v** indicates the patch version.

**Note:** Patches are only applicable to NCLs and MNCLs with matching r, w, and c values as the patch file.

Patching of the platform software is done through the Call Agent Manager.

Refer to the following flowchart for an overview of the platform patching procedure.

### Platform patching overview



## Call processing application patching

Patching of the call processing application is done through Post-Release Software Manager (PRSM). This tool is available through the MAP.

Refer to *Post-Release Software Manager Reference Manual*, 297-8991-540, for information about patching the call processing application.

## Transferring platform patch files

Verify that patch files are installed on the CS 2000 Core Manager or CBM before completing this procedure. Platform software patch files are stored in `/swd/3pc/patch` for the Call Agent.

For Linux warranty patching go to [www.nortel.com](http://www.nortel.com) to retrieve the patches. At the Nortel.com website, select Software Downloads->Families->(top right under Find Products)->Succession Product Family->Succession Communication Server 2000-Compact.

This procedure requires root privilege.

### At the Call Agent Manager

1 Enter the Transfer level:

- > **Admin**
- > **SWIM**
- > **Transfer**

```

CallAgent SYS CON APPL Unit: 0
. . . .

Transfer Current Load : 8.20.1.0
0 Quit Source : /3pc/patch
2 Select
3 Fetch # Patch Description Version
4 Source 1 ncgl_cca_patch 8.20.1.9
5 2 ncgl_cca_patch 8.20.1.8
6 3 ncgl_cca_patch 8.20.1.7
7 4 ncgl_cca_patch 8.20.1.6
8
9
10
11 Up
12 Down
13 LogQuery
14 Alarm Filesets on the source: 1 to 4 of 4
15
16
17 Help
18 Refresh
 mtc
Time 13:06 >

```

**Note 1:** If patch files do not appear in the list, verify that the patch files are installed on the CS 2000 Core Manager or

CBM in /swd/3pc/patch and have read permissions such as 777 or 755.

**Note 2:** If patch files are stored in a different directory, use the SOURCE command to change the source directory. The CS 2000 Core Manager or CBM prepends /swd to all values.

**Note 3:** If new patch files are available but have not been transferred to the CS 2000 Core Manager or CBM, refer to either [Transferring patch files from optical disk to a Core Manager on page 1880](#) or [Transferring patch files from ESD to a Core Manager on page 1884](#) (depending on the transfer media applicable to the office).

- 2 Select the patch file to transfer from the CS 2000 Core Manager or CBM:

> **Select num**

**num**

is the decimal value that indicates the fileset

- 3 Retrieve the selected patch file:

> **Fetch**

**Note:** If the FETCH command fails, verify that the patch files are installed and applied on the CS 2000 Core Manager or CBM and that the files have read permission set such as 777 or 755.

The fetch command retrieves the patch file and stores it on the active and inactive Call Agent cards by default. ACTIVE and INACTIVE options enable storage to a specific Call Agent card.

**Note:** If the patch fileset already exists, the Call Agent prompts to determine whether to override the existing file. Patch filesets can be overwritten.

Fileset already present. Overwrite?  
Please confirm ("YES", "Y", "NO", "N"):

- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Applying platform software patch

**CAUTION****Possible service interruption**

Do not perform any patching activity within the first 10 minutes following a Call Agent unlock.

***At the Call Agent Manager***

**1** Enter the Patch level:

```
> Admin
> SWIM
> Patch
```

```
CallAgent SYS CON APPL Unit: 0
. . . .

Patch Current Load : 8.20.1.0
0 Quit Filter : ALL
2 Select
3 Apply # Patch Description Version Status
4 Delete 1 ncgl_cca_patch 8.20.1.9 NEW
5 Commit 2 ncgl_cca_patch 8.20.1.8 VALIDATED
6 3 ncgl_cca_patch 8.20.1.7 VALIDATED
7 4 ncgl_cca_patch 8.20.1.6 VALIDATED
8
9
10
11
12
13 LogQuery
14 Alarm
15
16
17 Help
18 Refresh
 mtc
Time 14:14 >
```

- 2 Select the patch file to apply:
  - > **Select <num>**
  - num**  
is the integer value that indicates the patch
- 3 Display any warnings or special application instructions, and perform any special application instructions:
  - > **Disadmin**
- 4 Reselect the patch and verify that all dependencies are met:
  - > **Select <num>**
  - > **Validate**

| If                                                        | Do                                                                                                                                                                                                                                                |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dependencies are met and the patch validates successfully | <a href="#">step 5</a>                                                                                                                                                                                                                            |
| dependencies are not met and the validate fails           | Fetch, select, and validate earlier patches before attempting to apply this patch. For example, if the current patch level is 8.20.1.10 and patch file 8.20.1.13 fails validation, attempt to validate and apply patches 8.20.1.11 and 8.20.1.12. |

- 5 Reselect the patch and apply the patch file:
  - > **Select <num>**
  - > **Apply**

| If                                                                         | Do                                                |
|----------------------------------------------------------------------------|---------------------------------------------------|
| the patch applied successfully                                             | step <a href="#">6</a>                            |
| the patch fails to apply                                                   | Refer to <a href="#">Troubleshooting</a> .        |
| the patch is an older version or requires special application instructions | Refer to <a href="#">Additional information</a> . |

6

#### ATTENTION

At this point, the patch is applied and is part of the running load. Soak the patch according to operating company procedure before committing the patch. Patches are automatically committed 10 minutes after application unless manually committed earlier.

Reselect the patch and write the change to persistent storage. The committed load boots the next time the card is reset or rebooted:

```
> Select <num>
> Commit
```

**Note:** If the ACTIVE or INACTIVE options are used, committing a patch on one card raises a C\_MisM alarm. Committing the same patch on the second card clears the alarm. No alarms are raised or cleared if this is the first patch being committed.

- 7 If additional patches need to be applied, repeat from [step 2](#). Otherwise, this procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Troubleshooting

The following table describes causes of possible problems, and what actions are required.

| Problem                                                                          | Possible cause                                                                                                                           | Action                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SWACT while running patch commands                                               | The patch can be the cause of the SWACT.                                                                                                 | Patching does not continue and patches are rolled back on the formerly active Call Agent. Contact Nortel support personnel.                                                                                                                                                       |
| loss of mate communication while running patch commands                          | <ul style="list-style-type: none"><li>link failures at router</li><li>link pulls</li><li>abnormal software process termination</li></ul> | <p>Patching completes for the Call Agent on which patching was executing and looks for patch mismatch between the Call Agent cards.</p> <p>If communication fails during inactive Call Agent patching, patching completes successfully because the active is already patched.</p> |
| patch files available to only one Call Agent                                     | <ul style="list-style-type: none"><li>STORM failure</li><li>failure to retrieve patch files and write them to storage</li></ul>          | Correct STORM failure. Use the TRANSFER command to retrieve the files again. Attempt patch application again.                                                                                                                                                                     |
| patch levels out of synchronization between active and inactive Call Agent cards | A previous attempt to apply patches failed.                                                                                              | Contact Nortel support personnel for assistance with synchronizing the patch database files and determining the cause of failure.                                                                                                                                                 |



## Additional information

This section contains information about reverting to older patch levels and patch scenarios that require a platform upgrade.

### Reverting patches

Uncommit a patch from the running load with the UNCOMMIT command. Unless specified with the ACTIVE or INACTIVE options, the patch is uncommitted from the active Call Agent and then from the inactive Call Agent.

### Non-patchable versions

Non-patchable version patch files require a newer maintenance release than the currently running release.

Upgrade the platform software load first, then apply the patch file.

### Special application instructions

If the patch file contains special application instructions, use the DISADMIN to display the instructions. Execute the required instructions.

### PATCH level command reference

The following list of commands are available from the PATCH level.

- **SELECT** This command selects a patch file by integer value from the list of fetched patches for validation, display of administrative information, application, commit, or uncommit. For example, SELECT 5.
- **APPLY** This command applies a selected patch file to the running load. Unless specified with the ACTIVE or INACTIVE options, the selected patch is applied on the active Call Agent and then applied on the inactive Call Agent.
- **DELETE** This command deletes the selected patch file from storage. The patches cannot be in the APPLIED or COMMITTED state. Deleting patches in the APPLIED or COMMITTED state causes problems during booting and future attempts to remove the patches fail.
- **COMMIT** This command commits the selected patch file to the running load. The patch must be in the APPLIED state and when the card is reset or reboots, the patch is re-applied. This command accepts ACTIVE or INACTIVE options, though the options are expected to be used during platform and call processing application upgrades only.
- **UNCOMMIT** This command uncommits the selected patch file from the running load. The patch file remains in storage and remains

applied, but will not be re-applied after reset or a reboot. If other applied patch files depend on the selected patch file, a warning message is generated. Uncommit is permitted, but the dependencies are broken. Nortel does not recommend uncommitting patches that break dependencies. Use the REMOVE command to un-apply a patch from the running load.

- **FILTER** This command alters the list of patch files to show only the patch files that are in a specified state. The list of available states is ALL, NEW, VALIDATED, APPLIED, COMMITTED, and REMOVED.
- **REMOVE** This command un-applies the selected patch file from the running load. The patch file must not be in the COMMITTED state. The removed patch files are not deleted from storage. If other applied patches depend on the selected patch file, removal is refused. Remove uncommit and remove the patches that depend on the selected patch file first.
- **VALIDATE** This command validates that the selected patch file can be successfully applied to the running load. This command accepts ACTIVE and INACTIVE options though the options are useful only if the two Call Agent cards are running different patch levels.
- **DISADMIN** This command displays administrative data about the selected patch file.
- **UP** This command scrolls up the list of patch files.
- **DOWN** This command scrolls down the list of patch files.



# Media Gateway 15000 upgrade

This chapter describes how to upgrade the software on the Media Gateway 15000 (MG15k) nodes.

Formally known as Packet Voice Gateway (PVG), the Media Gateway is a software application built on a Multiservice Switch chassis with the addition of a Voice Services Processor (VSP) card. The Media Gateway 15000 creates a gateway between a time division multiplexed (TDM) network and a Multiservice Switch ATM or IP network.

## New in this release

This section describes changes to Media Gateway 15000 upgrades in (I)SN09U.

### Feature changes

None

### Other changes

None

## Upgrade paths

Nortel Networks supports the following upgrade paths:

- SN08 or SN09 to a SN09U software version, or from one SN09U software version to another SN09U software version within the context of a Packet Trunking - IP (PT-IP), Packet Trunking - AAL2, (PT-AAL2), Universal Access - Internet Protocol (UA-IP), Integrated Access Cable (IAC), or Integrated Access Wireline (IAW) solutions.

## Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

### Time to complete an upgrade

The following table lists the tasks to upgrade the software on a MG15k node and the estimated time to complete each task. The time varies depending on the node being upgraded. The maximum time estimate applies to the upgrade of the first node as it includes the activities performed once (e.g. reviewing release notes, backing up the views, etc.) for all the MG15K nodes.

**Table 1 Estimated time to complete a software upgrade**

| Task                         | Time           |
|------------------------------|----------------|
| Preparing for the upgrade    | 00:30 to 02:00 |
| Upgrading the software       | 00:35 to 00:45 |
| Completing the upgrade       | 00:15 to 00:20 |
| Total estimated upgrade time | 01:20 to 03:05 |

### Service impacts

The upgrade of MG15k software creates the following service impacts:



#### **CAUTION**

##### **Calls in process of being set up are dropped**

This strategy removes standby control and function processors from service. As a result, redundancy of the active shelf components is not available and some calls in the process of being set up (known as transient calls) are dropped. Stable calls are unaffected by the migration.

### Additional information

To perform the procedures discussed in this document, you should have a basic knowledge of Unix, Multiservice Data Manager (MDM), Multiservice Switch (MSS) software configuration, and Carrier Voice over IP portfolio architecture.

An upgrade of a Media Gateway 15000 node is also known as a hitless software migration (HSM). An operator performs a software migration using either the MDM Succession ATM Software Migration (SASM), or Succession IP Software Migration (SISM) tool. Once the HSM completes, the new functionality is added to the Media Gateway 15000 nodes by activating a new version of software.

During a HSM, the node logically splits into two shelves: the service shelf and the migration shelf. The service shelf contains the active FPs and is controlled by the active CP. The migration shelf contains the standby FPs and is controlled by the standby CP. The standby cards that are being loaded with the new version of software are referred to as the migrating cards.

Complete all the upgrade tasks before installing additional hardware and configuring additional capabilities.

In the event you need or want to downgrade the MG15k, refer to [Rollback of MSS 15000/MG 15000 nodes on page 995](#).

## System capacity

The software upgrade procedure can impact the system capacity.

## System performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade.

## System limitations during upgrade

The following limitations apply:

- During the migration, the active CP and FPs continue to operate using the old version of software while a new version of software is being loaded and provisioned on the migrating CP and FPs. The active cards remain active until the migrating cards have finished migrating to the new software and are ready to take over.
- The Media Gateway 15000 nodes in your network must be upgraded one at a time to ensure that no service interruption occurs. For in-band OAM configurations, Media Gateway 15000 nodes need to be upgraded in the sequence as listed in [Node upgrade order for in-band OAM configurations on page 2089](#).
- If you are performing a software upgrade on Multiservice Switch/Media Gateway 7480 elements or, a non-hitless software upgrade on Multiservice Switch/Media Gateway 15000/20000 elements, or an upgrade on out-of-service (OOS) MSS/Media Gateway 15000/20000 nodes, refer to the NN10600-272 *Nortel Multiservice Switch 7400/15000/20000 Upgrading Software* guide.
- MG15000 ASPEN media gateway control protocol is not supported in SN09U. ASPEN customers must have GNTS perform the conversion to H.248 before proceeding with an upgrade to SN09U. If you still have nodes using ASPEN, contact Nortel GNTS.

## Node upgrade order for in-band OAM configurations

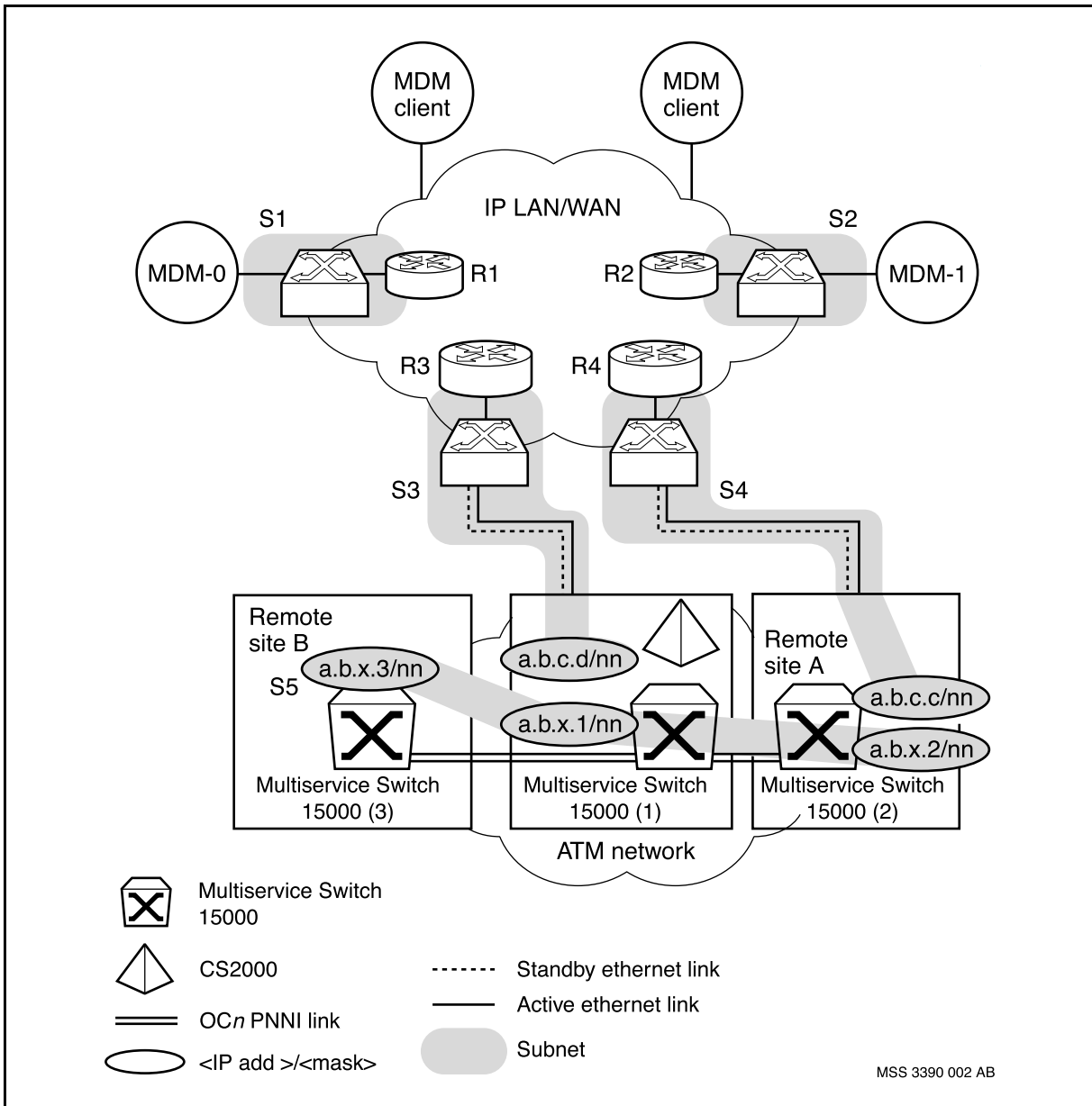
For in-band OAM configurations, Nortel Media Gateway 15000 nodes need to be upgraded in the sequence as listed in the procedure prerequisites. The following is a quick reference to key relationships you need to understand for in-band OAM migration.

Upgrade the MG 15000 nodes in your network one at a time to ensure that no service interruption occurs. For in-band OAM topologies, upgrade the nodes in the following sequence:

- all remote nodes first
- Gateway nodes next (non-preferred first and preferred, second). For more information about preferred and non-preferred gateways, see NN10028-111 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/PT-IP/UA-AAL1/UA-IP*.
- For all out-of-band OAM configurations, upgrade all the MG 15000 nodes:
  - not physically co-located with the CS2K first
  - physically co-located with the CS2K next

For more information about preferred and non-preferred gateways, see NN10028-111 *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/PT-IP/UA-AAL1/UA-IP*.

The figure [Sample in-band connectivity topology on page 2090](#) illustrates a typical in-band OAM configuration. A brief description of the items in this diagram and their relationship to each other is provided below.

**Figure 1 Sample in-band connectivity topology****MDM-0 and MDM-1**

These Nortel Multiservice Data Manager (MDM) servers manage Nortel Multiservice Switch network.

The chosen server is the server that the operator uses as a launching point for MDM applications, such as Command Console.

The alternate server is another MDM server that could be used to perform the same set of tasks, but wasn't chosen.

**Multiservice Switch -1**

This MG 15000 node is in the Carrier Voice over IP Office and is a Gateway node using out-of-band connectivity.

From the perspective of MDM-0, S3 represents subnet to the preferred MG 15000 node.

**Multiservice Switch-2**

This MG 15000 node is in a remote office and is a Gateway node using out-of-band connectivity.

From the perspective of MDM-0, S4 represents the subnet to the alternate MG 15000 node.

MG 15000

**Multiservice Switch-2 and Multiservice Switch-3**

S5 represents the in-band OAM subnet. Multiservice Switch-1 has a direct ATMMEPE ATM (PVC) connection to every other Multiservice Switch 15000 node.

These MG 15000 nodes are Remote nodes using in-band connectivity with Multiservice Switch-1.

Media Gateway 15000



---

## Upgrading the Media Gateway 15000

---

The following procedure provides the high-level steps to upgrade this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

You have completed the tasks in [Preparing to upgrade the Media Gateway 15000 on page 2093](#).

### Action

Perform the following tasks to upgrade the component.

1. Perform the HSM.

If performing HSM on a MG15k node configured for IP applications, use the procedure:

[HSM \(MDM SISM tool\) activation on page 968](#)

If performing HSM on a MG15k node configured for ATM applications, use the procedure:

[HSM \(MDM SASM tool\) activation on page 956](#)

2. The software upgrade is complete. Proceed to [Completing the Media Gateway 15000 upgrade on page 2098](#).

---

## Preparing to upgrade the Media Gateway 15000

---

The following procedure provides the high-level steps you need to execute prior to upgrading this component. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

This procedure has the following prerequisites:

- you have completed the tasks under [Preparing to upgrade the Carrier Voice over IP Network on page 9](#)
- you have upgraded all components that precede the Media Gateway 15000 under [Component Upgrade order on page 5](#)
- MDM GUI-based applications launched through a remote session must be launched on a trusted workstation. To start a trusted session, or to learn more about the MDM toolset, operator client interfaces, and processes that are common to all MDM tools, refer to 214-6001-122, *Using Toolset and Operator Client Interfaces*.

### Action

Perform the following tasks to prepare the component for upgrade. Once all the listed tasks are complete, you can proceed with the software upgrade.

Nortel recommends that you perform the tasks involving commands issued from the command line using MDM Command Console tool rather than a Telnet session. For more information on using the Command Console, see 241-6001-804 *Nortel Multiservice Data Manager Utilities*.

## Preparing to upgrade the Media Gateway 1500

### *At the command console*

- 1 Ensure you have the following user IDs:
  - user ID for Nortel web support.
  - user ID for MDM software download
  - user ID for general access to MDM
  - Media Gateway 15000 user ID configured for local access, and access to FTP, FMIP, Telnet and MDM server
  - Media Gateway 15000 user ID with a minimum command scope of device and a command impact of configuration.

To determine your command scope and impact, type **me**. Information about your user ID is displayed.
- 2 Collect information to identify and avoid any compatibility issues that can prevent a software migration from completing successfully. For this task, use the procedures in the section:  
[Information collection on page 932](#)
- 3 Download the new software version and patches and back up the current view of the Media Gateway 15000 software. For this task, use the procedures in the section:  
[Downloading and backing up MSS 15000/MG 15000 software on page 938](#)
- 4 Before performing the upgrade, ensure that all journal files are either used or purged by issuing this command: *display ProvisioningSystem restorePossible*.  
  
If the response is yes, purge the files by issuing the *commit force prov* command. Then re-issue the *display ProvisioningSystem restorePossible* disk to verify the files have been purged. To restore these journal files, see the Restore Prov command section in NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*.
- 5 If you have DS-1 IMA interfaces using the Edgelink100 MUX, ensure that you use Edgelink100 MUX software (R3.3) during the SN09U upgrade.  
  
For detailed steps, refer to the procedure [Determining the software version of the Edgelink 100 MUX on page 2096](#).
- 6 Ensure that all configuration changes from the Global Bulletin System (GBS) and any associated Method of Procedure (MOP) are reflected on the node before performing the upgrade.

- 7 Ensure that all components supporting the service intended to be hitless are enabled. Check all the components prior to activating the migration provisioning to minimize any impacts to associated services. For details, refer to the following procedures in the *Nortel Multiservice Switch 7400/15000/20000 Upgrading Software Guide*, NN10600-272.
  - "Verifying the node status before upgrading"
  - "Verifying specific node information"
  - "Verifying the VR status"
- 8 Ensure nodes are connected to MDM servers. The nodes must also be in service and capable of supporting traffic and network management functions..

From the MDM client nmstool, select **System -> Administration -> Host Group Administration**. Ensure that your MSS15K or MG15K appears in the list of nodes and belongs to an MSS Group .

From the MDM client nmstool, select **System -> Administration -> GMDR Administration**. Ensure that the node appears in the list of components when "Show Components" button is selected. Select the node from the list and ensure that the Raw State is "INSV". Close the Components dialog and GMDR Administration tool.
- 9 In addition, the nodes must not have any major or critical alarms raised on them. From the MDM client nmstool, select **Fault -> Alarm Display : Active**. Ensure that there are no active alarms associated to the node. Contact your next level of support if necessary.
- 10 Ensure that you have an alternate way to access the node in case you lose IP connectivity during the migration.

For example, you can connect an operator terminal as described in the section "Connecting an operator terminal" in the NN10600-130 *Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*. You can also use a modem or some other mode of out-of-band connectivity that was in place during the initial installation of the node.
- 11 If upgrading an ATM application, log into the MG15 and determine if there are Pbg components configured by executing the **display Pbg/\*** command. These components require some additional attention during the pause in the SASM HSM.
- 12 You have completed the pre-upgrade tasks. Proceed to [Upgrading the Media Gateway 15000 on page 2092](#).

## Determining the software version of the Edgeline 100 MUX

### *At the command console*

- 1 Log into the Edgeline 100.

Example response

```
EDGELINK100
ROOT MENU
1) CONFIGURATION MANAGEMENT
2) PERFORMANCE MANAGEMENT
3) FAULT MANAGEMENT
4) DIAGNOSTICS
5) SYSTEM CONFIGURATION STATUS
6) SYSTEM ADMINISTRATION
```

- 2 Select the number beside system configuration status (5).

Example response

```
EDGELINK100
SYSTEM CONFIGURATION STATUS
1) DS3 INTERFACE STATUS
2) DS1 INTERFACE STATUS
3) SYSTEM STATUS
4) IP ADDRESSES
5) CARD INVENTORY
6) PEER LAPD DATA
```

- 3 Select the number next to card inventory (5).

Example response

```
CARD INVENTORY
M13 CCA420 = G10
M13 CCA = E
M13 CCB = E
M13 CCP = E
M13 SERIAL# = 642010271
MANUFACTURE DATE = 11/22/01
CLEI = M3CMUN08AA
M13 SOFTWARE REV = 3.3
SW RELEASE DATE = 11/20/02
MAC ADDRESS = 00001F10C97A
```

- 4 The software version is listed on the 8th line (M13 SOFTWARE REV). Confirm it is version 3.3.

If not, contact your next level of support.

- 5 Log off the Edgeline 100 by pressing control + E (Ctrl E).

- 6** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Completing the Media Gateway 15000 upgrade

---

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

HSM has completed successfully.

### Action

Perform the following procedures to complete the component upgrade.

1. Activate and provision new features. For this task, use the procedures in the section:  
[Feature activation on MSS 15000/MG 15000 nodes on page 984](#)
2. Create a backup of the current view of the newly upgraded node(s). For this task, use the procedure [Back up the current view on page 952](#)
3. Upgrade the next component in the end-to-end upgrade. Refer back to [Component Upgrade order on page 5](#).



## CICM upgrade

### ATTENTION

If patch P1, P2, or P3 has been applied to 9.0 MR1 or 9.0 MR2 then the following must be applied before performing the maintenance release upgrades listed below:

9.0 MR1 P4 - if upgrading from 9.0 MR1 to 9.0 MR3.

9.0 MR2 P4 - if upgrading from 9.0 MR2 to 9.0 MR3.

### ATTENTION

SN09 sites that are at CICM SN09 MR3 (or higher) are at SN09U baseline and do not require an upgrade.

Centrex IP Client Manager (CICM) is part of Nortel's Carrier Hosted Services (CHS), which is a portfolio of products and services that provides IP-based solutions to IP network-based subscribers. CHS delivers legacy Digital Multiplex System (DMS) and Centrex capabilities to users connected to an IP network using voice multimedia integration. CICM delivers Centrex capabilities to users connected to an IP network using VoIP technology on a PC SoftClient or an IP P-phone.

A CICM upgrade procedure includes the required steps, preparation, and processes to upgrade the software of a redundant pair of Centrex IP Client Manager (CICM) element managers (EMs) and its pairs of CICM nodes.

### New in this release

#### Feature changes

SN09 sites that are at CICM SN09 MR3 (or higher) are at SN09U baseline and do not require an upgrade.



## Upgrade paths

Upgrading from SN08 requires the following two upgrades:

1. SN08 (MR2 or MR3) to SN09 MR1
  - Order code CICM0090
  - Order Code CICE0090
2. SN09 MR1 to SN09 MR3
  - Order code CICMM090

Upgrading from SN09 requires one of the following upgrades (depending on the release before beginning the upgrade):

- SN09 MR1 to SN09 MR3
  - Order code CICMM090
- SN09 MR2 to SN09 MR3
  - Order code CICMM090

SN09 sites that are patch current and at CICM SN09 MR3 (or higher) are at SN09U baseline and do not require an upgrade.

## Time to perform an upgrade

The following table lists the time required to upgrade CICM software.

### Estimated time to complete a software upgrade

| Task                         | Time                             |
|------------------------------|----------------------------------|
| Preparing for the upgrade    | 40 minutes <sup>1</sup>          |
| Upgrading the software       | 15 minutes per node <sup>2</sup> |
| Completing the upgrade       | 10 minutes <sup>3</sup>          |
| Total estimated upgrade time | 110 minutes <sup>4</sup>         |

1.Requires manually backing up the nodes and copying the upgrade files (2 for SN09-SN09U, 4 for SN08-SN09U). This time varies depending on the connection speed between the CICM-EM and the upgrade file source location.

2.Each CICM configuration consists of two CICM-EM nodes and multiple pairs of CICM (gateway) nodes. Allow 15 minutes for each individual node.

3.To delete obsolete upgrade files from the CICM-EM.

4.This estimate represents the time required to upgrade two CICM-EM nodes and two CICM gateway nodes. Add 30 minutes to the overall upgrade time for each additional pair of CICM gateway nodes.

## Service impacts

When upgrading from SN08 to SN09, during a switch of activity (SWACT) between the Master and Slave nodes, only established stable calls survive. Calls not yet established may drop. SWACT duration is approximately 2 minutes.

## System Capacity

Perform all software upgrade procedures during scheduled maintenance periods, as network capacity is reduced during the software upgrade.

## System limitations during upgrade

The following limitations apply:

- Upgrading from SN08 requires starting from a minimum SN08 MR3 load.
- Upgrading from SN08 to SN09U baseline requires the following upgrades:
  - SN08 to SN09 MR1
  - SN09 MR1 to SN09 MR3
- Upgrading from SN09 to SN09U baseline requires upgrading from SN09 MR1 or MR2 (whichever is installed) to SN09 MR3.
- During the upgrade, terminals are automatically transferred as part of the SWACT. That is, the CICM <new load> master (becoming the slave) transfers its terminals to the CICM <old load> slave (becoming the master) so that the new master has all of the terminals.
- During the upgrade when nodes temporarily have different versions of software, initiating a SWACT while the node is the master will cause the floating UNISim address to be unbound. Any terminals connected to this node will be lost. Manually transfer the terminals away from the node before the SWACT.
- During the upgrade to CICM Node A, the CICM selects its existing static UNISim address as the floating address.
- During the upgrade, the CICM does not update the S1 and S2 entries of the terminals connected to the CICM at the time of the upgrade. The operator must make any required configuration changes to the terminals following the upgrade (for example, through DHCP).

## CICM software versions

CICM-EM and CICM gateway software loads operate independently of each other. Each CICM pair must have the same software version, however the node pair and EM pair can run on different software versions during an upgrade. There should only be a brief time during an upgrade where the EM has been upgraded to a later release, but the CICM gateway nodes have not. For example; after the CICM-EM has been upgraded to SN09, it must continue to manage the CICM gateways still running an earlier release until they are also upgraded.

The software version has the format  
<release\_number>.<build\_number>

### Example

9.10.191

The release number is 9.10

The build number is 191

The lower left corner of the CICM-EM web pages shows the base release of the software version (for example, 9.0 for SN09). The web page maintenance (cicm-nnn) identifies the current CICM-EM or node pair software version.

## CICM upgrade types

Two types of CICM-EM or CICM node upgrades exist:

- product release
- maintenance release

### product release upgrade

An upgrade by product release involves loading an increment of a different version of software, that is, the software release number increments (for example, from x.y to x+1.y). Applying a product release over-writes previous software and will require a series of system restarts for each upgraded node.

CICM product releases are made available from the ISO vault. Each release includes its own upgrade file. Separate releases are available for each of the following:

- the CICM-EM using the CPV5370 cards
- the CICM-EM using the CPN5385 cards
- the CICM nodes using the CPV5370 cards
- the CICM nodes using the CPN5385 cards

**maintenance release upgrade**

An upgrade by maintenance release (MR) involves loading an increment of the build number within the same version of the software release. An MR software release is identified by the build number. For example, the build number would change from 9.10.xxx to 9.10.MRy.

To ensure that an MR is appropriate to a specific node (CICM-EM or CICM), the system also checks that the load is intended for the type of node it is being applied to, and for an appropriate range of load build numbers. The node and the load criteria must be met for the MR to be applied.

Applying an MR over-writes previous software and requires at least one system restart. Because of the over-writing, applying an MR is not influenced by any patch state. Since an MR includes all previous patches, the former patch history is erased from the system and a record of it is included in the Release Notes for the MR.

**Upgrade implementation guidelines**

The guidelines for implementing upgrades are as follows.

- Obtain and read any applicable technical bulletins
- Always read the release notes prior to an upgrade.
- The sequence of upgrading is to upgrade the CICM-EM, then the CICM gateways, then the terminals. If a primary and backup CICM-EM pair are deployed, both EMs must be upgraded prior to the first CICM gateway upgrade.

Terminal upgrades are addressed in [Upgrading firmware on IP phone sets on page 2164](#).

- Each node of the CICM is upgraded individually. However, paired nodes are upgraded to the same software version. Running paired nodes at different versions for can result in degradation in performance or behavior while the nodes are running different software versions.
- No network re-configurations are to occur during an upgrade. Rolling back from the upgrade, that is, returning operation to the former software version, is not possible.
- Do the upgrade during the lowest call traffic period to minimize impact on users.
- The upgrade takes one to two hours to complete. Service degradation by call capacity reduction occurs only for portions of the upgrade period.

- For MR upgrades only, resource use (that is, active call count) can be monitored from the CICM-EM.
- Upgrades procedures require administrator userids and passwords to login to the CICM-EM.
- Always perform a recent backup prior to an upgrade.

## **CICM-EM or CICM node patching**

With SN09 or later, a software patch can be applied to CICM-EMs or CICM nodes between MR upgrades. Patching for CICM is done manually per node and is not part the Network Patching Manager (NPM).

A patch includes either:

- third-party corrective component software, for example, a Microsoft security fix for the Windows operating system (OS) or an Intel patch for the VLAN drivers
- selective binary component software to fix a portion of an MR or product release

A patch typically includes one fix and does not include new functionality to the operation or maintenance of CICM-EMs or CICM nodes.

To ensure that a patch is appropriate to a specific node (CICM-EM or CICM), the system automatically compares what is running on the system with what is in the patch. According to preset version control rules, an incompatible load is prevented from being applied. The version control rules are:

### **Dependency list**

identifies the patches that must already be loaded on the node before this patch can be applied. If at least one dependent patch is missing, the new patch cannot be applied.

### **Conflict list**

identifies the patches that are incompatible with the patch to be applied. If at least one conflicting patch is present, the new patch cannot be applied.

Once this patch is applied, no patch within the conflict list can be applied until the new patch is removed.

### **Subsumation list**

identifies the previously-released patches that are included in this patch. Any of the previous patches that is not already loaded will be applied when this patch is applied.

**Removal list**

identifies the patches that will be removed by this patch. Once this patch is applied, none of the listed patches can be applied or re-applied.

To ensure that a patch is appropriate to a specific node (CICM-EM or CICM), the system also checks that the load is intended for the type of node it is being applied to, and for an appropriate load build number. The node, the load, and version control criteria must be met for a patch to be applied.

Applying a patch over-writes only a selective portion of the software and may or may not require a full or partial system restart. Information from Global Networks Platform Support (GNPS) indicates the amount of outage to expect per patch. Information is also supplied with each patch so that you know what it provides for an in-service system before applying it. It is not necessary for you to load each patch that is available, however, always follow the guidelines and recommendations provided by Nortel Networks GNPS.

A history of the applied and non-applied patches is provided at the CICM web pages. The task flow includes the procedure describing how to use the history.

**CICM software files**

The source of software upgrade or patch files for either the CICM-EMs or the CICM nodes are handled by the following computer setups and delivery methods:

- [Computer setups to handle software files](#)
- [Recognizing the type of source file for an upgrade or a patch](#)
- [Compact disks](#)
- [Web distribution](#)

With SN09 and later, each MR or patch file also has a separate file with an MD5 checksum. As part of an upgrade or patch, the checksum is displayed on a CICM-EM web page so that you can compare the expected file number with the actual number. Manually confirming matched checksums verifies the integrity of the upgrade file before applying it. This action is included in the procedures to apply an upgrade or patch.

The details of file management are included in various procedures that are invoked in sequence by the task flows in this document.

### Computer setups to handle software files

The computer setup you can use to handle the software files for CICM-EMs and CICM nodes must be able to access the CICM-EMs. The setup can involve one of the following:

- a personal computer (PC)
- a Nortel Networks server, such as a Server Foundation Platform Software (SPFS) or the Integrated Element Management System (IEMS)
- your own server

The PC and your server must comply with the specifications identified in *CICM Basics*, NN10044-111 and run the supported operating system (OS) software.

### Recognizing the type of source file for an upgrade or a patch

The source files for upgrades or patches have different naming convention to distinguish what each file applies to. The naming conventions are as follows:

For maintenance release (MR) upgrades (i.e. staying within the same release):

- for SN08 and earlier CICM-EM upgrade files: EM\_<version>.cab
- for SN08 and earlier CICM node upgrade files: GW\_<version>.cab
- for SN09 and later CICM-EM upgrade files: EM\_<version>.upg
- for SN09 and later CICM node upgrade files: GW\_<version>.upg

For SN09 and later patch files (i.e. applying a patch for critical bug fix content):

- for SN09 and later CICM-EM patch files:  
EM\_PATCH\_<version>\_P<patch number>.pat
- for SN09 and later CICM node patch files:  
GW\_PATCH\_<version>\_P<patch number>.pat
- for SN09 and later CICM-EM patch files, the file containing the patch information: EM\_PATCH\_<version>\_P<patch number>.txt
- for SN09 and later CICM node patch files, the file containing the patch information: GW\_PATCH\_<version>\_P<patch number>.txt

**Note:** Patching was not possible in SN08 and earlier releases, therefore patch files and the patching process apply only to SN09 and later releases.

For product release upgrades (i.e. upgrading to a later release):

- for CICM-EM upgrade files: EM\_UPGRADE\_<version>.cab
- for CICM node upgrade files: GW\_UPGRADE<version>.cab

Version numbering is described in [CICM software versions](#).

Patching is not supported prior to SN09, so there are no pre-SN09 patch file names.

### Compact disks

A series of compact disks (CDs) provides the following software for both the CICM-EMs and the CICM nodes:

- a product release (which is an MR zero) and any patches
- an MR and any post-MR patches

Patches are included on CD only if they are available for an initial installation of a product release or MR. (Otherwise, patches are made available by [Web distribution](#).)

The label on a CD containing CICM software begins *CICM...*, for example:

- on the 3 CDs associated with order code CICE0090:
  - CICE0090 MR3 EM Install - do not use this CD for an upgrade
  - CICE0090 Upgrade Software - upgrading from series 8.0 (must be at MR2 or MR3) to 9.0 MR1
  - CICE0090 Patches” - applying software patches to a CICE0090 running Series 9.0
- on the 4 CDs associated with order code CICE0090:
  - CICE0090 MR3 SAM21 Install - do not use this CD for an upgrade
  - CICE0090 MR3 SAM16 Install - do not use this CD for an upgrade



- CICM 9.0 Upgrade Software - upgrading from series 8.0 (must be at MR2 or MR3) to 9.0 MR1
- CICM0090 Patches” - applying software patches to a CICM running Series 9.0
- on the 1 CD associated with order code CICMM090:
  - CICM 9.0 MR3 Software - upgrading from series 9.0 MR1 or 9.0 MR2 to 9.0 MR3

**Note:** CICE0090 and CICM0090 both contain the same *CICM 9.0 Upgrade Software* CD.

CD labels designated as "GW" or "EM" represent base installation software for the SAM16 CICM platform. CD labels designated as "CMT" represent base installation software for the SAM21 CICM platform. Use the "Upgrade" CDs for the procedures described in this book.

### Web distribution

Patches or m6350 SoftClient software are downloaded through the Internet from a secure Nortel Networks web page and stored on your personal computer (PC) or server. The web page is [www.nortel.com](http://www.nortel.com) and the procedure to use it is invoked from a procedure in the task flow of CICM-EM and CICM node preparations.

## High-level methodology for applying upgrades or patches

The high-level methodology for handling upgrade or patch files is:

- copying the files from a source onto a computer that interfaces the CICM-EMs (this is not required if you are set up for point-of-use distribution)
- electronically transferring the files into appropriate directories on the master CICM-EM
- switching the activity of CICM-EM pairs to enable downloading the mate
- electronically transferring the files into appropriate directories on the new master CICM-EM
- for an MR or a patch, verifying the expected and actual checksums
- applying the appropriate files from the master CICM-EM to its slave mate or the slave CICM node
- verifying the success of the upgrade or patch

- switching the activity of node pairs to enable downloading to the mate
- verifying both nodes of a pair are operating normally and fully

## Hardware revision compatibility

The table [Hardware revision compatibility](#) summarizes the hardware to software compatibility with CICM SN09 and all previous releases.

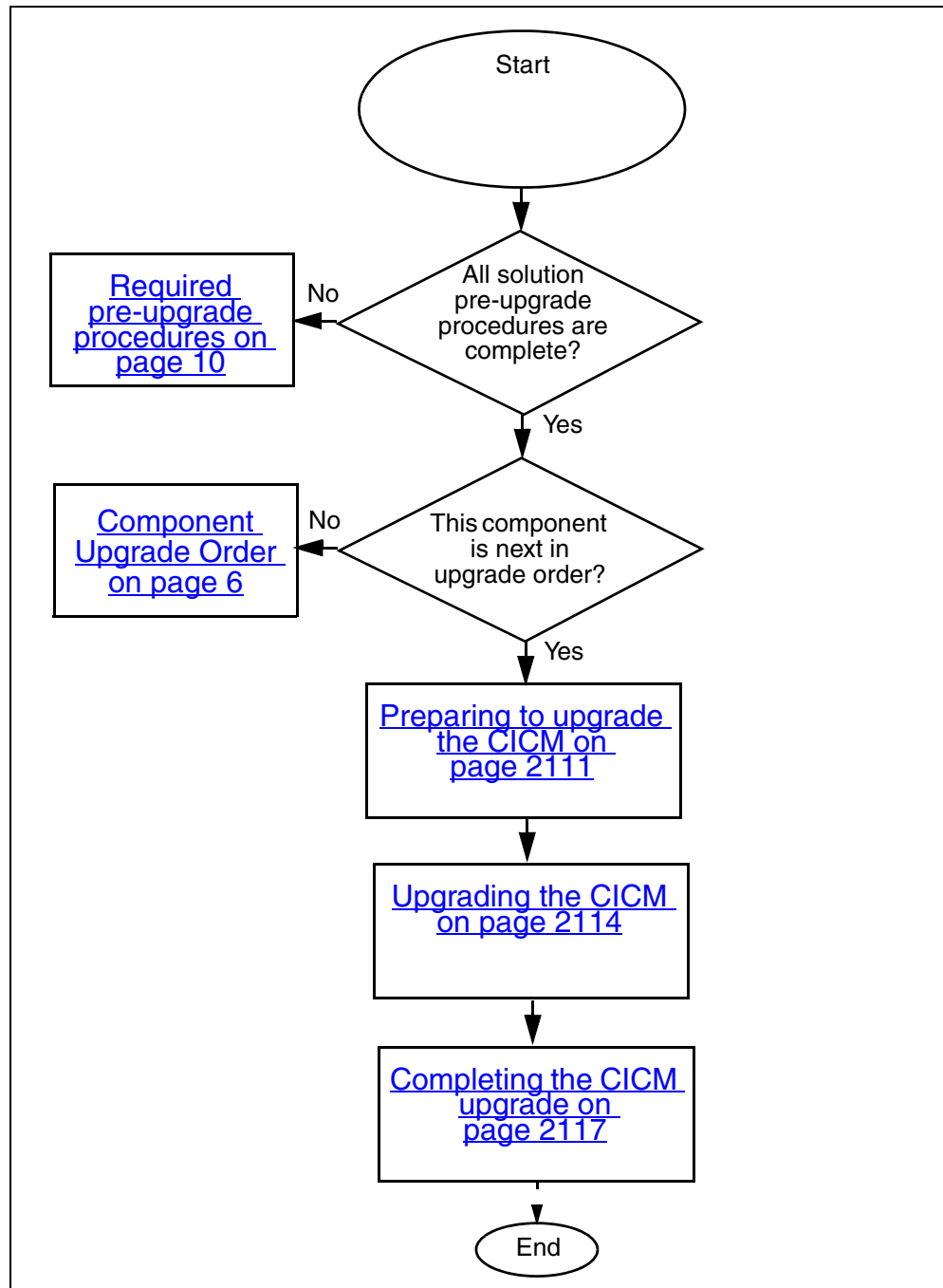
CICM with SN08 and later supports two hardware revisions. No new hardware is required to upgrade from SN08 or SN09. SN09 MR3 is required for SN09U network compatibility.

**Table 1 Hardware revision compatibility**

| Hardware revision | CICM node                           | CICM-EM                                | Supported software releases       |
|-------------------|-------------------------------------|----------------------------------------|-----------------------------------|
| B                 | SAM16 Shelf<br>CPV5370<br>processor | CXIP1204 Shelf<br>CPV5370<br>processor | SN6.12,<br>SN07,<br>SN08,<br>SN09 |
| C                 | SAM21 Shelf<br>CPN5385<br>processor | SAM21 Shelf<br>CPN5385<br>processor    | SN07,<br>SN08,<br>SN09            |
|                   |                                     |                                        |                                   |

## CICM upgrade tasks

The following taskflow provides a high level task sequence to perform this component software upgrade.

**Figure 1 CICM upgrade tasks**

---

## Preparing to upgrade the CICM

---

This section provides the high-level steps involved in preparing to upgrade this component. Where applicable, references to step-by-step procedures are provided.

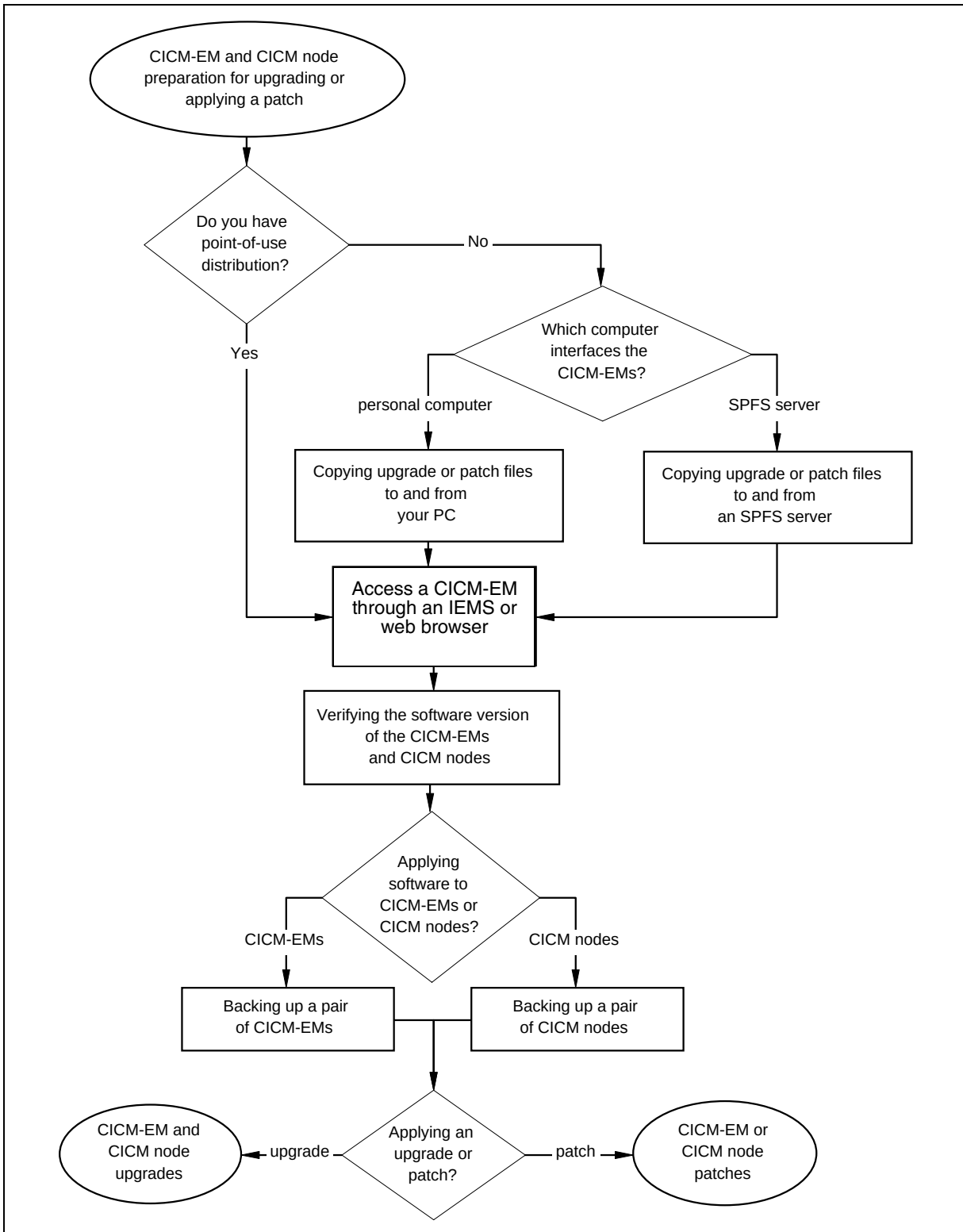
### Prerequisites

Before performing any procedures:

- Read the CICM Release Notes for updated information.
- Obtain and read any applicable technical bulletins
- the IEMS must be configured to enable accessing the CICM-EM and the CICM must be configured to interwork with the IEMS

### Task flow of CICM-EM and CICM node preparation

The task flow on the next page shows the high-level sequence for preparing a CICM EM and node upgrade.

**CICM-EM and CICM node upgrade preparation task flow**

**ATTENTION**

The flow chart suggests performing a backup immediately before the actual upgrade. The backup may be performed earlier in the process in order to accommodate available maintenance windows, however always perform a recent backup prior to performing any upgrade.

## Navigation

The procedures and tasks in the task flow are listed below.

- [Copying upgrade or patch files to and from an SPFS server](#)
- [Copying upgrade or patch files to and from your PC](#)
- [Getting CICM patch files from the Internet](#)
- [Accessing a CICM-EM through the IEMS](#)
- [Accessing a CICM-EM through a web browser](#)
- [Verifying the software version of the CICM-EM and CICM nodes](#)
- “Backing up a pair of CICM nodes” in *CICM Security and Administration*, NN10252-611 (Global - Carrier Hosted Services Collection)
- “Backing up a pair of CICM-EMs” in *CICM Security and Administration*, NN10252-611 (Global - Carrier Hosted Services Collection)
- [CICM-EM or a CICM node patches](#)

## Action

Refer to [Preparing to upgrade CICM software](#).

---

## Upgrading the CICM

---

Upgrading from SN08 requires the following two upgrades:

1. SN08 (MR3 or higher) to SN09 MR1
2. SN09 MR1 to SN09 MR3

Upgrading from SN09 requires one of the following upgrades (depending on the release before beginning the upgrade):

- SN09 MR1 to SN09 MR3
- SN09 MR2 to SN09 MR3

SN09 sites that are at CICM SN09 MR3 (or higher) are at SN09U baseline and do not require an upgrade.

### Prerequisites

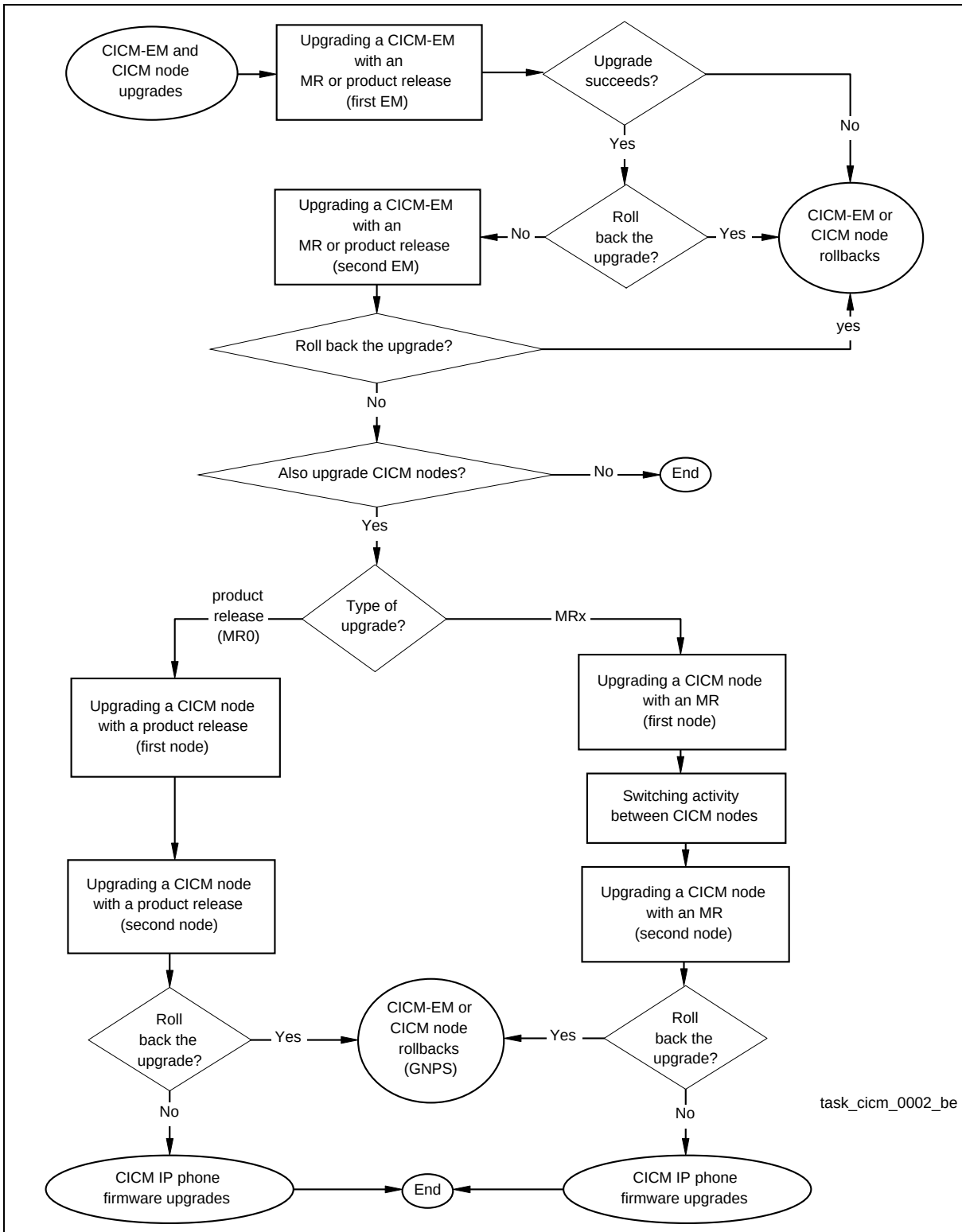
You have completed [Preparing to upgrade the CICM](#).

### Task flow of CICM-EM and CICM node upgrades

The task flow shows the sequence of procedures and other task flows that are required to prepare for applying an upgrade or patch to a redundant pair of CICM-EMs and a redundant pair of CICM nodes.

**Note:** Some rollback decision points do not appear in the upgrades task flow because they are included within more than one procedure.

## Task flow of CICM-EM and CICM node upgrades





## Navigation

The following procedures and tasks in the task flow are listed.

- [Upgrading a CICM-EM with an MR or product release](#)
- [Upgrading a CICM node with a product release](#)
- [Upgrading a CICM node with an MR](#)
- [Switching activity between CICM nodes](#)

**Note:** The procedure to switch activities between CICM gateway nodes is required for “Upgrading a CICM node with a product release” and “Upgrading a CICM node with an MR”.

- [Upgrading firmware on IP phone sets on page 2164](#)
- [CICM-EM or a CICM node patches](#)
- [Removing old CICM load files](#)

## Action

The upgrade process consists of upgrading:

- a redundant pair of CICM element managers (EMs)
- pairs of CICM nodes

Refer to [Upgrading CICM software](#).

## Rolling back an upgrade

If a software upgrade fails, refer to [Rolling back from a CICM-EM or CICM node upgrade on page 2190](#) for procedures.

---

## Completing the CICM upgrade

---

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

### Prerequisites

Complete the instructions for [Upgrading the CICM](#).

### Action

After the CICM upgrade has been completed, address the following.

- Node B's static UNISim address is no longer valid for use by terminals in the network. Once the upgrade is complete, it is recommended that the operator take the necessary steps to update all terminals in their network so that they do not attempt to contact the CICM on this (now) invalid address.

If using DHCP, its configuration must be changed. Refer to DHCP documentation for information on configuration DHCP servers.

- Leaving terminals configured with the old B UNISim address will not cause harm to the network. However, it can cause individual terminals to take longer to locate the CICM following a terminal reboot, since it can use the invalid address for its search.
- If a survivable remote gateway (SRG) is to be deployed, this can safely be done once the CICM has been upgraded. In doing so, the terminal must be reconfigured such that S1 is set to the CICM's floating UNISim address, and S2 is set to the SRG's address. These must not be reversed. The SRG uses S2.
- For those terminals in the network not serviced by an SRG, it is recommended that both their S1 and S2 entries be set to the CICM's floating UNISim address.
- Perform the procedure [Removing old CICM load files](#) to remove obsolete CICM upgrade files from the CICM-EM and free up disk space.

Perform the next required upgrade according to the [Component Upgrade Order on page 6](#). The required upgrade is the next component in the list according to your network configuration.

---

## Preparing to upgrade C1CM software

---

### ATTENTION

Before beginning the C1CM upgrade, obtain and read all applicable technical bulletins.

For more information regarding technical bulletins, refer to the Nortel web site <http://www.nortel.com>.

This section provides the software strategy to prepare for upgrading or patching the Centrex IP Client Manager (C1CM) element manager (EM) software and its pairs of C1CM nodes.

Always apply an upgrade or patch to both C1CM-EMs or both C1CM nodes of a redundant pair.

### Backing up and restoring the C1CM-EM and C1CM node software

Backing up the software of the C1CM-EM and C1CM nodes prior to an upgrade is a contingency plan to enable restoring a software image. The process, methodology, and procedures are in *C1CM Security and Administration*, NN10252-611.

Restoring the software configuration of the C1CM-EM and C1CM nodes is described in *C1CM Fault Management*, NN10233-911.

### Prerequisites for a C1CM software upgrade

Before the software of a C1CM node is upgraded, the following must be done.

1. Upgrade the CS2M, Core, and GWC.
2. Copy the C1CM-EM upgrade file to the location on the C1CM-EM that is used for an upgrade.
3. Copy the C1CM node upgrade file to the location on the C1CM-EM that is used for an upgrade.
4. Upgrade the C1CM-EMs.
5. Upgrade the C1CM nodes.

### C1CM-EM and C1CM node preparation for an upgrade or patch

Prepare a pair of Centrex IP Client Manager (C1CM) element managers (C1CM-EM) and their pairs of C1CM nodes for an upgrade or patch by doing a series of procedures in a task flow.

### Prerequisites to the task flow of CICM-EM and CICM node preparation

Before following the task flow, ensure that you have addressed these requirements.

- The task flow and all procedures in it apply to doing these upgrades for either SAM21 and SAM16 hardware:
  - an MR from your current release up to three increments apart, for example, 9.0 MRx to 9.0 MRy where x and y are less than or equal to three increments apart or for example  
9.0 MR1 with 9.0 MR2, 9.0 MR3, or 9.0 MR4
  - a product release from your current release to a subsequent release, for example, from:
    - 7.0.MRx or later to 8.10
    - 7.0.MR7 or later to 9.0
    - 8.0 MR2 to 9.0

Refer to the CICM Release Notes for the actual supported versions.

- All Carrier Voice over IP (VoIP) components that are non-gateway-specific (including the CS2000, CS2000 Management Tools server (formerly SESM), and gateway controllers) must already have been successfully upgraded to the target upgrade release and be fully in service.
- IEMS must be configured to enable accessing the CICM-EM, usually as part of an initial installation. Otherwise refer to *Integrated EMS Configuration Management*, NN10330-511.
- CICM must be configured to interwork with IEMS, usually as part of an initial installation. Otherwise refer to *Configuration Management*, NN10240-511.
- Read and understand [Preparing to upgrade CICM software](#).
- You must have access to the appropriate upgrade and patch files from Nortel Networks.

### Software upgrade strategy of CICM

The software upgrade strategy of CICM is divided into:

- [Prerequisites for a CICM software upgrade](#)
- [CICM software upgrade summary](#)
- [Follow-up after a CICM software upgrade](#)
- [Conversion from TDM](#)

**CICM software upgrade summary**

The CICM software upgrade strategy is summarized as follows.

- The supported software upgrade paths are from these CICM release versions:
  - SN08 to SN09 MNCL supporting SN09FF
  - SN09 to SN09 MNCL supporting SN09FF
- MR upgrades for the CICM-EM and CICM nodes may be performed by operating company CICM administrators.
- The CICM upgrade from SN08 to SN09 must be done remotely by operating company CICM administrators using a process similar to a maintenance release (MR) upgrade.
- No hardware changes are required for CICM upgrades

**Follow-up after a CICM software upgrade**

After an upgrade is completed, address or note the following.

- Node B's static UNISim address is no longer valid for use by terminals in the network. Once the upgrade is complete, it is recommended that the operator take the necessary steps to update all terminals in their network so that they do not attempt to contact the CICM on this (now) invalid address.

If using dynamic host configuration protocol (DHCP), its configuration should be changed. Refer to DHCP documentation for information on configuration DHCP servers.
- If a survivable remote gateway (SRG) is to be deployed, this can safely be done once the CICM has been upgraded. In doing so, the terminal must be reconfigured such that S1 is set to the CICM's floating UNISim address, and S2 is set to the SRG's address. These must not be reversed. The SRG uses S2.
- For those terminals in the network not serviced by an SRG, it is recommended that both their S1 and S2 entries be set to the CICM's floating UNISim address.

**Conversion from TDM**

CICM does not support a conversion from TDM to Carrier Voice over IP (VoIP).

## Copying upgrade or patch files to and from an SPFS server

Copy the upgrade files onto a Server Foundation Platform Software (SPFS) server from a Nortel Networks CD and then onto a redundant pair of CICM-EMs to make the files available for upgrading or patching the CICM-EMs and their CICM nodes.

### Prerequisites to copying upgrade or patch files to and from an SPFS server

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in [CICM-EM and CICM node preparation for an upgrade or patch](#).
- You must know the unique Administration IP addresses of each CICM-EM of the pair.
- Both CICM-EMs must be in-service to enable accepting the files.
- You must use a secured FTP (SFTP) session to copy files to or from a CICM-EM (but not from a CICM node to its EM). You are responsible for providing your own software for an SFTP, for example, WinSCP.
- An equivalent to the SPFS server can also be used, in which case, use the procedure as a guide to indicate directories and file names. For example, the SPFS login steps in the procedure will likely be different for a PC.

### Procedure steps to copying upgrade or patch files to and from an SPFS server

#### *At the UNIX-based SPFS server*

- 1 Load the CD with the upgrade files into the CD-ROM drive.
- 2 Log into the SPFS server by using a secure telnet session:  
**ssh <ip\_address\_SPFS> -l <username>**
- 3 At the prompt, confirm the R\_\_\_\_\_ S\_\_\_\_\_ A\_\_\_\_\_ (RSA) fingerprint is correct and when prompted, enter the user's password.
- 4 Become the root user by entering:  
**su root**
- 5 Go to the top level directory of the CDROM by entering:  
**cd /cdrom/cdrom0**  
The last character of *cdrom0* is a zero.

- 6 List the files at the directory by entering:  
**ls -al**
- 7 Go to the directory containing the upgrades files by entering, for example:  
**cd "Upgrade Files"**
- 8 SFTP to the master CICM-EM and log into it by entering:  
**sftp Administrator@<ip\_address>**  
where <ip\_address> is the static IP address of the CICM-EM (as opposed to the floating IP address).  
As logging in begins, the response is:  
Connecting to <ip\_address>...  
The authenticity of host '<ip\_address>' (<ip\_address>) can't be established.  
DSA key fingerprint is <string>  
Are you sure you want to continue connecting (yes/no)?  
9 Confirm the prompt:  
**yes**  
Logging in continues with:  
Warning: Permanently added '<ip\_address>' (DSA) to the list of known hosts.  
Administrator@<ip\_address>'s password:  
10 Enter the Administrator password:  
**<admin\_password>**  
A successful password is indicated by the command prompt for SFTP:  
**sftp>**  
11 Identify the directory you are at:  
**pwd**  
The home directory of the server is always indicated after login:  
Remote working directory: /HOME

- 12** Go to the directory on the CICM-EM where the EM upgrade files are to be copied:

---

**If the  
CICM-EM**

**Do**

is at SN08

**cd /D:/Centrexip/support/firmware/elementmgr\_MRs**

is at SN09 (or  
later)

**cd /D:/Centrexip/support/upgrades/em**

---

**Note:** The command prompt for SFTP re-appears:

sftp>

- 13** Confirm you have reached the directory:

**pwd**

The directory is echoed:

Remote working directory:

D:/Centrexip/support/upgrades/em

or before the first CICM-EM node is upgraded:

/D:/Centrexip/support/firmware/elementmgr\_MRs

- 14** Copy each EM\_ MR upgrade file to the CICM-EM directory  
/upgrades/em:

**put EM\_<release>.upg**

**Example**

EM\_9.10.203.upg

The progression of copying is indicated by:

Uploading <file\_name> to

/D:/Centrexip/support/upgrades/em

<file\_name> <percentage\_loaded> <file\_size>

<loading\_rate> <time>

or, before the first CICM-EM node is upgraded:

Uploading <file\_name> to

/D:/Centrexip/support/firmware/elementmgr\_MRs

<file\_name> <percentage\_loaded> <file\_size>

<loading\_rate> <time>

- 15** Repeat [step 14](#) for each EM\_ MR upgrade file in the directory.
- 16** Confirm all EM\_ MR upgrade files are present:

**ls -al**



At this directory, obsolete CICM-EM MR .cab or .upg files from previous releases should be removed or archived elsewhere to ensure there is enough space for the new software.

- 17** Go to the directory on the CICM-EM where the CICM node (gateway) MR upgrade files are to be copied:

| <b>If the<br/>CICM_EM</b> | <b>Do</b>                                            |
|---------------------------|------------------------------------------------------|
| is at SN08                | <b>cd /D:/Centrexip/support/firmware/gateway_MRs</b> |
| is at SN09 (or later)     | <b>cd /D:/Centrexip/support/upgrades/gw</b>          |

**Note:** The command prompt for SFTP re-appears:

```
sftp>
```

- 18** Confirm you have reached the directory:

**pwd**

The directory is echoed:

```
Remote working directory:
/D:/Centrexip/support/upgrades/gw
```

- 19** Copy each GW\_ MR upgrade file to the CICM node directory */upgrades/gw*.

**put GW\_<release>.upg**

The progression of copying is indicated by:

```
Uploading <file_name> to
/D:/Centrexip/support/upgrades/gw
<file_name> <percentage_loaded> <file_size>
<loading_rate> <time>
```

- 20** Repeat [step 19](#) for each GW\_ MR upgrade file in the directory.

- 21** Confirm all GW\_ MR upgrade files are present:

**ls -al**

At this directory, obsolete gateway .cab or .upg files from previous upgrades should be removed or archived elsewhere to ensure there is enough space for the new software.

- 22** Go to the directory on the CICM-EM where the EM patch files are to be copied:

**cd /D:/Centrexip/support/patches/em**

The command prompt for SFTP re-appears:

```
sftp>
```

- 23** Confirm you have reached the directory:  
**pwd**  
The directory is echoed:  
Remote working directory:  
/D:/Centrexip/support/patches/em
- 24** Copy each EM\_ patch file to the CICM-EM directory  
/patches/em:  
**put EM\_<release>.pat**  
The progression of copying is indicated by:  
Uploading <file\_name> to  
/D:/Centrexip/support/patches/em  
<file\_name> <percentage\_loaded> <file\_size>  
<loading\_rate> <time>
- 25** Repeat [step 24](#) for each EM\_ patch file in the directory.
- 26** Confirm all EM\_ patch files are present:  
**ls -al**  
At this directory, obsolete EM.pat files from previous upgrades should be removed or archived elsewhere to ensure there is enough space for the new software.
- 27** Go to the directory on the CICM-EM where the CICM node patch files are to be copied:  
**cd /D:/Centrexip/support/patches/gw**  
The command prompt for SFTP re-appears:  
sftp>
- 28** Confirm you have reached the directory:  
**pwd**  
The directory is echoed:  
Remote working directory:  
/D:/Centrexip/support/patches/gw
- 29** Copy each GW\_ patch file to the CICM-EM directory  
/patches/gw:  
**put GW\_<release>.pat**  
The progression of copying is indicated by:  
Uploading <file\_name> to  
/D:/Centrexip/support/patches/gw

```
<file_name> <percentage_loaded> <file_size>
<loading_rate> <time>
```

- 30 Repeat [step 24](#) for each GW\_ patch file in the directory.
- 31 Confirm all GW\_ patch files are present:  
**ls -al**  
At this directory, obsolete gateway .pat files from previous upgrades should be removed or archived elsewhere to ensure there is enough space for the new software.
- 32 Repeat the copying onto the second CICM-EM, starting from [step 7](#). Use the static IP address of the second CICM-EM.
- 33 Repeat the copying of each additional CD with required files, starting from [step 1](#). Repeat until all the files are copied.
- 34 Close the FTP session:  
**quit**  
or  
**bye**
- 35 Release the CD from the server:  
**cd /**  
**eject cdrom**
- 36 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Copying upgrade or patch files to and from your PC

Copy the upgrade or patch files onto a remote PC and then onto a redundant pair of CICM-EMs to make the files available for upgrading the CICM-EMs and their CICM nodes. Refer to the SN08 version of the *Upgrading CICM*, NN10230-461 for information on the upgrade paths seen for the CICM-EM in SN08.

### Prerequisites to copying upgrade or patch files to and from your PC

Address the prerequisites before starting the procedure.

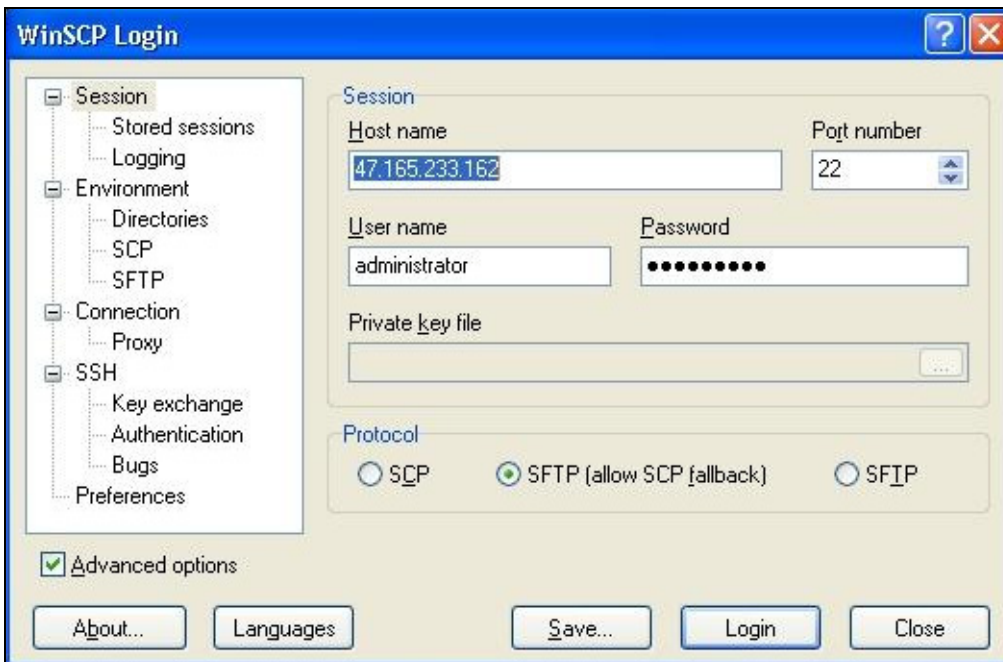
- You must follow the Prerequisites and sequence of procedures identified in [CICM-EM and CICM node preparation for an upgrade or patch](#).
- You must know the unique Administration IP addresses of each CICM-EM of the pair.
- Both CICM-EMs must be in-service to enable accepting the files.

- You must use a secured FTP (SFTP) session to copy files to or from a CICM-EM (but not from a CICM node to its EM). You are responsible for providing your own software for an SFTP, for example, WinSCP.
- The specifications of hardware and software for your personal computer (PC) must comply with the criteria identified in *CICM Basics*, NN10044-111.
- A PC is remote in context of not necessarily being located on the same site as the SAM16 or SAM21 hardware that runs the CICM software.
- You need a working knowledge of secure FTP and Microsoft Windows. The procedure uses WinSCP software as an example of a secure FTP.

### **Procedure steps to copying upgrade or patch files to and from your PC**

#### ***At your remote PC***

- 1 Create folders on your PC to copy the source files into. For simpler file management create separate folders for CICM-EMs and CICM nodes. Within those folders, the file names distinguish which files are for CICM-EMs or CICM nodes. Do not rename the files.
- 2 Access the source files of the upgrade files by doing one of the following:
  - inserting the Nortel Networks CD of upgrade files into your PC's CD-ROM and opening the folders
  - for patches only, accessing the website [www.nortel.com](http://www.nortel.com) on the Internet according to the procedure [Getting CICM patch files from the Internet](#)
- 3 With a CD, insert it into your PC's CD-ROM drive and copy each file from the CD into the appropriate folder on your PC.  
Without a CD, go to the next step.
- 4 Start a Secure FTP (SFTP) session on the CICM-EM that is to receive copies of the files. For example, on your PC Desktop double-click the icon for the WinSCP application.



- 5 Navigate from the remote directory to the directory on the CICM-EM where the upgrade, or (for SN09 and later) patch, files are to be copied.

**If the CICM-EM is at SN08:**

The directories for the CICM-EM upgrade files are:

*d:\centrexip\support\firmware\elementmgr\_MRs*

The directories for the CICM node upgrade or patch files are:

*d:\centrexip\support\firmware\gateway\_MRs*

**If the CICM-EM is at SN09:**

The directories for the CICM-EM upgrade or patch files are:

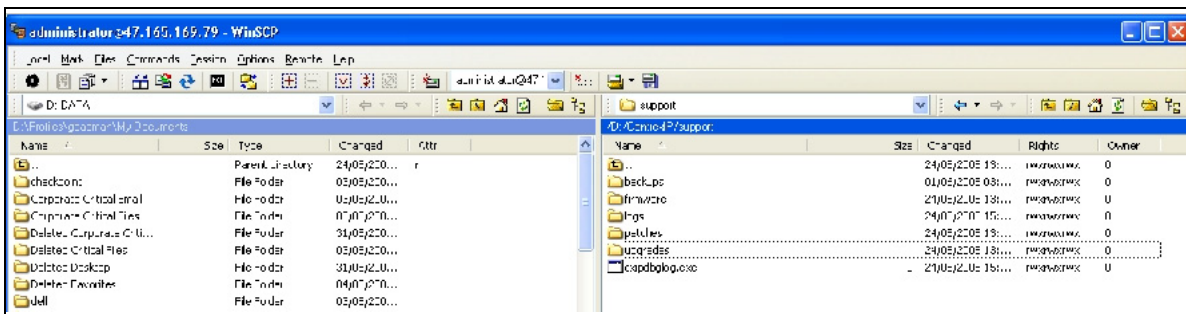
*d:\centrexip\support\upgrades\em*

*d:\centrexip\support\patches\em*

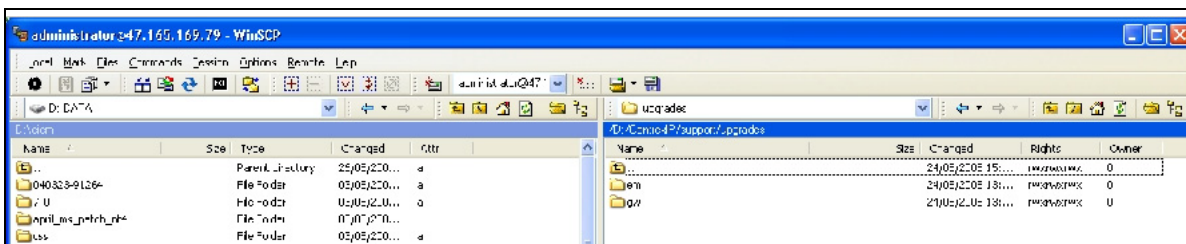
The directories for the CICM node upgrade or patch files are:

*d:\centrexip\support\upgrades\gw*

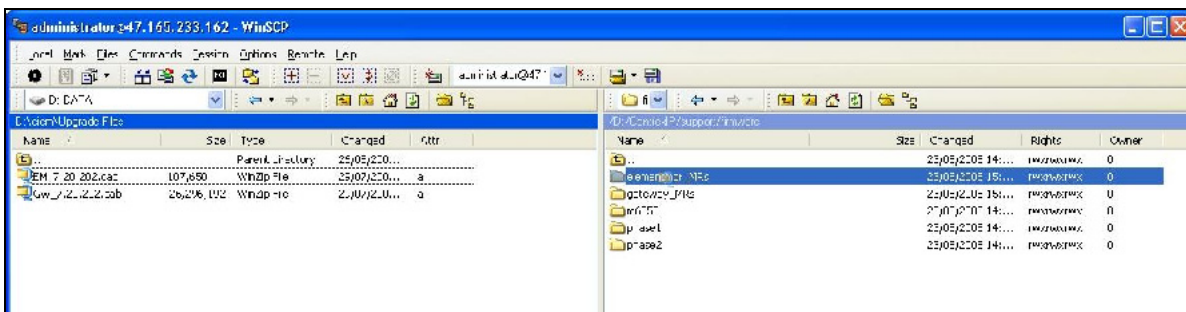
*d:\centrexip\support\patches\gw*



6 Open a local directory.

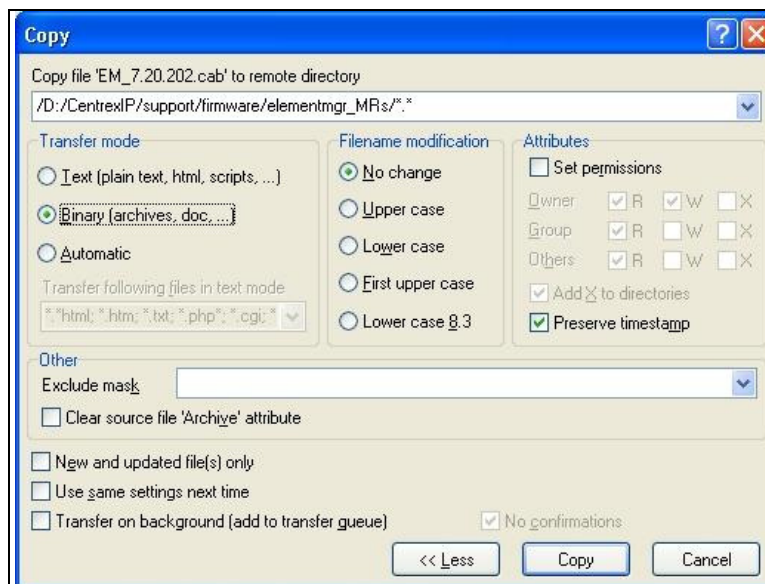


7 Drag each file from the local PC directory to the appropriate CICM-EM or CICM node remote directory.

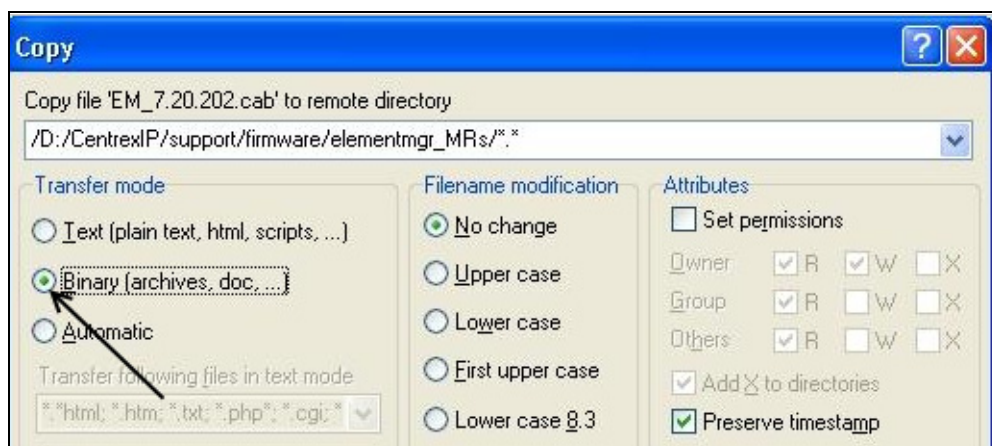


The box *Copy* appears.

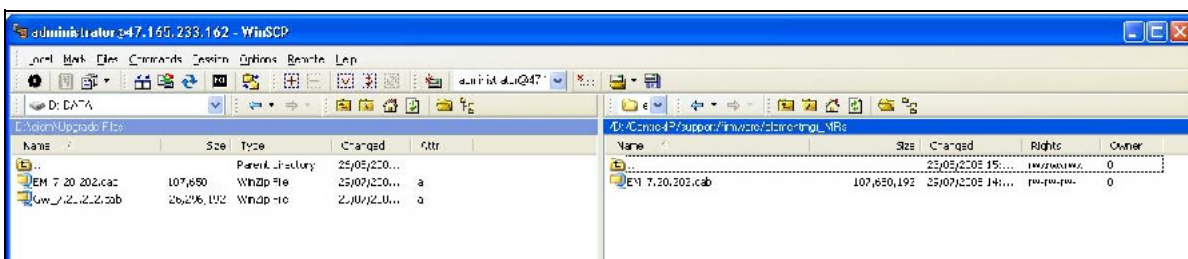




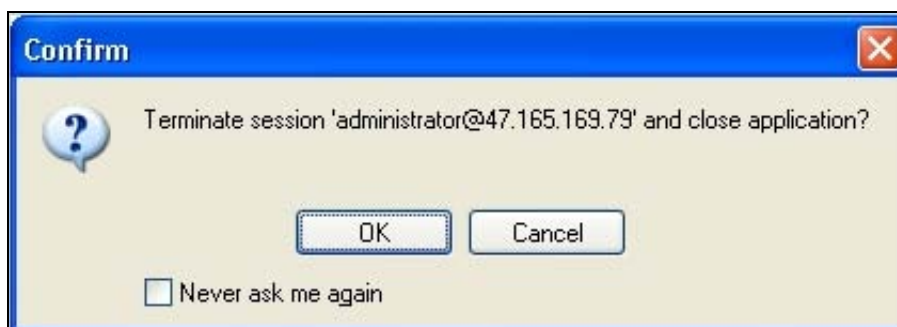
- 8 Since the upgrade and patch files are executable files, ensure that the transfer mode is set to binary.



- 9 Press enter to copy the files.
- 10 Refresh the directory display and confirm that all files have been copied.



- 11 Repeat from [step 5](#) to [step 10](#) to copy all upgrade and patch files to each appropriate CICM-EM directory.
- 12 When all upgrades and patches files are copied to the first CICM-EM, repeat [step 11](#) for the mate CICM-EM.
- 13 Quit the SFTP session. For WinSCP, click the upper right-hand X of the window and click **OK** of the confirmation prompt.



- 14 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Getting CICM patch files from the Internet

Download the patch files for CICM-EMs or CICM nodes from the Internet to your PC.

### Prerequisites to getting CICM upgrade files from the Internet

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in [CICM-EM and CICM node preparation for an upgrade or patch](#).
- You must have access to the Internet. Nortel Networks recommends you use a high-speed service provider to minimize file corruptions from prolonged downloads.
- You must know your userid and password to log into the Internet website nortel.com.
- The PC to interface the Internet must be the same PC that interfaces with the CICM-EMs. This facilitates simpler file transfers from the PC to the EMs.

### Procedure steps to getting CICM upgrade files from the Internet

#### *At your PC*

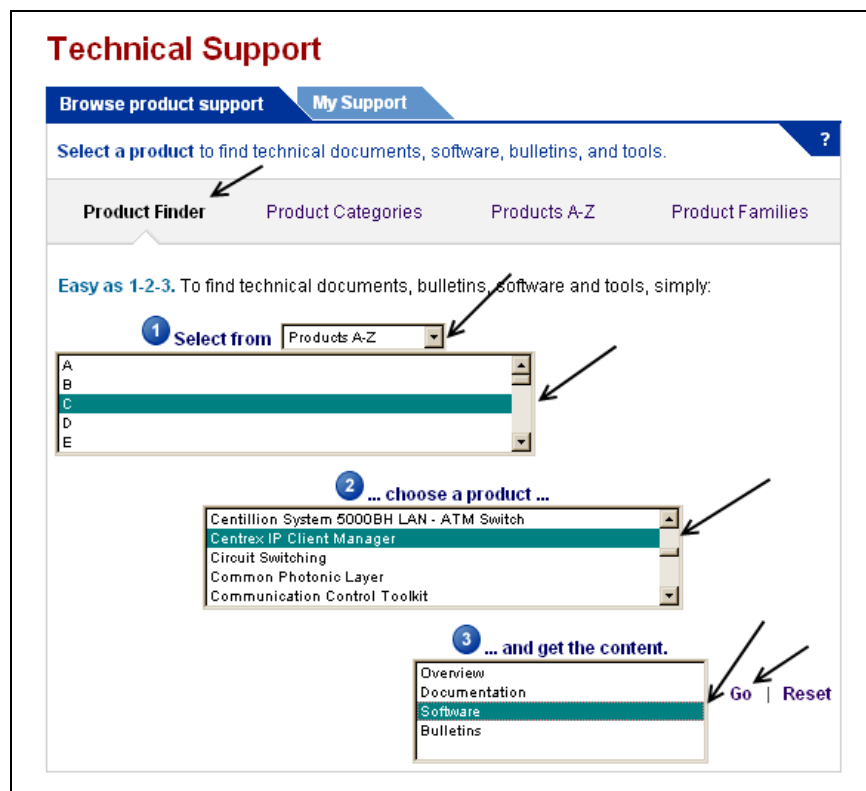
- 1 Access the Internet from your PC.



- 2 Access the Internet website where the upgrade files are stored:  
**https://www.nortel.com**

### **At the website**

- 3 From the pick-list under *SUPPORT & TRAINING*, select *SOFTWARE DOWNLOADS*.
- 4 At the window *Technical Support*, select the tab *Product Finder*. It may already be showing by default.



- 5 At 1 *Select from...*, from the pick-list select *Products A-Z*, then select *C* in the window below it.
- 6 At 2 *...choose a product...*, from the pick-list select *Centrex IP Client Manager*.
- 7 At 3 *...and get the content*, select *Software* and click **Go**.
- 8 At the window *Centrex IP Client Manager*, under *Title* click the version of software you want to download.

## Centrex IP Client Manager

Overview
Documentation
Software
Bulletins
Tools

Results: 1-4 of 4 Page: 1 of 1

| Title                                                 | Software Type | Release  | Format | Status   | Date        |
|-------------------------------------------------------|---------------|----------|--------|----------|-------------|
| CICM m6350 SoftClient TAPI Service Provider (8.0 MR2) | exe           | 8.0      | exe    | Released | 04 Aug 2005 |
| CICM m6350 SoftClient Branding Kit (8.0 MR2)          | exe           | 8.0      | exe    | Released | 04 Aug 2005 |
| CICM m6350 SoftClient (8.0 MR2)                       | exe           | 8.0      | exe    | Released | 04 Aug 2005 |
| accessControl.xml                                     | config file   | 7.11.184 | other  | Released | 17 Sep 2004 |

- 9** At the window *Software*, notice the indicated file size. Ensure that there is enough space on your PC to accept the downloads.

## Software

**Detail Information**

This area provides you with details regarding your software selection. Please note, you may need to right click on the and use the 'Save target as ...' option on your browser.

**Software Title:** CICM m6350 SoftClient (8.0 MR2)

**Software Type:** exe

**Release:** 8.0

**Associated Products:** [Centrex IP Client Manager](#)

**File Download:** [CICM m6350 SoftClient \(8.0 MR2\)](#) 7 MB (exe) English

- 10** At the window *Software*, beside *File Download* click the software load name.
- 11** Repeat [step 10](#) for each patch file to be downloaded.
- 12** When the downloading is complete, use the MD5 checksum to verify the file is complete and uncorrupted from the transfer.
- 13** Move the downloaded files from your PC desktop into folders. Do not rename the files.
- 14** This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Accessing a CICM-EM through the IEMS

Access a CICM-EM through the Integrated Element Management System (IEMS) to upgrade or patch the CICM-EM or CICM nodes or

both with a maintenance release (MR), a product release, or one or more patches.

### **Prerequisites to accessing a CICM-EM through the IEMS**

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in [CICM-EM and CICM node preparation for an upgrade or patch](#).
- To access IEMS, you must know the IP address of the IEMS server and be able to access it through a web browser.
- You need to know the administrator userid and password to log into the CICM-EM from IEMS. Otherwise your access is determined by whatever authentication structure you have configured.

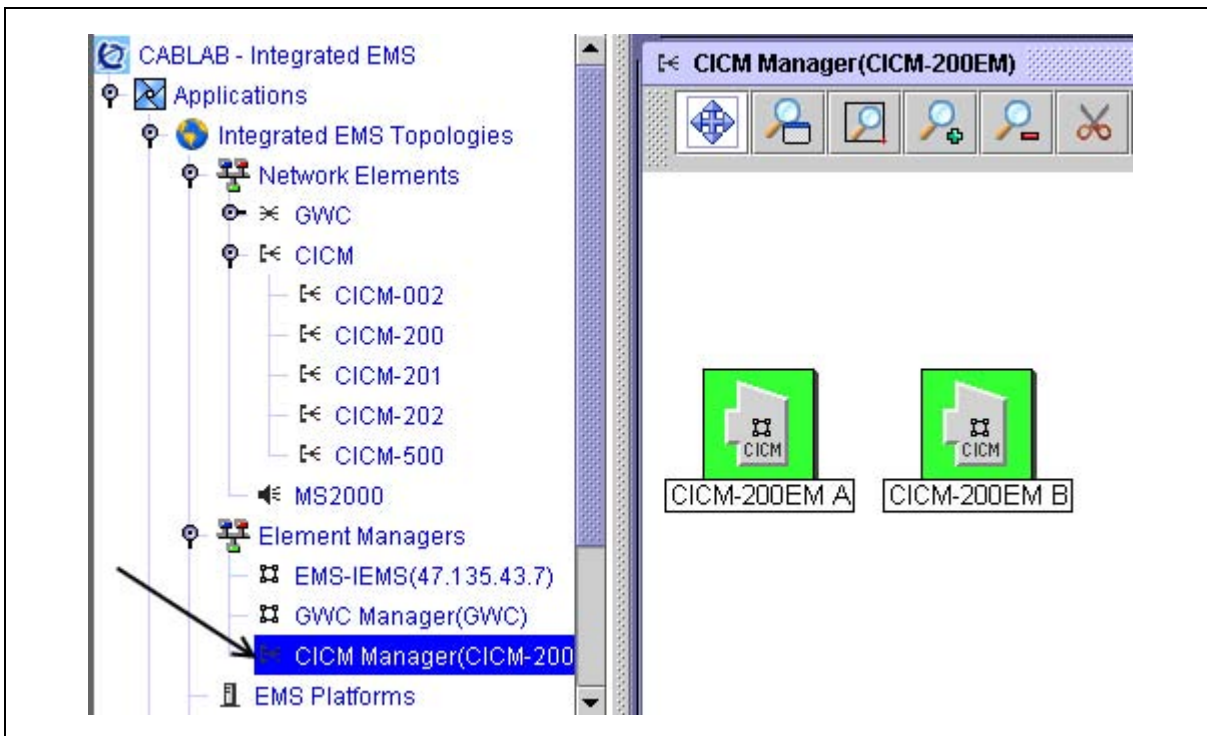
### **Procedure steps to accessing a CICM-EM through the IEMS**

#### ***At a web browser***

- 1 Access the IEMS by entering the command:  
`https://<iems_ip_address>:9091/LoginPage.do`
- 2 Once connected, click option Web Start Client (which uses JAVA rather than HTML).  
  
Unless already installed, you must install the version of JAVA that is provided at the Web Start Client link.

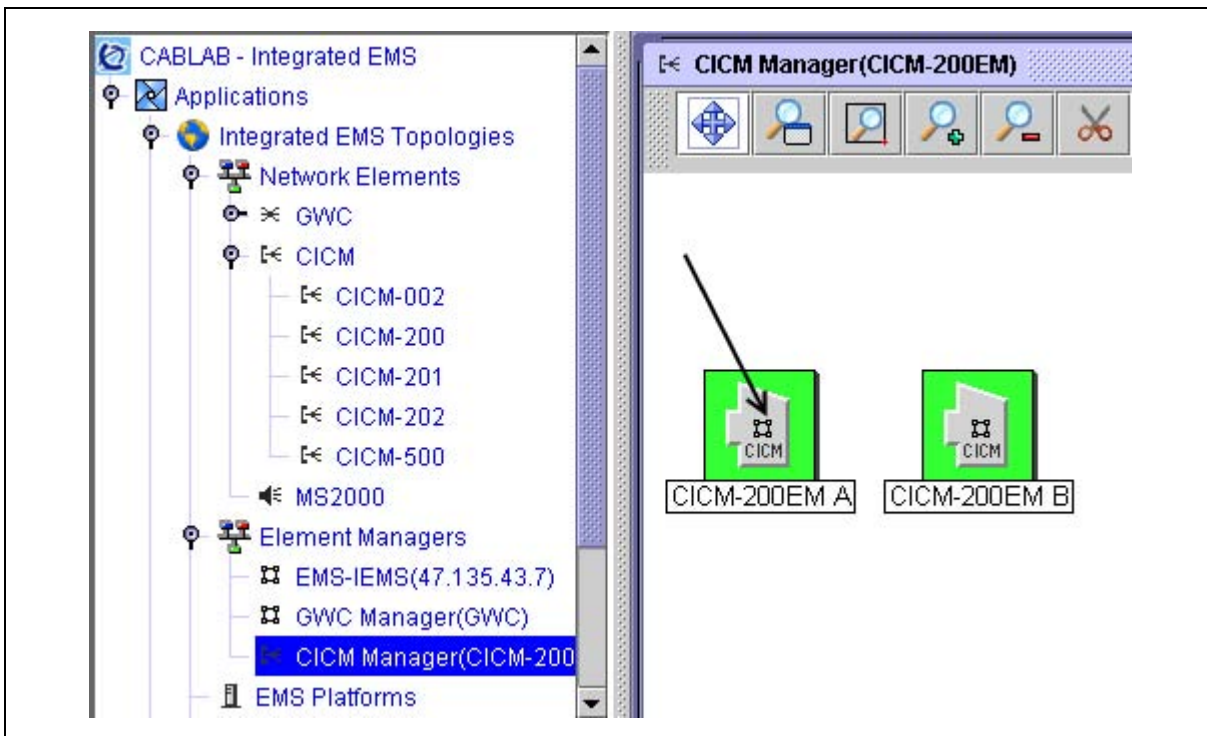
#### ***At the IEMS GUI***

- 3 At the IEMS menu of components, locate the item for the CICM-EM to undergo an upgrade. Ensure that the static IP address of the CICM-EM is for the one to be upgraded.



- 4 Right click the icon of the CICM-EM to undergo an upgrade, and select **Launch CICM Manager**.

A prompt occurs for the userid and password.



- 5 Enter the CICM-EM administrator userid and password.  
The CICM-EM web page opens.
- 6 Ensure that the node you selected is in-service.
- 7 To upgrade a pair of CICM-EM or CICM nodes, follow the other procedures in the task flow.
- 8 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

### Accessing a CICM-EM through a web browser

Upgrading the CICM element manager (CICM-EM) and gateways requires accessing the element manager through one of the following:

- web browser
- Integrated Element Management System (IEMS)

This procedure describes the process to access a CICM-EM through a web browser and requires the following information:

- the CICM-EM administration IP address
- the CICM-EM administration user id and password

## **Accessing a CICM-EM through a web browser**

### ***At the web browser***

- 1** Access the CICM-EM by entering:  
**`https://<unique_admin_ip_address_of_cicmem>/centrexip`**
- 2** At the userid and password prompt enter:  
**`<cicm_em_administrator_id>`**  
**`<cicm_em_administrator_pwd>`**
- 3** When the CICM-EM web page opens, ensure the selected node is in-service.
- 4** To upgrade a CICM-EM gateway, follow the appropriate procedures in the task flow.
- 5** This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Verifying the software version of the C1CM-EM and C1CM nodes

Verify the software version of a C1CM-EM and its C1CM nodes.

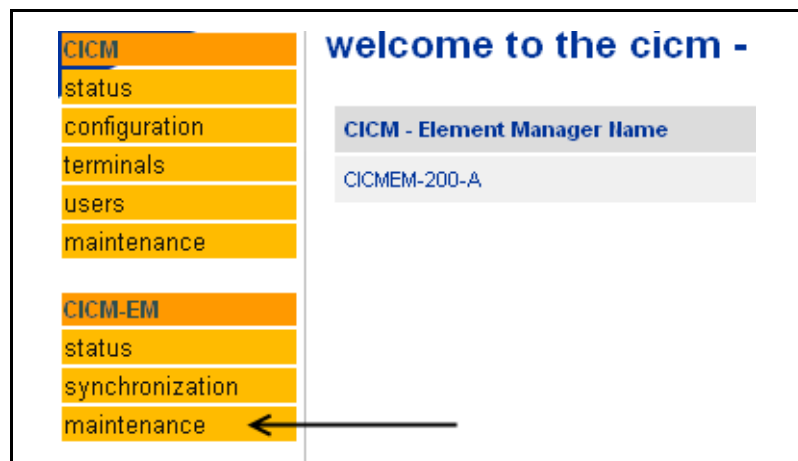
### Prerequisites to verifying the software version of the C1CM-EM and C1CM nodes

This procedure requires administrator userids and passwords to login to the C1CM-EM.

### Procedure steps to verifying the software version of the C1CM-EM and C1CM nodes

#### *At the page C1CM-EM home*

- 1 Click **maintenance** in the menu *C1CM-EM*.



#### *At the page maintenance status (c1cmem-*nnn*)*

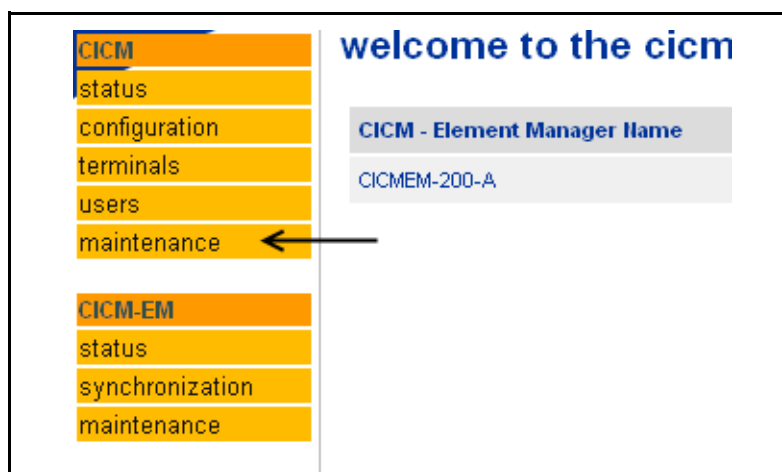
- 2 View the versions of each C1CM-EM beside *Version* under the status of each Node.

| Node A (CICMEM-200-A) ? |                                              |
|-------------------------|----------------------------------------------|
| Node status             | slave                                        |
| Node Maintenance status | system idle<br>(current reboot count: 0)     |
| Version                 | CICM-EM 8.0 Base Release<br>(Build 8.10.183) |
| Node B (CICMEM-200-B) ? |                                              |
| Node status             | master                                       |
| Node Maintenance status | system idle<br>(current reboot count: 0)     |
| Version                 | CICM-EM 8.0 Base Release<br>(Build 8.10.183) |

If the versions are identical, proceed with the upgrade.

If the versions are different, you must match them by applying whatever product release, MR, or patch is required. Both nodes must be in service and running the same version of software before an upgrade is attempted.

- 3 Compare the CICM nodes versions by clicking **maintenance** in the menu *CICM*.





- 4 From the pick-list under **perform maintenance on**, select the CICM to view.

When you select the node other than the one that is showing, the page *maintenance status* automatically opens.

When the displayed *Node* is already the one you want, click **perform maintenance on**.

**cicm maintenance**

- Perform status changes on the gateway service
- Switch activity of a CICM running in dual node
- View the maintenance release level on a CICM.
- Check the upgrade status of the CICM
- Download and apply a maintenance release to the CICM in one atomic action



The page *maintenance status (cicm-nnn)* opens.

**CICM**

status

configuration

terminals

users

**maintenance**

### maintenance status (cicm-002)

| Node A (47.135.43.18) ?   |                                           |
|---------------------------|-------------------------------------------|
| Status                    | master ( running )                        |
| Node Maintenance status   | system idle<br>(current reboot count: 0)  |
| Version                   | CICM 8.0 Base Release<br>(Build 8.10.183) |
| VMG Status                | active ( in service )                     |
| Active Half Calls         | 0 (total calls=418)                       |
| Terminal Status           | active                                    |
| Number of logged in users | 27 (total logins=27)                      |
| Active Terminals          | 4                                         |
| Terminal Recovery Status  | n/a                                       |

| Node B (47.135.43.19) ?   |                                           |
|---------------------------|-------------------------------------------|
| Status                    | slave ( running )                         |
| Node Maintenance status   | system idle<br>(current reboot count: 0)  |
| Version                   | CICM 8.0 Base Release<br>(Build 8.10.183) |
| VMG Status                | inactive ( in sync )                      |
| Active Half Calls         | n/a                                       |
| Terminal Status           | inactive ( in sync )                      |
| Number of logged in users | n/a                                       |
| Active Terminals          | n/a                                       |
| Terminal Recovery Status  | n/a                                       |

**▶ apply maintenance release**

Node Node A (47.135.43.18)

Maintenance Release GW\_UPGRADE\_8.10.183.cab

**Note:** Maintenance releases should be securely transferred to "D:\Centrex\IPsupport\firmware\gateway\_MRs" on the master Element Manager Node

---

**▶ node A service control**

Action Stop

---

**▶ node B service control**

Action Stop

---

**▶ switch activity**

---

**▶ reset counter**

Node Node A

Reset Counter Current Reboot Count

---

**▶ start auto refresh**

---

**▶ refresh now**

---

**▶ system status**

- 5 The software version for each CICM node is shown beside Version of the Node A and B status windows.

The software of the CICM-EM and CICM nodes should all be the same version.

- 6 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

### **Software upgrades to Nortel Networks IP Phone sets**

The Nortel Networks IP Phone sets that are connected to the CICM nodes receive their software upgrades over the IP network. A software upgrade for a phone set is referred to as a firmware upgrade. For details about handling phone set upgrades, see [Upgrading firmware on IP phone sets on page 2164](#).

---

## Upgrading CICM software

---

This section provides the task flow and procedures to upgrade the software of a pair of redundant Centrex IP Client Manager (CICM) element managers (CICM-EMs) and their pairs of redundant CICM nodes.

An SN09FF software load was not developed for the CICM component. The most recent SN09 node and element manager maintenance release (CICM0090 and CICE0090) brings the CICM software to an SN09FF baseline.

Upgrading from SN08 requires the following two upgrades:

1. SN08 (MR3 or higher) to SN09 MR1
2. SN09 MR1 to SN09 MR3

Upgrading from SN09 requires one of the following upgrades (depending on the release before beginning the upgrade):

- SN09 MR1 to SN09 MR3
- SN09 MR2 to SN09 MR3

### CICM-EM and CICM node upgrades

Upgrade a pair of Centrex IP Client Manager (CICM) element managers (CICM-EM) and their pairs of CICM nodes by doing a series of procedures in a task flow. The upgrade is divided into:

- [Prerequisites to the task flow of CICM-EM and CICM node upgrades](#)
- [Task flow of CICM-EM and CICM node preparation](#)

#### Prerequisites to the task flow of CICM-EM and CICM node upgrades

Before following the task flow, ensure that you have addressed these requirements.

- If patch P1, P2, or P3 has been applied to 9.0 MR1 or 9.0 MR2 then the following must be applied before performing the maintenance release upgrades listed below:
  - 9.0 MR1 P4 - if upgrading from 9.0 MR1 to 9.0 MR3
  - 9.0 MR2 P4 - if upgrading from 9.0 MR2 to 9.0 MR3
- The CICM-EM and CICM nodes must be in service without faults.
- Upgrading with an MR or product release is a manual operation. Start an upgrade during a period of lowest traffic for the CICM-EMs and CICM nodes.

- The pair of CICM-EM nodes must always be upgraded before the pair of CICM nodes for an MR or a product release, but not a patch.
- Once an upgrade has been started, do not attempt any software configuration changes to any node until each node-pair is confirmed to be upgraded and fully operational.

**CAUTION****Risk of service prevention**

Before starting the upgrades task, read each procedure to determine what data you will need for entries, especially the preboot and preboot upgrade IP addresses. It is critical to have all the data readily available before starting the upgrade.

## Upgrading a CICM-EM with an MR or product release

Upgrade a CICM element manager (CICM-EM) of a redundant pair with a maintenance release (MR) or a product release.

### Prerequisites to upgrading the CICM-EM with an MR or a product release

Prerequisites to upgrading the CICM-EM with an MR or a product release include the following.

- Follow the Prerequisites and sequence of procedures identified earlier in this document. The first occurrence of a procedure is for the slave CICM-EM, and the second occurrence is for the master after it becomes the slave.
- The CICM-EM node-pair can support CICM node-pairs running either the same version or one previous version temporarily during the upgrade (for example, the EMs running 9.0 while a pair of nodes run 8.0).
- You need a PC or equivalent to remotely access the CICM-EM web pages. Upgrading is not done locally to a CICM-EM.
- Both CICM-EMs must be in service before attempting the upgrade.
- This procedure requires web browser access to the CICM-EM Node A static IP address during the Node A upgrade and the CICM-EM floating IP address for the Node B upgrade.
- You must know the administrator userid and password to log into the CICM-EM for this upgrade.
- When upgrading to SN09 the node's status may not properly display properly on the CICM-EM and "Error getting version" appears on the Maintenance Page. Should this occur, the CICM-EM as a whole will remain in service as the other node will have assumed the role of Master. Also, the error condition of the newly upgraded CICM-EM node can be cleared with a node restart, which does not affect any service provided by the CICM since the CICM-EM is not a Call Processing node. To perform the node restart:
  - Telnet to the affected node (you may require a secure telnet session).
  - Issue the following command on the command line, once you have logged into the affected node: "shutdown /l /r /t:00".

Review debug logs to determine why the failure occurred.

- A failed CICM-EM upgrade is indicated by one of the following.
  - The upgrade aborts and the system stays at the pre-upgrade idle state.
  - The upgraded CICM-EM hangs and remains out of service.

Review debug logs to determine why the failure occurred.



#### **CAUTION**

##### **Risk of service prevention**

Before upgrading the first CICM-EM of a redundant pair to a different version of software, both must be running the same software version, including the same MR incremental version. For example, version 8.10.001 is the same release as 8.10.200 but not the same version.

#### **ATTENTION**

This procedure requires:

First connecting the web browser to the CICM-EM Node A static IP address.

Second, reconnecting the web browser to the CICM-EM floating IP address .

### **Procedure steps to upgrading the CICM-EM with an MR or a product release**

#### ***At the PC desktop for remote access to the CICM-EM***

- 1 Access the CICM-EM Node A from a web interface using the static IP address:

**`https://<cicmem_nodeA_static_ip_address>/centrexip`**

#### ***At the page maintenance status (cicmem-nnn)***

- 2 Identify from the display Node status whether Node A or B is the slave CICM-EM.

| <b>If Node A is</b> | <b>Do</b>               |
|---------------------|-------------------------|
| the slave node      | <a href="#">step 5</a>  |
| the master node     | <a href="#">step 10</a> |

- 3 Reconnect to the CICM-EM from a web interface using the floating static IP address:

**https://<cicmem\_floating\_ip\_address>/centrexip**

- 4

**ATTENTION**

Node A was first upgraded as the slave through the static IP address, therefore Node B should be the Master Node at this point of the procedure.

Go to [step 10](#) to restart the CICM-EM Node B and make it the slave node.

- 5 If the CICM-EM is at SN08:  
From the pick-list of Node under **apply maintenance release**, select the slave node to upgrade.

If the CICM-EM is at SN09:

From the pick-list of Node under **maintenance release management**, select the slave node to upgrade.

When the displayed Node is already selected, click **maintenance release management** to open the page.

- 6 From the pick-list under **apply maintenance release**, select the appropriate file for the MR or product release.

**Note:** Select the “EM\_<version>.cab” file for a product release upgrade.

After selecting the appropriate MR or product release filename, click **apply maintenance release**.

A prompt for confirmation appears for either an MR or a product release upgrade.

When *No Files* is shown, the upgrades files have not been copied to the CICM-EM or were copied to the wrong directory. You have not followed the task flow.

- 7 Click **confirm maintenance release application**.

***At the page maintenance release management (cicmem-nnn)***

- 8 Wait 10 seconds then track the progress of the upgrade to the slave EM by clicking **start auto refresh**.

The refresh button toggles to show **stop auto refresh**.

- 9 Wait until the CICM-EM being upgraded shows the following combination:

- the *Node Maintenance status* is *system idle*
- the Version is *w.xx.yyy* of the target upgrade version, for example, 9.10.191

If the EM is not in service and idle within 30 minutes, abort the upgrade. Review the debug logs to determine the cause of failure. Refer to the task flow in [Task flow of CICM-EM and CICM node preparation](#) for the procedures to roll back from an upgrade.

| If this was | Do                      |
|-------------|-------------------------|
| Node A      | <a href="#">step 3</a>  |
| Node B      | <a href="#">step 13</a> |

**At the page status (cicmem-nnn)**

- 10 Restart the CICM-EM node to make it the slave node. From the pick-list under **Restart CICM EM**, select the master node.

Click **Restart CICM EM**.

The page changes to show the confirmation prompt.

11

**ATTENTION**

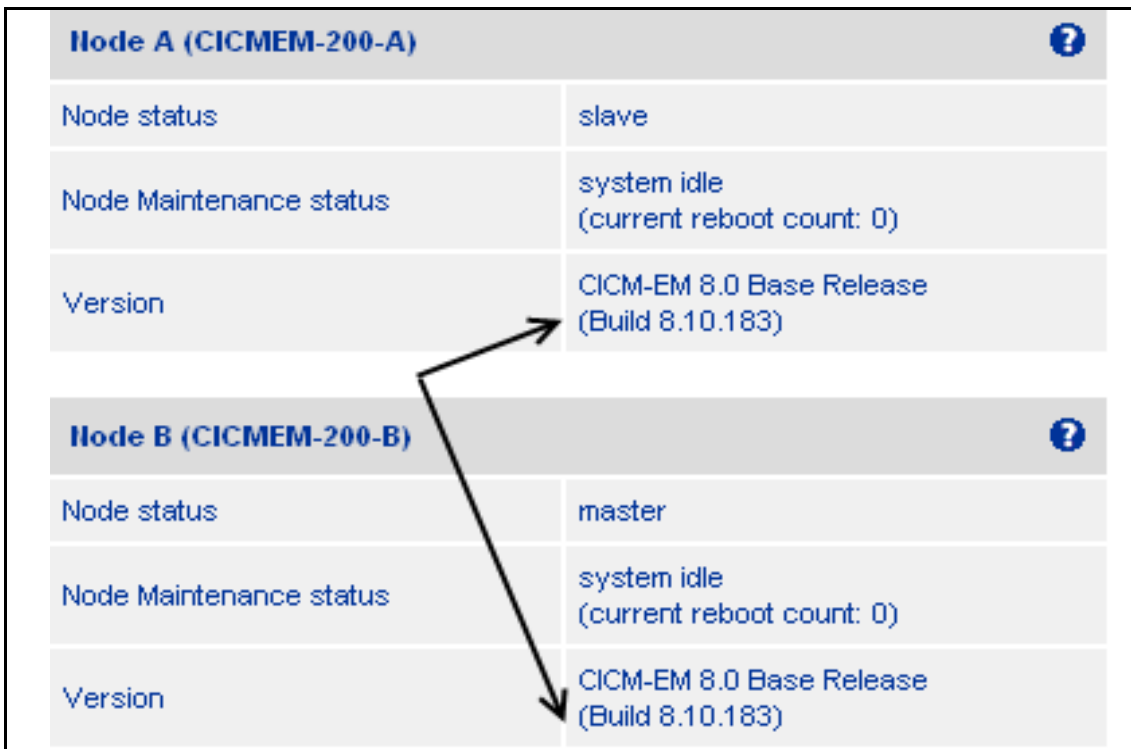
When switching activity the user interface may not be accessible for a brief period while the EM webpage access switches to the other master node.

Click **Confirm restart of CICM-EM**.

Monitor the restart progress by clicking **maintenance** in the CICM-EM menu.

- 12 The CICM-EM node to upgrade is now the slave node, return to [step 5](#).
- 13 When both EMs of a redundant pair are in service and running with identical versions of software (for example, 9.10.191), the upgrade is complete.





| Node A (CICMEM-200-A) ? |                                              |
|-------------------------|----------------------------------------------|
| Node status             | slave                                        |
| Node Maintenance status | system idle<br>(current reboot count: 0)     |
| Version                 | CICM-EM 8.0 Base Release<br>(Build 8.10.183) |

| Node B (CICMEM-200-B) ? |                                              |
|-------------------------|----------------------------------------------|
| Node status             | master                                       |
| Node Maintenance status | system idle<br>(current reboot count: 0)     |
| Version                 | CICM-EM 8.0 Base Release<br>(Build 8.10.183) |

#### ***At the IEMS interface***

- 14 Edit the object properties in the IEMS for the CICM network elements you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the field *Device Version*:

- [Editing and viewing object properties using Java Web Start Client](#)
- [Editing and viewing object properties using Web Client](#)

With the Java Web Client, CICM uses v2c for the *Version* in the *SNMP Details* page.

- 15 This procedure is complete with CICM-EM Node A as the Master Node. Return to the task flow or procedure that sent you to this procedure.

### **Upgrading a CICM node with a product release**

Upgrade the CICM slave node with a product release (MR0) as part of upgrading all CICM components in a network.

**Prerequisites to upgrading a CICM node with a product release**

Address the prerequisites before starting the procedure.

- Both CICM nodes must be in service before attempting the upgrade.
- When upgrading the CICM gateway nodes, CICM-EM Node A must be the master.
- You must know the administrator userid and password to log into the CICM-EM from a remote PC for this upgrade.
- During the upgrade to a CICM node, the node restarts several times.
- A CICM node fails an upgrade when it does not return to service and the version of the upgrade does not appear beside the Version status. Before re-attempting to upgrade the node, you must determine from the debug logs why it failed. If the upgrade was aborted, it will return to a pre-upgrade idle state with the previous software. If the upgrade was started and failed, you will need to roll back from the upgrade to restore service.

**Procedure steps to upgrading a CICM node with a product release*****At the page CICM home through the web interface***

- 1 When upgrading the second CICM node of a redundant pair, start this procedure from [step 18](#). Do not repeat the procedure a third time for the same upgrade to the same pair of nodes.

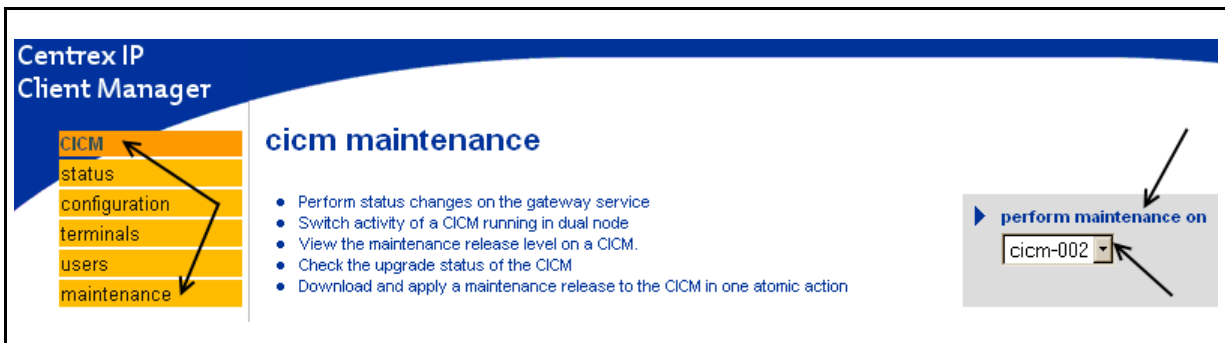
***At the PC desktop for remote access to the CICM node***

- 2 Access the CICM node from your PC through a web interface by entering:

**`https://<floating_admin_ip_address>/centrexip`**

***At the page welcome to the CICM***

- 3 In the menu *CICM*, click **maintenance**.  
The page *cicm maintenance* opens.



### ***At the page cicm maintenance***

- 4 From the pick-list under **perform maintenance on**, select the CICM node to upgrade.

Select the Node, click **perform maintenance on**.

The page *maintenance status* opens.

- 5 From the display *Node Maintenance Status*, determine the statuses of Nodes A and B.

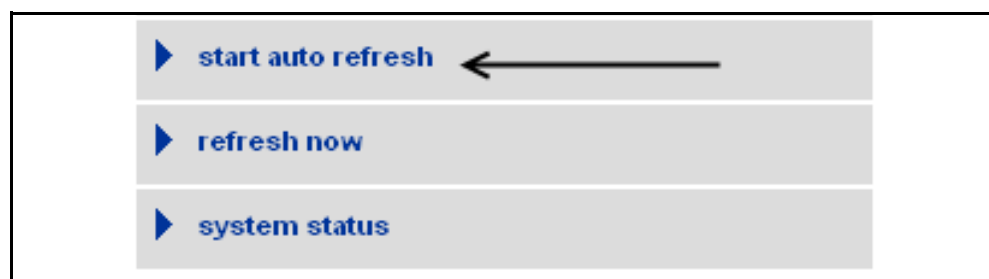
When upgrading Node A, Node B must be the master. When Node A is the master, do the procedure [Switching activity between CICM nodes](#) and return to this step.

When upgrading Node B, Node A must be the master. When Node B is the master, do the procedure [Switching activity between CICM nodes](#) and return to this step.

### ***At the page cicm maintenance status (cicm-nnn)***

- 6 Terminals are automatically transferred from the node being upgraded to its mate.
- 7 On the right menu, ensure that *start auto refresh* is showing, but do not click it.

If **stop auto refresh** is shown, click it to show **start auto refresh**.



- 8 From the pick-list of nodes under **maintenance release management**, select A or B, whichever is the slave.

When you select the node other than the one that is showing, the page *maintenance status* automatically opens.

When the displayed Node is the slave, click **maintenance release management** to open the page.

**maintenance status (cicm-002)**

| Node A (47.135.43.18) ? |                                                    |
|-------------------------|----------------------------------------------------|
| Status                  | slave ( running )                                  |
| Node Maintenance status | system idle<br>(current reboot count: 0)           |
| Version                 | CICM 9.0 Maintenance Release 1<br>(Build 9.10.186) |

▶ **maintenance release management**

Node

▶ **patch management**

Node

- 9 From the pick-list under **apply maintenance release**, select the appropriate upgrade file.

Select the appropriate product release filename, click **apply maintenance release management**.

**Note:** Select the “GW\_<release>.cab” file for a product release upgrade.

When *No Files* is shown, the upgrades files have not been copied to the CICM-EM or were copied to the wrong directory. You have not followed the task flow.

**maintenance release management (cicm-002)**

| Node A (47.135.43.18) ? |                            |
|-------------------------|----------------------------|
| Date                    | Event                      |
| 2005/08/04 10:37        | MR 0 applied successfully. |
| 2005/08/04 10:39        | MR 0 applied successfully. |
| 2005/08/08 22:30        | MR 1 applied successfully. |

▶ **apply maintenance release**

Maintenance Release

**Note:** Maintenance releases should be securely transferred to "D:\Centrex\IP\support\upgrades\gw" on the master Element Manager Node

- 10 Confirm applying the upgrade by clicking **confirm maintenance release application**.
- 11 Wait 10 seconds then track the progress of the upgrade to the slave CICM node by clicking **start auto refresh**.

- 12 Monitor Node A (or B) as it goes through a series of restarts as part of the upgrade process.

**Note:** During the CICM node restarts ignore error messages regarding contacting node while the node upgrades.

***At the page maintenance status (cicm-nnn)***

- 13 Monitor the first node's status until it is running as slave before proceeding.

**Note:** The floating address is always bound to the master node.

At this point you can choose to roll back the upgrade as described in [Rolling back from a CICM-EM or CICM node upgrade on page 2190](#) with no SWACT and no terminal transfers.

- 14 Do the procedure [Switching activity between CICM nodes](#).
- 15 Verify that the second node is working properly, which means:
- the *Node status* is *master*
  - the *Node Maintenance status* is *system idle*
  - the *Version* is *w.xx.yyy* of the target upgrade version, for example, 9.10.191

If the second node is not working properly, you must discontinue this procedure and follow the rollback path indicated in the task flow "CICM-EM or CICM node rollbacks".

At this point you can choose to roll back the upgrade as described in "CICM-EM or CICM node rollbacks" with a SWACT and no terminal transfers.

- 16 Terminals are automatically transferred from the node being upgraded to its mate.

17



**CAUTION**

**Risk of service prevention**

This is the last chance to roll back a node. Once an upgrade to the second node is attempted, a rollback then becomes a re-installation of the base software and upgrades for each node. Nortel Networks' GNPS must be requested to do the re-installation.

At this point you can choose to roll back the upgrade as described in [Rolling back from a CICM-EM or CICM node upgrade on page 2190](#).

- 18** When upgrading the second node and hosting no terminals, begin the upgrade repeating [step 8](#) to [step 12](#) and then do [Switching activity between CICM nodes](#).

**Note:** While the second node is starting, you can monitor its status. On start-up of the slave node, there is a delay before the load achieves a state of synchronization with the master. Only when this data synchronization is achieved is it possible to initiate a switch of activity.

- 19** Verify that the second node is working properly, which means:
- the *Node status* is *master*
  - the *Node Maintenance status* is *system idle*
  - the *Version* is *w.xx.yyy* of the target upgrade version, for example, 9.10.191

If the second node is not working properly, you must contact your next higher level of technical support to determine what to do next.

The command button for **terminal transfer** is no longer present.

#### **At the IEMS interface**

- 20** Edit the object properties in the IEMS for the CICM network elements you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the field *Device Version*:
- [Editing and viewing object properties using Java Web Start Client](#)
  - [Editing and viewing object properties using Web Client](#)

With the Java Web Client, CICM uses *v2c* for the *Version* in the *SNMP Details* page.

- 21** This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Upgrading a CICM node with an MR

Upgrade a CICM node with a maintenance release (MR) upgrade to CICM nodes already running the same software release (for example, both have release 9.10 MR1).

### Prerequisites to upgrading a CICM node with an MR

Address the prerequisites before starting the procedure.

- For MR zero (MR0), you must follow instead the procedure [Upgrading a CICM node with a product release](#).
- Both nodes of a CICM pair must operate with the same version of software prior to and after the upgrade. Operating within three MRs applies only during the transition of upgrading two nodes one at a time. The nodes are updated one at a time using the same procedure as indicated by the task flow.
- When upgrading the CICM gateway nodes, CICM-EM Node A must be the master.
- Always upgrade the slave node first and one node at a time.
- This procedure requires a switch of activity to upgrade the second node of a pair.
- Both CICM nodes must be in service for an upgrade to complete successfully.
- You must know the administrator userid and password to log into the CICM-EM for this upgrade.
- Terminals connected to the node being upgraded will maintain service while they locate the mate node.
- Active calls using resources on the node being upgraded are maintained.
- When the system detects an invalid software release or corrupt file for an upgrade, the CICM node does not apply the upgrade and will resume activity at its current software release.
- A CICM node fails an upgrade when it does not return to service and the version of the upgrade does not appear beside the Version status. Before re-attempting to upgrade the node, you must determine from the debug logs why it failed. If the upgrade was aborted, it will return to a pre-upgrade idle state with the previous software. If the upgrade was started and failed, you will need to roll back from the upgrade to restore service.

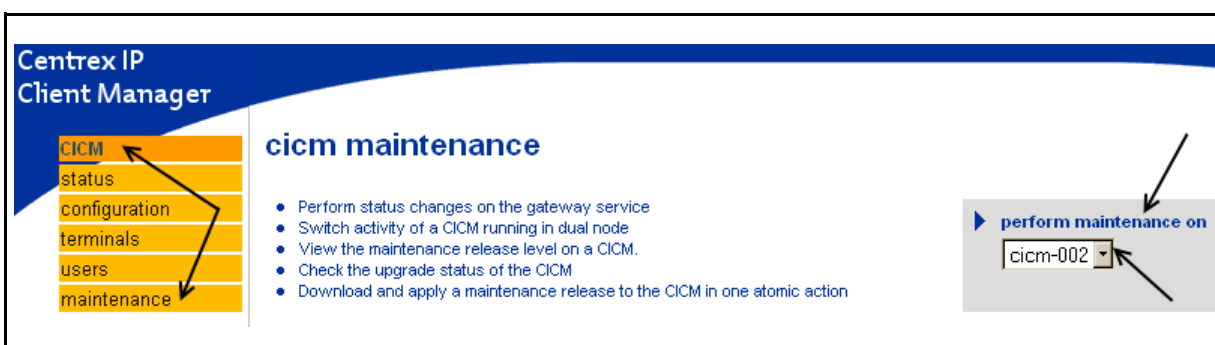
## Procedure steps to upgrading a CICM node with an MR

### ***At the PC desktop for remote access to the CICM***

- 1 Access the CICM node from your PC through a web interface by entering:  
**https://<floating\_admin\_ip\_address>/centrexip**

### ***At any CICM web page through the web interface***

- 2 In the menu *CICM*, click **maintenance**.  
The page *cicm maintenance* opens.



- 3 From the pick-list under **perform maintenance on**, select the CICM node to upgrade.  
When you select the node other than the one that is showing, the page *maintenance status* automatically opens.  
When the displayed Node is already the slave, click **perform maintenance on**.  
The page *maintenance status (cicm-nnn)* opens. The current software version for each node is displayed.  
The display *Node maintenance status* indicates the actions that are being performed on that node (for example, system idle, stopping the cxipboot service, and starting the cxipboot service). When the node is in service, it displays *system idle* or *system running*.



### maintenance status (cicm-002)

| Node A (47.135.43.18) <span style="float: right; color: #0056b3;">?</span> |                                                         |
|----------------------------------------------------------------------------|---------------------------------------------------------|
| Status                                                                     | slave ( running )                                       |
| Node Maintenance status                                                    | system idle<br>(current reboot count: 0)                |
| Version                                                                    | CICM 9.0 Maintenance Release 1<br>(Build 9.10.186)      |
| VMG Status                                                                 | inactive ( <span style="color: green;">in sync</span> ) |
| Active Half Calls                                                          | n/a                                                     |
| Terminal Status                                                            | inactive ( <span style="color: green;">in sync</span> ) |
| Number of logged in users                                                  | n/a                                                     |
| Active Terminals                                                           | n/a                                                     |
| Terminal Recovery Status                                                   | n/a                                                     |

| Node B (47.135.43.19) <span style="float: right; color: #0056b3;">?</span> |                                                          |
|----------------------------------------------------------------------------|----------------------------------------------------------|
| Status                                                                     | master ( running )                                       |
| Node Maintenance status                                                    | system idle<br>(current reboot count: 0)                 |
| Version                                                                    | CICM 9.0 Maintenance Release 1<br>(Build 9.10.186)       |
| VMG Status                                                                 | active ( <span style="color: green;">in service</span> ) |
| <u>Active Half Calls</u>                                                   | 0 (total calls=4062)                                     |
| Terminal Status                                                            | active                                                   |
| Number of logged in users                                                  | 15 (total logins=182)                                    |
| <u>Active Terminals</u>                                                    | 17                                                       |
| Terminal Recovery Status                                                   | n/a                                                      |

▶ **maintenance release management**  
Node Node A (47.135.43.18)

▶ **patch management**  
Node Node A (47.135.43.18)

▶ **node A service control**  
Action Stop

▶ **node B service control**  
Action Stop

▶ **switch activity**

▶ **reset counter**  
Node Node A  
Reset Counter Current Reboot Count

▶ **start auto refresh**

▶ **refresh now**

▶ **system status**

#### ***At the page maintenance status (cicm-nnn)***

- 4 Ensure that **start auto refresh** is showing. If **stop auto refresh** is displayed, click it. Stopping the auto refresh will stabilize the pick-lists used.
- 5 If the CICM is at SN08:  
From the pick-list of Node under **apply maintenance release**, select the slave node to upgrade.  
If the CICM is at SN09 or later:  
From the pick-list of Node under **maintenance release management**, select the slave node to upgrade.  
When the displayed Node is already selected, click **maintenance release management** to open the page.

When you select the node other than the one that is showing, the page *maintenance release management* automatically opens.

**maintenance status (cicm-002)**

| Node A (47.135.43.18) ? |                                                    |
|-------------------------|----------------------------------------------------|
| Status                  | slave ( running )                                  |
| Node Maintenance status | system idle<br>(current reboot count: 0)           |
| Version                 | CICM 9.0 Maintenance Release 1<br>(Build 9.10.186) |

► **maintenance release management**

Node

► **patch management**

Node

- 6 From the pick-list under **apply maintenance release**, select the appropriate upgrade file.

When you select a file other than the one that is showing, the page *maintenance release management* automatically opens.

When the file is already displayed, click **maintenance release management**.

The page *maintenance release management* opens.

When *No Files* is shown, the upgrades files have not been copied to the CICM-EM or were copied to the wrong directory. You have not followed the task flow.

**maintenance release management (cicm-002)**

| Node A (47.135.43.18) ? |                            |
|-------------------------|----------------------------|
| Date                    | Event                      |
| 2005/08/04 10:37        | MR 0 applied successfully. |
| 2005/08/04 10:39        | MR 0 applied successfully. |
| 2005/08/08 22:30        | MR 1 applied successfully. |

► **apply maintenance release**

Maintenance Release

**Note:** Maintenance releases should be securely transferred to "D:\CentrexIP\support\upgrades\gw" on the master Element Manager Node

- 7 Confirm applying the upgrade by clicking **confirm maintenance release application**.

**maintenance release application (cicm-002)** (no sync)

| Node B (47.165.172.210) |                                  |
|-------------------------|----------------------------------|
| Mr ID                   | MR0                              |
| Target System           | Undefined                        |
| MDS Checksum            | C95633B27804E7F4241517A25A7E5080 |

confirm maintenance release application

applying MR to : cicm-002

on : Node B (47.165.172.210)

with : gw\_9.10.188.upg

cancel

- 8 Wait 10 seconds, then to aid in monitoring the progress of the update, click **start auto refresh** for a periodic automatic refresh of the status pages.

To stop automatic refresh when monitoring is complete, click **stop auto refresh**.

The auto refresh option toggles between start and stop.

- 9 To monitor the progress of the upgrade, click **system status**.

The page *<cicm-nnn> cicm status* opens and displays the status details of the CICM.

**At the page *<cicm-nnn> cicm status***

- 10 Monitor the *<cicm-nnn>* status until *Service* shows *running*.

A manual restart of the node is not required.

- 11 Upon successful completion of the upgrade, click **perform maintenance on *<cicm-nnn>*** to return to the maintenance status.

**At the page *maintenance status (cicm-nnn)***

- 12 Check the new CICM node version as displayed beside *Version* of the Node A and B status.

- 13 To enable performing test calls, use the procedure [Switching activity between CICM nodes](#) to make the new MR active and upgrade the second node.

- 14 Perform test calls on the upgraded node to verify that the upgraded node is working.

If calls cannot occur on the first upgraded node, you must roll back the upgrade as described in the task flow “CICM-EM or CICM node rollbacks”.

15

**CAUTION****Risk of service prevention**

After upgrading the first CICM node, this is the last chance to roll back the upgrade. Once an upgrade to the second node is attempted, a rollback then becomes a re-installation of the base software and upgrades for each node. Nortel Networks' GNPS must be requested to do the re-installation.

If the tests pass for the first upgraded node, you can choose to roll back the upgrade as described in the task flow "CICM-EM or CICM node rollbacks".

- 16 When upgrading the second CICM node of a redundant pair, start this procedure from [step 3](#). Do not repeat the procedure a third time for the same upgrade to the same pair of nodes.

**At the IEMS interface**

- 17 Edit the object properties in the IEMS for the CICM network elements you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the field *Device Version*:

- [Editing and viewing object properties using Java Web Start Client](#)
- [Editing and viewing object properties using Web Client](#)

With the Java Web Client, CICM uses *v2c* for the *Version* in the *SNMP Details* page.

- 18 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Switching activity between CICM nodes

Switch the activity from the master CICM node to the slave node of the redundant pair.

**Prerequisites to switching activity between CICM nodes**

Address the prerequisites before starting the procedure.

- Follow the Prerequisites and sequence of procedures identified in this document.
- Both CICM nodes must be in-service to enable the switch of activity (SWACT) to occur.

- After the upgrade and before the SWACT, Node A is the slave with status running and with no terminals connected to it.
- When upgrading with an MR the CICM terminals are automatically transferred during the switch of activity.
- If you did [step 13](#) in the procedure [Upgrading a CICM node with an MR](#) to enable testing calls, then do not repeat this procedure to upgrade the mate node. The mate node is already the slave.

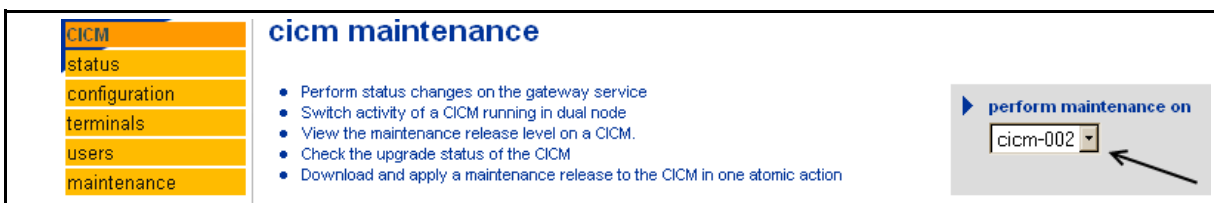
### Procedure steps to switching activity between CICM nodes

#### *At any CICM web page*

- 1 In the menu *CICM*, click **maintenance**.

#### *At the page cicm maintenance*

- 2 From the pick-list under **perform maintenance on**, select the CICM node identifier.



- 3 Click **perform maintenance on**.
- 4 Observe from the *Node Maintenance status* of each node which ones are master and slave.
- 5 Click **switch activity**.

The duration of the switchover varies according to the number of users configured on the nodes and the volume of calls being sustained in the node at the time of the SWACT.

When both nodes are not available for a SWACT, the command button is tinted grey and disabled. Ensure that both nodes are in service.
- 6 Click **confirm switch of activity**.
- 7 Confirm from the *Node Maintenance status* whether the master and slave have switched successfully:
  - the *Node status* is *master*
  - the *Node Maintenance status* is *system idle*

If not, then contact your next level of support to determine why.
- 8 This procedure is complete.

Return to the task flow or step in the procedure from where you came.

## Removing old CICM load files

After completing a successful CICM upgrade, and the network upgrade has been finalized, remove the older CICM element manager (EM) and gateway (GW) files which consist of the following file extensions:

- .upg
- .cab
- .pat

Perform this procedure after each successful upgrade to ensure adequate disk space remains available.

### Removing old CICM load files

#### *At the CICM terminal*

- 1 Log on to the master CICM-EM by entering:  
**ssh Administrator@<static\_ip\_address>**  
 Connecting to <ip\_address>...  
 The authenticity of host '<ip\_address>' (<ip\_address>) can't be established.  
 DSA key fingerprint is <string>  
 Are you sure you want to continue connecting (yes/no)?
- 2 Confirm the prompt:  
**yes**  
 Warning: Permanently added '<ip\_address>' (DSA) to the list of known hosts.  
 Administrator@<ip\_address>'s password:
- 3 Enter the Administrator password:  
**<admin\_password>**
- 4 Go to the appropriate directory where the obsolete .cab or .upg files reside:

| If             | Do                                                                 |
|----------------|--------------------------------------------------------------------|
| SN09 files     | <b>cd /D:/Centrexip/support/upgrades/em</b>                        |
|                | or                                                                 |
|                | <b>cd /D:/Centrexip/support/upgrades/gw</b>                        |
| pre-SN09 files | <b>cd /D:/Centrexip/support/&lt;old_directory&gt; <sup>1</sup></b> |

1.To locate the pre-SN09 directories, log on to the CICM-EM web maintenance page. Under the "CICM-EM" or "CICM menu select "maintenance" and the directory path appears on the left.

- 5 List the file load names in the directory to determine the loads for deletion:

**dir**

| If the file is | Do                     |
|----------------|------------------------|
| read only      | <a href="#">step 6</a> |
| not read only  | <a href="#">step 7</a> |

- 6 Remove the Read Only "R" file attribute setting before deleting the file:

**attrib -R <file\_name>**

*Example*

**attrib -R GW\_7.11.237.cab**

- 7 Individually delete all obsolete files :

**erase <file\_name>**

*Examples*

**erase GW\_7.11.237.cab**

**erase EM\_7.10.212.upg**

**erase GW\_7.12.226.pat**

- 8 This procedure is complete.



---

## Upgrading firmware on IP phone sets

---

This section provides the task flow and procedure to upgrade the firmware of the IP phone sets that connect to a Centrex IP Client Manager (CICM) node.

The topics in this section are:

- [CICM IP phone firmware upgrades](#)
- [Upgrading the firmware on an IP phone set](#)

### CICM IP phone firmware upgrades

This section includes the task flow to upgrade the firmware of the types of IP phones that can connect to the CICM nodes. The topics are:

- [Prerequisites to the task flow of CICM IP phone firmware upgrades](#)
- [Task flow of CICM IP phone firmware upgrades](#)

#### Prerequisites to the task flow of CICM IP phone firmware upgrades

Before following the task flow, ensure that you have addressed these requirements.

- The IP phone must already be installed as described in *m6350 SoftClient Installation Guide*, NN10182-113.
- The IP phones supported with CICM are:
  - IP Phone 2001
  - IP Phone 2002
  - IP Phone 2004
  - IP Audio Conference Phone 2033
  - IP Phone 2210 (wireless)

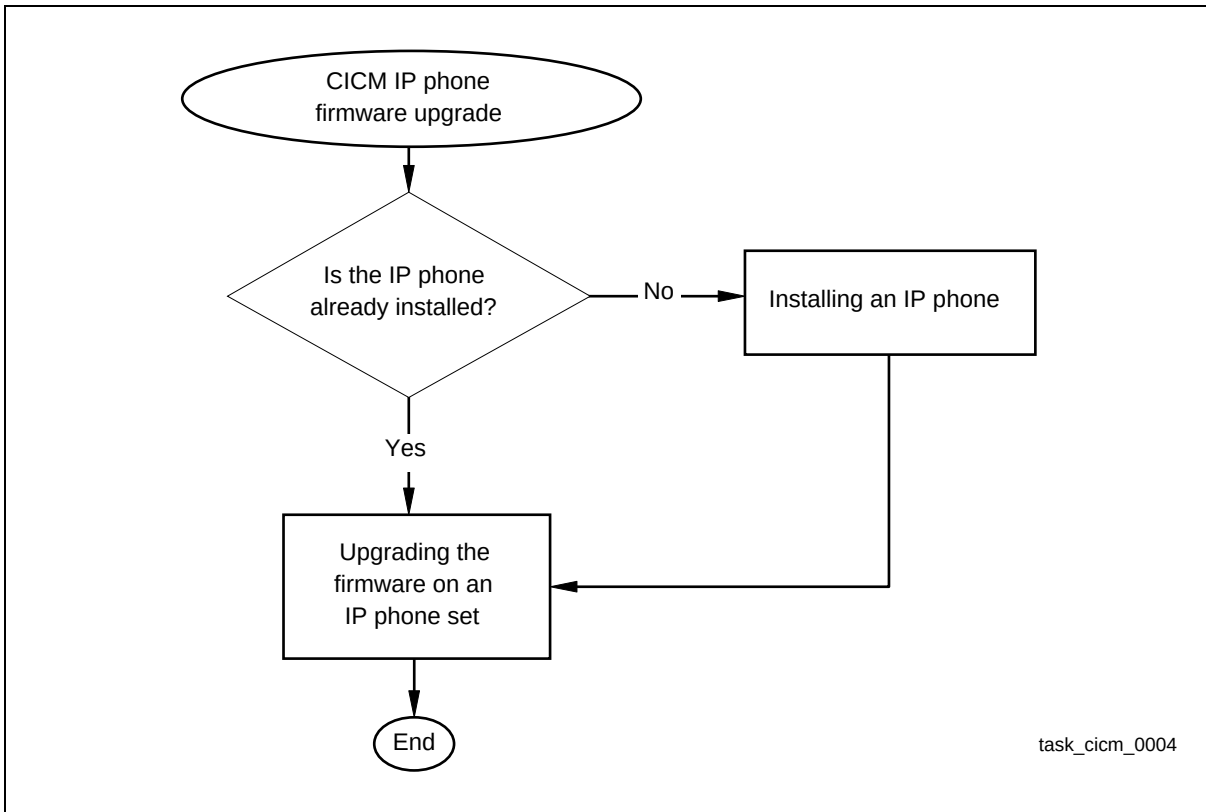
- IP Phone 2211 (wireless)
- IP Phone 2212 (wireless)
- You must be familiar with the user guide of the Nortel Networks IP phone you are upgrading. The user guides are:
  - *Nortel Networks IP Phone 2001 User Guide*, NN10300-005
  - *Nortel Networks IP Phone 2002 User Guide*, NN10300-007
  - *Nortel Networks IP Phone 2004 User Guide*, NN10300-009
  - *Nortel Networks IP Phone 2007 User Guide*, NN10300-020
  - *Nortel Networks IP Audio Conference Phone 2033 User Guide*, 555-4001-605
  - *Nortel Networks IP Phone Key Expansion Module User Guide*, NN10300-011

**Task flow of CICM IP phone firmware upgrades**

The task flow shows the sequence of procedures to upgrade the firmware of a CICM IP phone, as shown in the figure [Task flow of a CICM IP phone firmware upgrade](#).

To link any procedure, go to Navigation immediately following the figure.

## Task flow of a CICM IP phone firmware upgrade



### Navigation

The procedures and task flow in the task flow are listed alphabetically.

- “Installing an IP phone”. See the procedure in the appropriate user guide:
  - *Nortel IP Phone 2001 User Guide*, NN10300-005
  - *Nortel IP Phone 2002 User Guide*, NN10300-007
  - *Nortel IP Phone 2004 User Guide*, NN10300-009
  - *Nortel IP Audio Conference Phone 2033 User Guide*, 555-4001-605
  - *Nortel IP Phone Key Expansion Module User Guide*, NN10300-011
- [Upgrading the firmware on an IP phone set](#)

## Upgrading the firmware on an IP phone set

Upgrade the firmware of an IP phone set to ensure optimum operation of the phone and the CICM services supported by that model.

### Prerequisites to upgrading the firmware on an IP phone set

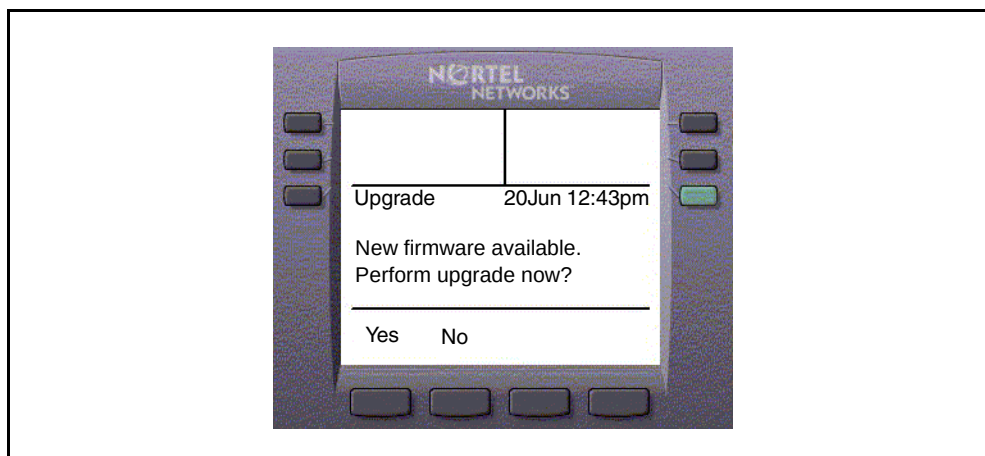
Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in [CICM IP phone firmware upgrades](#).
- The indication that a firmware upgrade is available for the IP phone is either:
  - an upgrade button is displayed at the login screen when the user is not logged in
  - an upgrade option is displayed in the options menu when the user is logged in
- When the IP Phone is notified of a firmware upgrade and the user is not logged in, the upgrade occurs automatically. No notification of auto-upgrade is given.

### Procedure steps to upgrading the firmware on an IP phone set

#### *At the IP phone set*

- 1 When the firmware icon Upgrade is shown on the login screen:
  - log in as described by the user guide for that model of IP phone, or let the auto-upgrade feature handle it in about a minute
  - if you are already logged in when Upgrade appears, decide whether to interrupt your call now or later



- 2** Press the key next to Yes to begin the upgrade, or next to No to post-pone it.

  - With Yes, your session is unavailable for less than 2 minutes while the softkey icons flash and the screen remains blank.
  - With No, the upgrade is delayed for the duration of the session. As soon as the session ends, the icon Upgrade re-appears.
  - When the prompt is ignored, the upgrade occurs automatically in about minute.
- 3** The appearance of a normal screen indicates the upgrade is completed.

If you were already logged in, and you have autologin enabled, you will automatically be re-logged in. Otherwise log in again. Confirm the operation of the phone by trying some of your capabilities.
- 4** This procedure is complete. Return to the task flow [Task flow of a CICM IP phone firmware upgrade](#).

---

## CICM-EM or a CICM node patches

---

This section provides the procedures to patch the software of a redundant pair of Centrex IP Client Manager (CICM) element managers (CICM-EMs) or a redundant pair of CICM nodes. Applying a patch occurs between maintenance release (MR) upgrades and is supported from SN09 and later.

The series of procedures to apply a patch to CICM-EMs or CICM nodes is provided in a task flow.

The topics in this document include:

- [Prerequisites to the task flow of CICM-EM or CICM node patches](#)
- [Task flow of CICM-EM or CICM node patches](#)
- [Patch procedures for CICM-EM or CICM nodes](#)

### Prerequisites to the task flow of CICM-EM or CICM node patches

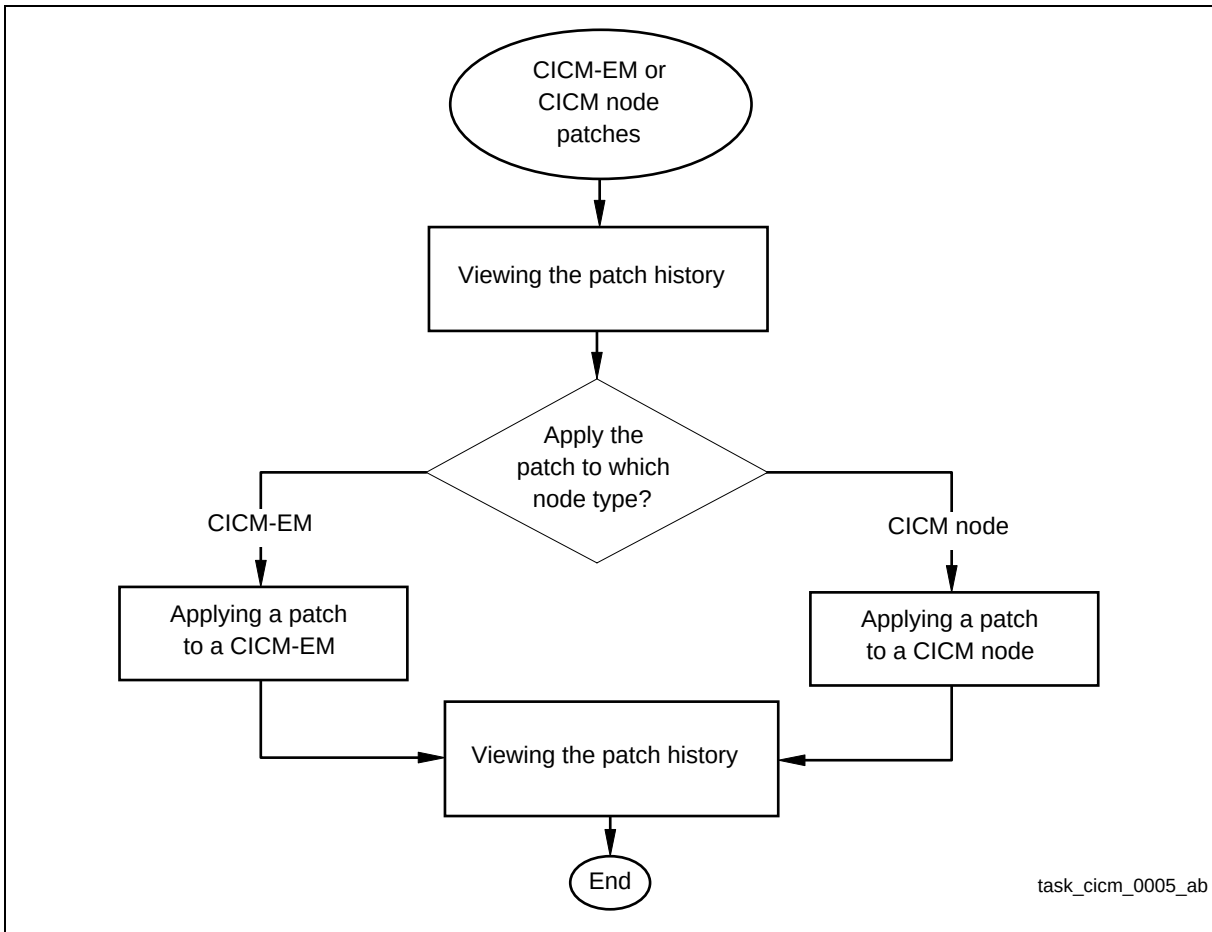
Before following the task flow, ensure that you have addressed these requirements.

- Read and understand [Preparing to upgrade CICM software](#), especially for applying patches.
- A patch can be applied in any sequence to a CICM-EM or a CICM node, but must always be to the slave node. Always follow the guidelines or recommendations of GNPS for applying a patch to in-service systems.
- Patch file names end with .pat as the file extension.

### Task flow of CICM-EM or CICM node patches

The task flow shows the sequence of procedures to patch a redundant pair of CICM-EMs or CICM nodes. The procedures are shown in the figure [Task flow of CICM-EM and CICM node patches](#). To link any procedure, go to Navigation immediately following the figure.

## Task flow of CICM-EM and CICM node patches



### Navigation

The procedures in the task flow are listed alphabetically.

- [Applying a patch to a CICM node](#)
- [Applying patch to a CICM-EM](#)
- [Viewing the patch history](#)

## Patch procedures for CICM-EM or CICM nodes

The procedures for patching the software of a CICM-EM pair and its CICM node pairs are listed alphabetically in this section. The actions you must do or understand prior to starting the task flow are identified in [Prerequisites to the task flow of CICM-EM or CICM node patches](#). The sequence of doing the procedures is identified in [Task flow of CICM-EM or CICM node patches](#).

To link any procedure or imbedded task flow, go to Navigation immediately following the figure.

**Note:** You must follow the prerequisites and sequence of procedures identified in the task flow in order to properly complete patching.



## Applying a patch to a CICM node

Apply a software patch to a pair of redundant CICM nodes one at a time.

### Prerequisites to applying a patch to a CICM node

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM or CICM node patches](#).
- You need a PC or equivalent to remotely access the CICM-EM web pages. Upgrading is not done locally from a CICM-EM to a CICM node.
- Both CICM nodes must be in service before attempting the patch.
- You must know the administrator userid and password to log into the CICM-EM for this maintenance activity.
- You do not have to apply every patch. To determine what a patch provides, use the procedure [Viewing the patch history](#) to read the provided description. The Release Notes also include information about each patch.
- When applying a patch, always apply it to both CICM nodes of a redundant pair.
- Always apply a patch to the slave first unless the slave is unavailable. An unavailable slave is indicated by a warning message.
- You must know the value of the MD5 checksum that arrived in a file with the patch source files before you copied the files to the CICM-EMs.

### Procedure steps to applying a patch to a CICM node

#### *At the PC desktop for remote access to the CICM*

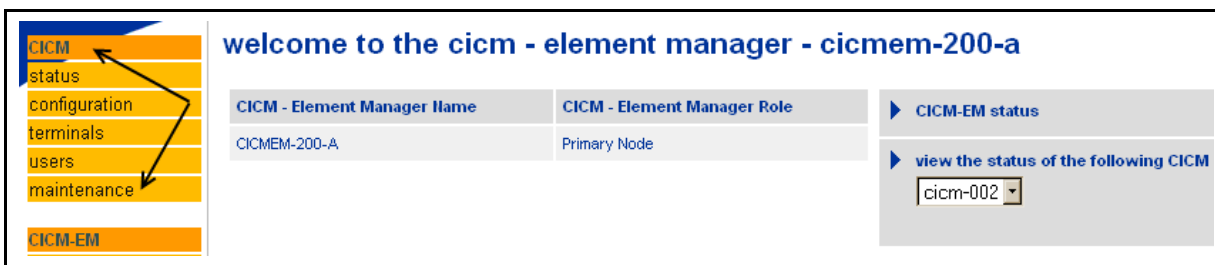
- 1 Access the CICM node from your PC through an Internet web interface by entering:

**`https://<unique_admin_ip_address_of_cicmem>/centrexip`**

Alternatively, access the CICM node using the procedure [Accessing a CICM-EM through the IEMS on page 2133](#).

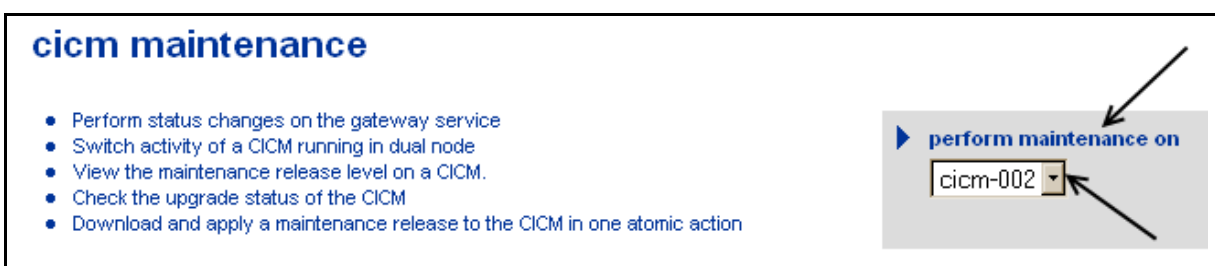
#### *At any CICM web page*

- 2 In the menu CICM, click maintenance.



The page cicm maintenance opens.

- 3 From the pick-list under perform maintenance on, select the CICM node to upgrade.



When you select the node other than the one that is showing, the page maintenance status automatically opens.

When the displayed Node is the slave, click perform maintenance on.

The page maintenance status cicm-nnn opens.

#### ***At the page maintenance status (cicm-nnn)***

- 4 Determine from the field Status which Node is the slave.
- 5 From the pick-list under patch maintenance, select the CICM node A or B to patch, whichever is the slave.

When you select the node other than the one that is showing, the page patch management automatically opens.

When the displayed Node is the slave, click patch management to open the page.

**maintenance status (cicm-002)**

| Node A (47.135.43.18)   |                                                    |
|-------------------------|----------------------------------------------------|
| Status                  | slave ( running )                                  |
| Node Maintenance status | system idle<br>(current reboot count: 0)           |
| Version                 | CICM 9.0 Maintenance Release 1<br>(Build 9.10.186) |
| VMG Status              | inactive ( in sync )                               |
| Active Half Calls       | n/a                                                |
| Terminal Status         | inactive ( in sync )                               |

▶ **maintenance release management**

Node

▶ **patch management**

Node

▶ **node A service control**

Action

### At the page patch management

- 6 From the pick-list beside Patch Release, select the patch file to be loaded onto the slave CICM node.

All files at this CICM-EM directory are listed:

D:\CentrexIP\support\patches\gw

**patch management (cicm-130)** no sync

| Patch                    | Status                                    | Description | Applied          | Removed |
|--------------------------|-------------------------------------------|-------------|------------------|---------|
| <a href="#">Patch P1</a> | The patch is fully, independently applied | Short 1     | 2005/05/06 17:15 | None    |
| <a href="#">Patch P2</a> | The patch is fully, independently applied | Short 2     | 2005/05/06 17:15 | None    |

▶ **select patch**

Patch Release

**Dropdown list of patches available for deployment**

Notes: Patches should be securely transferred to "D:\CentrexIP\support\patches\gw" on the master Element Manager Node

When you select the file other than the one that is showing, the page patch management automatically opens.

When the displayed file is already the one you want, click select patch. The page patch application (cicmem-nnn) opens.

At this page, the list of patches under Patch is always alphabetically sorted by Patch ID, which means P10 follows P1 and precedes P2.

When the display is full of Patch IDs and there are more, use the scroll bar that appears.

**At the page patch application**

7 Observe the patch information.

**patch application (cicm-002)** [\[no sign\]](#)

| Node B (47.165.172.210) |                                  |
|-------------------------|----------------------------------|
| Patch ID                | P18                              |
| Short Description       | Short 18                         |
| Subsumed Patches        | P8                               |
| Conflicting Patches     |                                  |
| PreRequisite Patches    |                                  |
| Removed Patches         | P6                               |
| Target System           | H248                             |
| Patch Type              | Application Patch                |
| Target Build Number     | 9.10.186                         |
| MD5 Checksum            | 7BDFF1E906A26D7FAF955B097645472F |
| Long Description        | Longer 18                        |
| Reboot Count            | 0                                |
| Apply Date              | None                             |
| Remove Date             | None                             |

confirm patch application

applying Patch to : cicm-002

on : Node B (47.165.172.210)

with : patch\_test\_9.10.186\_p18\_cicm.pat

cancel

The fields in the page patch application mean as follows.

**Patch ID**

uniquely identifies a patch as Pn where n is 1 to 999.

**Short Description**

is the title of the patch.

**Subsumed Patches**

identifies one or more patches that this patch subsumes.

**Conflicting Patches**

is blank or identifies one or more patches that conflict with this patch.

**PreRequisite Patches**

is blank or identifies one or more patches that must be applied before this patch.

**Removed Patches**

identifies the patch or patches that will be removed and replaced by this patch.

**Target System**

indicates H248 for a CICM node (or CICM EM for a CICM-EM).

**Patch Type**

is one of the following types of patch:

- Application Patch for an MR
- OS for operating system (for example, Microsoft Windows)

**Target Build Number**

indicates the version of software release that the patch must be compatible with.

**MD5 Checksum**

is an alphanumerical value to enable comparing the integrity of the patch files that are copied onto the CICM-EMs with the actual source files that were received from Nortel Networks.

**Long Description**

includes up to 255 characters of information about the patch.

**Reboot Count**

indicates the number of times the CICM-EM must automatically reboot while the patch is applied. The EM is briefly unavailable while it reboots.

A count of 0 (zero) means the CICM-EM will require only a partial service outage or no outage.

**Apply Date**

is None to indicate it is available on the CICM-EM but has not been applied yet.

**Remove Date**

is None to indicate the patch has not been removed yet.

***At the page patch application***

- 8 Compare the alphanumerical value of the displayed MD5 checksum to the checksum indicated in the file from GNPS that was provided with the upgrade files.

When the checksum characters are identical, proceed to the next step.

When the checksums are not identical, re-copy the files onto the CICM-EM by starting again at [CICM-EM and CICM node preparation for an upgrade or patch](#). If the checksums are still different after the second attempt at patching, contact GNPS to discuss your next actions.

- 9 Observe the upper right area of the page patch application.

When all of the pre-check patch criteria pass by the system, the command confirm patch application is shown and enabled.

When at least one of the following pre-check patch criteria fails by the system, the reason that prevents the system from attempting to apply the patch is shown.

- A Conflicting Patch is identified. Determine from it what you need to do to remove the problem before proceeding. You may need to contact GNPS to clarify the action.
- A PreRequisite Patch is identified. Use the procedure [Viewing the patch history](#) to determine whether the patches are available and have been applied. For any that have not been applied, apply them first.
- The Target System mismatches the type of node, for example, you selected a patch file for a CICM-EM instead of a patch for a CICM node.
- The Target Build Number, for example, 9.10.186, is not included in the file name under confirm patch application. A patch can only be applied to a specific version of an MR.
- The Apply Date is other than None, which means the patch has already been applied. A patch cannot be re-applied.

**10** When confirm patch application is enabled, click it.

**11** Observe the Apply Date.

When it changes from None to the current date, the patch has been successfully applied.

Meanwhile, observe the status of the CICM-EM at the page maintenance status. The status Maintenance in Progress appears for the CICM-EM while patching occurs.

When applying the patch fails, during consistency checking system service is not affected. When it fails during the actual applying, you will need to restore service to the node. In this case, contact your next level of support to determine your actions.

When applying the patch fails, the patch:

- remains unapplied
- is not included in the list of applied patches
- is not added to page patching history

**12** Test the functionality of the patch or run a sanity test on the slave CICM node.

Tests vary per patch. Refer to the Release Notes for how to test the functionality.

- 13** When the slave CICM node is verified to be operating normally and fully in-service, switch the activity of the node pair to make the master node into the slave. Follow the procedure [Switching activity between CICM nodes](#).

When applying patches has been attempted on both CICM nodes of a pair (successful or not), do not repeat this step.

- 14** Repeat [step 2](#) to [step 13](#) to patch the second CICM node of the redundant pair.
- 15** When both nodes are successfully patched, this procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Applying patch to a CICM-EM

Apply a software patch to a pair of redundant CICM-EMs one at a time.

### Prerequisites to applying a patch to a CICM-EM

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM or CICM node patches](#).
- The CICM-EM node-pair can support CICM node-pairs running either the same version or one previous version (for example, the EMs running 9.0 while a pair of nodes run 8.0).
- You need a PC or equivalent to remotely access the CICM-EM web pages. Upgrading is not done locally to a CICM-EM.
- You must know the administrator userid and password to log into the CICM-EM for this maintenance activity.
- You do not have to apply every patch. To determine what a patch provides, use the procedure [Viewing the patch history](#) to read the provided description. The Release Notes also include information about each patch.
- When applying a patch, always apply it to both CICM-EMs of a redundant pair.
- Always apply a patch to the slave first. A patch can be applied to a master node only if the slave is unavailable. An unavailable slave is indicated by a warning message.
- Know the value of the MD5 checksum that arrived in a file with the patch source files before you copied the files to the CICM-EMs.

### Procedure steps to applying a patch to a CICM-EM

#### *At the PC desktop for remote access to the CICM-EM*

- 1 Access the CICM-EM from your PC through an Internet web interface by entering:  
**https://<unique\_admin\_ip\_address\_of\_cicmem>/centrexip**  
Alternatively, access the CICM-EM using the procedure [Accessing a CICM-EM through the IEMS](#).

#### *At any CICM web page*

- 2 In the menu CICM-EM, click maintenance.  
The page maintenance status opens.



**maintenance status (cicmem-200)**

| Node A (CICMEM-200-A)   |                                              |
|-------------------------|----------------------------------------------|
| Node status             | master                                       |
| Node Maintenance status | system idle<br>(current reboot count: 0)     |
| Version                 | CICM-EM 9.0 Base Release<br>(Build 9.10.186) |

| Node B (CICMEM-200-B)   |                                                       |
|-------------------------|-------------------------------------------------------|
| Node status             | slave                                                 |
| Node Maintenance status | system idle<br>(current reboot count: 0)              |
| Version                 | CICM-EM 9.0 Maintenance Release 1<br>(Build 9.10.186) |

**patch management**

Node:

**start auto refresh**

**refresh now**

**system status**

- 3 Determine from the field Status which Node is the slave.

**At the page maintenance status (cicmem-nnn)**

- 4 From the pick-list of Node under patch management, select Node A or B, whichever is the slave.

When you select the node other than the one that is showing, the page patch management automatically opens.

When the displayed Node is the slave, click patch management to open the page.

**At the page patch management**

- 5 From the pick-list beside Patch Release, select the patch file to be loaded onto the slave CICM-EM.

All files at this CICM-EM directory are listed:

D:\CentrexIP\support\patches\em

**patch management (cicm-130)** no sync

| Node B (47.165.168.105)  |                                           |             |                  |         |
|--------------------------|-------------------------------------------|-------------|------------------|---------|
| Patch                    | Status                                    | Description | Applied          | Removed |
| <a href="#">Patch P1</a> | The patch is fully, independently applied | Short 1     | 2005/05/08 17:15 | None    |
| <a href="#">Patch P2</a> | The patch is fully, independently applied | Short 2     | 2005/05/08 17:15 | None    |

**select patch**

Patch Release:

Notes: Patches should be securely transferred to "D:\CentrexIP\support\patches\em" on the master Element Manager Node

At this page, the list of patches under Patch is always alphabetically sorted by Patch ID, which means P10 follows P1 and precedes P2.

When the display is full of Patch IDs and there are more, use the scroll bar that appears.

**6** Click select patch.

The page patch application (cicmem-nnn) opens.

When the selected file cannot be applied to the selected node, an ERROR message is displayed to indicate why not.

| Node B (47.165.172.218) |                                  |
|-------------------------|----------------------------------|
| Patch ID                | P18                              |
| Short Description       | Short 18                         |
| Subsumed Patches        | P8                               |
| Conflicting Patches     |                                  |
| PreRequisite Patches    |                                  |
| Removed Patches         | P6                               |
| Target System           | H248                             |
| Patch Type              | Application Patch                |
| Target Build Number     | 9.10.186                         |
| MD5 Checksum            | 7BDFF1E908A26D7FAF955B097645472F |
| Long Description        | Longer 18                        |
| Reboot Count            | 0                                |
| Apply Date              | None                             |
| Remove Date             | None                             |

confirm patch application

applying Patch to : cicm-002  
on : Node B (47.165.172.210)  
with : patch\_test\_9.10.186\_p18\_cicm.pat

confirm

cancel

The fields in the page patch application mean as follows.

**Patch ID**

uniquely identifies a patch as Pn where n is 1 to 999.

**Short Description**

is the title of the patch.

**Subsumed Patches**

identifies one or more patches that this patch subsumes.

**Conflicting Patches**

is blank or identifies one or more patches that conflict with this patch.

**PreRequisite Patches**

is blank or identifies one or more patches that must be applied before this patch.

**Removed Patches**

identifies the patch or patches that will be removed and replaced by this patch.

**Target System**

indicates CICM EM for a CICM-EM (or H248 for a CICM node).

**Patch Type**

is one of the following types of patch:

- Application Patch for an MR
- OS for operating system (for example, Microsoft Windows)

**Target Build Number**

indicates the version of software release that the patch must be compatible with.

**MD5 Checksum**

is an alphanumeric value to enable comparing the integrity of the patch files that are copied onto the CICM-EMs with the actual source files that were received from Nortel Networks.

**Long Description**

includes up to 255 characters of information about the patch.

**Reboot Count**

indicates the number of times the CICM-EM must automatically reboot while the patch is applied. The EM is briefly unavailable while it reboots.

A count of 0 (zero) means the CICM-EM will require only a partial service outage or no outage.

**Apply Date**

is None to indicate it is available on the CICM-EM but has not been applied yet.

**Remove Date**

is None to indicate the patch has not been removed yet.

***At the patch application page***

- 7** Compare the alphanumeric value of the displayed MD5 checksum to the checksum indicated in the file from GNPS that was provided with the upgrade files.

When the checksum characters are identical, proceed to the next step.

When the checksums are not identical, re-copy the files onto the CICM-EM by starting again at [CICM-EM and CICM node preparation for an upgrade or patch](#). If the checksums are still different after the second attempt at patching, contact GNPS to discuss your next actions.

- 8** Observe the upper right area of the page patch application.

When all of the pre-check patch criteria pass by the system, the command confirm patch application is shown and enabled.

When at least one of the following pre-check patch criteria fails by the system, the reason that prevents the system from attempting to apply the patch is shown.

- A Conflicting Patch is identified. Determine from it what you need to do to remove the problem before proceeding. You may need to contact GNPS to clarify the action.
- A PreRequisite Patch is identified. Use the procedure [Viewing the patch history](#) to determine whether the patches are available and have been applied. For any that have not been applied, apply them first.
- The Target System mismatches the type of node, for example, you selected a patch file for a CICM node instead of a patch for a CICM-EM.
- The Target Build Number, for example, 9.10.186, is not the same as the build number that the patch is intended for.

- 9** When confirm patch application is enabled, click it.

- 10** Observe the Apply Date.

When it changes from None to the current date, the patch has been successfully applied.

Meanwhile, observe the status of the CICM-EM at the web page maintenance status. The status Maintenance in Progress appears for the CICM-EM while patching occurs.

When applying the patch fails, during consistency checking system service is not affected. When it fails during the actual applying, you will need to restore service to the node. In this

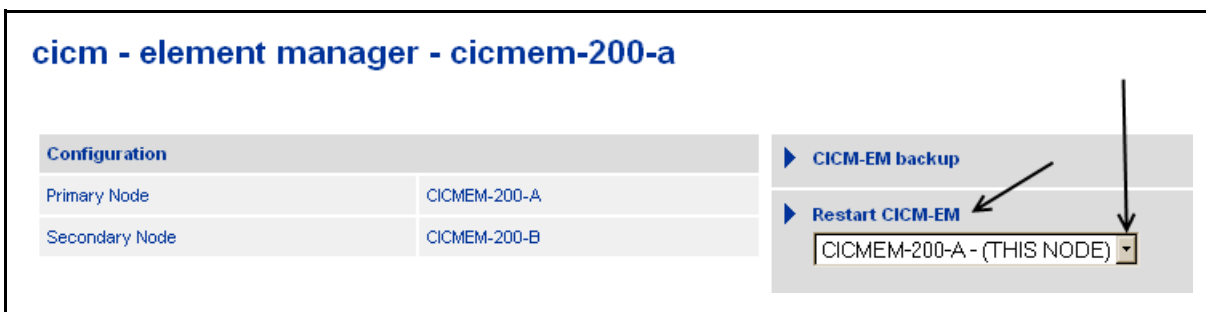
case, contact your next level of support to determine your actions.

When applying the patch fails, the patch:

- remains unapplied
- is not included in the list of applied patches
- is not added to page patching history

- 11** Test the functionality of the patch or run a sanity test on the slave CICM-EM. Tests vary per patch. Refer to the Release Notes for how to test the functionality.
- 12** When the slave CICM-EM is verified to be operating normally and fully in-service, repeat [step 2](#) to [step 11](#) on the master CICM-EM.
- 13** Switch activity between the CICM-EM pair by restarting the active node. From the pick-list under Restart CICM EM, select the active mate node.

Click Restart CICM EM.



The page changes to show the confirmation prompt.

- 14** Click Confirm restart of CICM-EM (CICMEM-nnn-x) where x is the node A or B you selected.  
Monitor the progress of the restart by clicking maintenance in the CICM-EM menu. When displayed status of node activity updates as soon as the switchover occurs.
- 15** When both nodes are successfully patched, this procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Viewing the patch history

View the history of patches for the CICM-EMs or CICM nodes since the last maintenance release (MR) to determine the availability of specific patches and whether the patch has been applied successfully.

### Prerequisites to viewing the patch history

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM or CICM node patches](#).
- The start of the procedure may not be where you are at. Use whichever path gets you to the page maintenance status for either a CICM-EM or a CICM node.

### Procedure steps to viewing the patch history

#### *At any CICM web page*

- 1 For the CICM nodes, in the menu CICM click maintenance.

For the CICM-EMs, in the menu CICM-EM click maintenance.

Alternatively, you can access either type of node from the IEMS as described in the procedure [Accessing a CICM-EM through the IEMS](#)



The page maintenance status opens.

#### *At the page maintenance status*

- 2 From the pick-list under patch management, select the node for the history to be viewed.

**maintenance status (cicm-002)**

| Node A (47.135.43.18)   |                                                    |
|-------------------------|----------------------------------------------------|
| Status                  | slave ( running )                                  |
| Node Maintenance status | system idle<br>(current reboot count: 0)           |
| Version                 | CICM 9.0 Maintenance Release 1<br>(Build 9.10.186) |

**maintenance release management**  
Node

**patch management**  
Node

**At the page patch management (cicm-nnn)**

3 Click view patching history.

The page patching history opens.

**patch management (cicm-130)** no sync

| Patch                    | Status                                    | Description | Applied          | Removed |
|--------------------------|-------------------------------------------|-------------|------------------|---------|
| <a href="#">Patch P1</a> | The patch is fully, independently applied | Short 1     | 2005/05/06 17:15 | None    |
| <a href="#">Patch P2</a> | The patch is fully, independently applied | Short 2     | 2005/05/06 17:15 | None    |
| <a href="#">Patch P3</a> | The patch is fully, independently applied | Short 3     | 2005/05/06 17:16 | None    |
| <a href="#">Patch P4</a> | The patch is fully, independently applied | Short 4     | 2005/05/06 17:16 | None    |
| <a href="#">Patch P5</a> | The patch is fully, independently applied | Short 5     | 2005/05/06 17:16 | None    |
| <a href="#">Patch P6</a> | The patch is fully, independently applied | Short 6     | 2005/05/06 17:17 | None    |
| <a href="#">Patch P7</a> | The patch is fully, independently applied | Short 7     | 2005/05/06 17:17 | None    |
| <a href="#">Patch P8</a> | The patch is fully, independently applied | Short 8     | 2005/05/06 17:17 | None    |

**Dropdown list of patches available for deployment**

**Access to patching history of this node**

**Click on patch to get information**



**At the page patch history (cicmem-nnn)**

- 4 View the status of each patch for either the pair of CICM-EMs or pairs of CICM nodes.

| patch history (cicmem-201) |                                      |
|----------------------------|--------------------------------------|
| Node B (CICMEM-201-B)      |                                      |
| Date                       | Event                                |
| 2005/07/11 22:56           | Patch P1 was applied.                |
| 2005/07/11 22:56           | Patch P2 was applied.                |
| 2005/07/11 22:57           | Patch P2 was removed by patch P6.    |
| 2005/07/11 22:57           | Patch P6 was applied.                |
| 2005/07/11 23:02           | Patch P22 was removed by patch P23.  |
| 2005/07/11 23:02           | Patch P23 was applied.               |
| 2005/07/11 23:13           | Patch P5 was subsumed by patch P10.  |
| 2005/07/11 23:13           | Patch P10 was applied.               |
| 2005/07/11 23:13           | Patch P1 was removed by patch P11.   |
| 2005/07/11 23:13           | Patch P11 was applied.               |
| 2005/07/11 23:14           | Patch P14 was applied.               |
| 2005/07/11 23:14           | Patch P4 was applied.                |
| 2005/07/11 23:15           | Patch P8 was applied.                |
| 2005/07/11 23:17           | Patch P10 was subsumed by patch P21. |
| 2005/07/11 23:17           | Patch P5 was removed by patch P21.   |
| 2005/07/11 23:17           | Patch P21 was applied.               |

The field Date indicates the year, month, day, and time of the occurrence in field Event. Events are listed by their date, oldest first. When the display is full, use the scroll bar to view other data.

The possible statuses under field Event are as follows (listed alphabetically).

**Patch Pn was applied.**

means the patch was fully, independently applied.



**Patch Pn was removed by patch Pn.**

means the patch was removed by the application of another patch. A removed patch cannot be re-applied.

A patch with a Date of none means the patch is available but has not been applied yet.

**Patch Pn was subsumed by patch Pn.**

means the patch was included as part of another patch.

- 5 From the patch status information, verify whether the patch is already present (that is, does not need to be copied onto the CICM-EM again) and has already been applied successfully.
- 6 For details about a patch, including its relationship to other patches, return to the page patch management (cicm-nnn) or patch management cicmem-nnn).

***At the page patch management***

- 7 Click any Patch Pn with status applied to expand information about the patch.

The page patch information opens.



| patch information (cicm-002) <a href="#">(no sync)</a> |                                           |
|--------------------------------------------------------|-------------------------------------------|
| Node B (47.165.172.218) ?                              |                                           |
| Patch ID                                               | P1                                        |
| Patch State                                            | The patch is fully, independently applied |
| Short Description                                      | Short 1                                   |
| Patch Type                                             | Application Patch                         |
| Long Description                                       | Longer 1                                  |
| Apply Date                                             | 2005/08/04 10:12                          |
| Remove Date                                            | None                                      |

View the patch information as follows.

**Patch ID**

uniquely identifies a patch as Pn where n is 1 to 999.

**Patch State**

is Applied, Subsumed, or Removed.

**Short Description**

is the title of the patch.

**Patch Type**

is one of the following types of patch:

- Application Patch for an MR
- OS for operating system (for example, Microsoft Windows)

**Long Description**

includes up to 255 characters of information about the patch.

**Apply Date**

is the year, month, day, and time that the patch was applied. It cannot be None at this stage to indicate it is available on the CICM-EM but has not been applied yet.

**Remove Date**

is None to indicate the patch has not been removed yet.

- 8 This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Rolling back from a CICM-EM or CICM node upgrade

This section provides the procedures to roll back from upgrading the software of a single Centrex IP Client Manager (CICM) element manager (CICM-EM) or a single CICM node. Rolling back from an upgrade means restoring the previous version of software.

The series of procedures to roll back CICM-EMs or CICM nodes are provided in a task flow.

The topics in this section are:

- [Prerequisites to the task flow of CICM-EM and CICM rollbacks](#)
- [Task flow of CICM-EM and CICM node rollbacks](#)
- [Rollback procedures for CICM-EM and CICM nodes](#)

### Prerequisites to the task flow of CICM-EM and CICM rollbacks

Before following the task flow, ensure that you have addressed these requirements.

**CAUTION****Risk of service prevention**

To roll back from upgrading both CICM-EMs or both CICM nodes of a redundant pair, the software must be re-imaged as if doing an initial installation. Contact Nortel Networks's GNPS to assist with re-imaging a pair of CICM-EMs or CICM nodes.

**CAUTION****Risk of service prevention**

Before starting the rolling back task, read each procedure to determine what data you will need for your re-imaging, especially the preboot IP addresses. It is critical to have all the data readily available before starting any procedure in [Rolling back from a CICM-EM or CICM node upgrade](#).

Before following the task flow, ensure that you have addressed these requirements.

- Only one CICM-EM of the redundant pair can have been upgraded, or one CICM node of a redundant pair.
- Be very familiar with the configuration and setup choices that were made when the CICM-EM or CICM node was initially installed. Rolling back requires a partial re-configuration through the command preboot.
- The task flow applies to doing a rollback to release 8.0 MRx or 7.0 MRx from either:
  - a maintenance release (MR) 9.0 MRx or earlier
  - a product release from 9.xx or earlier

Rolling back from a patch is not supported. If you must remove a patch, contact your Nortel Networks account prime to request another patch be created to overwrite the applied one.

- Ensure that you have all of the necessary software files to re-install your previous base CICM software, upgrade, MRs, and patches into the node being rolled back.

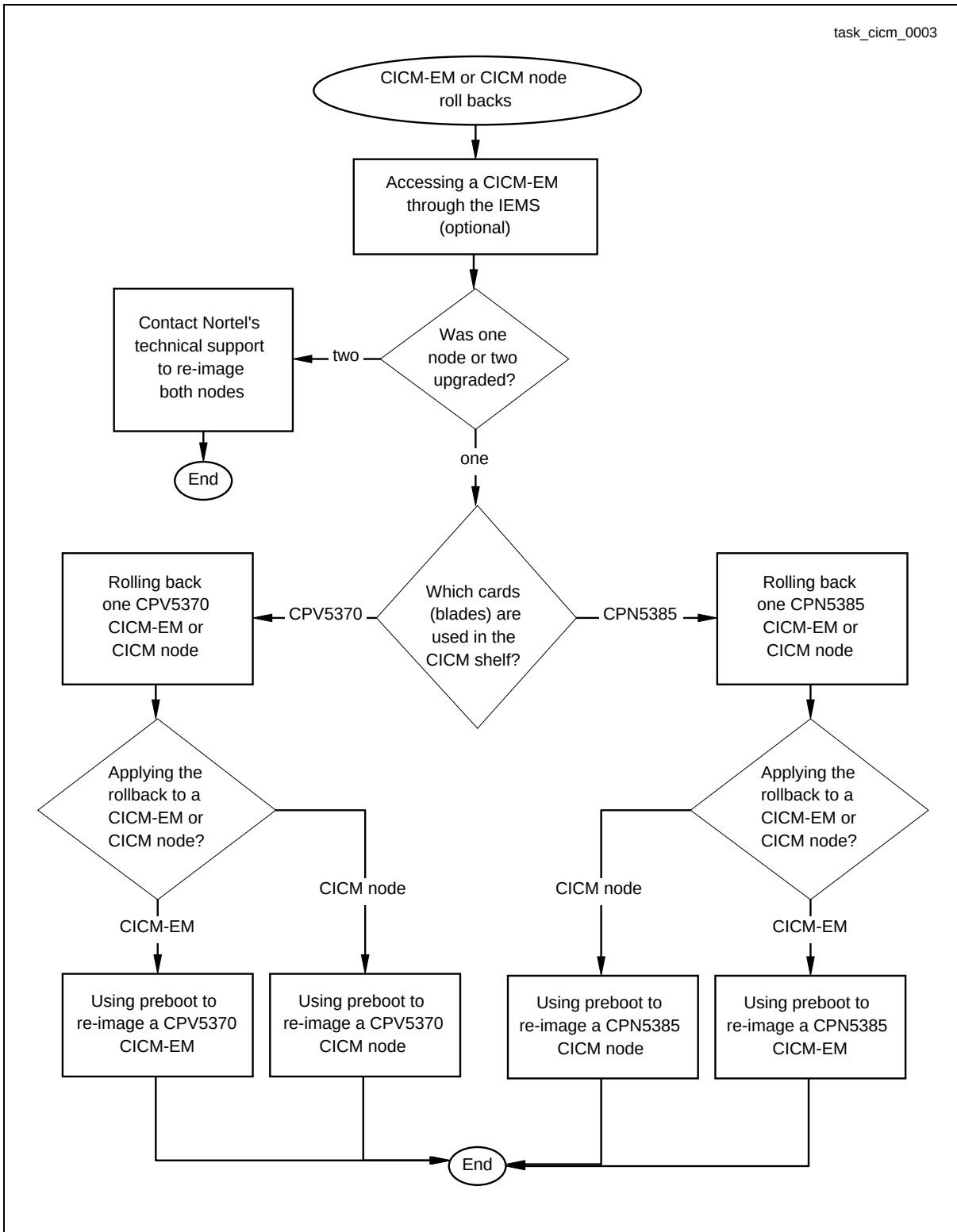
Also for a CPN5385, at the EM of the SAM 21 in the provisioning tab of the node's card view, verify that the image and load files can be located in the directory /data/swd/cicm on the CS2100 Management Tool server (also known as the SPFS server).

- Rolling back a CICM-EM node or a CICM node is basically reloading the base software onto the node, configuring software using command preboot, and waiting for data synchronization to occur. Details in the procedures may vary for the CICM-EM and a CICM node, but the rollback approach is essentially the same for either type of node.
- The task flow supports rolling back a node only on-site with the hardware (that is, it does not support doing a remote rollback). You need a console serial port available on each CPU card of the SAM 16 shelf (with CPV5370 cards) or SAM 21 shelf (with CPN5385 cards). The serial port is the access portal to the command prompt associated with each of the processors. If you are connecting your external personal computer (PC) to a CICM-EM card, then you will be accessing the command prompt for the CICM-EM through its serial port. If you are connecting your external personal computer (PC) to a CICM node card (using a null modem cable), then you will be accessing the command prompt for the CICM node through its serial port. The PC must have a hyperterminal software application.

- A CICM node must always be rolled back before either of its CICM-EMs.
- Since rolling back from an upgrade is a manual operation, start it during a period of lowest traffic for the CICM-EMs and CICM nodes unless it is due to system recovery.
- Once a rollback has been started, do not attempt any software configuration changes until each node-pair is confirmed to be fully in service according to the node's status and maintenance menus.
- When entering values for the command preboot, if you enter a typo you can exit the preboot sequence with keys Ctrl plus c, then re-enter the command preboot and scroll using the space bar to the last step of entry. Correct the typo and continue. Otherwise a captured error means you must re-image and re-do the preboot procedure.

### **Task flow of CICM-EM and CICM node rollbacks**

The task flow shows the sequence of procedures to roll back an upgraded CICM-EM or CICM node. The procedures are shown in the figure [Task flow of CICM-EM and CICM node rollbacks](#). To link any procedure, go to Navigation immediately following the figure.

**Task flow of CICM-EM and CICM node rollbacks**

## Navigation

The procedures in the task flow are listed alphabetically.

- “Accessing the CICM through the IEMS” in this document
- [Following up a rollback for IEMS](#)
- [Rolling back one CPN5385 CICM-EM or CICM node](#)
- [Rolling back one CPV5370 CICM-EM or CICM node](#)
- [Switching activity between CICM nodes for a rollback](#)
- [Transferring terminals for a rollback](#)
- [Using preboot to re-image a CPN5385 CICM node](#)
- [Using preboot to re-image a CPN5385 CICM-EM](#)
- [Using preboot to re-image a CPV5370 CICM node](#)
- [Using preboot to re-image a CPV5370 CICM-EM](#)

## Rollback procedures for CICM-EM and CICM nodes

The procedures for rolling back the software of a CICM-EM pair and its CICM node pairs are listed alphabetically in this section. The sequence of doing the procedures is identified in [Task flow of CICM-EM and CICM node rollbacks](#).

**Note:** You must follow the sequence of procedures identified in the task flow in order to properly complete rolling back.

## Following up a rollback for IEMS

Follow up a rollback by ensuring that the object properties of IEMS align with the software that each node pair is running.

### *At the IEMS interface*

- 1 If you already changed the object properties in the IEMS for the CICM network elements following an upgrade and prior to the rollback, re-edit the object properties to reflect the current software version. Refer to either of the procedures that follow to update the software version in the field Device Version:

- [Editing and viewing object properties using Java Web Start Client](#)
- [Editing and viewing object properties using Web Client](#)

With the Java Web Client, CICM uses v2c for the Version in the SNMP Details page.

- 2 This procedure is complete. Return to the procedure that sent you to this procedure.

## Rolling back one CPN5385 CICM-EM or CICM node

Roll back to the previous software of one CICM-EM or CICM node with CPN5385 CPU blades (cards) that was upgraded with an MR or product release.

### Prerequisites to rolling back one CPN5385 CICM-EM or CICM node

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM and CICM node rollbacks](#).
- Since upgrading a CICM node always starts with Node A, the rolling back applies to Node A. From the upgrade, Node A should already be the slave and not running terminal service.
- The CICM-EM can be either the master or the slave.

### Procedure steps to rolling back one CPN5385 CICM-EM or CICM node

#### *At an address window of the Internet*

- 1 Access the master or slave CICM-EM by entering:  
**http://<https\_IP\_address>/centrexip**

#### *At the page maintenance status (cicm-nnn)*

- 2 When rolling back a CICM node that has had a successful upgrade, followed by a successful SWACT and terminal transfer but has terminals that will not operate, transfer its terminals to its mate by using the procedure [Transferring terminals for a rollback](#). Do not transfer terminals for any other rollback.  
This step does not apply to a CICM-EM.

#### *At the page maintenance status (cicmem-nnn) or (cicm-nnn)*

- 3 Observe from the *Node Maintenance status* which nodes are master and slave.  
  
When rolling back a CICM node that has had a successful upgrade followed by a successful SWACT or that has had a successful upgrade followed by a successful SWACT and terminal transfer, but in either scenario has terminals that will not operate, ensure that Node A is the slave. If not, do the procedure [Switching activity between CICM nodes for a rollback](#) and return to this step.  
  
When rolling back a CICM-EM, it can be either master or slave.



***At the PC desktop for remote access to the CICM-EM***

- 4 Locally access the node being rolled back by:
  - connecting the serial port of your PC to the serial port of the CICM-EM or CICM blade (card)
  - starting the program hyperterminal on your PC
  - using hyperterminal to connect to the blade's console session

The Windows command prompt appears:

*login:*

- 5 Enter the userid of the node.
- 6 Enter the password of the node.

When access is successful, the command prompt is:

*C:\temp>*

- 7 Reset the node's bootflag by entering:

**cxippreboot /bootflag /clear**

When complete, the response is:

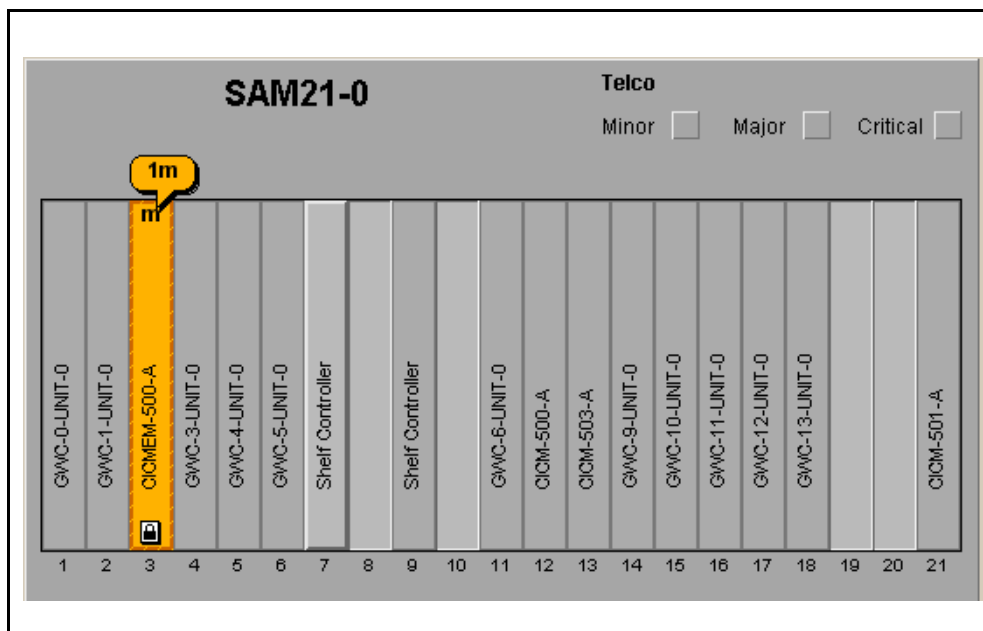
Active Boot Flag was Cleared Successfully.

***At the element manager for the SAM 21 shelf with CPN5385s***

- 8 Lock the node being rolled back by placing the cursor on the card, right-clicking, and selecting Lock.
- 9 Click on the card, then on the Provisioning tab and verify the Load name.

**Note:** Use a load version that has a backup file. If the load does not have a backup, it is recommended to apply any required MRs to bring the target node to the correct release and MR level.
- 10 Unlock the node being rolled back by placing the cursor on the card, right-clicking, and selecting Unlock.
- 11 Observe the change of states by right-clicking and selecting Card View.

The locked card turns orange and shows a padlock symbol.



12

**CAUTION****Risk of service interruption**

Wait until the unlocking has completed. Do not affect the state of the card (blade). If unlocking takes longer than 30 minutes, contact GNPS for help.

Wait for the node to fully unlock.

Unlocking is complete after the following *Card View... State History* is displayed and when the *Card View...* above changes to indicate that the card is fully in service.

**SAM21-0 : Slot 21**

Alarms | Equip | States | Provisioning |

OSI

Card Status:

Operational:

Availability:

History

Element Manager initiated Lock request received  
Resetting board  
Reset complete  
Application locked successfully  
Element Manager initiated Unlock request received  
Resetting board  
Reset complete  
Waiting for application to register  
Application unlocked successfully ←

- 13** This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Rolling back one CPV5370 CICM-EM or CICM node

Roll back to the previous software of one CICM-EM or CICM node with CPV5370 CPU blades (cards) that was upgraded with an MR or product release.

### Prerequisites to rolling back one CPV5370 CICM-EM or CICM node

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM and CICM node rollbacks](#).
- Since upgrading a CICM node always starts with Node A, the rolling back applies to Node A. From the upgrade, Node A should already be the slave and not running terminal service.
- The CICM-EM can be either the master or the slave.
- You must have Nortel Networks's CD available with the upgrade files for the same software release that the mate has (for example, 7.0 MR7). Refer to [Prerequisites to the task flow of CICM-EM and CICM node upgrades](#) for examples of CD labels.

### Procedure steps to rolling back one CPV5370 CICM-EM or CICM node

#### *At an address window of the Internet*

- 1 Access the master or slave CICM-EM by entering:  
**http://<https\_IP\_address>/centrexip**

#### *At the page maintenance status (cicm-nnn)*

- 2 When rolling back a CICM node, transfer its terminals to its mate by using the procedure [Transferring terminals for a rollback](#). (This does not apply to a CICM-EM.)

#### *At the page maintenance status (cicmem-nnn) or (cicm-nnn)*

- 3 Observe from the Node Maintenance status which nodes are master and slave.

When rolling back a CICM node, ensure that Node A is the slave. If not, do the procedure [Switching activity between CICM nodes for a rollback](#) and return to this step.

When rolling back a CICM-EM it can be either master or slave.

#### *At the SAM 16 shelf containing CPV5370 cards*

- 4 Open the drawer of the CD-ROM drive for Node A of the CICM-EM or CICM node being rolled back.

- 5** Place the CD of CICM-EM or CICM node software into the drawer. Avoid getting finger prints on the flat surfaces of the disk.
- 6** Close the drawer.
- 7** On node A's CPV5370 CPU card, press the small Reset button using a non-metallic stick (such as a tooth pick with a flat end).  
The LED next the CD-ROM drawer flashes amber to indicate loading (reboot) is in progress.
- 8** Wait for the CD-ROM drawer to automatically open when loading is complete.
- 9** Remove the disk and close the drawer again.
- 10** With the disk removed, press the Reset button again.
- 11** This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Switching activity between CICM nodes for a rollback

Switch the activity from the master CICM node to the slave node of the redundant pair.

### Prerequisites to switching activity between CICM nodes

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM and CICM node rollbacks](#) or use this procedure only when invoked from another procedure.
- Both nodes must be in-service to enable the switch of activity (SWACT) to occur.
- When an upgrade to the first node of a redundant pair does not succeed, do not use this procedure as part of the rollback. Use this procedure for all other rollbacks.

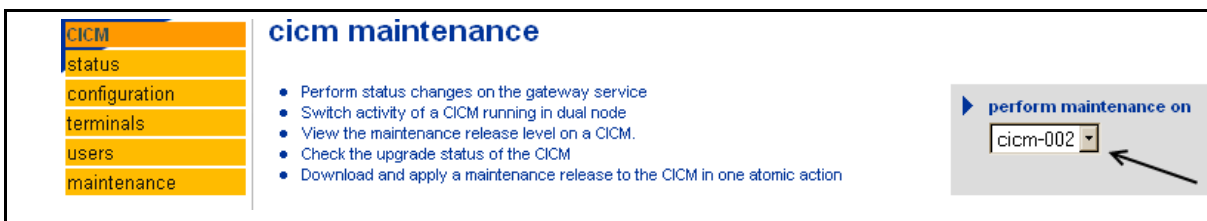
### Procedure steps to switching activity between CICM nodes

#### *At the home page of CICM*

- 1 In the menu CICM, click maintenance.

#### *At the page cicm maintenance*

- 2 From the pick-list, select the CICM node identifier.



- 3 Click perform maintenance on.
- 4 Observe from the Node Maintenance status of each node which ones are master and slave.

### maintenance status (cicm-002)

| Node A (47.135.43.18) <span style="float: right;">?</span> |                                                         |
|------------------------------------------------------------|---------------------------------------------------------|
| Status                                                     | slave ( running )                                       |
| Node Maintenance status                                    | system idle<br>(current reboot count: 0)                |
| Version                                                    | CICM 9.0 Maintenance Release 1<br>(Build 9.10.186)      |
| VMG Status                                                 | inactive ( <span style="color: green;">in sync</span> ) |
| Active Half Calls                                          | n/a                                                     |
| Terminal Status                                            | inactive ( <span style="color: green;">in sync</span> ) |
| Number of logged in users                                  | n/a                                                     |
| Active Terminals                                           | n/a                                                     |
| Terminal Recovery Status                                   | n/a                                                     |

| Node B (47.135.43.19) <span style="float: right;">?</span> |                                                          |
|------------------------------------------------------------|----------------------------------------------------------|
| Status                                                     | master ( running )                                       |
| Node Maintenance status                                    | system idle<br>(current reboot count: 0)                 |
| Version                                                    | CICM 9.0 Maintenance Release 1<br>(Build 9.10.186)       |
| VMG Status                                                 | active ( <span style="color: green;">in service</span> ) |

**maintenance release management**

Node Node A (47.135.43.18)

---

**patch management**

Node Node A (47.135.43.18)

---

**node A service control**

Action Stop

---

**node B service control**

Action Stop

---

**switch activity**

---

**reset counter**

Node Node A

Reset Counter Current Reboot Count

**5** Click switch activity.

The duration of the switchover varies according to the number of users configured on the nodes and the volume of calls being sustained in the node at the time of the SWACT.

When both nodes are not available for a SWACT, the command button is tinted grey and disabled. Ensure that both nodes are in service.

**6** Click Confirm switch of activity.

**7** Confirm from the Node Maintenance status that CICM Node A is the slave and they have switched successfully.

If not, then contact your next level of support to determine why.

**8** This procedure is complete. Return to the step in the procedure from where you came:

- [step 3](#) in [Rolling back one CPN5385 CICM-EM or CICM node](#)
- [step 3](#) in [Rolling back one CPV5370 CICM-EM or CICM node](#)

## Transferring terminals for a rollback

Transfer the terminals (clients) from one node to another to ensure that service can be restored.

### Prerequisites to transferring terminals for a rollback

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM and CICM node rollbacks](#) or use this procedure only when invoked from another procedure.
- Have a working CICM terminal (for example, an m6350 or IP Phone 200x) available to test the operation of a rolled back node.
- Do not use this procedure as part of the rollback:
  - when an upgrade to the first node of a redundant pair fails
  - when operational tests fail after the SWACT that follows a successful upgrade
  - The section “Terminal transfers” and the procedure “Perform a terminal transfer” in *CICM Security and Administration*, NN10252-611.



#### CAUTION

##### Risk of service loss

Do not attempt to abort a terminal transfer during a rollback. Aborting may cause the terminals to hang without a connection.

### Procedure steps to transferring terminals for a rollback

#### *At the page maintenance status (cicm-nnn)*

- 1 On the right menu, ensure that start auto refresh is showing, but do not click it.

If stop auto refresh is shown, click it to show start auto refresh.





- 2 When rolling back a CICM node, which is always node A, transfer its terminals to the mate by clicking from node A to node B at the Node pick-list menu.
- 3 From the Terminal Shutdown Timeout pick-list menu, select the minutes. The minutes indicate to a CICM clients how much time they have before they are automatically affected by the transfer. When rolling back they are transferred without having to log off.
- 4 Click transfer terminals.
- 5 When the confirmation screen appears, click confirm terminal transfer.

*The terminal transfer will commence immediately upon confirmation, and will terminate when the selected timeout interval has expired.*

- 6 Click start auto refresh of the page maintenance status (cicm-nnn).

The button stop auto refresh appears.

**Note:** In *CICM Security and Administration*, NN10252-611 the section “Terminal handover” and the procedure “Perform a terminal handover” provide details on terminal handovers.

Observe that portions of the terminal statuses for Nodes A and B are greyed out during the transfer.

| Node B (47.135.154.40) ?  |                                                    | Node A (47.135.154.40) |                      |
|---------------------------|----------------------------------------------------|------------------------|----------------------|
| Node status               | slave                                              | Action                 | Stop                 |
| Service Status            | running                                            | ▶ switch activity      |                      |
| Node Maintenance status   | system idle<br>(current reboot count: 0)           | ▶ reset counter        |                      |
| Version                   | CICM 7.0 Maintenance Release 4<br>(Build 7.20.177) | Node                   | Node A               |
| VMG Status                | inactive ( in sync )                               | Reset Counter          | Current Reboot Count |
| Active Half Calls         | n/a                                                | ▶ stop auto refresh    |                      |
| Terminal Status           | inactive ( Started )                               | ▶ refresh now          |                      |
| Number of logged in users | n/a                                                | ▶ system status        |                      |
| Active Terminals          | n/a                                                |                        |                      |
| Terminal Recovery Status  | n/a                                                |                        |                      |

7

**CAUTION****Risk of service interruption**

Wait until the terminal transfer has completed before proceeding. If the transfer does not complete, discontinue the procedure and contact your next level of technical support to determine your next actions.

When the terminals have transferred, all should be hosted on CICM Node B. Completion of the transfer is indicated by stopped or inactive appearing for Terminal status.

| Node B (47.135.154.40) ?          |                                                    |
|-----------------------------------|----------------------------------------------------|
| Node status                       | master ←                                           |
| Service Status                    | running                                            |
| Node Maintenance status           | system idle<br>(current reboot count: 0)           |
| Version                           | CICM 7.0 Maintenance Release 4<br>(Build 7.20.177) |
| <a href="#">Active Half Calls</a> | 0 (total calls=0)                                  |
| Terminal Service                  | started                                            |
| Number of logged in users         | 1 (total logins=5)                                 |
| <a href="#">Active Terminals</a>  | 1 ↗                                                |

- 8 Have the telco test the operation of each CICM terminal on the node that is supposed to have them connected. Ensure that all terminals are registered on the node. A registered terminal means the S1 and S2 addresses point to the floating UNISim IP address.

If the tests fail, contact your next level of support to determine your next actions.

- 9** This procedure is complete. Return to the step in the procedure from where you came:
- [step 2](#) in [Rolling back one CPN5385 CICM-EM or CICM node](#)
  - [step 2](#) in [Rolling back one CPV5370 CICM-EM or CICM node](#)

## Using preboot to re-image a CPN5385 CICM node

Use preboot to re-image a CICM node with CPN5385 CPU blades (cards) to a base CICM software release.

### Prerequisites to using preboot to re-image a CPN5385 CICM node

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM and CICM node rollbacks](#).
- When the CICM node's software has been restored, its data is automatically synchronized with the mate CICM node.
- Output from the progression of preboot is shown by `this font`. Command entries are shown by **this font**.
- When more appears on the screen, press the keyboard spacebar to advance the screen.



#### CAUTION

##### Risk of service prevention

Using preboot means re-entering specific configuration data that would normally be handled by an initial installation. While configuring, extreme care must be taken to ensure accurate entries especially with IP addresses.

### Procedure steps to using preboot to re-image a CPN5385 CICM node

#### *At the PC desktop for remote access to the CICM node*

- 1 Locally access CICM Node A through the console serial port.
- 2 Pressing enter in the terminal window will eventually get the login prompt.  
`login:`
- 3 For the userid enter Administrator and for the password enter Administrator.  
The screen prompt becomes:  
`C:\Documents and Settings\Administrator>`
- 4 At the command line interface (CLI) of a Windows XP session, enter:  
**preboot**
- 5 Press CTRL-C at any prompt to abort preboot.  
Press ENTER now to start preboot configuration.

This CICM-EM is Node A.

Press enter to start *preboot*.

- 6** STEP 1: Configure BOOTP options (CPV5370 ONLY)  
Skipping option bootp (skip configured in mib)  
No user input is required. The output indicates CPV5370 even though this is a CPN5385 procedure.

- 7** STEP 2: Configure IPsec

This step configures IPsec. You will be prompted for the IPsec pre-shared key. This is the key that is used to connect to the IPsec protected ports on the CICM[EM]. A hash of this pre-shared key will be used for the software account (comuser) password. It is important to remember the pre-shared key entered, as this key **MUST** be the same on both the CICM and the CICM EM. The IPsec step can only be run once.

To re-key IPsec use the following command:

```
preboot ipsec /rekey
```

Enter the IPsec Pre-Shared Key:

**<customer\_configuration\_password>**

Record the pre-shared key (password) for your records.

Re-enter to confirm:

**<customer\_configuration\_password>**

Secure the telnet port? [Y|N, default=Y]:

**N**

At this point in the configuration, Nortel Networks recommends not securing the telnet port. It can be configured later after the rollback is completed.

- 8** STEP 3: Configure the gateway type

This Gateway is automatically set up in a H248 configuration. Gateway configured to support H248.

No user input is required.

- 9** STEP 4: Configure the workgroup and computer name

The CICM/CICM-EM can operate in either a single or dual node configuration. In a dual node configuration, the CICM/CICM-EM has two nodes,

A and B. The two nodes belong to a unique workgroup. The node(s) will be named as the workgroup name with an '-A' (or '-B' appended). In a single node configuration, only node A can be installed. It's name will be the workgroup name with an '-A' appended.

No user input is required.

**10** STEP 5: Configure the administration accounts

The CICM and the CICMEM both have a Administration Account. The preboot section is used to configure this account.

Enter the local Administrator account password:

**<customer\_configuration\_password>**

The password (up to 8 alphanumeric characters) can be different than the one you specified earlier for the pre-shared key. Record the password for your records.

Re-enter to confirm:

**<customer\_configuration\_password>**

**11** STEP 6: Configure the software user account

The CICM/CICM-EM use a single security [aka COMUSER] account under which all software is executed. This account should be configured with the same username and password on each system (CICM-EMs and CICMs).

NOTE: this account should \*NOT\* be used for interactive logins.

The /display option will display the comuser password [only do this over a secure connection]. Note that this will display the auto-generated password based on the IPSec pre-shared key (which you must re-enter). If you enter the wrong key then an incorrect software account password will be displayed.

Enter a username under the software will run (hit ENTER to accept "COMUSER"):

**<customer\_userid>**

Nortel Networks recommends you press enter to accept the default value of *COMUSER* as the userid for the COMUSER account. Note that the CICM-EM and all subtending CICM nodes must have the same COMUSER userid. Record the userid for your records.

Software account successfully configured.

**12** STEP 7: Configure the Static adapter settings

This section creates and configures the 'Static' LAN Adapters. There are two static adapters per node - A1/A2 and B1/B2. Each has a single IP address. Heartbeat messages are sent between the addresses on A and the addresses on B. These addresses are restricted to the CICM and they must be in a distinct subnet from any other addresses used on the CICM or in the network in general.

Enter Admin VLAN id [1...4094, default=2]:

**<customer\_admin\_vlan\_value>**

Enter H248 VLAN id [1...4094, default=4]:

**<customer\_h248\_vlan\_value>**

The static addresses have been autogenerated based on the system ID of <specified in provisioning tab for CICM node at SAM 21 Element Manager>.

The base address is <auto generated IP address> and will be used to create a subnet range with mask 255.255.255.248.

Do you wish to use the base address? [Y|N, default=Y]

**<customer\_static\_address>**

Nortel Networks recommends entering Y (yes) to accept it provided the auto-generated address does not conflict with an existing IP address in the network. Entering N (no) means you must provide the valid static address values.

**13** STEP 8: Configure the Unistim LAN settings

This section configures the CICM's Unistim LAN adapter. The Unistim LAN is used for call signalling between CICM and its clients (terminals). The LAN's port filter only permits those UDP ports used to communicate with clients. [OAMP functions are blocked on the Unistim LAN.]

Enter Unistim VLAN id [1...4094, default=3]:

**<unistim\_vlan\_id>**

Enter the Unistim IP address for this node:

**<unistim\_static\_ip\_address\_for\_the\_node>**

Enter the network mask for the Unistim IP network:

**<network\_mask\_for\_unistim\_ip\_network>**

Enter the default route for the Unistim IP network (Enter 0.0.0.0 for no route):

**<default\_route\_for\_unistim\_ip\_network>**

Enter a no route only if you do not have a default and you understand the consequences of not having one.

#### 14 STEP 9: Configure the H248 LAN settings

This section configures the H248 floating adapter. The floating H248 IP address will be bound to the A4/B4 adapter on whichever CICM node is Master. Therefore, datafill the same address on each node. This address will be used for all communication with the Gateway Controller and should match the Media Gateway IP Address provisioned for the CICM on the Gateway Controller EM.

Enter the Floating H248 IP address for this CICM:

**<floating\_h248\_ip\_address\_for\_cicm>**

Enter the Static H248 IP address for Node A:

**<static\_h248\_ip\_address\_for\_node\_A>**

Enter the Static H248 IP address for Node B:

**<static\_h248\_ip\_address\_for\_node\_B>**

Enter the network mask for the H248 IP network:

**<network\_mask\_for\_h248\_ip\_network>**

Enter the default route for the H248 IP network (Enter 0.0.0.0 for no route):

**<default\_route\_for\_h248\_ip\_network>**

Enter a no route only if you do not have a default and you understand the consequences of not having one.

#### 15 STEP 10: Configure the VMG settings

This step configures the Virtual Media Gateway. The CICM can support up to 3069 lines (up to 1023



on the 5370 hardware) [for Nortel Networks testing purposes \*ONLY\*, a lower value may be entered.]

WARNING - in a dual node configuration, the number of lines must be datafilled the same on both nodes of the CICM.

To re-size the VMG to the maximum number of lines use the following command:

```
preboot vmg /resize
```

Enter the number of lines for the gateway  
[1...3069, default=3069]:

Nortel Networks recommends you accept the default number of lines.

**<number\_of\_lines\_for\_the\_gateway>**

Enter the Media Gateway Controller IP address:

**<media\_gateway\_controller\_ip\_address>**

Enter the Media Gateway Controller UDP port  
[0...65535, default=2944]:

**<media\_gateway\_controller\_udp\_port>**

**16** STEP 11: Configure the Floating Admin adapter settings

This section configures the Floating Admin adapter information. The floating Admin IP address will be bound to the most available interface on the Gateway node.

Enter the Node A Admin address:

**<node\_A\_admin\_address>**

Enter the Node B Admin address:

**<node\_B\_admin\_address>**

Enter the network mask for the Admin IP network:

**<network\_mask\_for\_admin\_ip\_network>**

Enter the default router for the Admin IP network:

**<default\_router\_for\_admin\_ip\_network>**

**17** STEP 12: Configure the SNMP settings

**<customer\_snmp\_configuration>**

Configure the *SNMP settings* by entering your configuration values or if not using SNMP, press enter to accept all the default values. The progression of information is not shown in this step.

... ---Finished

**18** STEP 13: Configure the time settings for the gateway

You can use this utility to set the time and time zone on the CICM. It will inform any running software of the time change.

Current time zone is n.n hours from GMT (GMT Standard Time).

Daylight time zone is n.n hours from GMT (GMT Daylight Time)

Do you want to change it [Y|N, default=N]:

Entering **Y** presents a choice of time zones. Select the time zone by entering the number associated with it or press enter to accept the default.

**Y**

Current local date is <value>.

Do you want to change it [Y|N, default=N]:

Enter **N** to accept the local date or enter **Y** to change it. After **Y**, answer the prompts to specify the day, month, and year.

**Y**

Current local time is <value>.

Do you want to change it [Y|N, default=N]:

Enter **N** to accept the local time or enter **Y** to change it. After **Y**, answer the prompts to specify the hours and minutes.

**Y**

Current time for scheduled backups is 02:00.

Do you want to change it [Y|N, default=N]:

Accept the default or configure a different time to schedule the automatic backup of the software image by entering **Y** (yes), then a 24-hour time as <hh:mm>.

**N**

**19** STEP 14: Configure the Hard disk

No user input is required.

The CICM and CICM-EM have two disk partitions, C: and D:. These must be converted to the NTFS file system.

Setting system to convert C: and D: to NTFS file system on next boot.

**20** STEP 15: Apply the CICM software load

Apply the default software image to the Gateway.

Wait while preboot configures the software. The progression of information is not shown in this step.

... Registry Flush Complete.

A reboot must now be performed to complete installation. Do you want to restart now? [Y|N, default=N]:

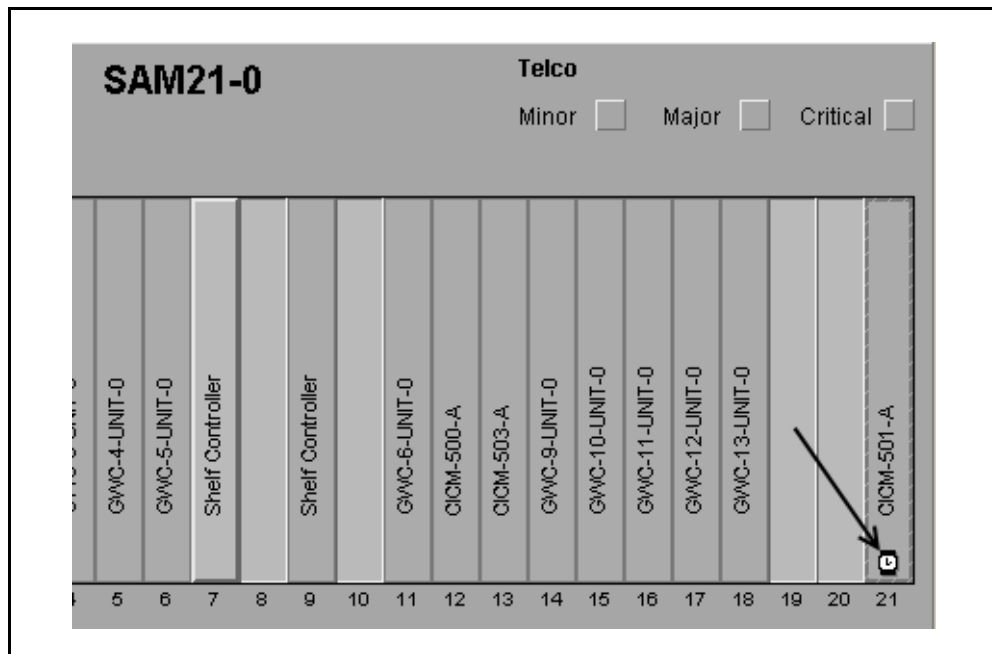
**Y**

The computer is shutting down .....  
Console disconnected.

***At the element manager for the SAM 21 shelf with CPN5385s***

**21** At the GUI of the SAM 21 EM, place the cursor on the card, right-click, and select Card View.

The rebooting card shows a watch symbol, which appears three times.



Rebooting is complete when the watch symbol disappears and the card State History (right-click) indicates

Application initiated reset completed successfully.

***At the page maintenance (cicm-nnn)***

- 22** Wait for the node to synchronize data with its mate node. While waiting, click refresh now.

When synchronized, the node is fully in service as shown by the status system idle or system running.

Node B shows active terminals if they were active before Node A was reloaded.

| Node B (47.135.154.40) <span>?</span> |                                                    |
|---------------------------------------|----------------------------------------------------|
| Node status                           | master ←                                           |
| Service Status                        | running                                            |
| Node Maintenance status               | system idle<br>(current reboot count: 0)           |
| Version                               | CICM 7.0 Maintenance Release 4<br>(Build 7.20.177) |
| <a href="#">Active Half Calls</a>     | 0 (total calls=0)                                  |
| Terminal Service                      | started                                            |
| Number of logged in users             | 1 (total logins=5)                                 |
| <a href="#">Active Terminals</a>      | 1 ↗                                                |

- 23** Apply additional MRs and patches as needed to restore the node to the same MR level as its mate node.

Refer to the procedures:

- [Upgrading a CICM node with an MR](#)
- [Upgrading a CICM-EM with an MR or product release](#)

***At the maintenance status (cicm-nnn)***

- 24** Verify the CICM node pair is fully in service.
- 25** Leave the CICM terminals on Node B, the active master.

***At the PC desktop for remote access to the CICM node***

- 26** Locally access CICM Node A through the console serial port.
- 27** At the prompt, log in.

login:

For the userid enter Administrator and for the password enter Administrator.

The screen prompt becomes:

C:\Documents and Settings\Administrator>

- 28** At the CLI of a Windows session, you apply your SNMP data to enable a connection with IEMS by entering:

**preboot snmp /interactive**

***At the IEMS interface***

- 29** If you edited the object properties of IEMS for an upgrade to a CICM-EM or a CICM node, do the procedure [Following up a rollback for IEMS](#).
- 30** This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Using preboot to re-image a CPN5385 CICM-EM

Use preboot to re-image a CICM-EM with CPN5385 CPU cards (blades) to a base CICM-EM software release.

### Prerequisites to using preboot to re-image a CPN5385 CICM-EM

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM and CICM node rollbacks](#).
- When the CICM-EM's software has been restored, its data is automatically synchronized with the mate EM.
- Output from the progression of preboot is shown by `this font`. Command entries are shown by **this font**.
- When more appears on the screen, press the keyboard spacebar to advance the screen.



#### CAUTION

##### Risk of service prevention

Using preboot means re-entering specific configuration data that would normally be handled by an initial installation. While configuring, extreme care must be taken to ensure accurate entries especially with IP addresses.

### Procedure steps to using preboot to re-image a CPN5385 CICM-EM

#### *At the PC desktop for remote access to the CICM-EM*

- 1 Locally access Node A through the console serial port.
- 2 Pressing enter in the terminal window will eventually get the login prompt.  
`login:`
- 3 For the userid enter Administrator and for the password enter Administrator.
- 4 At the command line interface (CLI) of a Windows 2000 session, enter preboot.
- 5 Press CTRL-C at any prompt to abort preboot.  
Press ENTER now to start preboot configuration.  
`This CICM-EM is Node A.`  
Press enter to start *preboot*.
- 6 Wait while preboot starts.

- STEP 1: Configure BOOTP options (CPV5370 ONLY)  
Skipping option bootp (skip configured in mib).
- 7** STEP 2: Configure SSH
- Access to the CICM EM may be achieved either by using a secured SSH connection or via the EM's serial port. SSH keys are generated during this step (which takes some time). On completion the SSH fingerprint will be displayed. Use this fingerprint for server validation when connecting to the CICM EM. Do not trust any other fingerprint.
- To display the SSH fingerprint after the SSH step use the following:  
preboot ssh /fingerprint  
Generating SSH keys ...  
...  
The CICM EM SSH Fingerprint is:  
<fingerprint\_code>  
Press ENTER to continue.  
SSH Configuration Complete.
- Complete configuring the *SSH* by pressing enter.
- 8** Flushing Registry Data...  
Registry Flush Complete.
- A reboot must now be performed to complete installation. Do you want to restart now? [Y|N, default=N]:
- Y**
- Rebooting now...
- The following prompt appears and then lockout occurs.
- C:\>
- 9** Pressing enter in the terminal window will eventually get the login prompt.
- login:
- 10** For the userid enter *Administrator* and for the password enter *Administrator*.
- The screen prompt becomes:
- C:\Documents and Settings\Administrator>



- 11 At the command line interface (CLI) of a Windows XP session, enter:
- preboot**
- 12 Press CTRL-C at any prompt to abort preboot. Press ENTER now to start preboot configuration. This CICM-EM is node A.
- Press enter to start *preboot*.
- 13 STEP 1: Configure BOOTP options (CPV5370 ONLY)  
Skipping option bootp (skip configured in mib).  
STEP 3: Configure SSH  
Skipping option ssh (already complete).
- 14 STEP 3: Configure IPsec
- This step configures IPsec. You will be prompted for the IPsec pre-shared key. This is the key that is used to connect to the IPsec protected ports on the CICM[EM]. A hash of this pre-shared key will be used for the software account (comuser) password.
- It is important to remember the pre-shared key entered, as this key **MUST** be the same on both the CICM and the CICM EM. The IPsec step can only be run once.
- To re-key IPsec use the following command:  
preboot ipsec /rekey  
...
- NB: <cicmname> must be identical to the name specified in the /permitcicm.
- Enter the IPsec Pre-Shared Key:
- <customer\_configuration\_password>**
- Record the pre-shared key (password) for your records.
- Re-enter to confirm:
- <customer\_configuration\_password>**
- Secure the telnet port? [Y|N, default=Y]:
- N**
- At this point in the configuration, Nortel Networks recommends not securing the telnet port. It can be configured later after the rollback is completed.

- 15** STEP 4: Configure the workgroup and computer name

No user input is required.

The CICM/CICM-EM can operate in either a single or dual node configuration. In a dual node configuration, the CICM/CICM-EM has two nodes, A and B. The two nodes belong to a unique workgroup. The node(s) will be named as the workgroup name with an '-A' (or '-B' appended). In a single node configuration, only node A can be installed. It's name will be the workgroup name with an '-A' appended.

Setting machine name to CICMEM-nnn-A.  
Configuring node A [CICMEM-nnn-A].  
Configuring node B [CICMEM-nnn-B].  
Setting workgroup name to CICMEM-nnn.

- 16** STEP 5: Configure the administration accounts

The CICM and the CICMEM both have an Administration Account. The preboot section is used to configure this account.

Enter the local Administrator account password:

**<customer\_configuration\_password>**

The password (up to 8 alphanumerical characters) can be different than the one you specified earlier for the pre-shared key. Record the password for your records.

Re-enter to confirm:

**<customer\_configuration\_password>**

Successfully set administrator password.

- 17** STEP 6: Configure the software user account

The CICM/CICM-EM use a single security [aka COMUSER] account under which all software is executed. This account should be configured with the same username and password on each system (CICM-EMs and CICMs).

NOTE: this account should \*NOT\* be used for interactive logins.

The /display option will display the comuser password [only do this over a secure connection]. Note that this will display the auto-generated password based on the IPSec pre-shared key (which you must re-enter). If you

enter the wrong key then an incorrect software account password will be displayed.

Enter a username under which the software will run (hit ENTER to accept "COMUSER"):

**<customer\_userid>**

Nortel Networks recommends you press enter to accept the default value of *COMUSER* as the userid for the COMUSER account. Note that the CICM-EM and all subtending CICM nodes must have the same COMUSER userid. Record the userid for your records.

Using default account name "comuser".  
Creating user account.  
Configuring user group.  
Setting user account expiry to UNLIMITED.  
Setting failed login attempts to UNLIMITED.  
Configuring access permissions.  
Configuring launch permissions.  
Configuring logon rights.  
Configuring applications.....  
Installing cxippreboot.  
Reinstalling cxippreboot.  
Software account successfully configured.

**18** STEP 7: Configure the element manager environment

No user input is required.

The Element Manager has additional data that needs to be set [EM domain/machine names, DCOM protocols preferences etc].

Setting up Element Manager environment.

Setting up DCOM protocols.

WARNING: An important change was made to DCOM protocols preferences. You MUST reboot after install has finished to make the changes take effect.

Element Manager environment successfully configured.

**19** STEP 8: Configure the Static adapter settings

This section creates and configures the 'Static' LAN Adapters. There are two static adapters per node - A1/A2 and B1/B2. Each has a single IP address. Heartbeat messages are sent between the addresses on A and the addresses on B. These addresses are restricted to the CICM-EM and they

must be in a distinct subnet from any other addresses used on the CICM-EM or in the network in general.

The static addresses have been autogenerated based on the system ID of nnn.

The base address is <auto\_generated\_IP\_address> and will be used to create a subnet range with mask 255.255.255.248.

Do you wish to use the base address? [Y|N, default=Y]

**<customer\_static\_address>**

Nortel Networks recommends entering **Y** (yes) to accept it provided the auto-generated address does not conflict with an existing IP address in the network. Entering **N** (no) means you must provide the valid static address values.

Configuring A1

Configuring A2

Configuring B1

Configuring B2

Configuring RPC...

[SC] ChangeServiceConfig SUCCESS.

## **20** STEP 9: Configure the Floating Admin adapter settings

This section configures the Floating Admin adapter information. The floating Admin IP address will be bound to the most available interface on the Element Manager node.

Enter the Node A Admin address:

**<node\_A\_admin\_address>**

Enter the Node B Admin address:

**<node\_B\_admin\_address>**

Enter the network mask for the Admin IP network:

**<network\_mask\_for\_admin\_ip\_network>**

Enter the default router for the Admin IP network:

**<default\_router\_for\_admin\_ip\_network>**

Configuring PA

Configuring PB

Configuring route for A1

Configuring route for A2

**21** STEP 10: Configure the Floating Http adapter settings

This section configures the HTTP floating adapter information. The floating HTTP address will be bound to the most available adapter on whichever node of the CICM-EM is the Master. Therefore the same address should be datafilled on each CICM-EM node. The address will be used for all Web Browser communication.

Enter the Http IP address for this CICM-EM:

**<http\_ip\_address\_for\_cicmem>**

**22** STEP 10: Configure PAM authentication

Will this CICM-EM use PAM to authenticate users? [Y|N, default=N]:

Enter **Y** (yes) to enable PAM authentication or **N** (no). With **Y** you must answer the prompts to configure PAM data (for example, the proxy server). With **N** the response is:

The Element Manager will use local NT authentication.

**23** STEP 12: Configure the SNMP settings

The Element Manager can be managed remotely by an SNMP management station. Most of the data accessible via SNMP is derived directly from the CentrexIP internal MIB but certain data must be entered during initial configuration. This data includes ...

**<customer\_snmp\_configuration>**

Configure the *SNMP settings* by entering your configuration values or if not using SNMP, press enter to accept all the default values. The progression of information is not shown in this step.

Are you satisfied with the above responses [Y|N, default=Y]:

Enter **Y** (yes) to accept or **N** (no) to make changes.

--- Starting

--- Looking up system description from host OS

--- ...

--- Finished

**24** STEP 13: Configure the time settings for the EM

You can use this utility to set the time and time zone on the EM.

Current time zone is n.n hours from GMT (GMT Daylight Time).

Standard zone is n.n hours from GMT (GMT Standard Time)

Do you want to change it [Y|N, default=N]:

Entering **Y** presents a choice of time zones. Select the time zone by entering the number associated with it or press enter to accept the default.

**Y**

Current local date is <value>.

Do you want to change it [Y|N, default=N]:

Enter **N** to accept the local date or enter **Y** to change it. After **Y**, answer the prompts to specify the day, month, and year.

**Y**

Current local time is <value>.

Do you want to change it [Y|N, default=N]:

Enter **N** to accept the local time or enter **Y** to change it. After **Y**, answer the prompts to specify the hours and minutes.

**Y**

Current time for scheduled backups is 02:00.

Do you want to change it [Y|N, default=N]:

Configure a different time to schedule the automatic backup of the software image by entering **Y** (yes), then a 24-hour time as <hh:mm>.

**N**

Found NTP Server Configuration: -

Primary NTP Server Address = <ip\_address>

Backup NTP Server Address = <ip\_address>

Configuring W32Time Service with NTP Server parameters...

Successfully configured NTP Server Parameters

## 25 STEP 14: Configure the Hard disk

No user input is required.

The CISM and CISM-EM have two disk partitions, C: and D:. These must be converted to the NTFS file system.

Setting system to convert C: and D: to NTFS file system on next boot.

**26** STEP 15: Apply the EM software load

Apply the default software image to the Element Manager.

Registering {...

Wait while preboot configures the software. The progression of information is not shown in this step.

... Registry Flush Complete.

A reboot must now be performed to complete installation. Do you want to restart now? [Y|N, default=N]:

**Y**

Rebooting now...

Temporary lockout occurs at the command prompt.

***At the page maintenance cicmem-nnn***

**27** Wait for the node to synchronize data with its mate node.

When synchronized, the node is fully in service as shown by the status system idle or system running.

**28** Apply additional MRs and patches as needed to restore the node to the same MR level as its mate node.

Refer to the procedures:

- [Upgrading a CICM node with an MR](#)
- [Upgrading a CICM-EM with an MR or product release](#)

**29** Verify the CICM-EM pair is fully in service.

***At the PC desktop for remote access to the CICM node***

**30** Locally access CICM Node A through the console serial port.

**31** At the prompt, log in.

login:

For the userid enter Administrator and for the password enter Administrator.

The screen prompt becomes:

C:\Documents and Settings\Administrator>

- 32** At the CLI of a Windows session, you apply your SNMP data to enable a connection with IEMS by entering:

**preboot snmp /interactive**

***At the IEMS interface***

- 33** If you edited the object properties of IEMS for an upgrade to a CICM-EM or a CICM node, do the procedure [Following up a rollback for IEMS](#).
- 34** This procedure is complete. Return to the task flow or procedure that sent you to this procedure.



## Using preboot to re-image a CPV5370 CICM node

Use preboot to re-image a CICM node with CPV5370 CPU cards (blades) to a base CICM software release.

### Prerequisites to using preboot to re-image a CPV5370 CICM node

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM and CICM node rollbacks](#).
- When the CICM node's software has been restored, its data is automatically synchronized with the mate EM.
- Output from the progression of preboot is shown by `this font`. Command entries are shown by **this font**.
- When more appears on the screen, press the keyboard spacebar to advance the screen.



#### CAUTION

##### Risk of service prevention

Using preboot means re-entering specific configuration data that would normally be handled by an initial installation. While configuring, extreme care must be taken to ensure accurate entries especially with IP addresses.

### Procedure steps to using preboot to re-image a CPV5370 CICM node

#### *At the PC desktop for remote access to the CICM-EM*

- 1 Locally access Node A through the console serial port.
- 2 Pressing enter in the terminal window will eventually get the login prompt.  
`login:`
- 3 For the userid enter Administrator and for the password enter Administrator.
- 4 At the command line interface (CLI) of a Windows XP session, enter:  
**preboot**
- 5 Press CTRL-C at any prompt to abort preboot. Press ENTER now to start preboot configuration.  
Press enter to start *preboot*.
- 6 Is this node A of the CICM? [Y|N, default=Y]:

Ensure that you are prebooting node A and enter **Y** (yes).

**7 STEP 1: Configure BOOTP options (CPV5370 ONLY)**

BOOTP Settings must be entered by the craftsperson for CPV5370 CPUs since network BOOTP is only possible on hardware installed in a SAM 21 chassis i.e. CPN5385 slave CPUs. This is a CICM Node. The identifier (name) for this node has the format CICM-000-X where 000 is the numeric system identifier for this node and its mate node and X is the node identifier and can be either 'A' or 'B'.

Enter the 3 digit system identifier for this chassis [range 000-511]:

**<3\_digit\_system\_identifier>**

Node name recorded as CICM-nnn-A.

Enter the Public Admin Network IP Address for this node:

**<public\_admin\_network\_ip\_address\_for\_cicm>**

Enter the Public Admin Network Subnet mask for this node:

**<public\_admin\_network\_subnet\_mask\_for\_cicm>**

Enter the default route for the Public Admin Network (Enter 0.0.0.0 for no route):

**<default\_route\_for\_public\_admin\_network>**

Enter a no route only if you do not have a default and you understand the consequences of not having one.

Enter the Primary NTP Server IP Address:

**<primary\_ntp\_server\_ip\_address>**

Enter the Secondary NTP Server IP Address:

**<secondary\_ntp\_server\_ip\_address>**

Enter the Primary EM IP Address:

**<primary\_em\_ip\_address>**

Enter the Backup EM IP Address for the public admin network. (Enter 0.0.0.0 for no Backup EM):

**<backup\_em\_ip\_address\_for\_public\_admin\_net>**

Flushing Registry Data...  
Registry Flush Complete.

- 8** A reboot must now be performed to complete installation. Do you want to restart now? [Y|N, default=N]:

**Y**

Rebooting now...

- 9** Pressing enter in the terminal window will eventually get the login prompt.

login:

- 10** For the userid enter *Administrator* and for the password enter *Administrator*.

The screen prompt becomes:

*C:\Documents and Settings\Administrator>*

- 11** At the command line interface (CLI) of a Windows XP session, enter:

**preboot**

- 12** Press CTRL-C at any prompt to abort preboot. Press ENTER now to start preboot configuration.

Press enter to start *preboot*.

This CICM is node A.

- 13** STEP 1: Configure BOOTP options (CPV5370 ONLY)  
Skipping option bootp (already complete).

No user input is required.

- 14** STEP 2: Configure IPsec

This step configures IPsec. You will be prompted for the IPsec pre-shared key. This is the key that is used to connect to the IPsec protected ports on the CICM[EM]. A hash of this pre-shared key will be used for the software account (comuser) password. It is important to remember the pre-shared key entered, as this key **MUST** be the same on both the CICM and the CICM EM. The IPsec step can only be run once.

To re-key IPsec use the following command:

preboot ipsec /rekey

To toggle the security setting of telnet use the following command

preboot ipsec /telnet

To deactivate the ipsec policy:

preboot ipsec /deactivate

```
To re activate the ipsec policy:
preboot ipsec /activate
```

Enter the IPSec Pre-Shared Key:

**<customer\_configuration\_password>**

Record the pre-shared key (password) for your records.

Re-enter to confirm:

**<customer\_configuration\_password>**

Secure the telnet port? [Y|N, default=Y]:

**N**

At this point in the configuration, Nortel Networks recommends not securing the telnet port. It can be configured later after the rollback is completed.

**15** STEP 3: Configure the gateway type

This Gateway is automatically set up in a H248 configuration. Gateway configured to support H248.

No user input is required.

**16** STEP 4: Configure the workgroup and computer name

The CICM/CICM-EM can operate in either a single or dual node configuration. In a dual node configuration, the CICM/CICM-EM has two nodes, A and B. The two nodes belong to a unique workgroup. The node(s) will be named as the workgroup name with an '-A' (or '-B' appended). In a single node configuration, only node A can be installed. It's name will be the workgroup name with an '-A' appended.

No user input is required.

Setting machine name to CICM-nnn-A.

Configuring node A [CICM-nnn-A].

Configuring node B [CICM-nnn-B].

Setting workgroup name to CICM-nnn.

**17** STEP 5: Configure the administration accounts

The CICM and the CICMEM both have an Administration Account. The preboot section is used to configure this account.

Enter the local Administrator account password:

**<customer\_configuration\_password>**

The password (up to 8 alphanumerical characters) can be different than the one you specified earlier for the pre-shared key. Record the password for your records.

Re-enter to confirm:

**<customer\_configuration\_password>**

Successfully set administrator password.  
Creating Nortel Networks Networks TAS account.  
Successfully created Nortel Networks TAS account.

## 18 STEP 6: Configure the software user account

The CICM/CICM-EM use a single security [aka COMUSER] account under which all software is executed. This account should be configured with the same username and password on each system (CICM-EMs and CICMs).

NOTE: this account should *\*NOT\** be used for interactive logins.

The /display option will display the comuser password [only do this over a secure connection]. Note that this will display the auto-generated password based on the IPSec pre-shared key (which you must re-enter). If you enter the wrong key then an incorrect software account password will be displayed.

Enter a username under which the software will run (hit ENTER to accept "COMUSER"):

**<customer\_userid>**

Nortel Networks recommends you press enter to accept the default value of *COMUSER* as the userid for the COMUSER account. Note that the CICM-EM and all subtending CICM nodes must have the same COMUSER userid. Record the userid for your records.

Using default account name "comuser".

Creating user account.

Configuring user group.

Setting user account expiry to UNLIMITED.

Setting failed login attempts to UNLIMITED.

Configuring access permissions.

Configuring launch permissions.

Configuring logon rights.

Configuring applications.....  
Installing cxippreboot.  
Reinstalling cxippreboot.  
Software account successfully configured.

- 19** STEP 7: Configure the Static adapter settings
- This section creates and configures the 'Static' LAN Adapters. There are two static adapters per node - A1/A2 and B1/B2. Each has a single IP address. Heartbeat messages are sent between the addresses on A and the addresses on B. These addresses are restricted to the CICM and they must be in a distinct subnet from any other addresses used on the CICM or in the network in general.
- Enter Admin VLAN id [1...4094, default=2]:
- <customer\_admin\_vlan\_value>**
- Enter H248 VLAN id [1...4094, default=4]:
- <customer\_h248\_vlan\_value>**
- The static addresses have been autogenerated based on the system ID of nnn.  
The base address is <auto generated IP address> and will be used to create a subnet range with mask 255.255.255.248.
- Do you wish to use the base address? [Y|N, default=Y]
- Nortel Networks recommends entering Y (yes) to accept it provided the auto-generated address does not conflict with an existing IP address in the network. Entering N (no) means you must provide the valid static address values.
- Configuring adapter A1 - this may take a few minutes...  
...  
Configuring adapter A2 - this may take a few minutes...  
...  
Configuring adapter A4 - this may take a few minutes...  
...  
[SC] ChangeServiceConfig SUCCESS.
- 20** STEP 8: Configure the Unistim LAN settings

This section configures the CICM's Unistim LAN adapter. The Unistim LAN is used for call signalling between CICM and its clients (terminals). The LAN's port filter only permits those UDP ports used to communicate with clients. [OAMP functions are blocked on the Unistim LAN.]

Enter Unistim VLAN id [1...4094, default=3]:

**<unistim\_vlan\_id>**

Enter the Unistim IP address for this node:

**<unistim\_static\_ip\_address\_for\_the\_node>**

Enter the network mask for the Unistim IP network:

**<network\_mask\_for\_unistim\_ip\_network>**

Enter the default route for the Unistim IP network (Enter 0.0.0.0 for no route):

**<default\_route\_for\_unistim\_ip\_network>**

Enter a no route only if you do not have a default and you understand the consequences of not having one.

Configuring Unistim Adapter - this may take a few minutes...

...

Applying Default Gateway: The ReturnValue is nn (4 byte int)

## **21** STEP 9: Configure the H248 LAN settings

This section configures the H248 floating adapter. The floating H248 IP address will be bound to the A4/B4 adapter on whichever CICM node is Master. Therefore, datafill the same address on each node. This address will be used for all communication with the Gateway Controller and should match the Media Gateway IP Address provisioned for the CICM on the Gateway Controller EM. The H248 LAN's port filter permits only the UDP traffic used to communicate with the Gateway Controller. [OAMP functions are blocked on the H248 LAN.] You must also enter two static addresses for the H248 LAN. One is for Node A and the other is for Node B.

Enter the Floating H248 IP address for this CICM:

**<floating\_h248\_ip\_address\_for\_cicm>**

Enter the Static H248 IP address for Node A:

**<static\_h248\_ip\_address\_for\_node\_A>**

Enter the Static H248 IP address for Node B:

**<static\_h248\_ip\_address\_for\_node\_B>**

Enter the network mask for the H248 IP network:

**<network\_mask\_for\_h248\_ip\_network>**

Enter the default route for the H248 IP network  
(Enter 0.0.0.0 for no route):

**<default\_route\_for\_h248\_ip\_network>**

Enter a no route only if you do not have a default and you understand the consequences of not having one.

Applying IP Address and Subnet Mask

## 22 STEP 10: Configure the VMG settings

This step configures the Virtual Media Gateway. The CICM can support up to 3069 lines (up to 1023 on the 5370 hardware) [for Nortel Networks testing purposes \*ONLY\*, a lower value may be entered.]

WARNING - in a dual node configuration, the number of lines must be datafilled the same on both nodes of the CICM.

To re-size the VMG to the maximum number of lines use the following command:

preboot vmg /resize

Enter the number of lines for the gateway  
[1...1023, default=1023]:

Nortel Networks recommends you accept the default number of lines.

**<number\_of\_lines\_for\_the\_gateway>**

Enter the Media Gateway Controller IP address:

**<media\_gateway\_controller\_ip\_address>**

Enter the Media Gateway Controller UDP port  
[0...65535, default=2944]:

**<media\_gateway\_controller\_udp\_port>**



**23** STEP 11: Configure the Floating Admin adapter settings

This section configures the Floating Admin adapter information. The floating Admin IP address will be bound to the most available interface on the Gateway node.

Enter the Node A Admin address:

**<node\_A\_admin\_address>**

Enter the Node B Admin address:

**<node\_B\_admin\_address>**

Enter the network mask for the Admin IP network:

**<network\_mask\_for\_admin\_ip\_network>**

Enter the default router for the Admin IP network:

**<default\_router\_for\_admin\_ip\_network>**

Configuring PA

Configuring PB

Configuring route for A1

Configuring route for A2

**24** STEP 12: Configure the SNMP settings

The Gateway can be managed remotely by an SNMP management station. Most of the data accessible via SNMP is derived directly from the CentrexIP internal MIB but certain data must be entered during initial configuration. This data includes ...

**<customer\_snmp\_configuration>**

Configure the *SNMP settings* by entering your configuration values or if not using SNMP, press enter to accept all the default values. The progression of information is not shown in this step.

... ---Finished

Are you satisfied with the above responses [Y|N, default=Y]:

Enter **Y** (yes) to accept or **N** (no) to make changes.

--- Starting

--- Looking up system description from host OS

--- ...

--- Finished

**25** STEP 13: Configure the time settings for the gateway

You can use this utility to set the time and time zone on the CICM. It will inform any running software of the time change.

Current time zone is n.n hours from GMT (GMT Daylight Time).

Standard zone is n.n hours from GMT (GMT Standard Time)

Do you want to change it [Y|N, default=N]:

Entering **Y** presents a choice of time zones. Select the time zone by entering the number associated with it or press enter to accept the default.

**Y**

Current local date is <value>.

Do you want to change it [Y|N, default=N]:

Enter **N** to accept the local date or enter **Y** to change it. After **Y**, answer the prompts to specify the day, month, and year.

**Y**

Current local time is <value>.

Do you want to change it [Y|N, default=N]:

Enter **N** to accept the local time or enter **Y** to change it. After **Y**, answer the prompts to specify the hours and minutes.

**Y**

Current time for scheduled backups is 02:00.

Do you want to change it [Y|N, default=N]:

Configure a different time to schedule the automatic backup of the software image by entering **Y** (yes), then a 24-hour time as <hh:mm>.

**N**

**26** STEP 14: Configure the Hard disk

No user input is required.

The CICM and CICM-EM have two disk partitions, C: and D:. These must be converted to the NTFS file system.

Setting system to convert C: and D: to NTFS file system on next boot.

- 27** STEP 15: Apply the CICM software load
- Apply the default software image to the Gateway.
- Wait while preboot configures the software. The progression of information is not shown in this step.
- Registering ...  
... Registry Flush Complete.
- A reboot must now be performed to complete installation. Do you want to restart now? [Y|N, default=N]:
- Y**
- Rebooting now...
- Temporary lockout occurs at the command prompt.

***At the page maintenance (cicm-nnn)***

- 28** Wait for the node to synchronize data with its mate node.
- When synchronized, the node is fully in service as shown by the status system idle or system running, and the VMG Status is also synchronized (shown with the Node status).
- 29** Apply additional MRs and patches as needed to restore the node to the same MR level as its mate node.
- Refer to the procedures:
- [Upgrading a CICM node with an MR](#)
  - [Upgrading a CICM-EM with an MR or product release](#)

***At the page maintenance status (cicm-nnn)***

- 30** Verify the CICM node pair fully in service.
- 31** Leave the CICM terminals on Node B, the active master.

***At the PC desktop for remote access to the CICM node***

- 32** Locally access CICM Node A through the console serial port.
- 33** At the prompt, log in.
- login:
- For the userid enter Administrator and for the password enter Administrator.
- The screen prompt becomes:
- C:\Documents and Settings\Administrator>

- 34** At the CLI of a Windows session, you apply your SNMP data to enable a connection with IEMS by entering:

**preboot snmp /interactive**

***At the IEMS interface***

- 35** If you edited the object properties of IEMS for an upgrade to a CICM-EM or a CICM node, do the procedure [Following up a rollback for IEMS](#).
- 36** This procedure is complete. Return to the task flow or procedure that sent you to this procedure.

## Using preboot to re-image a CPV5370 CICM-EM

Use preboot to re-image a CICM-EM with CPV5370 CPU cards (blades) to a base CICM-EM software release.

### Prerequisites to using preboot to re-image a CPV5370 CICM-EM

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in [Task flow of CICM-EM and CICM node rollbacks](#).
- When the CICM-EM's software has been restored, its data is automatically synchronized with the mate EM.
- Output from the progression of preboot is shown by `this font`. Command entries are shown by **this font**.
- When more appears on the screen, press the keyboard spacebar to advance the screen.



#### CAUTION

##### Risk of service prevention

Using preboot means re-entering specific configuration data that would normally be handled by an initial installation. While configuring, extreme care must be taken to ensure accurate entries especially with IP addresses.

### Procedure steps to using preboot to re-image a CPV5370 CICM-EM

#### *At the PC desktop for remote access to the CICM-EM*

- 1 Locally access Node A through the console serial port.
- 2 Pressing enter in the terminal window will eventually get the login prompt.  
`login:`
- 3 For the userid enter Administrator and for the password enter Administrator.
- 4 At the command line interface (CLI) of a Windows 2000 session, enter preboot.
- 5 Press CTRL-C at any prompt to abort preboot.  
Press ENTER now to start preboot configuration.  
Press enter to start *preboot*.
- 6 Is this node A of the CICM? [Y|N, default=Y]:  
Ensure that you are prebooting node A and enter **Y** (yes).

This CICM-EM is Node A.

**7** STEP 1: Configure BOOTP options (CPV5370 ONLY)

BOOTP Settings must be entered by the craftsperson for CPV5370 CPUs since network BOOTP is only possible on hardware installed in a SAM 21 chassis i.e. CPN5385 slave CPUs. This is a CICM-EM Node. The identifier (name) for this node has the format CICMEM-000-X where 000 is the numeric system identifier for this node and its mate node and X is the node identifier and can be either 'A' or 'B'.

Enter the 3 digit system identifier for this chassis [range 000-511]:

**<3\_digit\_system\_identifier>**

Node name recorded as CICM-nnn-A.

Enter the Public Admin Network IP Address for this node:

**<public\_admin\_network\_ip\_address\_for\_cicm>**

Enter the Public Admin Network Subnet mask for this node:

**<public\_admin\_network\_subnet\_mask\_for\_cicm>**

Enter the default route for the Public Admin Network (Enter 0.0.0.0 for no route):

**<default\_route\_for\_public\_admin\_network>**

Enter a no route only if you do not have a default and you understand the consequences of not having one.

Enter the Primary NTP Server IP Address:

**<primary\_ntp\_server\_ip\_address>**

Enter the Secondary NTP Server IP Address:

**<secondary\_ntp\_server\_ip\_address>**

**8** STEP 2: Configure SSH

Access to the CICM EM may be achieved either by using a secured SSH connection or via the EM's serial port. SSH keys are generated during this step (which takes some time). On completion the SSH fingerprint will be displayed. Use this fingerprint for server validation when connecting to the CICM EM. Do not trust any

```
other fingerprint.
To display the SSH fingerprint after the SSH
step use the following:
preboot ssh /fingerprint
Generating SSH keys ...
```

```
...
The CICM EM SSH Fingerprint is:
<fingerprint_code>
```

No user input is required.

```
Press ENTER to continue.
SSH Configuration Complete.
```

- 9** **Messages:** Flushing Registry Data...  
Registry Flush Complete.

```
A reboot must now be performed to complete
installation. Do you want to restart now? [Y|N,
default=N]:
```

**Y**

```
Rebooting now...
```

- 10** Pressing enter in the terminal window will eventually get the login prompt.

```
login:
```

- 11** For the userid enter Administrator and for the password enter Administrator.

The screen prompt becomes:

```
C:\Documents and Settings\Administrator>
```

- 12** At the command line interface (CLI) of a Windows XP session, enter:

**preboot**

- 13** Press CTRL-C at any prompt to abort preboot.  
Press ENTER now to start preboot configuration.

Press enter to start *preboot*.

```
This CICM-EM is node A.
```

- 14** STEP 1: Configure BOOTP options (CPV5370 ONLY)  
Skipping option bootp (already complete).

No user input is required.

- 15** STEP 2: Configure SSH  
Skipping option ssh (already complete).

No user input is required.

- 16** This step configures IPsec. You will be prompted for the IPsec pre-shared key. This is the key that is used to connect to the IPsec protected ports on the CISM[EM]. A hash of this pre-shared key will be used for the software account (comuser) password. It is important to remember the pre-shared key entered, as this key **MUST** be the same on both the CISM and the CISM EM. The IPsec step can only be run once.

To re-key IPsec use the following command:

```
preboot ipsec /rekey
```

```
preboot ipsec /telnet
```

To deactivate the ipsec policy:

```
preboot ipsec /deactivate
```

To re activate the ipsec policy:

```
preboot ipsec /activate
```

NB: <cismname> must be identical to the name specified in the /permitcism.

Enter the IPsec Pre-Shared Key:

**<customer\_configuration\_password>**

Record the pre-shared key (password) for your records.

Re-enter to confirm:

**<customer\_configuration\_password>**

Secure the telnet port? [Y|N, default=Y]:

**N**

At this point in the configuration, Nortel Networks recommends not securing the telnet port. It can be configured later after the rollback is completed.

- 17** STEP 4: Configure the workgroup and computer name

No user input is required.

The CISM/CISM-EM can operate in either a single or dual node configuration. In a dual node configuration, the CISM/CISM-EM has two nodes, A and B. The two nodes belong to a unique workgroup. The node(s) will be named as the workgroup name with an '-A' (or '-B' appended). In a single node configuration, only node A can be installed. It's name will be the workgroup name with an '-A' appended.



Setting machine name to CICMEM-nnn-A.  
Configuring node A [CICMEM-nnn-A].  
Configuring node B [CICMEM-nnn-B].  
Setting workgroup name to CICMEM-nnn.

- 18** STEP 5: Configure the administration accounts  
The CICM and the CICMEM both have an Administration Account. The preboot section is used to configure this account.

Enter the local Administrator account password:

**<customer\_configuration\_password>**

The password (up to 8 alphanumerical characters) can be different than the one you specified earlier for the pre-shared key. Record the password for your records.

Re-enter to confirm:

**<customer\_configuration\_password>**

Successfully set administrator password.

- 19** STEP 6: Configure the software user account  
The CICM/CICM-EM use a single security [aka COMUSER] account under which all software is executed. This account should be configured with the same username and password on each system (CICM-EMs and CICMs).

NOTE: this account should *\*NOT\** be used for interactive logins.

The /display option will display the comuser password [only do this over a secure connection]. Note that this will display the auto-generated password based on the IPSec pre-shared key (which you must re-enter). If you enter the wrong key then an incorrect software account password will be displayed.

Enter a username under which the software will run (hit ENTER to accept "COMUSER"):

**<customer\_userid>**

Nortel Networks recommends you press enter to accept the default value of *COMUSER* as the userid for the COMUSER account. Note that the CICM-EM and all subtending CICM nodes must have the same COMUSER userid. Record the userid for your records.

```
Using default account name "comuser".
Creating user account.
Configuring user group.
Setting user account expiry to UNLIMITED.
Setting failed login attempts to UNLIMITED.
Configuring access permissions.
Configuring launch permissions.
Configuring logon rights.
Configuring applications.....
Installing cxippreboot.
Reinstalling cxippreboot.
Software account successfully configured.
```

**20** STEP 7: Configure the element manager environment

**No user input is required.**

The Element Manager has additional data that needs to be set [EM domain/machine names, DCOM protocols preferences etc].  
Setting up Element Manager environment.  
Setting up DCOM protocols.  
WARNING: An important change was made to DCOM protocols preferences. You MUST reboot after install has finished to make the changes take effect.  
Element Manager environment successfully configured.

**21** STEP 8: Configure the Static adapter settings

This section creates and configures the 'Static' LAN Adapters. There are two static adapters per node - A1/A2 and B1/B2. Each has a single IP address. Heartbeat messages are sent between the addresses on A and the addresses on B. These addresses are restricted to the CICM-EM and they must be in a distinct subnet from any other addresses used on the CICM-EM or in the network in general.  
The static addresses have been autogenerated based on the system ID of nnn.  
The base address is <auto generated IP address> and will be used to create a subnet range with mask 255.255.255.248.

Do you wish to use the base address? [Y|N,  
default=Y]

**<customer\_static\_address>**

Nortel Networks recommends entering **Y** (yes) to accept it provided the auto-generated address does not conflict with an existing IP address in the network. Entering **N** (no) means you must provide the valid static address values.

Configuring A1  
Configuring A2  
Configuring B1  
Configuring B2  
Configuring RPC...  
[SC] ChangeServiceConfig SUCCESS.

- 22** This section configures the Floating Admin adapter information. The floating Admin IP address will be bound to the most available interface on the Element Manager node.

Configure the *Floating Admin Adapter settings* by entering:

**<node\_A\_admin\_address>**

**<node\_B\_admin\_address>**

**<network\_mask\_for\_admin\_ip\_network>**

**<default\_router\_for\_admin\_ip\_network>**

Configuring PA  
Configuring PB  
Configuring route for A1  
Configuring route for A2

- 23** STEP 9: Configure the Floating Admin adapter settings

This section configures the HTTP floating adapter information. The floating HTTP address will be bound to the most available adapter on whichever node of the CICM-EM is the Master. Therefore the same address should be datafilled on each CICM-EM node. The address will be used for all Web Browser communication.

Enter the Node A Admin address:

**<node\_A\_admin\_address>**

Enter the Node B Admin address:

**<node\_B\_admin\_address>**

Enter the network mask for the Admin IP network:

**<network\_mask\_for\_admin\_ip\_network>**

Enter the default router for the Admin IP network:

**<default\_router\_for\_admin\_ip\_network>**

Configuring PA

Configuring PB

Configuring route for A1

Configuring route for A2

**24** STEP 10: Configure PAM authentication

Will this CICM-EM use PAM to authenticate users?  
[Y|N, default=N]:

Enter **Y** (yes) to enable PAM authentication or **N** (no). With **Y** you must answer the prompts to configure PAM data (for example, the proxy server). With **N** the response is:

The Element Manager will use local NT authentication.

**25** STEP 12: Configure the SNMP settings

The Element Manager can be managed remotely by an SNMP management station. Most of the data accessible via SNMP is derived directly from the CentrexIP internal MIB but certain data must be entered during initial configuration. This data includes ...

**<customer\_snmp\_configuration>**

Configure the *SNMP settings* by entering your configuration values or if not using SNMP, press enter to accept all the default values. The progression of information is not shown in this step.

Are you satisfied with the above responses [Y|N, default=Y]:

Enter **Y** (yes) to accept or **N** (no) to make changes.

--- Starting

--- Looking up system description from host OS

--- ...

--- Finished

**26** STEP 13: Configure the time settings for the EM

You can use this utility to set the time and time zone on the EM.

Current time zone is n.n hours from GMT (GMT

Daylight Time).  
Standard zone is n.n hours from GMT (GMT  
Standard Time)  
Do you want to change it [Y|N, default=N]:  
Entering **Y** presents a choice of time zones. Select the time zone  
by entering the number associated with it or press enter to  
accept the default.

**Y**

Current local date is <value>.  
Do you want to change it [Y|N, default=N]:  
Enter **N** to accept the local date or enter **Y** to change it. After **Y**,  
answer the prompts to specify the day, month, and year.

**Y**

Current local time is <value>.  
Do you want to change it [Y|N, default=N]:  
Enter **N** to accept the local time or enter **Y** to change it. After **Y**,  
answer the prompts to specify the hours and minutes.

**Y**

Current time for scheduled backups is 02:00.  
Do you want to change it [Y|N, default=N]:  
Accept the default or configure a different time to schedule the  
automatic backup of the software image by entering **Y** (yes),  
then a 24-hour time as <hh:mm>.

**27** STEP 14: Configure the Hard disk

No user input is required.

The CISM and CISM-EM have two disk partitions,  
C: and D:. These must be converted to the NTFS  
file system.  
Setting system to convert C: and D: to NTFS file  
system on next boot.

**28** STEP 15: Apply the EM software load

Apply the default software image to the Element  
Manager.  
Registering {...

Wait while preboot configures the software. The progression of  
information is not shown in this step.

... Registry Flush Complete.

```
A reboot must now be performed to complete
installation. Do you want to restart now? [Y|N,
default=N]:
```

```
Y
```

```
Rebooting now...
```

Temporary lockout occurs at the command prompt.

### ***At the page maintenance (cicmem-nnn)***

- 29** Wait for the node to synchronize data with its mate node.

When synchronized, the node is fully in service as shown by the status system idle or system running, and the VMG Status is also synchronized (shown with the Node status).

- 30** Apply additional MRs and patches as needed to restore the node to the same MR level as its mate node.

Refer to the procedures:

- [Upgrading a CICM node with an MR](#)
- [Upgrading a CICM-EM with an MR or product release](#)

- 31** Verify the CICM-EM pair is fully in service.

### ***At the PC desktop for remote access to the CICM node***

- 32** Locally access CICM Node A through the console serial port.

- 33** At the prompt, log in.

```
login:
```

For the userid enter Administrator and for the password enter Administrator.

The screen prompt becomes:

```
C:\Documents and Settings\Administrator>
```

- 34** At the CLI of a Windows session, you apply your SNMP data to enable a connection with IEMS by entering:

```
preboot snmp /interactive
```

### ***At the IEMS interface***

- 35** If you edited the object properties of IEMS for an upgrade to a CICM-EM or a CICM node, do the procedure [Following up a rollback for IEMS](#).

- 36** This procedure is complete. Return to the task flow or procedure that sent you to this procedure.



## Original Equipment Manufacturer (OEM) gateways and gateway managers

Refer to OEM/third-party media gateway upgrade documentation and perform the upgrade(s) in the following sequence:

- upgrade the gateway manager for one gateway type
- upgrade all the associated gateways of the same type
- upgrade the gateway manager for the next gateway type
- upgrade all the associated gateways of the same type
- continue for all remaining OEM gateway types



## MCS upgrade

### **ATTENTION**

Due to the complexity of the upgrade for the MCS 5200, Border Control Point 7100/7200, and Session Server-Lines product, Nortel requires that all customers contact their Nortel Customer Service representative to engage the appropriate Nortel Software Delivery team to perform this upgrade.

There will be no service charges incurred for this activity.







## BCP upgrade

### **ATTENTION**

Due to the complexity of the upgrade for the MCS 5200, Border Control Point 7100/7200, and Session Server-Lines product, Nortel requires that all customers contact their Nortel Customer Service representative to engage the appropriate Nortel Software Delivery team to perform this upgrade.

There will be no service charges incurred for this activity.



---

## Editing and viewing object properties using Java Web Start Client

---

### Application

Use this procedure to edit or view the properties of objects that are displayed in the IEMS topology using Java Web Start Client.

### Prerequisites

There are no prerequisites for this procedure.

### Action

#### ***At the IEMS workstation***

- 1** Launch the IEMS Java Web Start Client. Refer to procedure "Launching the IEMS Java Web Start Client".
- 2** Select the required object in the IEMS Topologies tree under Applications.  
  
The properties of an object from the Inventory panel of IEMS tree can also be viewed. To view the Inventory object properties, select the object in the Integrated Topologies tree, under Applications to open the Inventory view. Double-click the required row in the Inventory view.
- 3** Right-click the map symbol and select the Managed Object Properties menu item or double-click the map symbol to open the Object Properties window.

*A window similar to the following figure opens. The object properties displayed can differ for each component.*

**Object Properties ----iems-sf2**

**Base Properties**

Name: raghuram-SAM21-Mgr

Display Name: raghuram

Type: SAM21 Mgr

Status: Unknown

IP-Address: 192 . 168 . 118 . 160

Platform: None

Managed: ☒

Time Zone: Etc/GMT+12

Device Version: 8.0

Enable System Unmanage: ☒

Fault Interface State: NORMAL

**Other Properties**

Poll Interval (in seconds): 300

Status Change Time: Tue Mar 01 07:29:43 GMT+05:30 2005

Back Next

Modify Help Close

Done

- 4 If required, modify the object properties. Use the following table to assist you in understanding the fields.

#### Managed object properties in Java Web Client

| Field        | Description                                                            |
|--------------|------------------------------------------------------------------------|
| Name         | Displays a unique name for the object                                  |
| Display Name | Edit the name displayed in the topology for the object                 |
| Type         | Displays the type of object (element manager, EMS, EMS platform or NE) |

## Managed object properties in Java Web Client

| Field                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Description                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Displays the status of the object                                                                                                                                                                  |
| IP-Address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Edit the IP address of the object                                                                                                                                                                  |
| Platform                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Select the platform where the object resides from the drop-down list                                                                                                                               |
| Managed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Indicates whether the object is managed or unmanaged                                                                                                                                               |
| Time Zone                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Select the time zone of the geographical location where the object exists from the drop-down list                                                                                                  |
| Device Version                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Select the device version of the managed object from the drop-down list                                                                                                                            |
| Enable System Unmanage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Enable or disable the System_Unmanaged state. Refer to section "System_Unmanaged state" in "Configuring the Message Overload Controller parameters" in <i>IEMS Fault Management</i> , NN10334-911. |
| Poll Interval                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Edit the Poll Interval for status updates                                                                                                                                                          |
| Status Change Time                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Displays the last status change time of the object                                                                                                                                                 |
| <p><b>Note 1:</b> For the following auto-discovered element objects and element managers that have auto-discovered child nodes, only the Display Name and the Managed field can be modified: SDM platform, APS Manager, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Portal, SSLines. To change the IP address of these objects, you must delete and then re-add the appropriate element manager.</p> <p><b>Note 2:</b> You cannot modify the fields of the MG 7480/15000/20000 and MSS 15000.</p> |                                                                                                                                                                                                    |

### 5 Select your next step.

| If                                                                                 | Do                           |
|------------------------------------------------------------------------------------|------------------------------|
| you do not want to modify any other properties                                     | go to <a href="#">step 6</a> |
| you want to view or modify the fault interface or performance interface properties | go to <a href="#">step 8</a> |

- 6 Click the Modify button to update the changes.
- 7 Go to [step 16](#).
- 8 Click the Next button to proceed to the Fault Interface window.  
*A window similar to the following figure opens.*

The screenshot shows a window titled "Object Properties ----Nortel". Inside, there's a "Fault Interface" section. Under "SNMP Details", the "Port" is set to 161, "Community" is empty, and "Version" is set to v3. Under "V3 Security Details", the "Security Level" is set to NoAuthNoPriv, "User name" is v3admin, "Context name" is saul, "Auth Protocol" is MD5, "Privacy Protocol" is CBC-DES, "Auth Password" is empty, and "Privacy Password" is empty. At the bottom, there are buttons for "Back", "Next", "Modify", "Help", "Close", and a green "Done" button.

- 9 Edit or view the fault interface properties of the object as required.

The Details panel dynamically changes according to the fault interface of the EMS/NE.

For MS 2000, do the following. Enter v2c as the SNMP version. The SNMP read Community and write Community strings by default are public and private. If these values were changed, enter the correct values here.

**10** Select your next step.**If****Do**

you do not want to modify any other properties

[step 11](#)

you want to view or modify the performance interface properties

[step 13](#)

**11** Click the Modify button to update the changes.**12** Go to [step 16](#).**13** Click the Next button to proceed to the Performance Interface window.

*A window similar to the following figure opens.*

The screenshot shows a window titled "Object Properties ----Nortel". Inside, there is a section for "Performance Interface" which contains "SNMP Details" and "V3 Security Details".

**SNMP Details:**

- Port: 161
- Community: (empty text box)
- Version: v3 (dropdown menu)

**V3 Security Details:**

- Security Level: NoAuthNoPriv (dropdown menu)
- User name: v3admin
- Context name: saul
- Auth Protocol: MD5 (dropdown menu)
- Auth Password: (empty text box)
- Privacy Protocol: CBC-DES
- Privacy Password: (empty text box)

At the bottom of the window, there are buttons for "Back", "Next", "Modify", "Help", and "Close". A green bar at the very bottom contains the text "Done".



- 14** Edit or view the performance interface properties of the object as required.

For MS 2000, do the following. Enter v2c as the SNMP version. The SNMP read Community and write Community strings by default are public and private. If these values were changed, enter the correct values here.
- 15** Click the Modify button to update the changes.
- 16** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Editing and viewing object properties using Web Client

---

### Application

Use this procedure to modify or view the properties of an object in the IEMS topology using Web Client.

### Prerequisites

There are no prerequisites for this procedure.

### Action

#### ***At the IEMS workstation***

- 1 Launch the IEMS Web Client. Refer to procedure “Launching the IEMS Web Client” in *IEMS Overview*, NN10329-111.
- 2 Select the Integrated EMS Topologies tab.
- 3 Navigate to the required topology node in the IEMS Topologies tree.
- 4 Click the map symbol label to open the General Information window.

*A window similar to the following figure opens. The object properties displayed can differ for each component.*

Integrated EMS Topologies → Network Elements

**rajagopal-MS2000**

**General Information**

|                |                                                               |
|----------------|---------------------------------------------------------------|
| Name           | rajagopal-MS2000                                              |
| Device Type    | NE-MS2000                                                     |
| Status         | <input checked="" type="radio"/> Clear                        |
| Is Managed ?   | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Display Name   | raj                                                           |
| Device Version | 8.0                                                           |
| IP Address     | 192.168.113.201                                               |
| Web User Name  | rajagopal                                                     |
| Web Password   | ****                                                          |

Update Object Reset

- 5 If necessary, select each vertical tab and modify the object properties listed in the following table.

#### Managed object properties in Web Client

| Field          | Description                                                            |
|----------------|------------------------------------------------------------------------|
| <b>General</b> |                                                                        |
| Name           | Displays the unique object name of the managed object                  |
| Device Type    | Displays the type of object (element manager, EMS, EMS platform or NE) |
| Status         | Displays the status of the object                                      |
| Is Managed?    | Indicates whether the object is managed or unmanaged                   |
| Display Name   | Displays the name or label displayed in map symbol                     |

**Managed object properties in Web Client**

| Field                          | Description                                                          |
|--------------------------------|----------------------------------------------------------------------|
| Device Version                 | Select the version of the device from the drop-down list             |
| IP Address                     | Modify the IP address of the object                                  |
| Web User name                  | Enter your web user name                                             |
| Web Password                   | Enter your web password                                              |
| <b>Monitoring</b>              |                                                                      |
| Last Status Update Time        | Displays the time when the status of the managed object last changed |
| Last Status Change Time        | Displays the time when the status of the managed object last changed |
| Status Polling Interval (secs) | Modify the Poll Interval for status updates                          |

**Managed object properties in Web Client**

| Field                        | Description                                                                      |
|------------------------------|----------------------------------------------------------------------------------|
| <b>Fault Interface</b>       | If the details are present for the selected object, the details can be modified. |
| <b>Performance Interface</b> | If the details are present for the selected object, the details can be modified. |

- 6** Click the Update Object button to update the changes.
- 7** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



# Carrier Voice over IP Network patching

## ATTENTION

For all components that do not use the Network Patch Manager (NPM), if a patch file contains a “.patch” extension, remove that extension before applying the patch.

Contact your next level of support if assistance is required.

## Overview

Patches and maintenance releases provide enhancements or corrections to an existing software release. Patches provide temporary changes until the next software release becomes available while maintenance releases represent a new software release with corrective content. Normally a new software release incorporates all patches assigned to the previous release.

This section discusses patching for the following Carrier Voice over IP components that support the patching capability:

- core manager, which can be one of the following platforms:
  - CS 2000 Core Manager on a AIX platform
  - Core and Billing Manager (CBM) on an SPFS platform
- Server Platform Foundation Software (SPFS)
- Patching Server Element (PSE)
- Integrated Element Management System (IEMS)
- IEMS security component (IEMSCSS and IEMSCSS\_DS)
- Core Element Manager (COREM)
- Client Session Monitor (CSMONITOR)
- Key Manager (PKMGR\_SERVER)

- CS 2000 Management Tools components
  - CS 2000 SAM21 Manager (SAM21EM)
  - Succession Element and Sub-network Manager (SESM)
  - QoS Collector Application (QCA)
- Network Patch Manager (NPM)
- Multi-service Data Manager (MDM)
- Media Gateway (MG) 3200
- Media Gateway (MG) 3500
- Media Gateway (MG) 7400
- Media Gateway (MG) 9000
- Media Gateway (MG) 15000
- Media Gateway (MG) 9000 Manager
- Multiservice Switch 15000
- Session Server Trunks
- Centrex IP Client Manager (CICM)
- CICM Element Manager (CICE)
- Software Inventory Manager (SWIM)
- Compact Call Agent
- Gateway Controller (GWC)
- Multi-service Gateway (MG) 4000
- Inter-Working Spectrum Peripheral Module (IW SPM)
- Dynamic Packet Trunking Spectrum Peripheral Module (DPT SPM)
- Legacy peripherals (for example, LIU7, DTC, SPM)
- Communication Server 2000 (CS 2000)
- Media Server 2000 Series

**Delivery**

Patches can be delivered at the same time a new software release is delivered (upgrade with patching), or between software releases (maintenance patching).

For software upgrades, a CD with the software load and a CD with any patches released to date are delivered. Any patches released after the patch CD was created can be delivered through Electronic Software

Delivery if the site is set up for ESD, or downloaded from a secure Nortel Networks web page.

### **Electronic Software Distribution**

Patch files are pushed from Nortel Networks to an external drop box location. The drop box can exist on Nortel Networks' Customer Access Network (CAN), or the customer's wide area network (WAN).

**Note:** For information on how to deploy ESD, contact your Nortel Networks representative.

### **Web distribution**

Patches are pulled through the Internet from a secure Nortel Networks web page and stored on a customer-provided server.

Web distribution is done through [www.nortel.com](http://www.nortel.com). Patches are located under "Support & Training> Technical Support> Software Downloads > Categories".

**Note:** Use the filter criteria to only display a selected set of patches.

Also, to facilitate patch management, the Patch Audit and Pre Upgrade Patch Calculator tools are available under "Support & Training> Technical Support > Software Downloads > Categories". The Patch Audit tool enables customers to perform a site-specific audit and determine any missing patches as well as patches that require customer action. The Pre Upgrade Patch Calculator enables customers to retrieve any patches before the upgrade starts that have been released after the software was shipped. The *Patch Audit User Guide* and *Pre Upgrade Patch Calculator Readme* file, located at the same location as the tools, provide more details.



## Tools and utilities

The following table lists the tools and utilities used to patch the components that support the patching capability in a Carrier Voice over IP network.

| Tool/utility | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PRSM         | <p>The Post-Release Software Manager (PRSM) is a command line interface (CLI) utility on the CS 2000. The PRSM is used for patching activities on the following components:</p> <ul style="list-style-type: none"><li>• CS 2000</li><li>• MG 4000</li><li>• IW SPM</li><li>• DPT SPM</li><li>• Legacy peripherals, for example, the Spectrum Peripheral Module (SPM)</li><li>• manually activated patches</li></ul> <p><b>Note:</b> Patches are also referred to as Post-Release Software Updates (PRSUs).</p> |

| Tool/utility | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NPM          | <p>The Network Patch Manager (NPM) is a patching tool with both a command line user interface (CLUI) and a webstart-based graphical user interface (GUI). The NPM is used for patching activities on the following components:</p> <ul style="list-style-type: none"><li>• Core and Billing Manager (CBM)</li><li>• GWC</li><li>• CS 2000 SAM21 Manager (SAM21EM)</li><li>• MG 9000</li><li>• MG 9000 Manager</li><li>• PSE</li><li>• NPM</li><li>• SESM</li><li>• QCA</li><li>• SPFS</li><li>• IEMS</li><li>• IEMS security component (IEMSCSS and IEMSCSS_DS)</li><li>• Core Element Manager (COREM)</li><li>• Client Session Monitor (CSMONITOR)</li><li>• Key Manager (PKMGR_SERVER)</li></ul> <p><b>Note:</b> You can obtain help information on the NPM through the Help menu of the GUI or by typing “help” in the CLUI.</p> |
| MDM          | <p>The MDM when configured as a software distribution site (SDS), manages, stores, and provides access to patch files. The MDM is used for patching activities on the following components:</p> <ul style="list-style-type: none"><li>• MDM</li><li>• Multiservice Switch 15000</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SWIM         | <p>The Software Inventory Manager (SWIM) is a utility integrated in the maintenance interface of the CS 2000 core manager, and is used to apply patch files, also referred to as fix filesets, on the CS 2000 core manager.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Tool/utility                             | Description                                                                                                   |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Integrated Element Manager System (IEMS) | The IEMS provides a graphical user interface (GUI) tool for applying Media Server 2000 Series patch software. |

## Patching order

When patches are available with the new software version for a component, apply the patches immediately following the software upgrade.

When patches are available between upgrades (maintenance patching), patch the components in the order shown for one of the following two office configurations:

- [Separate IEMS and CS 2000 Management Tools SPFS-based servers on page 2271](#)
- [Combined IEMS and CS 2000 Management Tools SPFS-based server on page 2272](#)

**Note:** Only the components that support the patching capability are listed.

**Separate IEMS and CS 2000 Management Tools SPFS-based servers (Sheet 1 of 2)**

|   | Component                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | <a href="#">CS 2000 Core Manager on page 2273</a><br>or<br>CBM850 SPFS-based server <ul style="list-style-type: none"><li>• <a href="#">SPFS on page 2274</a></li><li>• <a href="#">PSE on page 2274</a></li><li>• <a href="#">CBM 850 on page 2274</a></li></ul>                                                                                                                                                                              |
| 2 | IEMS SPFS-based server <ul style="list-style-type: none"><li>• <a href="#">SPFS on page 2274</a></li><li>• <a href="#">PSE on page 2274</a></li><li>• <a href="#">IEMS on page 2274</a></li><li>• <a href="#">Core Element Manager on page 2275</a></li><li>• <a href="#">IEMS security components on page 2275</a></li><li>• <a href="#">Client Session Monitor on page 2276</a></li><li>• <a href="#">Key Manager on page 2276</a></li></ul> |
| 3 | CS 2000 Management Tools SPFS-based server <ul style="list-style-type: none"><li>• <a href="#">SPFS on page 2274</a></li><li>• <a href="#">PSE on page 2274</a></li><li>• <a href="#">CS 2000 Management Tools components on page 2277</a></li></ul>                                                                                                                                                                                           |
| 4 | MG 9000 Manager SPFS-based server <ul style="list-style-type: none"><li>• <a href="#">SPFS on page 2274</a></li><li>• <a href="#">PSE on page 2274</a></li><li>• <a href="#">MG 9000 Manager components on page 2278</a></li></ul>                                                                                                                                                                                                             |
| 5 | IEMS SPFS-based server <ul style="list-style-type: none"><li>• <a href="#">NPM on page 2279</a></li></ul>                                                                                                                                                                                                                                                                                                                                      |
| 6 | <a href="#">Multi-service Data Manager on page 2279</a>                                                                                                                                                                                                                                                                                                                                                                                        |
| 7 | <a href="#">Multiservice Switch 15000 on page 2280</a>                                                                                                                                                                                                                                                                                                                                                                                         |

### Separate IEMS and CS 2000 Management Tools SPFS-based servers (Sheet 2 of 2)

|    | Component                                              |
|----|--------------------------------------------------------|
| 8  | <a href="#">GWC on page 2280</a>                       |
| 9  | <a href="#">MG 4000 on page 2280</a>                   |
| 10 | <a href="#">MG 9000 on page 2281</a>                   |
| 11 | <a href="#">IW-SPM on page 2281</a>                    |
| 12 | <a href="#">DPT-SPM on page 2281</a>                   |
| 13 | <a href="#">Legacy Peripheral Modules on page 2281</a> |
| 14 | <a href="#">CS 2000 on page 2281</a>                   |
| 15 | <a href="#">Media Server Series 2000 on page 2282</a>  |

### Combined IEMS and CS 2000 Management Tools SPFS-based server (Sheet 1 of 2)

|   | Component                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | <a href="#">CS 2000 Core Manager on page 2273</a><br>or<br>CBM850 SPFS-based server <ul style="list-style-type: none"> <li>• <a href="#">SPFS on page 2274</a></li> <li>• <a href="#">PSE on page 2274</a></li> <li>• <a href="#">CBM 850 on page 2274</a></li> </ul>                                                                                                                                                                                                                                                                                  |
| 2 | CS 2000 Management Tools SPFS-based server <ul style="list-style-type: none"> <li>• <a href="#">SPFS on page 2274</a></li> <li>• <a href="#">PSE on page 2274</a></li> <li>• <a href="#">IEMS on page 2274</a></li> <li>• <a href="#">Core Element Manager on page 2275</a></li> <li>• <a href="#">IEMS security components on page 2275</a></li> <li>• <a href="#">Client Session Monitor on page 2276</a></li> <li>• <a href="#">Key Manager on page 2276</a></li> <li>• <a href="#">CS 2000 Management Tools components on page 2277</a></li> </ul> |

**Combined IEMS and CS 2000 Management Tools SPFS-based server (Sheet 2 of 2)**

|    | Component                                                                                                                                                                                                                          |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3  | MG 9000 Manager SPFS-based server <ul style="list-style-type: none"><li>• <a href="#">SPFS on page 2274</a></li><li>• <a href="#">PSE on page 2274</a></li><li>• <a href="#">MG 9000 Manager components on page 2278</a></li></ul> |
| 4  | CS 2000 Management Tools SPFS-based server <ul style="list-style-type: none"><li>• <a href="#">NPM on page 2279</a></li></ul>                                                                                                      |
| 5  | <a href="#">Multi-service Data Manager on page 2279</a>                                                                                                                                                                            |
| 6  | <a href="#">Multiservice Switch 15000 on page 2280</a>                                                                                                                                                                             |
| 7  | <a href="#">GWC on page 2280</a>                                                                                                                                                                                                   |
| 8  | <a href="#">MG 4000 on page 2280</a>                                                                                                                                                                                               |
| 9  | <a href="#">MG 9000 on page 2281</a>                                                                                                                                                                                               |
| 10 | <a href="#">IW-SPM on page 2281</a>                                                                                                                                                                                                |
| 11 | <a href="#">DPT-SPM on page 2281</a>                                                                                                                                                                                               |
| 12 | <a href="#">Legacy Peripheral Modules on page 2281</a>                                                                                                                                                                             |
| 13 | <a href="#">CS 2000 on page 2281</a>                                                                                                                                                                                               |
| 14 | <a href="#">Media Server Series 2000 on page 2282</a>                                                                                                                                                                              |

**Patching procedures**

The sections that follow provide patching information for the individual components that support the patching capability, including references to the documents or the procedures that contain the detailed steps.

Review the [Patching order on page 2270](#) prior to patching the components.

**CS 2000 Core Manager**

Refer to [CS 2000 Core Manager upgrade on page 546](#)

**CBM 850**

Refer to [Core and Billing Manager 850 Upgrades on page 747](#)

**SPFS**

Refer to procedure [Applying patches using the NPM on page 2319](#).

**PSE**

The table below lists the procedures you must perform to patch the Patching Server Element (PSE). The procedures must be performed in the order they are listed.

**Note:** Ensure you have applied any [SPFS](#) patches prior to patching the PSE software.

Use this table as a checklist during the patching process. Place a check (✓) in the ✓column as you complete each procedure.

**Patching procedures checklist for the PSE**

| Activities |                                                                        | ✓ | Procedures                                                                         |
|------------|------------------------------------------------------------------------|---|------------------------------------------------------------------------------------|
| 1          | Apply the patches to the PSE device.                                   |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .    |
| 2          | Restart PSE device to which you applied patches to enable the patches. |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> . |

**IEMS**

The table below lists the procedures you must perform to patch the Integrated Element Management System (IEMS). The procedures must be performed in the order they are listed.

**Note:** Ensure you have applied any [SPFS](#) and [PSE](#) patches prior to patching the IEMS software.

Use this table as a checklist during the patching process. Place a check (✓) in the ✓column as you complete each procedure.

### Patching procedures checklist for the IEMS

| Activities                                        | ✓ | Procedures                                                                         |
|---------------------------------------------------|---|------------------------------------------------------------------------------------|
| 1 Apply the patches to the IEMS.                  |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .    |
| 2 Restart the IEMS to enable the applied patches. |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> . |

### Core Element Manager

The table below lists the procedures you must perform to patch the Core Element Manager (COREM). The procedures must be performed in the order they are listed.

**Note:** Ensure you have applied any [SPFS](#) and [PSE](#) patches prior to patching the Core Element Manager software.

Use this table as a checklist during the patching process. Place a check (✓) in the ✓column as you complete each procedure.

### Patching procedures checklist for the Core Element Manager

| Activities                                         | ✓ | Procedures                                                                         |
|----------------------------------------------------|---|------------------------------------------------------------------------------------|
| 1 Apply the patches to the COREM.                  |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .    |
| 2 Restart the COREM to enable the applied patches. |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> . |

### IEMS security components

The table below lists the procedures you must perform to patch the Integrated Element Management System (IEMS) security components. The procedures must be performed in the order they are listed.

**Note:** Ensure you have applied any [SPFS](#) and [PSE](#) patches prior to patching the IEMS security components software.



Use this table as a checklist during the patching process. Place a check (✓) in the ✓column as you complete each procedure.

### Patching procedures checklist for the Integrated EMS security components

| Activities                                                                                                                                        | ✓ | Procedures                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------|---|------------------------------------------------------------------------------------|
| 1 Apply the patches to the IEMS security components as follows: <ul style="list-style-type: none"> <li>• IEMSCSS</li> <li>• IEMSCSS_DS</li> </ul> |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .    |
| 2 Restart the IEMS security components to enable the applied patches.                                                                             |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> . |

#### Client Session Monitor

The table below lists the procedures you must perform to patch the Client Session Monitor (CSMONITOR). The procedures must be performed in the order they are listed.

**Note:** Ensure you have applied any [SPFS](#) and [PSE](#) patches prior to patching the CSMONITOR software.

Use this table as a checklist during the patching process. Place a check (✓) in the ✓column as you complete each procedure.

### Patching procedures checklist for the CSMONITOR

| Activities                                                    | ✓ | Procedures                                                                         |
|---------------------------------------------------------------|---|------------------------------------------------------------------------------------|
| 1 Apply the patches to the CSMONITOR device                   |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .    |
| 2 Restart the CSMONITOR device to enable the applied patches. |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> . |

#### Key Manager

The table below lists the procedures you must perform to patch the Key Manager (PKMGR\_SERVER). The procedures must be performed in the order they are listed.

**Note:** Ensure you have applied any [SPFS](#) and [PSE](#) patches prior to patching the PKMGR\_SERVER software.

Use this table as a checklist during the patching process. Place a check (✓) in the ✓column as you complete each procedure.

### Patching procedures checklist for the CS 2000 Management Tools components

| Activities                                                       | ✓ | Procedures                                                                         |
|------------------------------------------------------------------|---|------------------------------------------------------------------------------------|
| 1 Apply the patches to the PKMGR_SERVER device                   |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .    |
| 2 Restart the PKMGR_SERVER device to enable the applied patches. |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> . |

### CS 2000 Management Tools components

The table below lists the procedures you must perform to patch the CS 2000 Management Tools components (CS 2000 SAM21 Manager, SESM, and QCA). The procedures must be performed in the order they are listed.

**Note:** Ensure you have applied any [SPFS](#) and [PSE](#) patches prior to patching the CS 2000 Management Tools components software.

Use this table as a checklist during the patching process. Place a check (✓) in the ✓column as you complete each procedure.

### Patching procedures checklist for the CS 2000 Management Tools components (Sheet 1 of 2)

| Activities                                                                    | ✓ | Procedures                                                                               |
|-------------------------------------------------------------------------------|---|------------------------------------------------------------------------------------------|
| 1 Audit the devices for existing patch activity.                              |   | Perform procedure <a href="#">Performing a device audit using the NPM on page 2313</a> . |
| 2 Apply the patches to the CS 2000 SAM21 Manager.                             |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .          |
| 3 Restart the CS 2000 SAM21 Manager to enable the applied patches.            |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> .       |
| 4 Apply the patches to the Succession Element and Sub-network Manager (SESM). |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .          |
| 5 Restart the SESM to enable the applied patches.                             |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> .       |

**Patching procedures checklist for the CS 2000 Management Tools components  
(Sheet 2 of 2)**

| Activities |                                                           | ✓ | Procedures                                                                         |
|------------|-----------------------------------------------------------|---|------------------------------------------------------------------------------------|
| 6          | Apply the patches to the QoS Collector Application (QCA). |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .    |
| 7          | Restart the QCA to enable the applied patches.            |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> . |

**MG 9000 Manager components**

The table below lists the procedures you must perform to patch the Media Gateway (MG) 9000 Manager components. The procedures must be performed in the order they are listed.

**Note:** Ensure you have applied any [SPFS](#) and [PSE](#) patches prior to patching the MG 9000 Manager components software.

**ATTENTION**

Before you apply disruptive dcc patches, you must ensure the node is not aps switched by displaying the master shelf for the dcc pair you are patching. If the node is aps switched, an “S” appears on the inactive dcc card. Refer to procedure “Recovery from APS split-mode” in the MG9000 Fault Management document, NN10074-911, to correct the condition. Only apply dcc disruptive patches when the node is not aps switched. In addition, ensure no alarms are present on the dcc card you are patching, through the Alarms menu. Refer to the MG9000 Fault Management document, NN10074-911, for instructions on how to post and clear alarms. Only apply dcc disruptive patches when the dcc card is alarm free.

Use this table as a checklist during the patching process. Place a check (✓) in the ✓column as you complete each procedure.

### Patching procedures checklist for the MG 9000 Manager components

| Activities                                                                                                                                                                             | ✓ | Procedures                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|------------------------------------------------------------------------------------|
| 1 Apply the patches to the MG 9000 Manager components as follows: <ul style="list-style-type: none"> <li>• mg9kemserver (MG9KSERVER)</li> <li>• mg9kemmidtier (MG9KMIDTIER)</li> </ul> |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .    |
| 2 Restart the MG 9000 Manager components to enable the applied patches.                                                                                                                |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> . |

### NPM

The table below lists the procedures you must perform to patch the Network Patch Manager (NPM). The procedures must be performed in the order they are listed.

**Note:** Ensure you have applied any [SPFS](#) and [PSE](#) patches prior to patching the NPM software.

Use this table as a checklist during the patching process. Place a check (✓) in the ✓column as you complete each procedure.

### Patching procedures checklist for the NPM

| Activities                                              | ✓ | Procedures                                                                         |
|---------------------------------------------------------|---|------------------------------------------------------------------------------------|
| 1 Apply the patches to the Network Patch Manager (NPM). |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .    |
| 2 Restart the NPM to enable the applied patches.        |   | Perform procedure <a href="#">Restarting a device using the NPM on page 2364</a> . |

### Multi-service Data Manager

Refer to [Multiservice Data Manager upgrade on page 833](#)

## Multiservice Switch 15000

Refer to section “Installing and downloading Multiservice Switch 15000 software and patches” in [Downloading and backing up MSS 15000/MG 15000 software on page 938](#).

## GWC

Patching activities occur when new patches become available and need to be installed and activated. They also occur when an older patch becomes obsolete and must be deactivated and removed.

The table below lists the procedures you must perform to patch the GWC. The procedures must be performed in the order they are listed.

Use this table as a checklist during the patching process. Place a check (✓) in the ✓ column as you complete each procedure.

**Note:** Apply all patches to the Gateway Controller (GWC), including the ACT category patches that apply to your site. Contact Nortel customer support to determine which ACT category patches are to be activated in your site. Do not activate any other GWC ACT category patches unless advised to do so by Nortel customer support.

### Patching procedures checklist for the GWC

| Activities                                        | ✓ | Procedures                                                                               |
|---------------------------------------------------|---|------------------------------------------------------------------------------------------|
| 1 Audit the GWC unit for existing patch activity. |   | Perform procedure <a href="#">Performing a device audit using the NPM on page 2313</a> . |
| 2 Apply the patches to the standby GWC unit.      |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .          |
| 3 Activate the applicable patches.                |   | Perform procedure <a href="#">Activating patches using the NPM on page 2334</a> .        |
| 4 Take an image of the standby GWC unit.          |   | Refer to <a href="#">Take a manual GWC software image on page 1536</a> .                 |

## MG 4000

If you are performing an upgrade with patching, refer to the upgrade procedure in this document. If you are performing maintenance patching, refer to the *Post-Release Software Manager (PRSM) Reference Guide*, 297-8991-540.

## MG 9000

The table below provides the procedures you must perform to patch the Media Gateway 9000 (MG 9000). The procedures must be performed in the order they are listed.

Use this table as a checklist during the patching process. Place a check (✓) in the ✓column as you complete each procedure.

### Patching procedures checklist for the MG 9000

| Activities |                                                | ✓ | Procedures                                                                               |
|------------|------------------------------------------------|---|------------------------------------------------------------------------------------------|
| 1          | Audit the devices for existing patch activity. |   | Perform procedure <a href="#">Performing a device audit using the NPM on page 2313</a> . |
| 2          | Apply the patches to the MG 9000.              |   | Perform procedure <a href="#">Applying patches using the NPM on page 2319</a> .          |

**Note:** You have the capability to perform an image on an MG 9000 device, which allows you to upgrade the remaining MG 9000 devices in the office with the newly imaged load. You also have the capability to schedule imaging so that it occurs automatically. Refer to section [Patch management on page 2283](#) for more details.

## IW-SPM

If you are performing an upgrade with patching, refer to the upgrade procedure in this document. If you are performing maintenance patching, refer to the *Post-Release Software Manager (PRSM) Reference Guide*, 297-8991-540.

## DPT-SPM

If you are performing an upgrade with patching, refer to the upgrade procedure in this document. If you are performing maintenance patching, refer to the *Post-Release Software Manager (PRSM) Reference Guide*, 297-8991-540.

## Legacy Peripheral Modules

Refer to the *Post-Release Software Manager (PRSM) Reference Guide*, 297-8991-540.

## CS 2000

Refer to the *Post-Release Software Manager (PRSM) Reference Guide*, 297-8991-540.

**Media Server Series 2000**

Media Server 2010 and 2020 patches are available through web access, service delivery, or CD-ROM. When applying a patch always refer to either the *Readme* or the *Disk Admin* file for installation instructions.

## Patch management

The procedures available to manage your patching activities using the Network Patch Manager (NPM), are listed in the table that follows.

### Patch management procedures

| Procedure                                                                             | Page |
|---------------------------------------------------------------------------------------|------|
| <a href="#">Defining NPM patching sets</a>                                            | 2374 |
| <a href="#">Defining NPM patching tasks</a>                                           | 2382 |
| <a href="#">Setting field values using the NPM</a>                                    | 2388 |
| <a href="#">Defining NPM patching reports</a>                                         | 2393 |
| <a href="#">Defining NPM patching plans</a>                                           | 2401 |
| <a href="#">Modifying NPM patching plans</a>                                          | 2409 |
| <a href="#">Prioritizing or aborting a patching maintenance request using the NPM</a> | 2421 |
| <a href="#">Performing a device image using the NPM</a>                               | 2327 |

To automate a task, perform procedure [Defining NPM patching tasks on page 2382](#) to define the task, for example autoimaging, then perform procedure [Modifying NPM patching plans on page 2409](#) to include the task you saved, for example autoimaging, in the plan.



---

## Accessing the Network Patch Manager CLUI

---

### Application

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

**Note 1:** You can also access the NPM CLUI from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to *IEMS Basics*, NN10329-111.

**Note 2:** The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

### Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

### Action

Perform the following steps to complete this procedure.

#### At your workstation

- 1 Establish a login session to the server, using one of the following methods:

| If using          | Do                     |
|-------------------|------------------------|
| telnet (unsecure) | step <a href="#">2</a> |
| ssh (secure)      | step <a href="#">3</a> |

- 2 Log in to the server using telnet (unsecure) as follows:
  - a Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SPFS-based server
  - b When prompted, enter your user ID and password.

Proceed to step [4](#).

- 3** Log in using ssh (secure) as follows:

- a** Log in to the server by typing

```
> ssh -l <userID> <server>
```

and pressing the Enter key.

where

**server**

is the IP address or host name of the SPFS-based server

**Note:** If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter *yes* at the prompt.

- b** When prompted, enter your password.

- 4** Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

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

*Example response:*

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

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

---

## Launching CS 2000 Management Tools and NPM client applications

---

### Application

Use this procedure to launch any one of the following client applications:

- Trunk Maintenance Manager (TMM)
- CS2000 Management Tools
- Line Maintenance Manager (LMM)
- SAM21 Element Manager
- Batch Configuration Monitor
- Network Patch Manager (NPM), when installed and enabled on the same SPFS-based server as the CS 2000 Management Tools

**Note:** The NPM also has a command line user interface (CLUI). Refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

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

- [Launching applications from a web browser on page 2288](#). You must use this method when launching an application for the first time.
- [Launching applications from the JWS Application Manager on page 2291](#).
- [Launching applications from a desktop icon or Start menu \(Windows only\) on page 2293](#).
- [Launching specific applications using a URL on page 2295](#).

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

You can also launch applications from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to document *IEMS Basics*, NN10329-111.

### Prerequisites

Ensure the client workstation meets the minimum requirements. Refer to section “Client workstation requirements” under “CS 2000

Management Tools” in the Basics document for your solution.

**CAUTION**

If you have an ATI Raedon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you can experience the “blue screen of death” in your Windows environment. You can obtain information on this issue at the following website:

<http://developer.java.sun.com/developer/bugParade/bugs/4713003.html>

A workaround for this issue is to download the latest ATI graphics driver from the following web site:

<http://mirror.ati.com/support/driver.html>

Contact your IT support team if you need assistance.

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

**Note:** Users of the CS 2000 Management Tools client applications must belong to the primary user group “succssn” for login access, and to one or more secondary user groups, which specify the operations a user is authorized to perform. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2\_08 and Java™ Web Start (JWS) version 1.4.2\_08 installed to launch the following applications:

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

**Note:** JWS 1.4.2\_08 is included as part of JRE 1.4.2\_08.

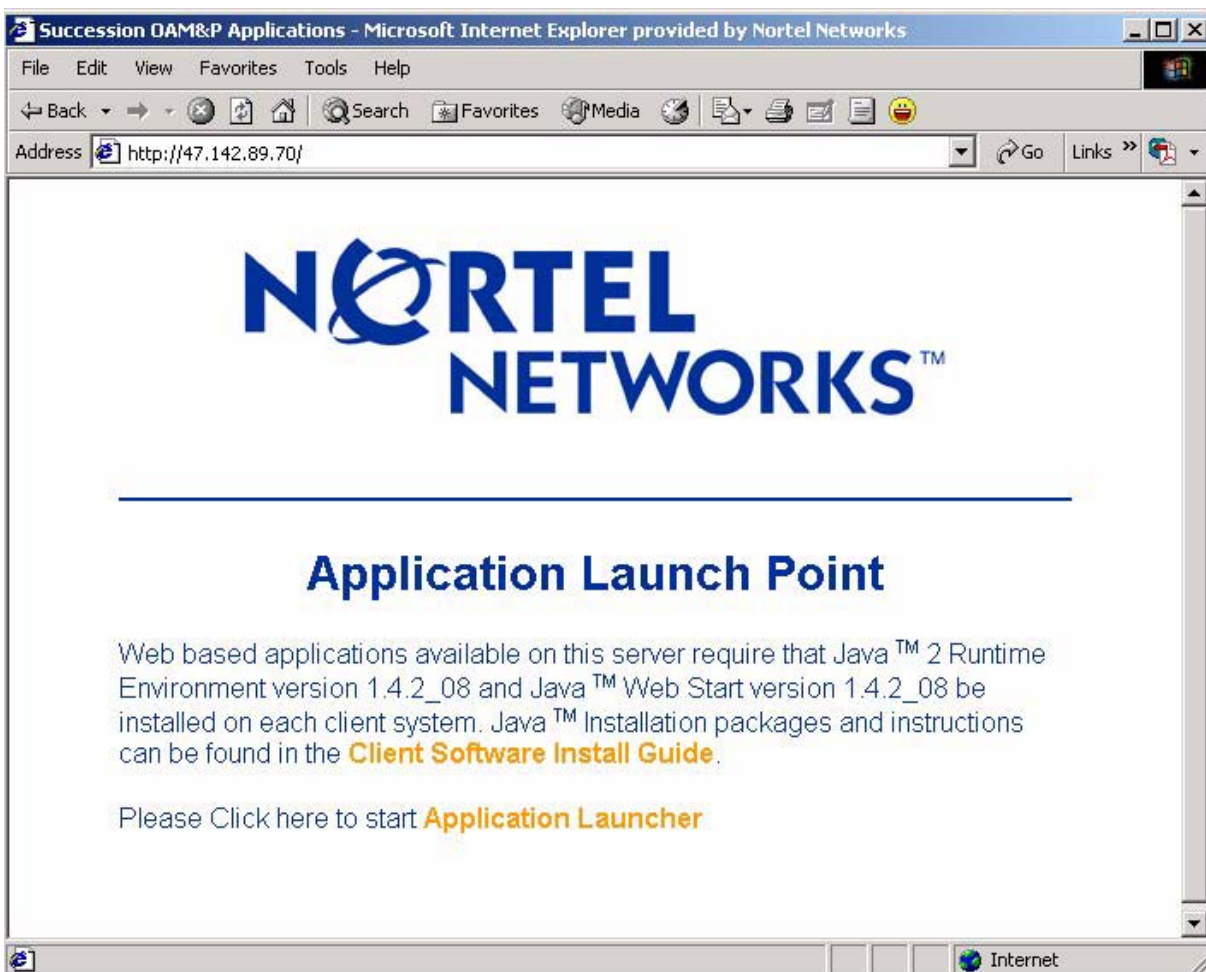
## Action

### Launching applications from a web browser

#### *At your workstation*

- 1 Launch your web browser.
- 2 In the Address field, enter the name or IP address of the SPFS-based server where the CS 2000 Management Tools are installed.

The Application Launch Point page appears.



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

| If                                                      | Do                     |
|---------------------------------------------------------|------------------------|
| you have JRE 1.4.2_08 and JWS 1.4.2_08 installed        | step <a href="#">9</a> |
| you do not have JRE 1.4.2_08 and JWS 1.4.2_08 installed | step <a href="#">4</a> |
| you do not know which version of JRE and JWS you have   | step <a href="#">4</a> |

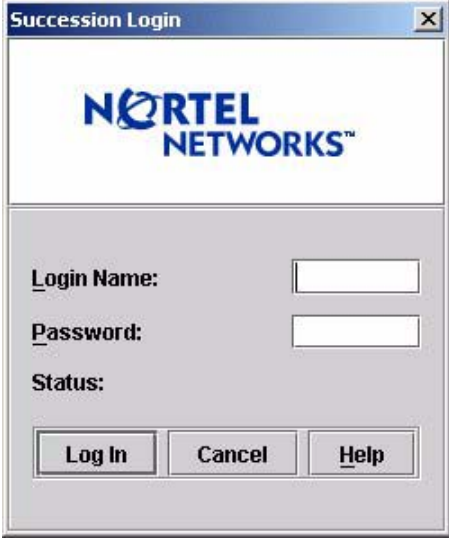
- 4 Click **Client Software Install Guide** and follow the instructions under How to check version to verify your client setup.

| If                                                      | Do                     |
|---------------------------------------------------------|------------------------|
| you have JRE 1.4.2_08 and JWS 1.4.2_08 installed        | step <a href="#">8</a> |
| you do not have JRE 1.4.2_08 and JWS 1.4.2_08 installed | step <a href="#">5</a> |

- 5 Click **Java 2 Runtime Environment Install Guide** under Microsoft Windows or Sun Solaris for system requirements and installation instructions.
- 6 Once you have read through the Java 2 Runtime Environment Install Guide, click **Back** to return to the Client Software Installation page.
- 7 Click **Java 2 Runtime Environment Software Download** under Microsoft Windows or Sun Solaris to download and install the software.
- Note:** You must have administrative privileges to install the software on the workstation.
- 8 Click **Back** to return to the Application Launch Point.

9 Click **Application Launcher**.

The Login window appears.

A screenshot of a web browser window titled "Succession Login". The window has a blue header bar with the title and a close button. Below the header is the Nortel Networks logo. The main content area is light gray and contains three labels: "Login Name:", "Password:", and "Status:". Each label is followed by a text input field. At the bottom of the window are three buttons: "Log In", "Cancel", and "Help".

Succession Login

**NORTEL  
NETWORKS™**

Login Name:

Password:

Status:

Log In Cancel Help

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

The Application Launch Point, similar to following, appears.

A screenshot of a web browser window titled "Application Launch Point - 47.142.117.20 (CM CLI: RLGHNCPR5M8)". The window has a blue header bar with the title and standard window controls. The main content area is white and features the Nortel Networks logo at the top. Below the logo is the title "Application Launch Point" in a large, bold, blue font. Underneath this title is the text "Web based applications available on this server ( 47.142.117.20 )". A bulleted list of application names follows: "CS2000 Management Tools", "Line Maintenance Manager", "Trunk Maintenance Manager", "Batch Configuration Monitor", "Succession SAM21 Element Manager", and "Network Patch Manager". At the bottom of the window is a gray bar with the text "Applet running...".

Application Launch Point - 47.142.117.20 (CM CLI: RLGHNCPR5M8)

**NORTEL  
NETWORKS™**

**Application Launch Point**

Web based applications available on this server ( 47.142.117.20 )

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

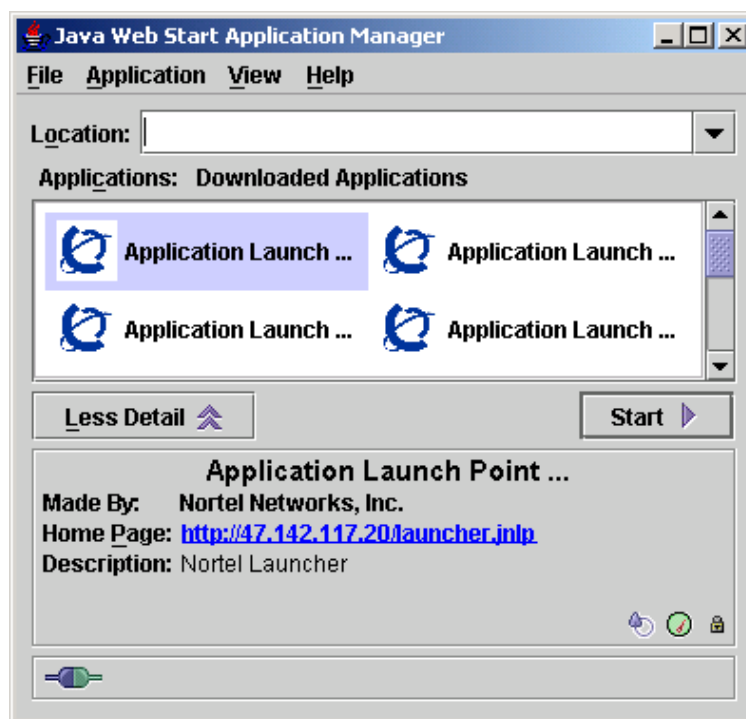
Applet running...

- 11 Click the link for the application you want to launch.  
If you delay clicking an application link by 5 minutes or more after you log in, the login window will appear requiring you to log in again.  
The interface for the application you launched, is displayed.
- 12 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

## Launching applications from the JWS Application Manager

### *At your workstation*

- 1 Launch the Java Web Start Application Manager.



- 2 If you do not see the downloaded applications as shown in the previous figure, then on the View menu click **Downloaded Applications**. Otherwise, skip to the next step.



- 3 Double-click the Application Launch Point you want to access, or select the Application Launch Point and click Start.

The Login window appears.

A small dialog box titled "Succession Login" with a close button (X) in the top right corner. The dialog box has a light gray background. At the top, there is a white rectangular area containing the "NORTEL NETWORKS" logo. Below this, there are three labels: "Login Name:", "Password:", and "Status:". Each label is followed by a white rectangular input field. At the bottom of the dialog box, there are three buttons: "Log In", "Cancel", and "Help".

- 4 Enter your user name and password, then click **Log In**.  
The Application Launch Point, similar to following, appears.

A window titled "Application Launch Point - 47.142.117.20 (CM CLI: RLGHNCPR5M8)" with standard window controls (minimize, maximize, close) in the top right corner. The window has a white background. At the top, there is a large "NORTEL NETWORKS" logo. Below the logo, the text "Application Launch Point" is displayed in a bold, dark blue font. Underneath, it says "Web based applications available on this server ( 47.142.117.20 )". A bulleted list of applications follows: "CS2000 Management Tools", "Line Maintenance Manager", "Trunk Maintenance Manager", "Batch Configuration Monitor", "Succession SAM21 Element Manager", and "Network Patch Manager". At the bottom of the window, there is a gray status bar that says "Applet running...".

- 5 Click the link for the application you want to launch.

The interface for the application you launched, is displayed.

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

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

#### *At your workstation*

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

| If you want to launch an application from | Do                     |
|-------------------------------------------|------------------------|
| a desktop icon                            | step <a href="#">2</a> |
| the Start menu                            | step <a href="#">4</a> |

- 2 To launch a CS 2000 Management Tools client application from a desktop icon, locate the short-cut icon on your desktop, and double-click it to start the application.

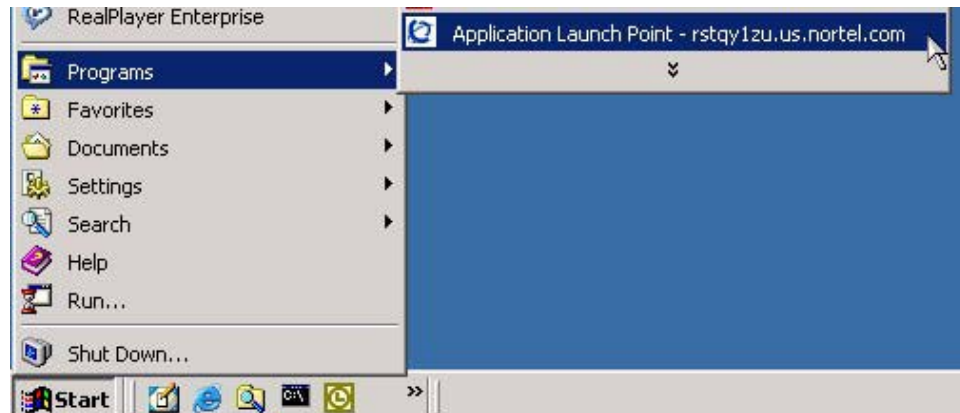
**Note:** For short-cut icons to be present on your desktop, you must have the correct settings under the Shortcut Options tab. Access the Shortcut Options tab through File->Preferences in the JWS Application Manager.



The Login window appears.

- 3 Proceed to step [5](#).

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



The Login window appears.

- 5 Enter your user name and password, then click **Log In**.  
The Application Launch Point, similar to following, appears.



- 6 Click the link for the application you want to launch.  
The interface for the application you launched, is displayed.
- 7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

### Launching specific applications using a URL

#### 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.

#### ATTENTION

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2\_08 and Java™ Web Start (JWS) version 1.4.2\_08 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in this procedure [Launching applications from a web browser on page 2288](#).

### *At your workstation*

- 1 Launch your web browser.
- 2 In the Address field, enter one of the following URLs for the application you want to launch:

| Application              | URL                                                  |
|--------------------------|------------------------------------------------------|
| CS2000 Management Tools  | http://<host>:8080/launch/servlet/Launch?app=sesm    |
| Line Maintenance Manager | http://<host>:8080/launch/servlet/Launch?app=lmm     |
| CS2000 SAM21 Manager     | http://<host>:8080/launch/servlet/Launch?app=sam21em |
| Network Patch Manager    | http://<host>:8080/launch/servlet/Launch?app=npm     |

Where

**host**

is the host name or IP address of the SPFS-based server where the application resides

The Login window appears.



- 3 Enter your user name and password, then click **Log In**.  
The interface for the application you launched, is displayed.
- 4 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

### Additional information

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and SAM21 Manager) connect to their corresponding server-side application through a Socks proxy.

**Note:** The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

When you launch a client application that connects through a Socks proxy, you can receive an error message indicating that the Socks connection to the server has failed, the server is down and needs to be rebooted. Once the server has rebooted, you can relaunch the client application.

---

## Transferring patches delivered on CD to the NPM database

---

### Application

Use this procedure when you received a patch CD with the software release you are upgrading to, and you need to transfer the patches to the Network Patch Manager (NPM) database and retrieve them for processing.

**Note:** Once NPM is installed and configured, you can enable automatic patch file delivery to the NPM database, including patch retrieval for processing, by enabling the Patch File Receipt System (PFRS). Refer to procedure “Configuring NPM for automatic patch file delivery” in *ATM/IP Solution-level Configuration Management*, NN10409-500, to enable PFRS or determine if it is already enabled.

Also use this procedure when you are either attempting to apply patches that have a blank patch category, or you are preparing for an HA cluster upgrade.

### Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

### Action

Perform the steps that follow to complete this procedure.

#### **At the server**

- 1 Insert the CD that contains the patches into the drive of the SPFS-based server where the NPM resides. In a two-server configuration, insert the CD into the drive of the active server.

***At your workstation***

- 2** Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.
- In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.
- For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 3** Determine if a tmp directory exists in the npm directory by typing
- ```
# ls -d /data/npm/tmp
```
- and pressing the Enter key.
- 4** Use the following table to determine your next step.
- | If | Do |
|--------------------------------|------------------------|
| a tmp directory does not exist | step 5 |
| otherwise | step 6 |
- 5** Make a temporary directory for the patchlist file by typing
- ```
mkdir /data/npm/tmp
```
- and pressing the Enter key.
- 6** Change the permissions on the temporary directory by typing
- ```
# chmod 777 /data/npm/tmp
```
- and pressing the Enter key.
- 7** If you have already retrieved patches that have been released since the software was shipped, such as during the CBM upgrade, you do not need to perform the next step. Go to step [9](#)
- 8** Retrieve the patches that have been released since the software was shipped by using the Pre Upgrade Patch Calculator.
- The Pre Upgrade Patch Calculator will require a label and a date. The label is the eight character product name of the software component being upgraded and the date is the date the CD was shipped. This label and date are written on the CD.
- Use the **/data/npm/tmp** directory to receive any patch files obtained from using the Pre Upgrade Patch Calculator and use the NPM CLUI getpatch command to transfer them into the NPM database.
- For detailed steps, refer to [Ensuring patch currency on page 12](#).

- 9 Create the .patchlist file for all the patches that are on the CD in the temporary directory by typing (as a single command on a continuous line)

```
# find /cdrom -name '*.patch' >
/data/npm/tmp/current.patchlist
```

and pressing the Enter key.

- 10 Access the directory you just created by typing

```
# cd /data/npm/tmp
```

and pressing the Enter key.

- 11 Verify the NPM server application is running by typing

```
# servquery -status -group NPM
```

and pressing the Enter key.

If the NPM server application is	Do

not running	step 12

running	step 13

- 12 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

- 13 Access the NPM command line user interface (CLUI) by typing

```
# npm
```

and pressing the Enter key.

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

Note: Do not change directories.

- 15 Retrieve the patch files copied from the CD by typing

```
npm> getpatch current.patchlist
```


and pressing the Enter key.

Note: Ignore the following error message which may appear if an older load cannot verify a patch for a newer load:

```
Error: Patch file
/data/npm/patch_upgrade/lex83o9s.ptchoamp
cannot be verified. Copying to golden
directory.
```

- 16** Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

- 17** Change to the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- 18** Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

and pressing the Enter key.

```
# /etc/init.d/volmgt start
```

and pressing the Enter key.

Then, press the eject button located on the front of the DVD drive.

- 19** Remove the CD or DVD from the drive.

If	Do
you have other patch CDs to install	insert the next CD and go to step 9
otherwise	close the cdrom tray and proceed to the next step

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

Manually placing patches in the NPM database

Application

Use this procedure when you receive new patches after the software release via nortel.com or when new patches have been placed on the patch drop box and you need to transfer the patches to the Network Patch Manager (NPM) database for processing.

Prerequisites

This procedure has the following prerequisites:

- You must know the name or IP address of the SPFS-based server that is hosting the NPM.
- To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.
- If you are using patches retrieved from nortel.com they must be already resident on the server where the NPM is running and you must know the directory (or directories) on the NPM server where they reside. Furthermore these patch files must have read permissions for all users.
- If you are using the patch drop box to retrieve patches, the Patch File Retrieval System (PFRS) must be configured. If required, refer to the procedure [Configuring NPM for automatic patch file delivery on page 493](#). Note you do not have to enable the GETPATCH or GENREPORT plans to complete this procedure.
- If you are using the patch drop box the new patches to be placed in the NPM database must be resident on the patch drop box.

Action

Perform the steps that follow complete this procedure.

At your workstation

- 1 Establish a connection to the server that is hosting the NPM through telnet or SSH, and log in using a valid user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **ubmstat** command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

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

If	Do
patch files to be placed in the NPM database are resident on the server where the NPM is running	step 5
patch files to be placed in the NPM database are resident on the patch drop box	step 3

- 3 Use one of the following methods to transfer the patches from the patch drop box to the server:

- [Using the NPM CLUI on page 2304](#)
- [Using the NPM GUI on page 2306](#)

- 4 Proceed to [step 19](#).

- 5 Access the directory where patch files were downloaded.

Example

```
# cd /esd_patches
```

- 6 List all the patch files in the directory by typing

```
# ls *.patch
```

and pressing the Enter key.

- 7 If you want to place all of the patches in this directory in the NPM database create a .patchlist file by typing:

```
# ls *.patch > current.patchlist
```

and pressing the Enter key.

- 8 Verify the NPM server application is running by typing

```
# servquery -status -group NPM
```

and pressing the Enter key.

- 9 Use the following table to determine your next step:

If the NPM server is	Do
running	step 11
not running	step 10

- 10 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

- 11 Ensure you are in the directory where you downloaded the patches by typing

```
# pwd
```

and pressing the Enter key.

The response must be the directory where the patch files reside.

Example response

```
/esd_patches
```

If	Do
you are in the directory where the patches reside	step 13
otherwise	step 12

- 12 Access the directory by typing

```
# cd /<directory>
```

and pressing the Enter key.

where

directory

is the directory where the patches reside

Example

```
# cd /esd_patches
```

- 13 Access the NPM command line interface (CLUI) by typing

```
# npm
```

and pressing the Enter key.

If required, refer to [Accessing the Network Patch Manager CLUI on page 2284](#).

14 When prompted, enter your user ID and password.

15 To retrieve all the patch files in the directory type

```
npm> getpatch current.patchlist
```

and press the Enter key.

To retrieve a specific patch file in the directory type

```
npm> getpatch <filename>
```

and press the Enter key.

Note: Ignore the following error message which may appear if an older load cannot verify a patch for a newer load:

```
Error: Patch file  
/data/npm/patch_upgrade/lex83o9s.ptchoamp  
cannot be verified. Copying to golden  
directory.
```

16 Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

17 Access the directory that contains the downloaded patch files by typing

```
# cd /<directory>
```

and pressing the Enter key.

where

directory

is the directory where the patch files reside

Example

```
# cd /esd_patches
```

18 Erase the downloaded patch files from the directory by typing

```
# rm *.patch
```

and pressing the Enter key.

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

Using the NPM CLUI

At your workstation

1 Access the NPM command line interface (CLUI) by typing

npm

and pressing the Enter key.

If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

At the NPM CLUI

- 2 Verify Patch File Retrieval Settings (PFRS) are configured by typing

npm> **viewpfrs**

If response is	Do
Retrieving PFRS settings... No PFRS Preferences have currently been set	Configuring NPM for automatic patch file delivery on page 493
otherwise	step 3

- 3 Retrieve the new patch(es) present on the patch drop box by typing

npm> **runtask pfrsgetpatch**

and pressing the Enter key.

Example response of successful transfer:

```
npm>
Reason : Passed
Detail : The PFRSGETPATCH task was successful.
Number of patches transferred: 14
```

If the response indicates the patch transfer was not successful, then use the following to determine the corrective action:

- If response is

```
npm>
Reason : Passed
Detail : The PFRSGETPATCH task executed
successfully, however, there were no new
patches to down load to the NPM.
```

This indicates the new patches are not on the patch drop box. Get the new patches you want placed in the NPM database transferred to the patch drop box or contact your next level of support to do this and then redo this step.

- If response is

java.lang.Exception: An Exception occurred while verifying the remote server information during a PFRS operation. Connection refused

This indicates the configured patch drop box does not have its FTP server running. Either start the FTP server on the patch drop box or reconfigure PFRS to another patch drop box server by performing the procedure [Configuring NPM for automatic patch file delivery on page 493](#) and then redo this step.

- If response is

java.lang.Exception: An Exception occurred while verifying the remote server information during a PFRS operation. Not logged in - password incorrect

This indicates the configured password has expired. Reconfigure PFRS by performing the procedure [Configuring NPM for automatic patch file delivery on page 493](#) and then redo this step.

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

Using the NPM GUI

At your workstation

- 1 Access the NPM GUI.

If required, refer to the procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

At the NPM GUI

- 2 Select **Edit > Preferences...**

The Preferences window opens.

- 3 Click on the **System Preferences** tab.

- 4 Verify the Patch File Retrieval Settings (PFRS) are configured.

If the settings are configured, then close the Preferences window and proceed to step 5. If the PFRS fields are blank, then perform the procedure [Configuring NPM for automatic patch file delivery on page 493](#).

- 5 Select **Tasks > Maintenance...**

The Maintenance window opens.

- 6 Click the **Task List** tab.

- 7 Select the PFRSGETPATCH task and click **Execute**.
*The **PFRSGetPatch Task** popup window opens displaying the PRFS configuration.*
- 8 Click **Continue**.
*The PFRSGETPATCH task executes and the results are displayed in the **PFRSGetPatch Results** window that opens.*
- 9 Review the results to verify that the patch retrieval was successful.

Result	Reason	Detail
Pass	Passed	The PFRSGETPATCH task was successful. Number of patches transfered: 2

If the results indicate the patch transfer was not successful, then use the following to determine the corrective action:

- If response in the Detail column is
The PFRSGETPATCH task executed successfully, however, there were no new patches to download to the NPM.
This indicates the new patches are not on the patch drop box. Get the new patches you want placed in the NPM database transferred to the patch drop box or contact your next level of support to do this and then go to [step 4](#).
- If response in the Detail column is
java.lang.Exception: An Exception occurred while verifying the remote server information during a PFRS operation. Connection refused
This indicates the configured patch drop box does not have its FTP server running. Either start the FTP server on the patch drop box or reconfigure PFRS to another patch drop box server by performing the procedure [Configuring NPM for automatic patch file delivery on page 493](#) and then go to [step 4](#).
- If response in the Detail column is
java.lang.Exception: An Exception occurred while verifying the remote server information during a PFRS operation. Not logged in - password incorrect
This indicates the configured password has expired. Reconfigure PFRS by performing the procedure [Configuring](#)

[NPM for automatic patch file delivery on page 493](#) and then go to [step 4](#).

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

Transferring patches delivered as an ISO image file to the NPM database

Application

Use this procedure when you received a patch ISO image file with the software release you are upgrading to, and you need to transfer the patches to the Network Patch Manager (NPM) database and retrieve them for processing.

Note: Once NPM is installed and configured, you can enable automatic patch file delivery to the NPM database, including patch retrieval for processing, by enabling the Patch File Receipt System (PFRS). Refer to procedure “Configuring NPM for automatic patch file delivery” in *ATM/IP Solution-level Configuration Management*, NN10409-500, to enable PFRS or determine if it is already enabled.

Also use this procedure when you are either attempting to apply patches that have a blank patch category, or you are preparing for an HA cluster upgrade.

Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

Action

Perform the steps that follow to complete this procedure.

At your workstation

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the `ubmstat` command.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

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

If	Do
you have already mounted the patch ISO image file as part of the procedure that referred you here	step 3
otherwise	Mount the patch ISO image. For detailed steps, refer to procedure Transferring and mounting an ISO image on an SPFS-based server on page 426 .

- 3 Determine if a tmp directory exists in the npm directory by typing
`# ls -d /data/npm/tmp`
 and pressing the Enter key.

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

If	Do
a tmp directory does not exist	step 5
otherwise	step 6

- 5 Make a temporary directory for the patchlist file by typing
`# mkdir /data/npm/tmp`
 and pressing the Enter key.

- 6 Change the permissions on the temporary directory by typing
`# chmod 777 /data/npm/tmp`
 and pressing the Enter key.

- 7 Create the .patchlist file for all the patches in the temporary directory by typing

```
# find /tmpmnt -name "*.patch" >
/data/npm/tmp/current.patchlist
```

and pressing the Enter key.

- 8 Access the directory you just created by typing

```
# cd /data/npm/tmp
```

and pressing the Enter key.

- 9 Verify the NPM server application is running by typing
servquery -status -group NPM
and pressing the Enter key.
If the NPM server application is	Do
not running	step 10
running	step 12
- 10 Start the NPM server application by typing
servstart NPM
and pressing the Enter key.
- 11 Change directories:
cd /
- 12 Access the NPM command line user interface (CLUI) by typing
npm
and pressing the Enter key.
- 13 When prompted, enter your user ID and password.
- 14 Retrieve the patch files copied from the ISO image file by typing
npm> getpatch /data/npm/tmp/current.patchlist
and pressing the Enter key.
- Note:** Ignore the following error message which may appear if an older load cannot verify a patch for a newer load:
- ```
Error: Patch file
/data/npm/patch_upgrade/lex83o9s.ptchoamp
cannot be verified. Copying to golden
directory.
```
- 15     Exit the NPM CLUI by typing  
**npm> quit**  
and pressing the Enter key.
- 16     Change directories by typing  
# **cd /**  
and pressing the Enter key.
- 17     Delete the files in the temporary directory by typing  
# **rm /data/npm/tmp/\*.\***

and pressing the Enter key.

**18** Unmount the patch ISO image

For detailed steps, refer to procedure [Unmounting and removing an ISO image from an SPFS-based server on page 450](#).

**Note:** The procedure you are returning to may include the unmount as the step following the one that brought you to this procedure. If so, skip the redundant unmounting patch ISO image step.

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

---

## Performing a device audit using the NPM

---

### Application

Use this procedure to perform a device audit using the Network Patch Manager (NPM).

An audit determines whether the NPM database has accurate device patch information. If the patch category or patch status fields are blank for any patches, complete one of the following procedures to transfer the patches to the NPM database: .

- if you received patches with your software release on CD, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#)
- if you received patches with your software release through ESD, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#)
- if you received patches through ESD after the software release, refer to procedure [Manually placing patches in the NPM database on page 2301](#)

#### ATTENTION

It is recommended that you perform an audit on devices prior to patching.

### Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

### Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2314](#)
- [Using the NPM GUI on page 2315](#)

## Using the NPM CLUI

### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

**At the NPM CLUI**

- 2 Perform a query to list the devices that can be audited by typing  
npm> **q devicelist**  
and pressing the Enter key.
- 3 Audit the device by typing  
npm> **auditd <devices>**  
and pressing the Enter key.  
where

**devices**

is a list of one or more device IDs for which you want to run the audit, which uses the following syntax

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

**Example**

npm> auditd GWC-8-UNIT-1

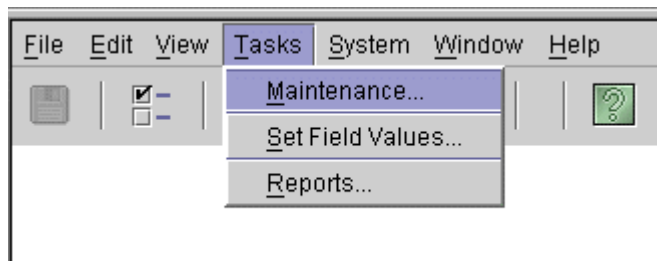
- 4 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

**Using the NPM GUI****At your workstation**

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

**At the NPM GUI**

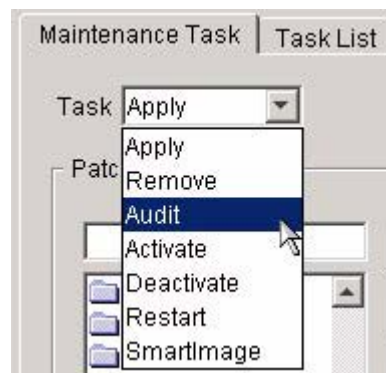
- 2 On the Tasks menu, click **Maintenance...**



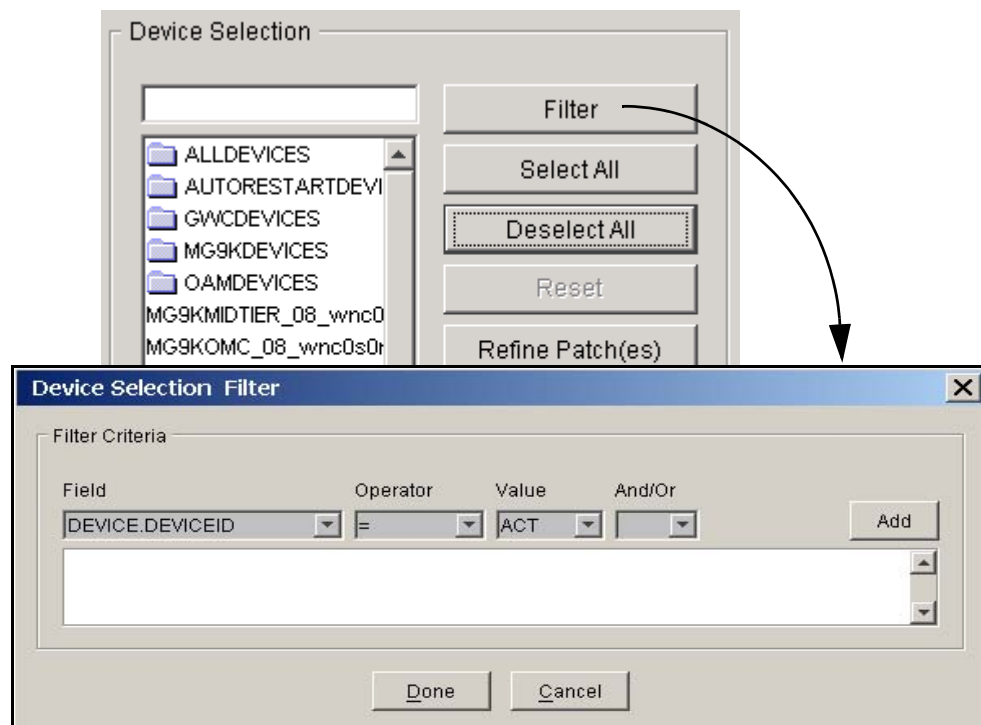
The Maintenance window is displayed.



- 3 In the Task list, click **Audit**.

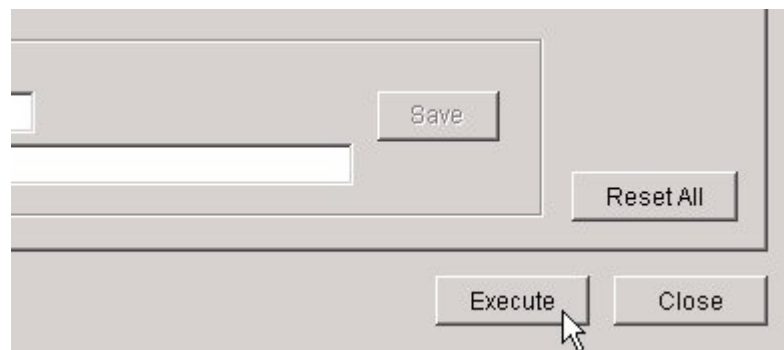


- 4 In the Device Selection list, select the devices or device sets that you want to audit.

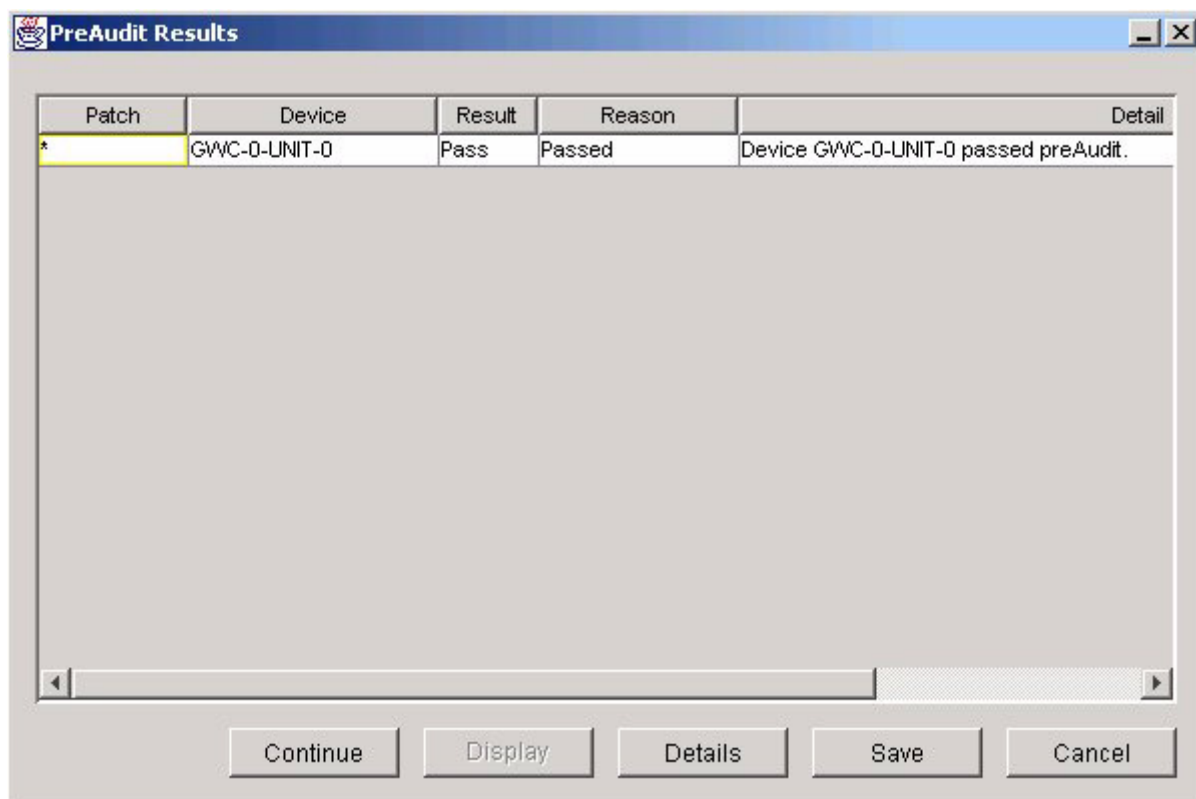


- 5 To limit the devices displayed in the Device Selection list, click **Filter** to configure a filtering criteria.

- 6 Click **Execute** to begin the audit process.



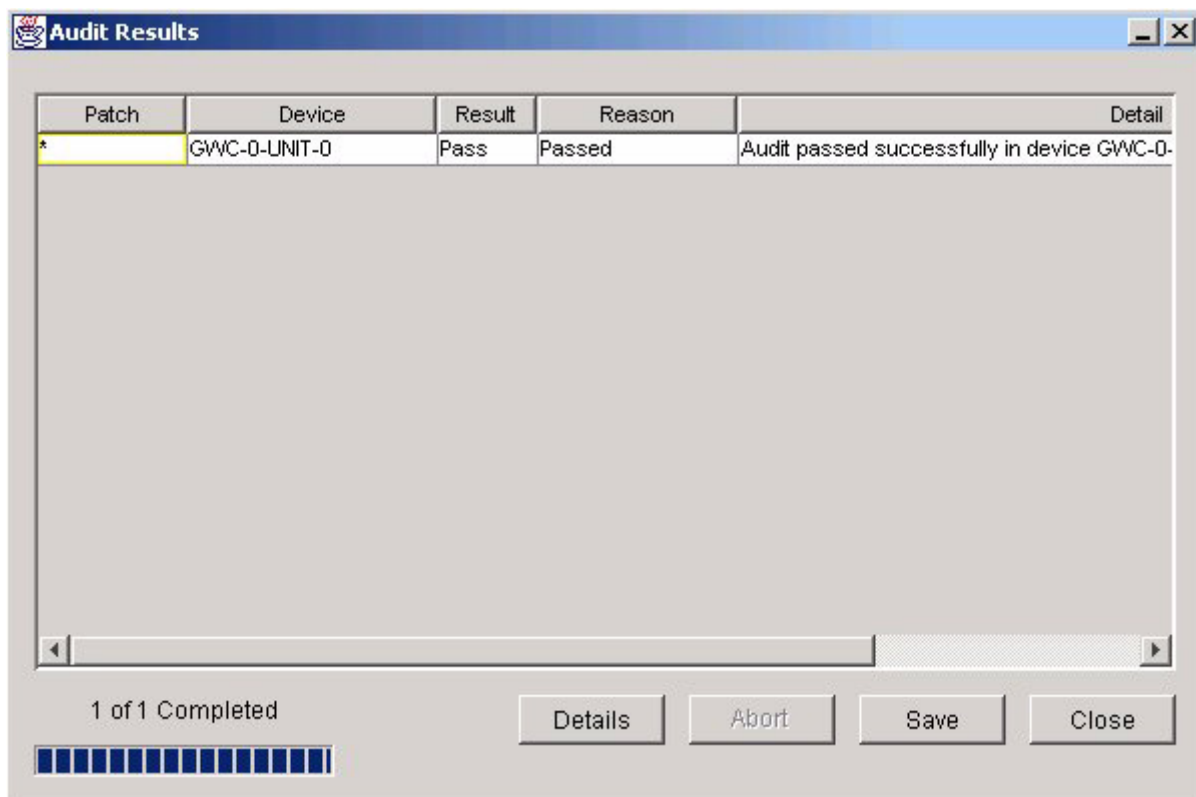
The results of the PreAudit phase are displayed.



- 7 Review the PreAudit Results, then click **Continue** to proceed.

**Note:** The Patch field in the Results Table will have an asterisk (\*) for each operation since only the device is related to the operation.

The Audit Results window is displayed with results added as each action is completed. Failures from the PreAudit phase are also included in the results.



- 8 Click **Save** to save the results to a file, or click Close.
- Note:** If the audit does not successfully complete, abort the audit procedure and contact your next level of support.
- 9 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

## Applying patches using the NPM

---

### Application

Use this procedure to apply patches using the Network Patch Manager (NPM).

### Prerequisites

The patches must have already been transferred to the NPM database. Contact your network administrator to determine if this has already been done. If required, transfer the patches to the NPM database using one of the following procedures:

- if you received patches with your software release on CD, refer to procedure [Transferring patches delivered on CD to the NPM database on page 2297](#)
- if you received patches with your software release through ESD, refer to procedure [Transferring patches delivered as an ISO image file to the NPM database on page 2309](#)
- if you received patches after the software release via nortel.com or patch drop box, refer to procedure [Manually placing patches in the NPM database on page 2301](#)

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

It is recommended that you perform an audit on the devices prior to patching. If required, refer to procedure [Performing a device audit using the NPM on page 2313](#).

### Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2319](#)
- [Using the NPM GUI on page 2322](#)

#### Using the NPM CLUI

##### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

**At the NPM CLUI**

- 2** Perform a query to list patches that can be applied and to list devices that can be patched by typing

```
npm> q patchlist
```

and pressing the Enter key.

- 3** Apply one or more patches to one or more devices by typing

```
npm> apply <patches> [in <devices>]
```

and pressing the Enter key.

where

**patches**

is a list of one or more patch IDs you want to apply using the following syntax

```
<patchid> [<patchid>...<patchid>]
```

or

```
SET <predefined set definition>
```

**devices**

is a list of one or more device IDs to which you want to apply the patches using the following syntax (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and applies them)

```
<deviceid> [<deviceid>...<deviceid>]
```

or

```
SET <predefined set definition>
```

**Example**

```
npm> apply ACT02GAX in GWC-8-UNIT-1
```

- 4** When prompted, press the Enter key.
- 5** Generate a device query report to verify the patches are applied by typing

```
npm> q device
```

- 6** Enter the device name in the format **<deviceid>** that you input in step [3](#).

A device report of known patch activity for the particular device associated with the <device id> is returned.

- 7 Verify from the report that the desired patches are applied (status =A).  
**Note:** If the patches do not successfully apply, abort the patching procedure and contact your next level of support.
- 8 If you applied patches to any of the following devices, restart the device to enable the patches for the following devices or applications:
  - Patching Server Element (PSE)
  - Integrated Element Management System (IEMS)
  - IEMS security components (IEMSCSS\_DS and IEMSCSS)
  - CS 2000 SAM21 Manager (SAM21EM)
  - Succession Element Sub-network Manager (SESM)
  - QoS Collector Application (QCA)
  - Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
  - Core Element Manager (COREM)
  - Network Patch Manager (NPM)
  - Client Session Monitor (CSMONITOR)
  - Key Manager (PKMGR\_SERVER)
  - Core and Billing Manager (CBM)

To restart a device, refer to procedure [Restarting a device using the NPM on page 2364](#) if required.
- 9 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

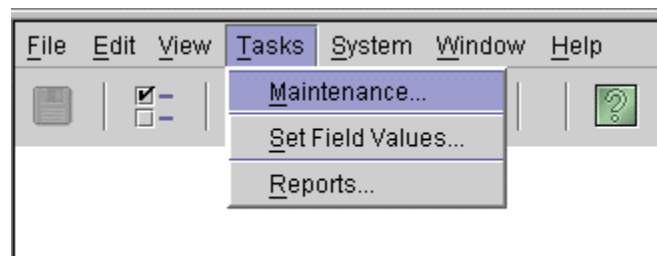
## Using the NPM GUI

### *At your workstation*

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

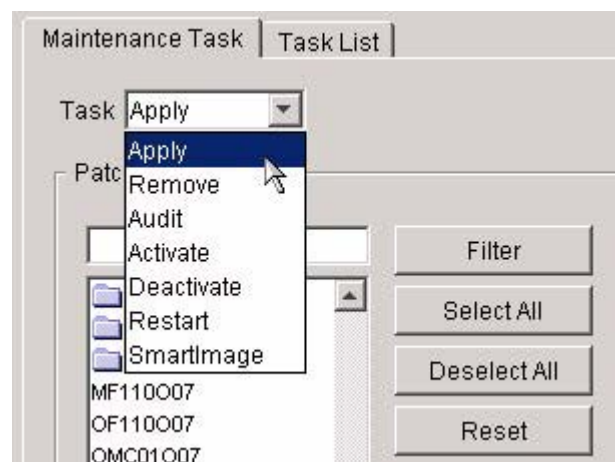
### *At the NPM GUI*

- 2 On the Tasks menu, click **Maintenance**.



The Maintenance window is displayed.

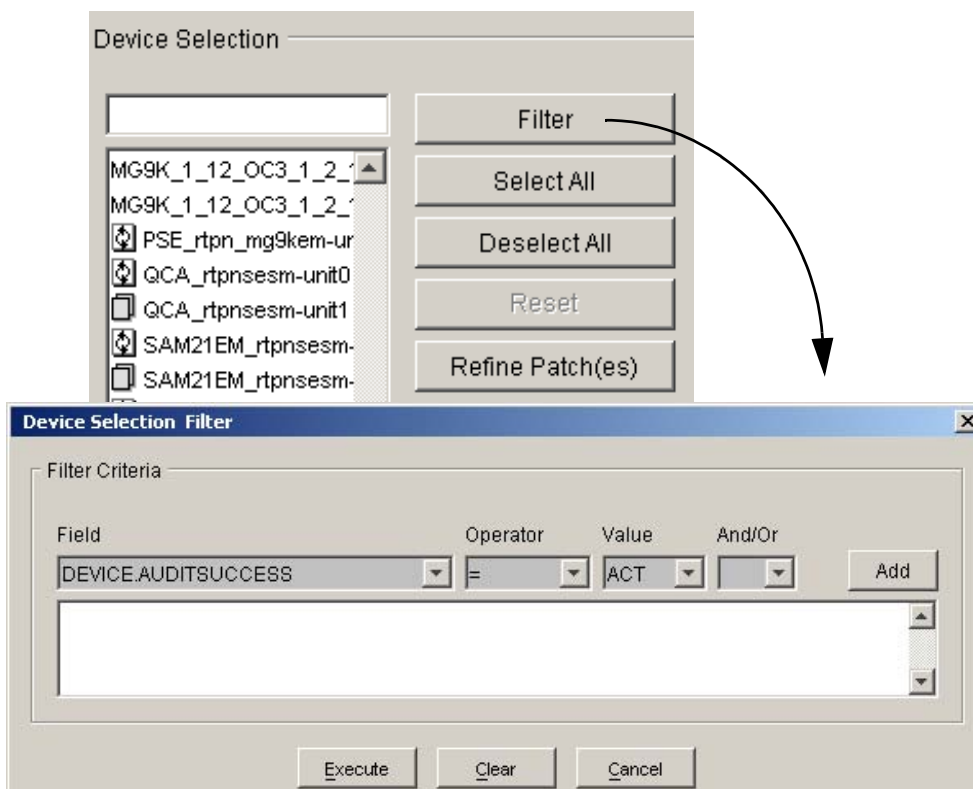
- 3 Within the MaintenanceTask tab, select **Apply** from the Task drop down menu.



- 4 In the Device Selection list, select the devices you want to apply patches to. Click **Refine Patch(es)** to display a list of patches to which devices belong.

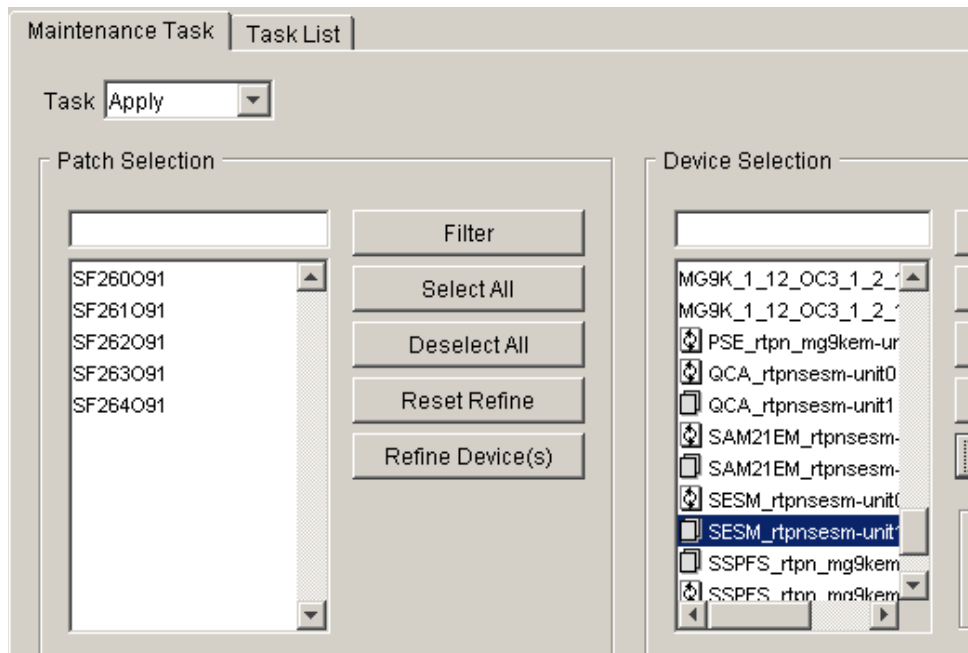
**Note:** The Refine Patch(es) button will not work on device sets.

- 5 To limit the devices displayed in the Device Selection list, click **Filter** to configure a filtering criteria.

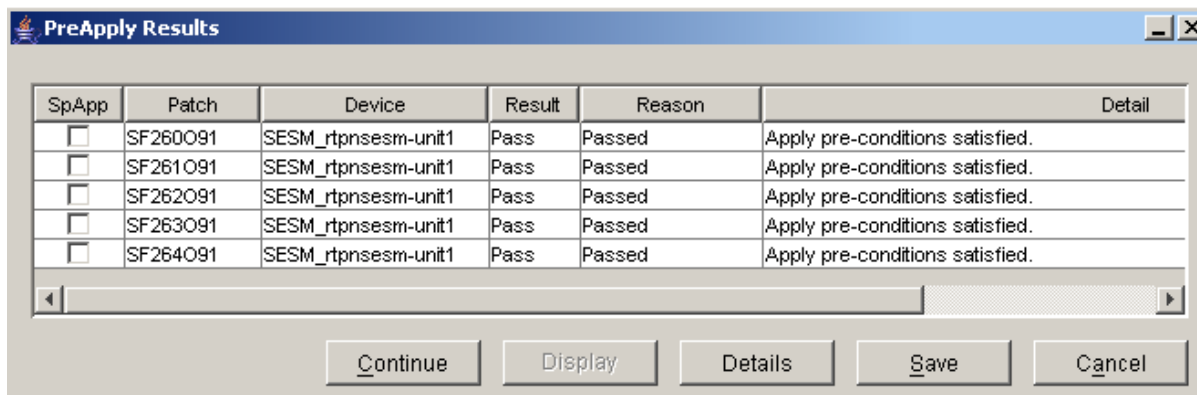




- 6 The list of patches shows only the patches applicable to the selected devices.



- 7 Click **Select All** to select the refined list of patches.
- 8 Click **Execute** to begin the patching process.  
The results of the PreApply phase are displayed.

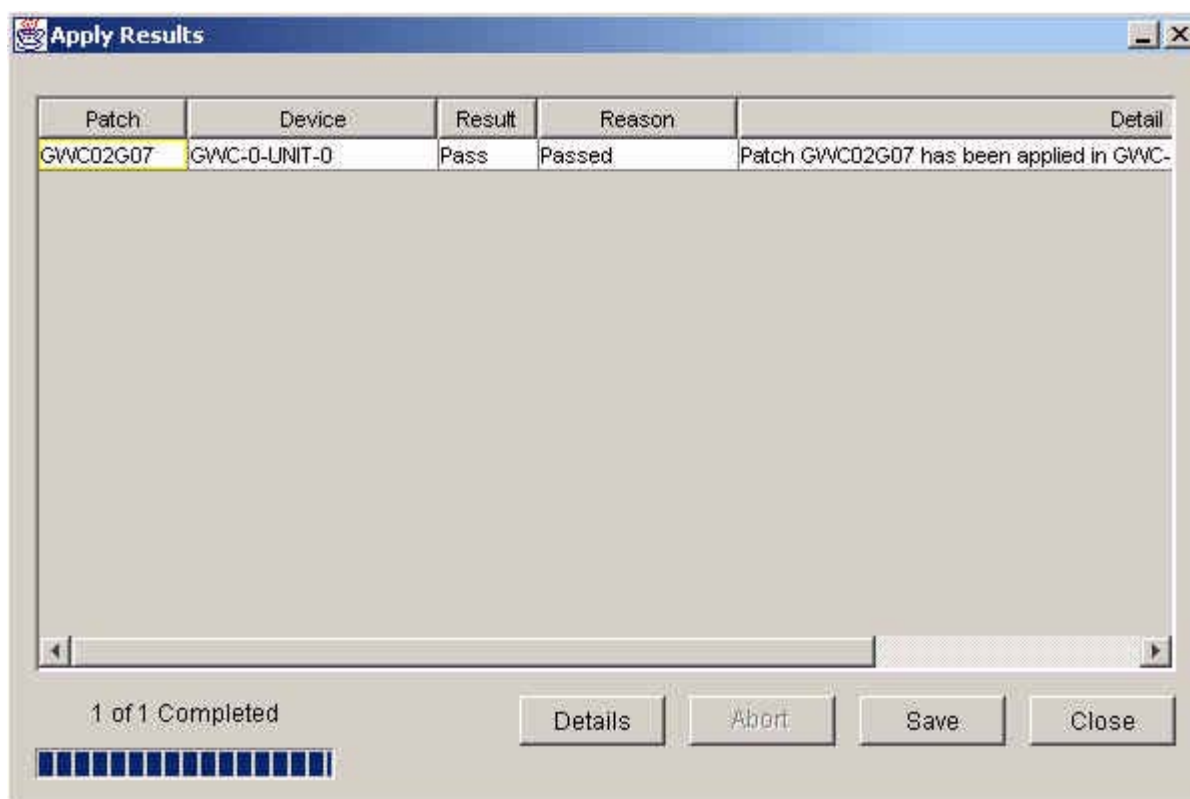


- 9 Review the PreApply Results, then click **Continue** to proceed. If any of the patches have their corresponding SpApp box checked, you must select the patch and click on **Display** before

the system will allow the request to continue. Repeat for each SpApp box that is checked.

If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Apply Results window is displayed with results added as each action is completed. Failures from the PreApply phase are also included in the results.



- 10 Click **Save** to save the results to a file, or click Close.

**Note:** If the patches do not successfully apply, abort the patching procedure and contact your next level of support.

**11** If you applied patches to any of the following devices, you need to restart the device in order to enable the patches on the device:

- Patching Server Element (PSE)
- Integrated Element Management System (IEMS)
- IEMS security components (IEMSCSS\_DS and IEMSCSS)
- CS 2000 SAM21 Manager (SAM21EM)
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
- Core Element Manager (COREM)
- Network Patch Manager (NPM)
- Client Session Monitor (CSMONITOR)
- Key Manager (PKMGR\_SERVER)
- Core and Billing Manager (CBM)

To restart a device, refer to procedure [Restarting a device using the NPM on page 2364](#) if required.

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

---

## Performing a device image using the NPM

---

### Application

Use this procedure to perform a device image using the Network Patch Manager (NPM).

**Note:** Performing a device image using the SmartImage command, is only supported for MG 9000 devices at this time.

Performing an image on an MG 9000 device allows you to upgrade the remaining MG 9000 devices in the office with the newly imaged load.

#### ATTENTION

The SmartImage command, used to perform a device image, must be used in offices where all MG 9000 devices of the same type are patched with the same patches. It is not intended for use in offices where the MG 9000 devices of the same type use a different set of patches.

For imaging to occur automatically, you can save the SmartImage command as a task (refer to procedure [Defining NPM patching tasks on page 2382](#) if required), and schedule that task as part of the NPM System Plan (refer to procedure [Modifying NPM patching plans on page 2409](#) if required).

### Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

### Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2328](#)
- [Using the NPM GUI on page 2330](#)

## Using the NPM CLUI

### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

### *At the NPM CLUI*

- 2 Perform a device image by typing

```
npm> smartimage <devices>
```

and pressing the Enter key.

where

#### **devices**

is a list of one or more device IDs you want to image using the following syntax

```
<deviceid> [<deviceid>...<deviceid>]
```

or

```
SET <predefined set definition>
```

#### **Example**

```
npm> smartimage UD16_16_62_OC3_0_2_10
```

**Note:** It is highly recommended that you use the predefined device set MG9KDEVICES to ensure the image taken is from a the device that contains the highest patch content.

For example

```
npm> smartimage SET MG9KDEVICES
```

#### *Response*

```
WARNING: You are about to perform a smartimage
on the specified devices. Note that if all
devices for a particular load are not chosen for
imaging, a device may be chosen that does not
contain the highest patch content.
If you wish to continue with this maintenance
request enter Yes (Y or y). Otherwise, just
enter return.
```

- 3 When prompted, confirm you want to continue with the maintenance request by typing  
**y**  
and pressing the Enter key.  
*Example response:*  
Patch: \*  
Device: UD16\_16\_62\_OC3\_0\_2\_10  
Result: true  
Reason: Passed  
Details: SmartImage pre-conditions satisfied.  
If you wish to continue with this maintenance request, enter Yes (Y or y). Otherwise, just enter return.
- 4 When prompted, confirm you want to continue with the maintenance request by typing  
**y**  
and pressing the Enter key.  
*Example response:*  
npm>  
Patch: \*  
Device: UD16\_16\_62\_OC3\_0\_2\_10  
Reason: Passed  
Detail: Device UD16\_16\_62\_OC3\_0\_2\_10 has been successfully imaged.
- 5 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

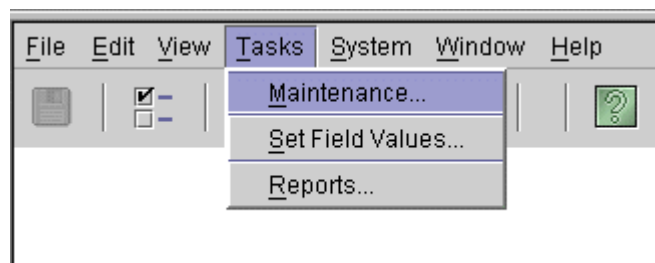
## Using the NPM GUI

### *At your workstation*

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

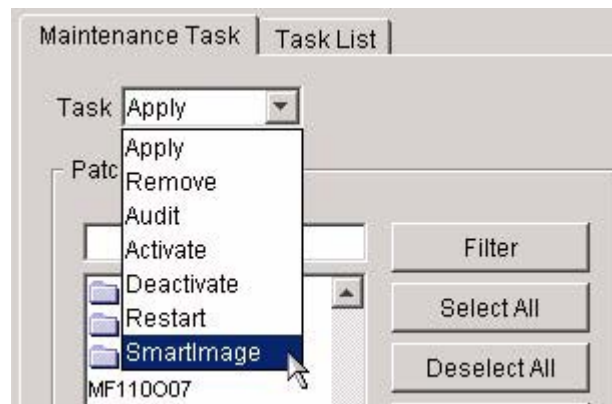
### *At the NPM GUI*

- 2 On the Tasks menu, click **Maintenance....**

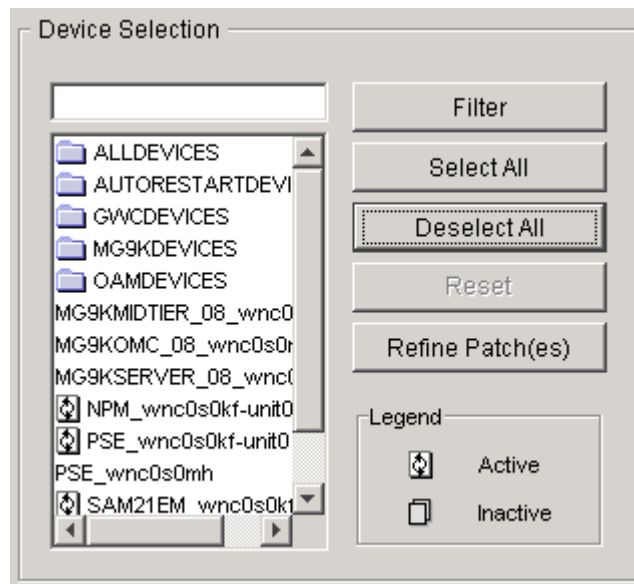


The Maintenance window is displayed.

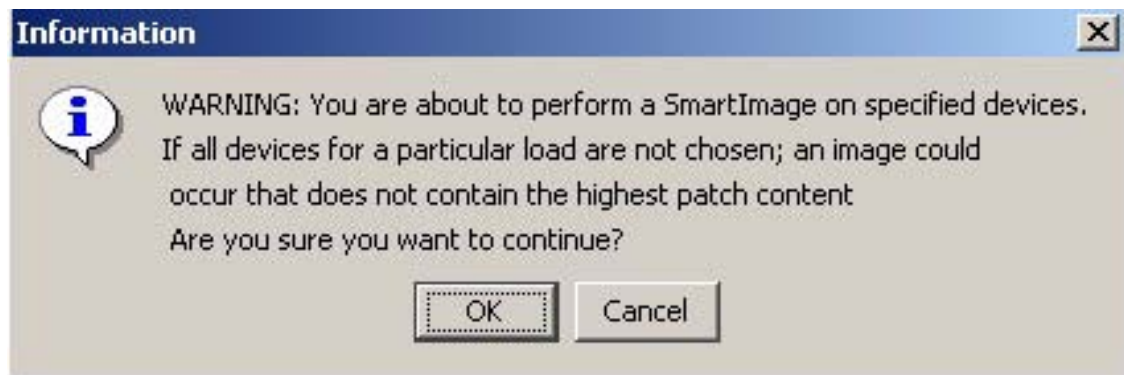
- 3 In the Task list, click **SmartImage**.



- 4 In the Device Selection list, select the device, device list, or device set that you want to image.



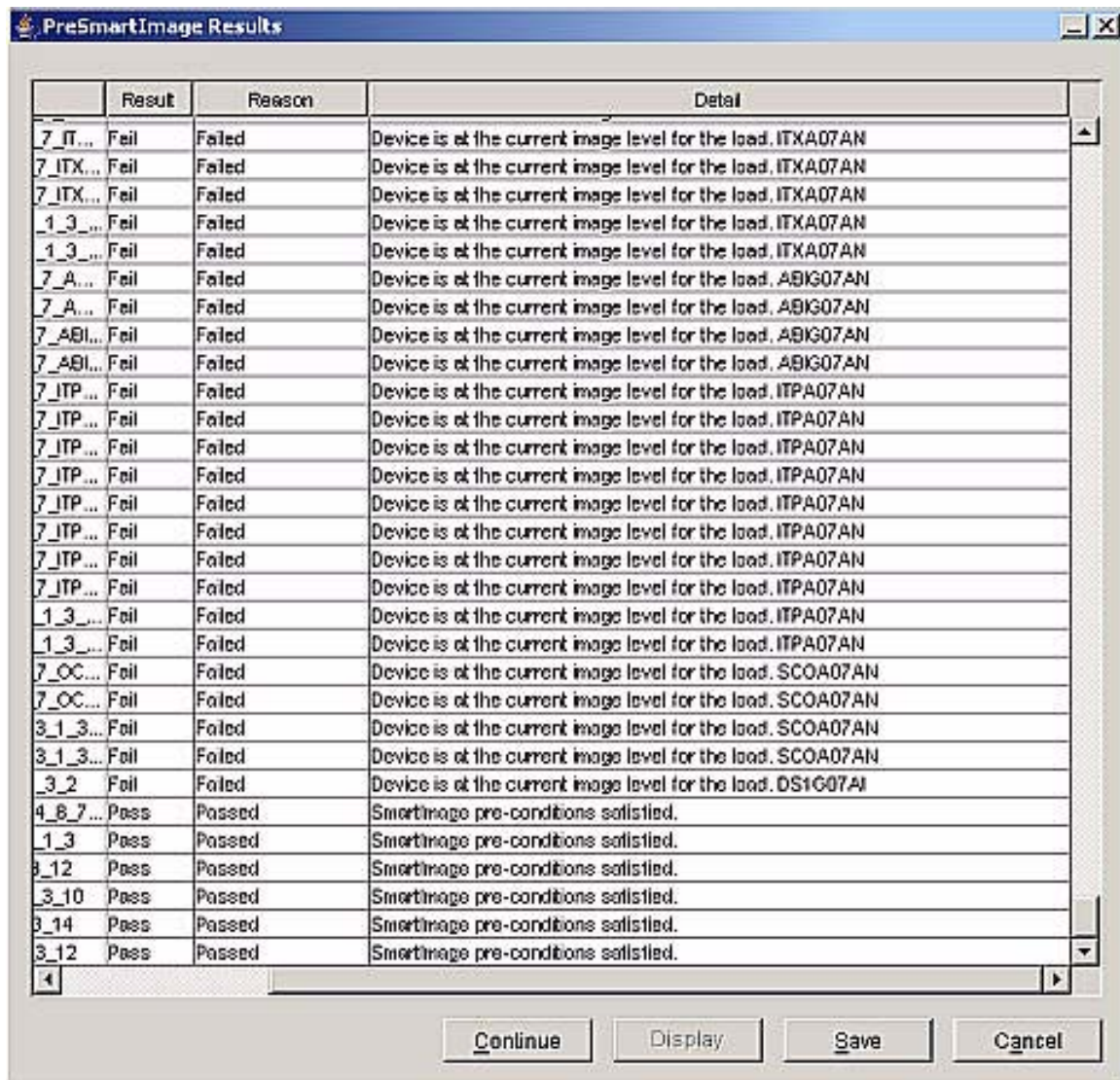
- 5 Click **Execute** to begin the restart.  
The system returns the following warning.





- 6 If you agree that the devices chosen are the ones you want evaluated, click **OK** to begin imaging.

The results of the PreSmartImage phase are displayed.

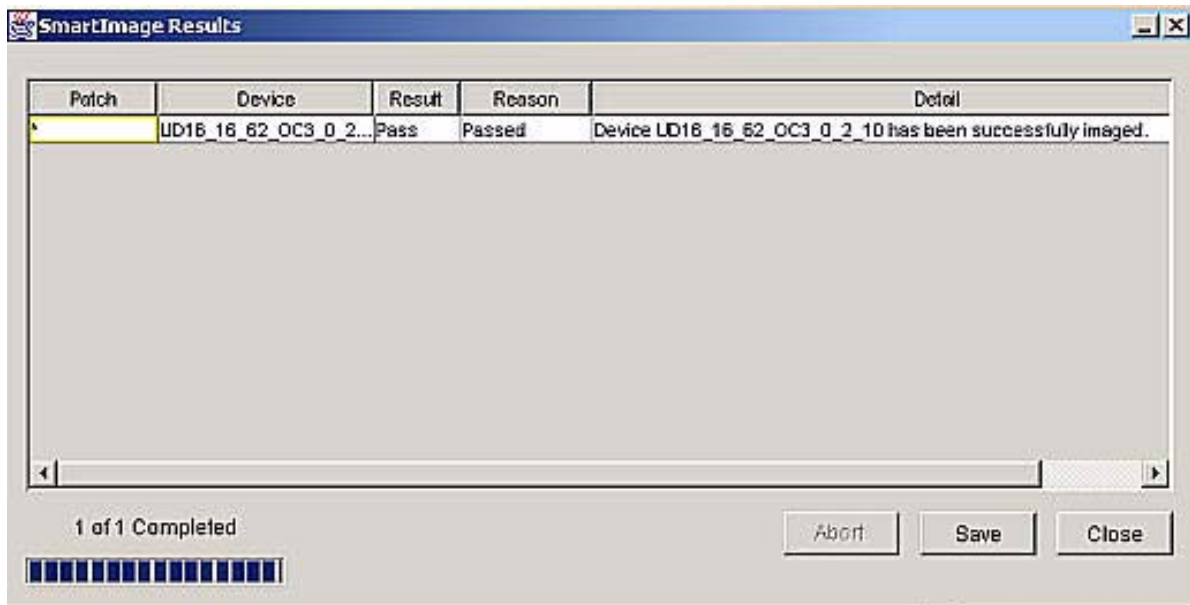


|          | Result | Reason | Detail                                                      |
|----------|--------|--------|-------------------------------------------------------------|
| 7_IT...  | Fail   | Failed | Device is at the current image level for the load, ITXA07AN |
| 7_ITX... | Fail   | Failed | Device is at the current image level for the load, ITXA07AN |
| 7_ITX... | Fail   | Failed | Device is at the current image level for the load, ITXA07AN |
| _1_3...  | Fail   | Failed | Device is at the current image level for the load, ITXA07AN |
| _1_3...  | Fail   | Failed | Device is at the current image level for the load, ITXA07AN |
| 7_A...   | Fail   | Failed | Device is at the current image level for the load, ABK07AN  |
| 7_A...   | Fail   | Failed | Device is at the current image level for the load, ABK07AN  |
| 7_ABI... | Fail   | Failed | Device is at the current image level for the load, ABK07AN  |
| 7_ABI... | Fail   | Failed | Device is at the current image level for the load, ABK07AN  |
| 7_ITP... | Fail   | Failed | Device is at the current image level for the load, ITPA07AN |
| 7_ITP... | Fail   | Failed | Device is at the current image level for the load, ITPA07AN |
| 7_ITP... | Fail   | Failed | Device is at the current image level for the load, ITPA07AN |
| 7_ITP... | Fail   | Failed | Device is at the current image level for the load, ITPA07AN |
| 7_ITP... | Fail   | Failed | Device is at the current image level for the load, ITPA07AN |
| 7_ITP... | Fail   | Failed | Device is at the current image level for the load, ITPA07AN |
| 7_ITP... | Fail   | Failed | Device is at the current image level for the load, ITPA07AN |
| _1_3...  | Fail   | Failed | Device is at the current image level for the load, ITPA07AN |
| _1_3...  | Fail   | Failed | Device is at the current image level for the load, ITPA07AN |
| 7_OC...  | Fail   | Failed | Device is at the current image level for the load, SCOA07AN |
| 7_OC...  | Fail   | Failed | Device is at the current image level for the load, SCOA07AN |
| 3_1_3... | Fail   | Failed | Device is at the current image level for the load, SCOA07AN |
| 3_1_3... | Fail   | Failed | Device is at the current image level for the load, SCOA07AN |
| _3_2     | Fail   | Failed | Device is at the current image level for the load, DS1G07AI |
| 4_8_7... | Pass   | Passed | SmartImage pre-conditions satisfied.                        |
| _1_3     | Pass   | Passed | SmartImage pre-conditions satisfied.                        |
| 3_12     | Pass   | Passed | SmartImage pre-conditions satisfied.                        |
| _3_10    | Pass   | Passed | SmartImage pre-conditions satisfied.                        |
| 3_14     | Pass   | Passed | SmartImage pre-conditions satisfied.                        |
| 3_12     | Pass   | Passed | SmartImage pre-conditions satisfied.                        |

Continue Display Save Cancel

- 7 Review the PreSmartImage Results, then click **Continue** to proceed.

The SmartImage Results window is displayed with results added as each action is completed. Failures from the PreSmartImage phase are also included in the results.



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

## Activating patches using the NPM

### Application

Use this procedure to activate patches, which are deemed activatable by the ACT category, using the Network Patch Manager (NPM).

**Note:** Currently, only GWC can have ACT category patches.

#### ATTENTION

Certain GWC patches are ACT category patches that require activation. It is important to note that not all ACT category patches require activating. The patches to be activated depend on the requirements for the GWC load. Prior to activating the ACT category patches, it is important that you read and understand the administration section of the patch and make sure the ACT patch enables the functionality you require. If you are unsure about the impact of activating an ACT patch in your office, contact your next level of support to determine if the patches can be activated.

### Prerequisites

You can activate a patch if all of the following criteria have been fulfilled:

- the patch has been identified by your support team and Nortel as being applicable and necessary for your site
- the patch is not on hold
- the patch has a category of ACT
- the patch has been applied



#### CAUTION

##### Potential for partial loss of service

Do not activate patches for your components that have not been identified as needing activation without first consulting with your network administrator and your Nortel customer support representative. Failure to do so can result in partial loss of service.

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user

settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

## Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2335](#)
- [Using the NPM GUI on page 2336](#)

### Using the NPM CLUI

#### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

#### *At the NPM CLUI*

- 2 Query the NPM for a list of patches that can be activated by typing

```
npm> q actlist
```

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime. If no patches are in the actlist, then the NPM responds with the message “Empty Results”.

- 3 Activate one or more patches for one or more devices by typing  

```
npm> activate <patches> [in <devices>]
```

and pressing the Enter key.

where

#### **patches**

is a list of one or more patch IDs you want to activate using the following syntax

```
<patchid> [<patchid>...<patchid>]
```

or

```
SET <predefined set definition>
```

**devices**

is a list of one or more device IDs for which you want to activate the patches using the following syntax (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and activates them)

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

**Example**

npm> activate ACT02GAX in GWC-8-UNIT-1

- 4 When prompted, press the Enter key.
- 5 Query the NPM to verify the patches are activated by typing

npm> **q actlist**

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime.

- 6 Verify from the list that the desired patches are activated.  
**Note:** If the patches do not successfully activate, abort the patching procedure and contact your next level of support.
- 7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

**Using the NPM GUI*****At your workstation***

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

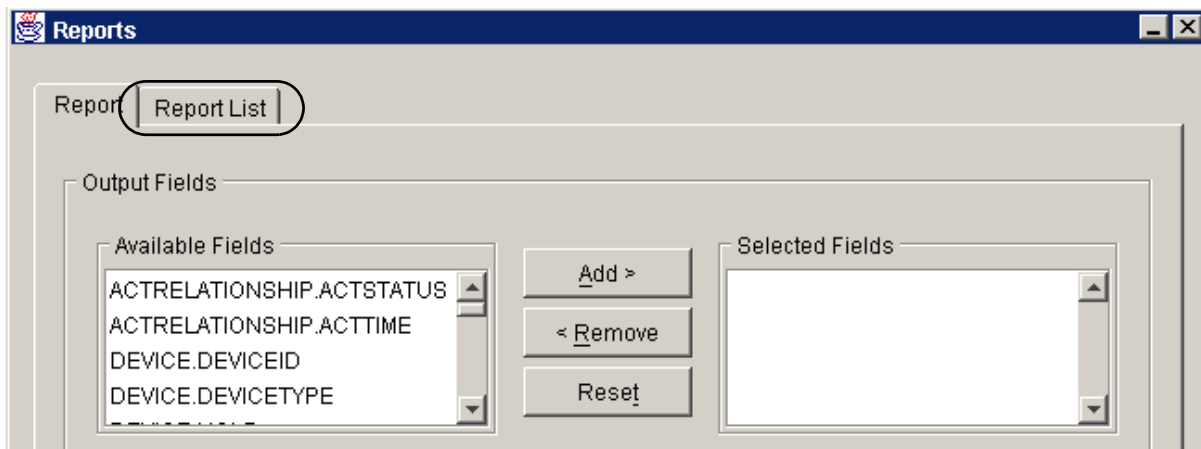
**At the NPM GUI**

- 2 On the Tasks menu, click **Reports....**



The Reports window is displayed.

- 3 Click the **Report List** tab.



4 Click the **ACTLIST** entry in the Report field, then click **Execute**.

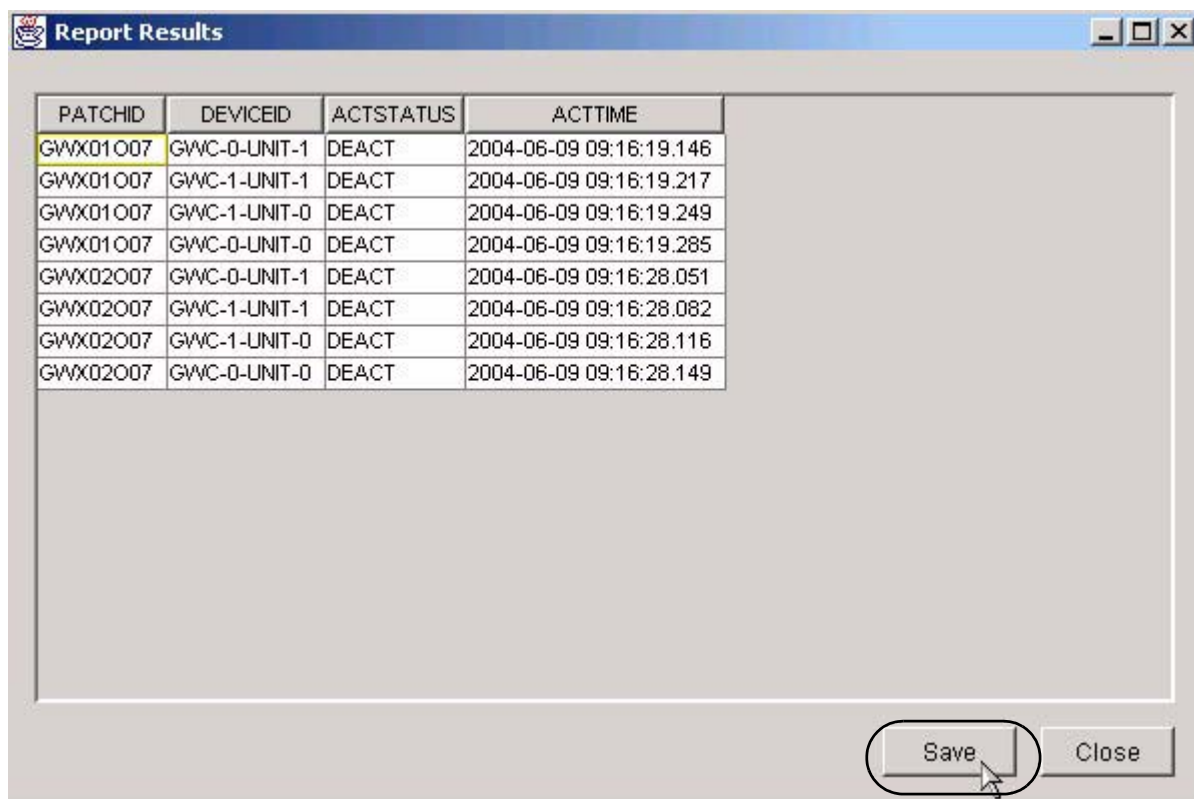
The screenshot shows a 'Report List' dialog box with a table of reports. The 'ACTLIST' entry is selected. The 'Execute' button is highlighted with a dashed border.

| Report           | Description                                                      | Type   |
|------------------|------------------------------------------------------------------|--------|
| <b>ACTLIST</b>   | RPS activation patch information.                                | System |
| CALCLIST         | RPS Patch Calculation Report.                                    | System |
| DEVICE           | Information about a specific Device (prompt).                    | System |
| DEVICELIST       | Information about patchable Device(s) on the system.             | System |
| DEVICE_ACTIVITY  | All devices and their activity states                            | System |
| DEVICE_ACTLE...  | Displays how many patches are activated in each device.          | System |
| DEVICE_APPLE...  | Displays how many patches are applied to each device.            | System |
| DISABLEDAPPLI... | Patches that are applied and disabled.                           | System |
| DISABLEDREM...   | Patches that are removed and disabled.                           | System |
| ENABLEDAPPLI...  | Patches that are applied and enabled.                            | System |
| ENABLEDREMO...   | Patches that are removed and enabled.                            | System |
| FULLDEVICELIST   | Information about every Device(s) on the system.                 | System |
| INVALID_LOAD...  | Device(s) with invalid loads. Audit required.                    | System |
| LOADLIST         | RPS Device Load Report.                                          | System |
| PATCH            | Information about a specific patch (prompt).                     | System |
| PATCHES_SINCE    | Patch Activity since a specific date (prompt).                   | System |
| PATCHINFO        | Full information about a specific patch (prompt).                | System |
| PATCHLIST        | Information about patches and their relationships on the system. | System |

Buttons: Edit, View, Delete, **Execute**, Close

- 5 Review the list of patches displayed, and note which are activated and which are deactivated. Consult with your Nortel customer support representative to determine which patch files are applicable to your site configuration and must be activated.

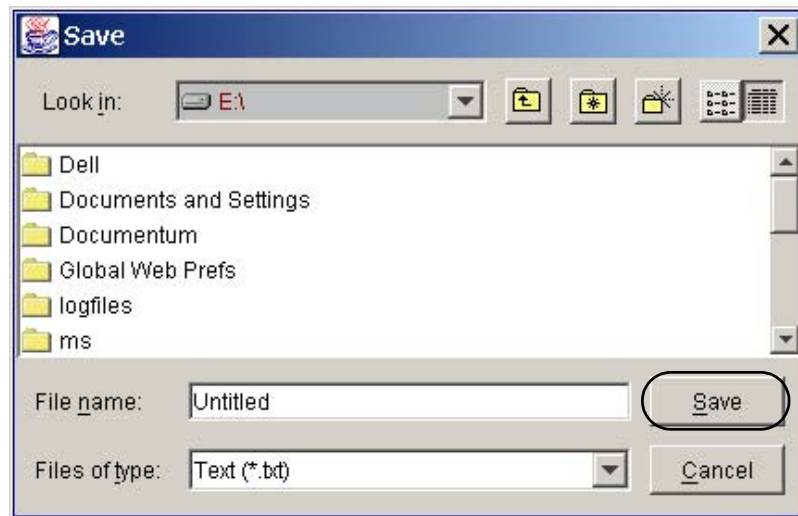
**Note:** If there are no patches to activate, the system returns a dialog box indicating that the report has “empty results”.



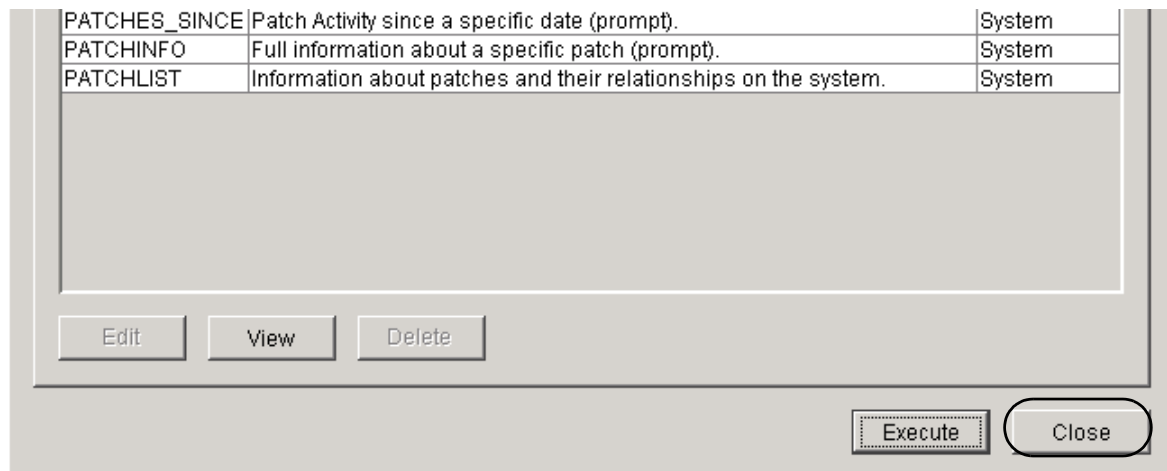
- 6 If necessary, save a copy of the report to a text file as follows:
  - a Click **Save**.



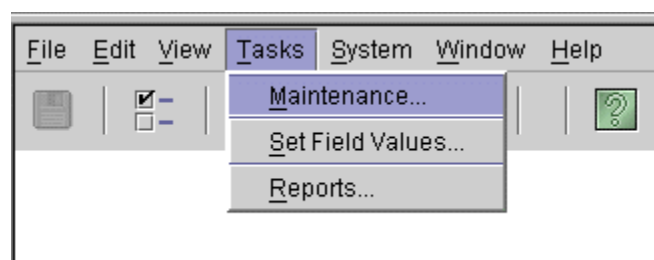
- b Type a file name in the File name: box, and click **Save**.



- 7 Click **Close** to close the Reports window.

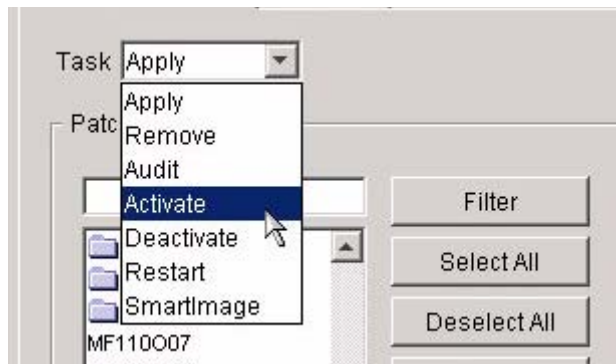


- 8 On the Tasks menu, click **Maintenance...**



The Maintenance window is displayed.

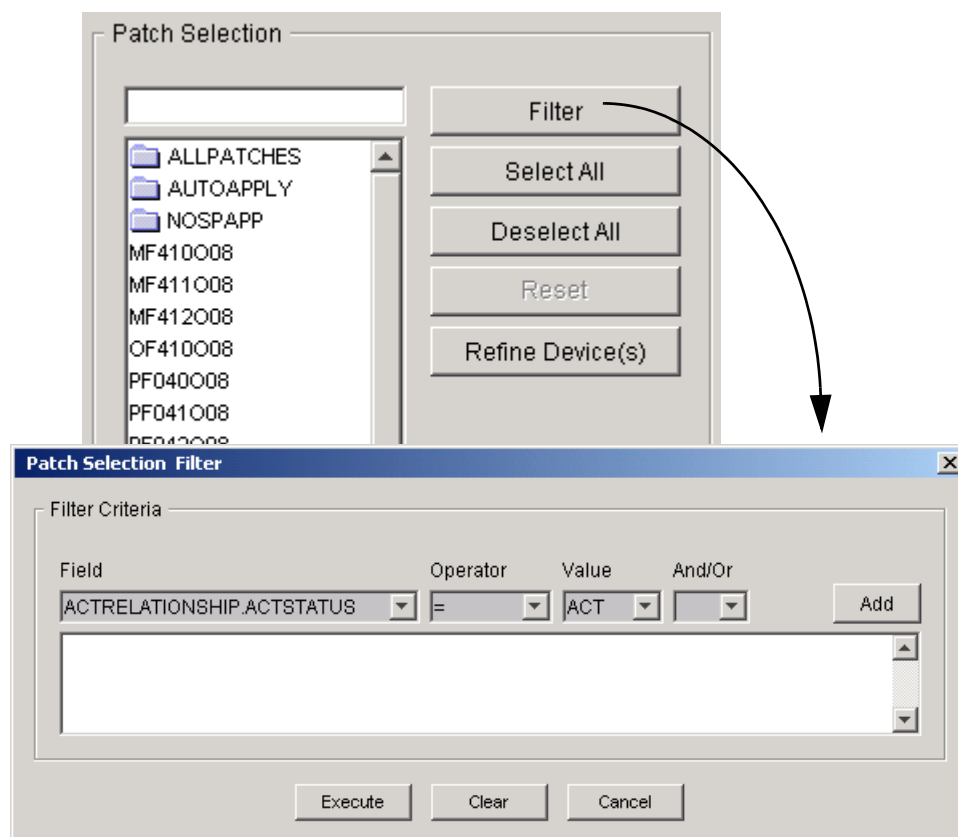
- 9 In the Task list, click **Activate**.



- 10 In the Patch Selection list, select the patch files or patch sets you want to activate, then click **Refine Device(s)** to display a list of devices to which the patches apply.

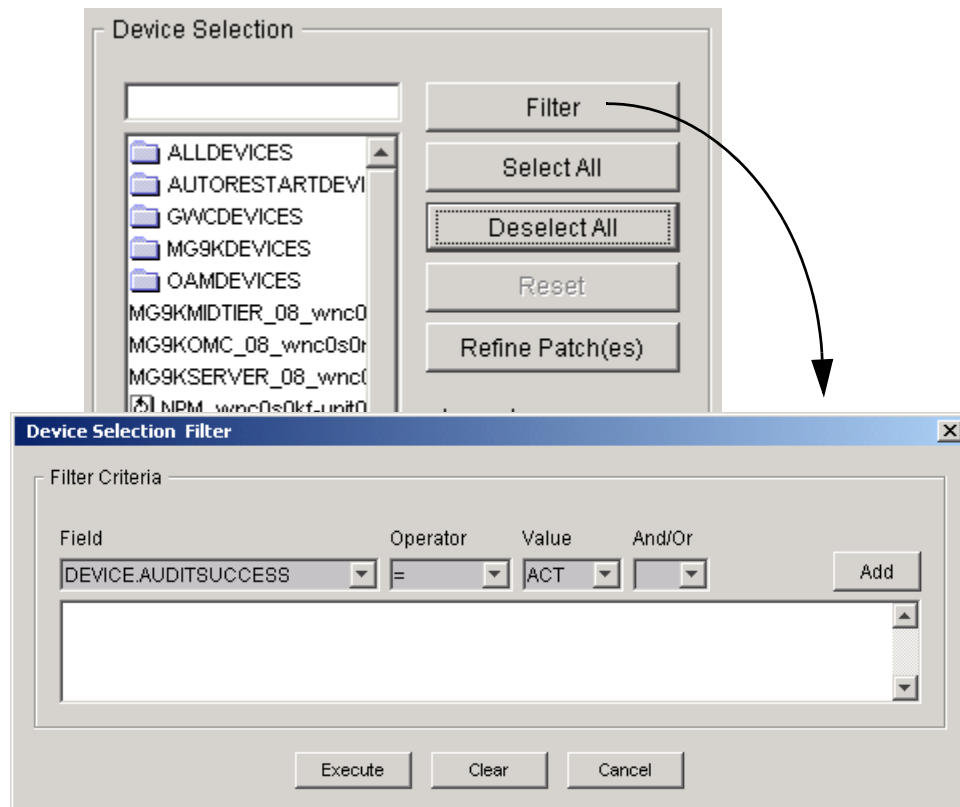
To limit the patches displayed in the Patch Selection list, click **Filter** to configure a filtering criteria.

**Note:** The patches must have a category of ACT.

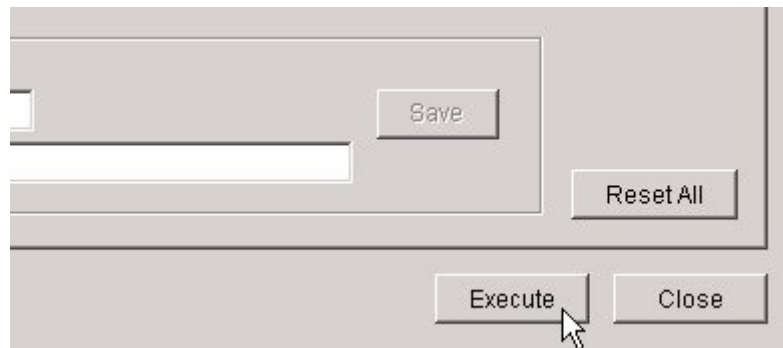


- 11 In the Device Selection list, select the devices or device sets that have the applied patches you want to activate.

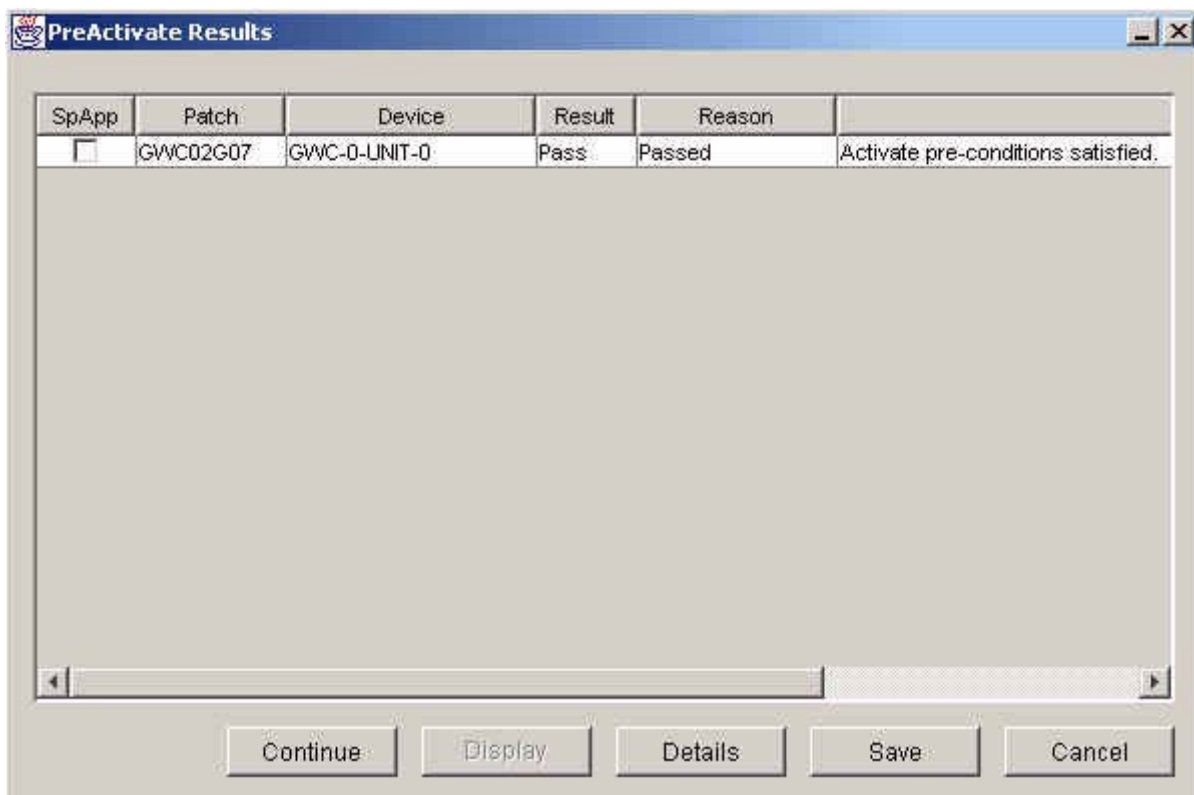
To limit the devices displayed in the Device Selection list, click **Filter** to configure a filtering criteria.



- 12 Click **Execute** to begin the patch activation process.



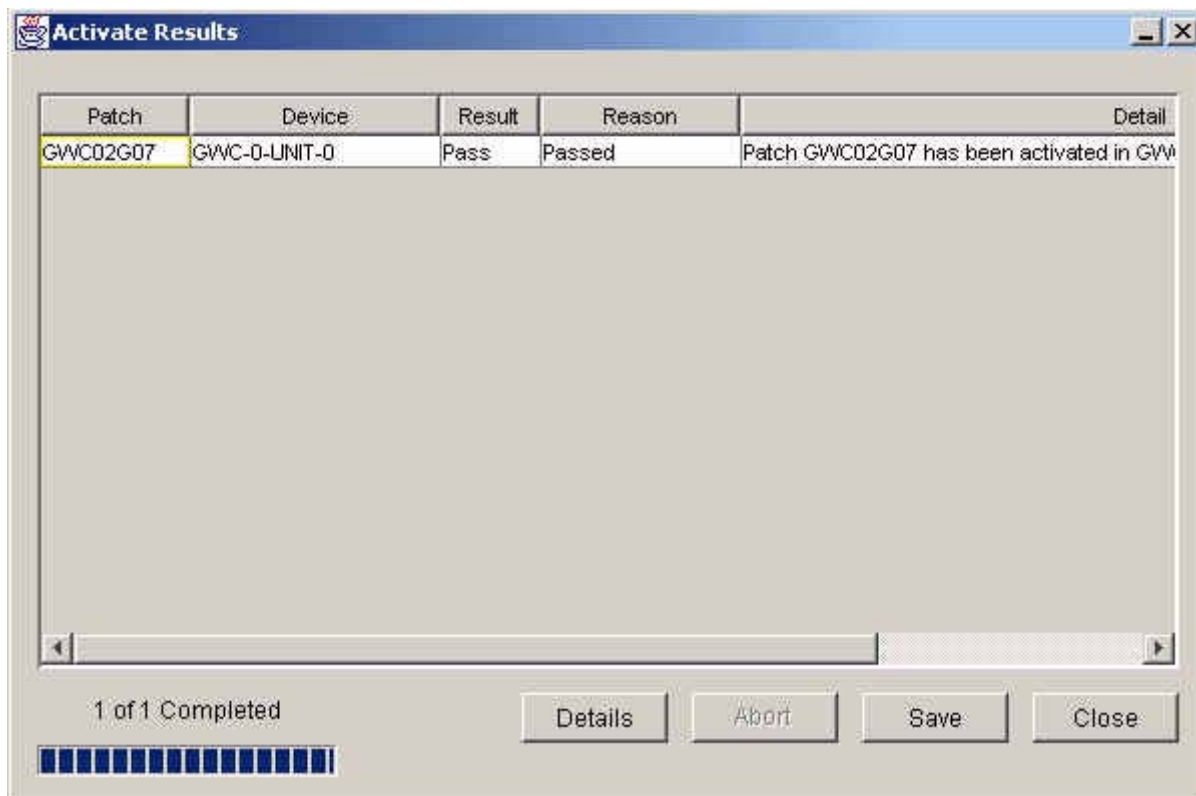
The results of the Pre-activate phase are displayed.



- 13 Review the PreActivate Results, then click **Continue** to proceed.

**Note:** If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Activate Results window is displayed with results added as each action is completed. Failures from the PreActivate phase are also included in the results.



- 14 Click **Save** to save the results to a file, or click Close.
- Note:** If the patches do not successfully activate, abort the patching procedure and contact your next level of support.
- 15 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

## Deactivating patches using the NPM

---

### Application

Use this procedure to deactivate one or more ACT category patches using the Network Patch Manager (NPM).

**Note:** Currently, only GWC can have ACT category patches.

### Prerequisites

You can deactivate a patch if the following criteria apply:

- the patch to be deactivated has been identified by your support team and Nortel as being applicable for your site and be recommended for deactivation
- the patch has been activated
- the patch is not on hold

**CAUTION****Potential for partial loss of service**

Do not deactivate patches for your components that have not been identified as needing deactivation without first consulting with your network administrator and your Nortel customer support representative. Failure to do so can result in partial loss of service.

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

## Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2346](#)
- [Using the NPM GUI on page 2347](#)

### Using the NPM CLUI

#### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

#### *At the NPM CLUI*

- 2 Query the NPM for a list of patches that are activated by typing

```
npm> q actlist
```

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime. If no patches are in the actlist, then the NPM responds with the message "Empty Results".

- 3 Deactivate one or more patches for one or more devices by typing

```
npm> deactivate <patches> [in <devices>]
```

and pressing the Enter key.

where

#### **patches**

is a list of one or more patch IDs you want to deactivate using the following syntax

```
<patchid> [<patchid>...<patchid>]
```

or

```
SET <predefined set definition>
```

**devices**

is a list of one or more device IDs for which you want to deactivate the patches using the following syntax (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and deactivates them)

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

**Example**

npm> deactivate ACT02GAX in GWC-8-UNIT-1

- 4 When prompted, press the Enter key.
- 5 Query the NPM to verify the patches are deactivated by typing

npm> **q actlist**

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime.

- 6 Verify from the list that the desired patches are deactivated.  
**Note:** If the patches do not successfully deactivate, abort the patching procedure and contact your next level of support.
- 7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

**Using the NPM GUI*****At your workstation***

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).



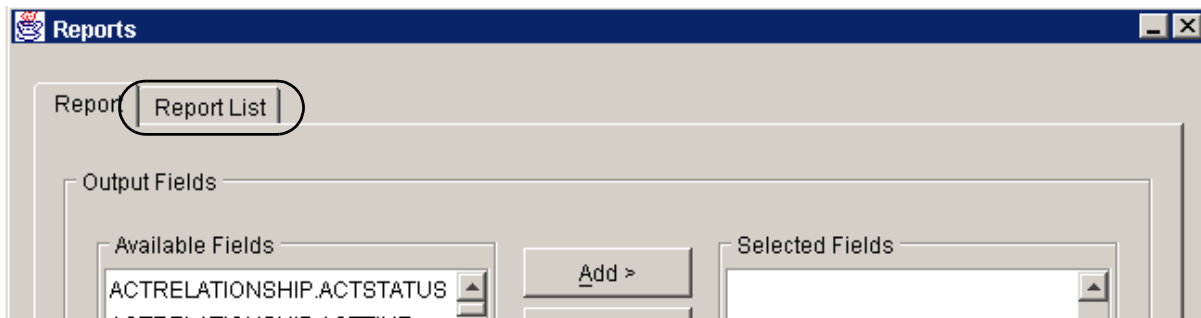
***At the NPM GUI***

- 2 Query the NPM for a list of patches that are activated as follows:
  - a On the Tasks menu, click **Reports....**



The Reports window is displayed.

- b Click the **Report List** tab.



- c Click the **ACTLIST** entry in the Report field, then click **Execute**.

Report Report List

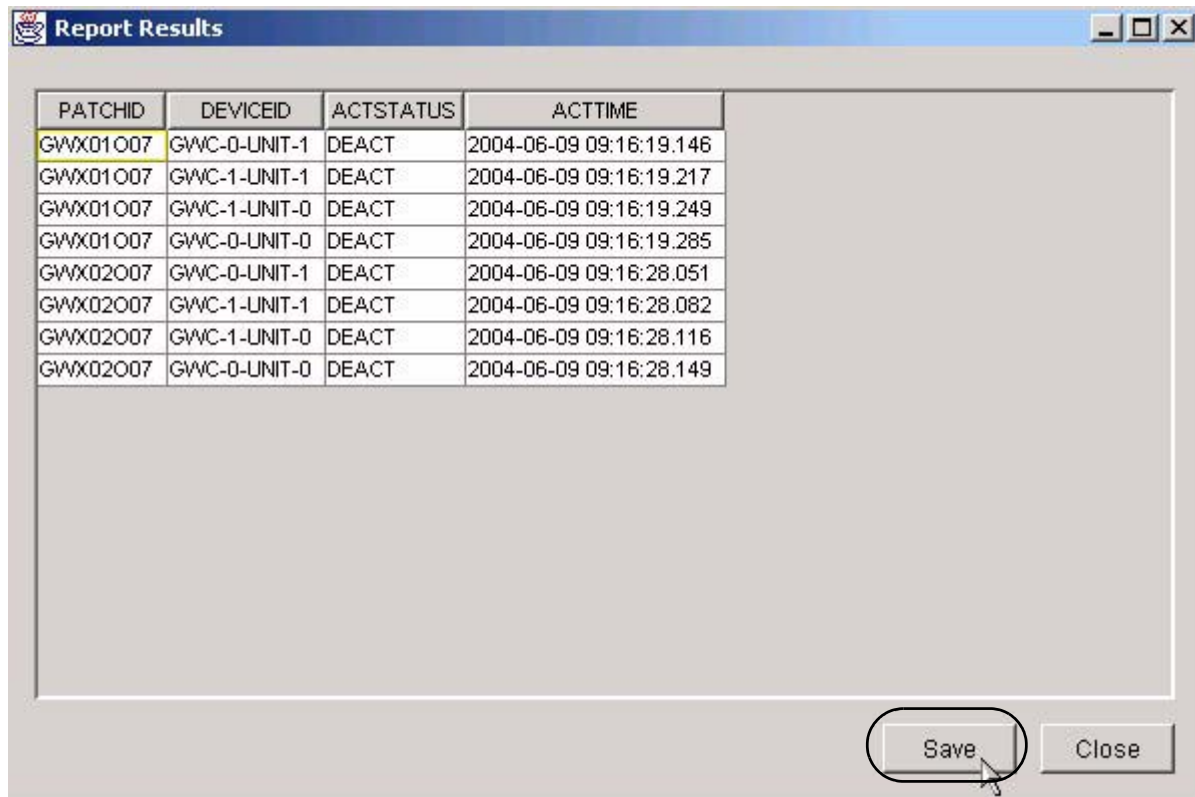
| Report           | Description                                                      | Type   |
|------------------|------------------------------------------------------------------|--------|
| ACTLIST          | RPS activation patch information.                                | System |
| CALCLIST         | RPS Patch Calculation Report.                                    | System |
| DEVICE           | Information about a specific Device (prompt).                    | System |
| DEVICELIST       | Information about patchable Device(s) on the system.             | System |
| DEVICE_ACTIVITY  | All devices and their activity states                            | System |
| DEVICE_ACTLE...  | Displays how many patches are activated in each device.          | System |
| DEVICE_APPLE...  | Displays how many patches are applied to each device.            | System |
| DISABLEDAPPLI... | Patches that are applied and disabled.                           | System |
| DISABLEDREM...   | Patches that are removed and disabled.                           | System |
| ENABLEDAPPLI...  | Patches that are applied and enabled.                            | System |
| ENABLEDREMO...   | Patches that are removed and enabled.                            | System |
| FULLDEVICELIST   | Information about every Device(s) on the system.                 | System |
| INVALID_LOAD...  | Device(s) with invalid loads. Audit required.                    | System |
| LOADLIST         | RPS Device Load Report.                                          | System |
| PATCH            | Information about a specific patch (prompt).                     | System |
| PATCHES_SINCE    | Patch Activity since a specific date (prompt).                   | System |
| PATCHINFO        | Full information about a specific patch (prompt).                | System |
| PATCHLIST        | Information about patches and their relationships on the system. | System |

Edit View Delete

Execute Close

- d Review the list of patches displayed and note which are activated and which are deactivated. Consult with your Nortel customer support representative to determine which patch files are applicable to your site configuration and need to be deactivated.

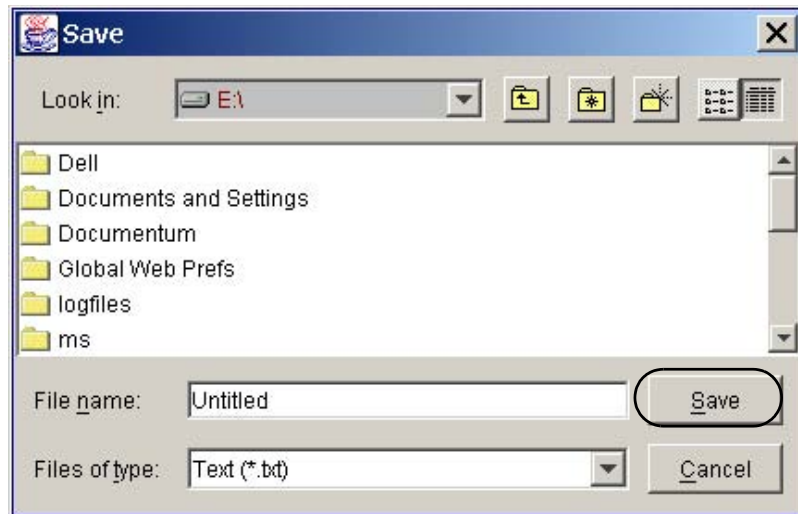
**Note:** If there are no patches to deactivate, the system returns a dialog box indicating that the report has “empty results”.



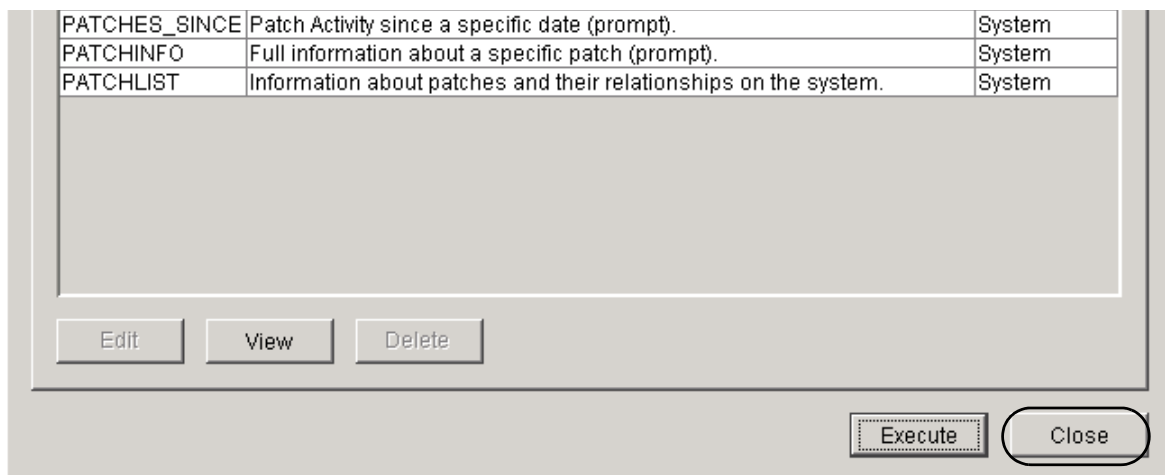
The screenshot shows a window titled "Report Results" with a table containing patch information. The table has four columns: PATCHID, DEVICEID, ACTSTATUS, and ACTTIME. There are eight rows of data, all showing a status of "DEACT". The first row is highlighted in yellow. At the bottom right of the window, there are "Save" and "Close" buttons. The "Save" button is circled with a mouse cursor pointing to it.

| PATCHID  | DEVICEID     | ACTSTATUS | ACTTIME                 |
|----------|--------------|-----------|-------------------------|
| GWX01007 | GWC-0-UNIT-1 | DEACT     | 2004-06-09 09:16:19.146 |
| GWX01007 | GWC-1-UNIT-1 | DEACT     | 2004-06-09 09:16:19.217 |
| GWX01007 | GWC-1-UNIT-0 | DEACT     | 2004-06-09 09:16:19.249 |
| GWX01007 | GWC-0-UNIT-0 | DEACT     | 2004-06-09 09:16:19.285 |
| GWX02007 | GWC-0-UNIT-1 | DEACT     | 2004-06-09 09:16:28.051 |
| GWX02007 | GWC-1-UNIT-1 | DEACT     | 2004-06-09 09:16:28.082 |
| GWX02007 | GWC-1-UNIT-0 | DEACT     | 2004-06-09 09:16:28.116 |
| GWX02007 | GWC-0-UNIT-0 | DEACT     | 2004-06-09 09:16:28.149 |

- e If necessary, save a copy of the report to a text file as follows:
  - i Click **Save**.
  - ii Type a file name in the File name: box, and click **Save**.

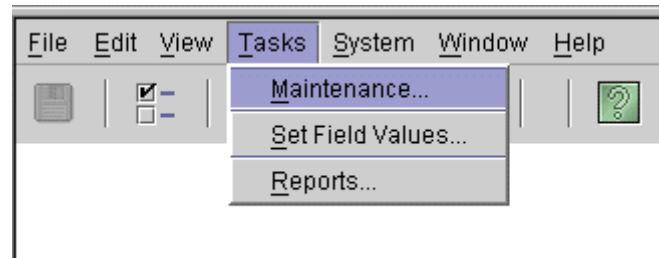


- f Click **Close** to close the Reports window.



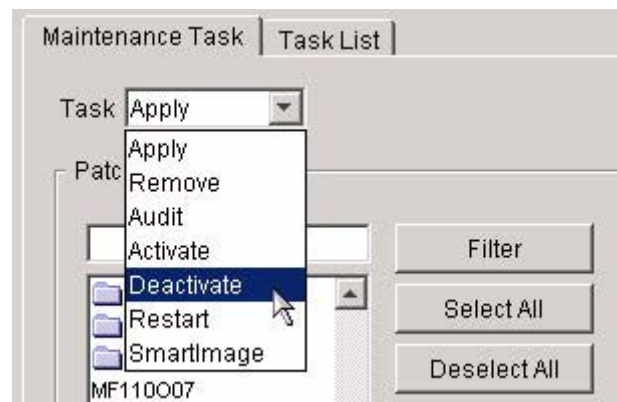
- 3 Deactivate one or more patches for one or more devices as follows:

- a On the Tasks menu, click **Maintenance...**



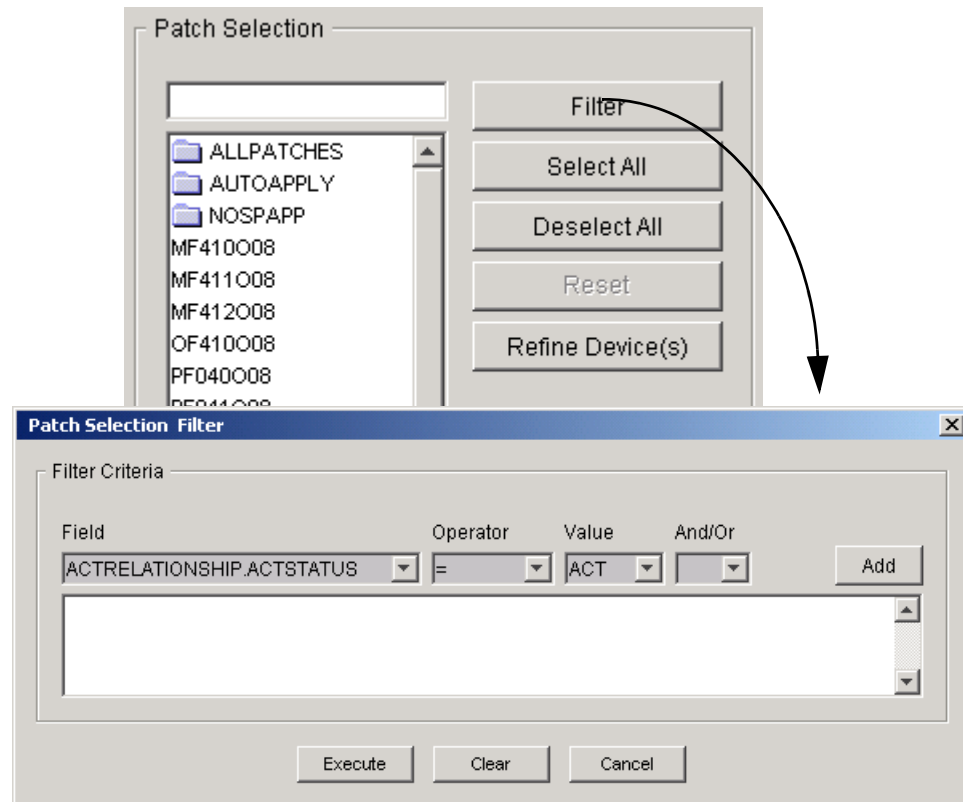
The Maintenance window is displayed.

- b In the Task list, click **Deactivate**.



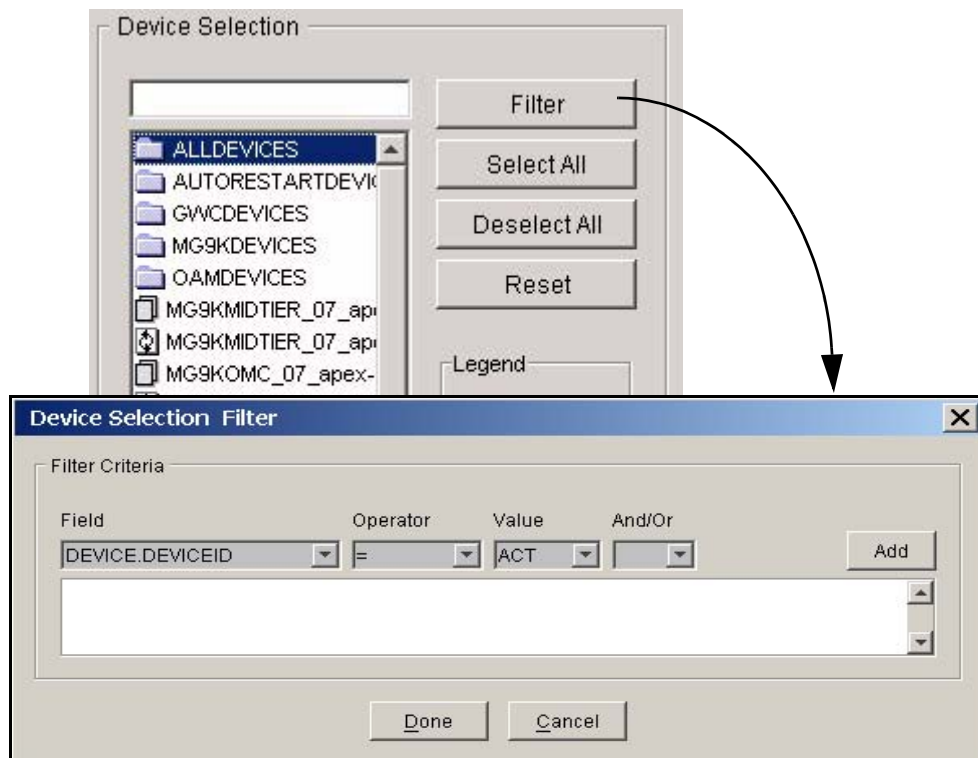
- c In the Patch Selection list, select the patch files or patch sets you want to deactivate, then click **Refine Device(s)** to display a list of devices to which the patches apply.

To limit the patches displayed in the Patch Selection list, click **Filter** to configure a filtering criteria.

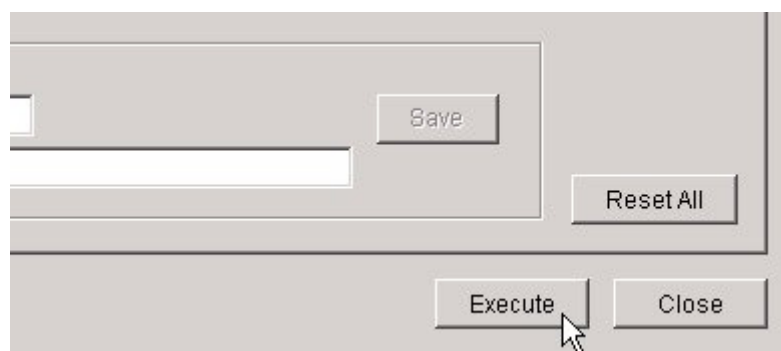


- d In the Device Selection list, select the devices or device sets that have the applied patches you want to deactivate.

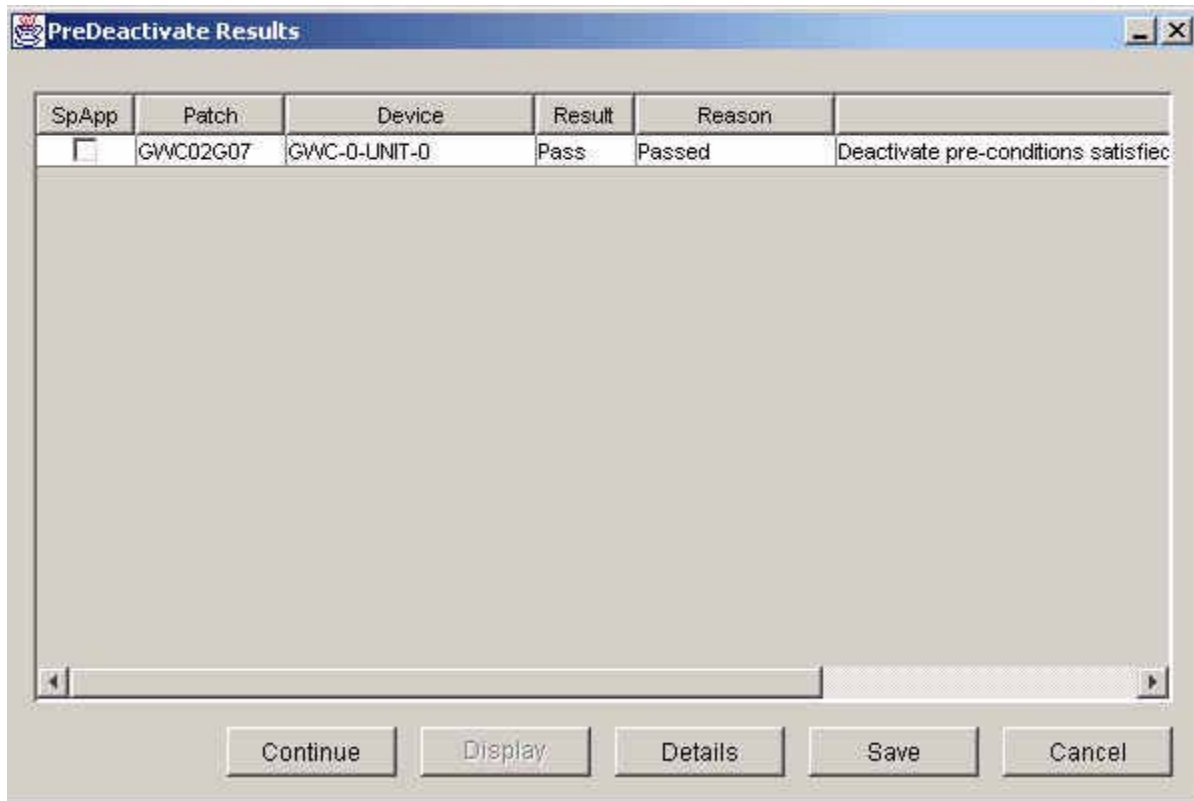
To limit the devices displayed in the Device Selection list, click **Filter** to configure a filtering criteria.



- e Click **Execute** to begin the patch deactivation process.



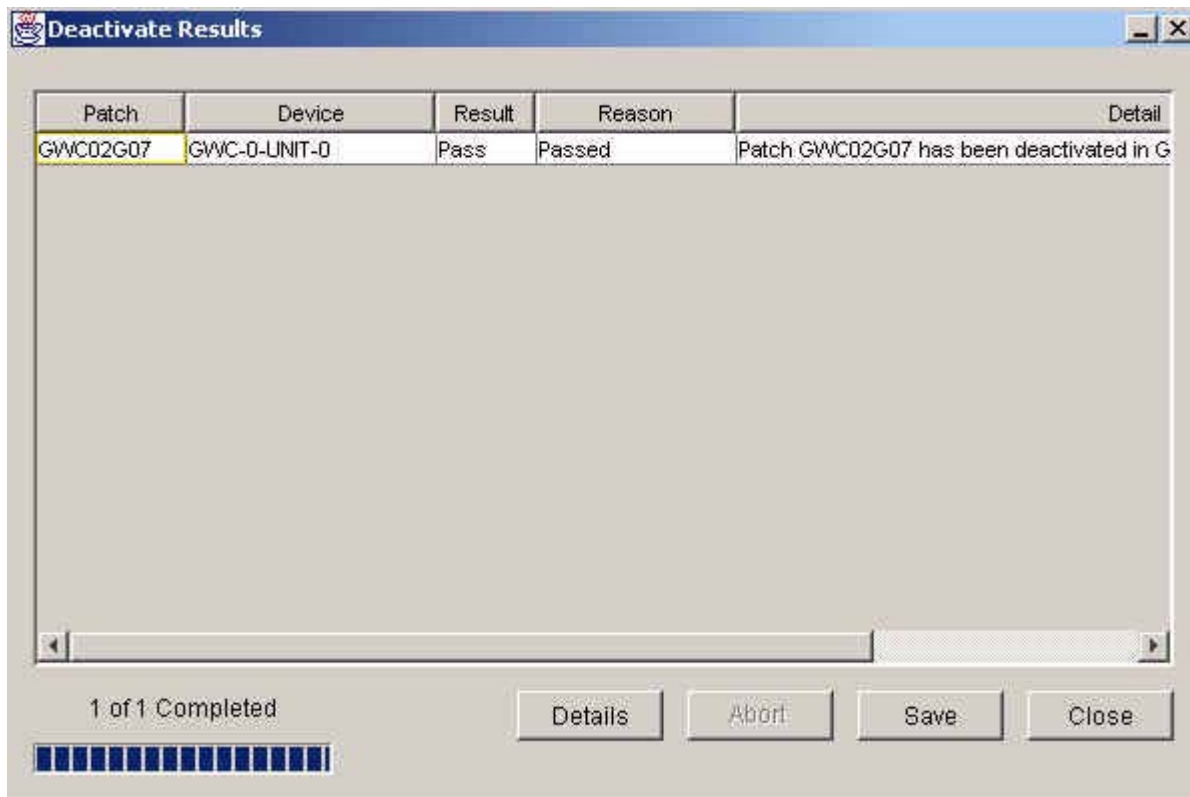
The results of the Pre-deactivate phase are displayed.



- f Review the PreDeactivate Results, then click **Continue** to proceed.



The Deactivate Results window is displayed with results added as each action is completed. Failures from the PreDeactivate phase are also included in the results.



- g** Click **Save** to save the results to a file, or click Close.

**Note:** If the patches do not successfully deactivate, abort the patching procedure and contact your next level of support.

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

---

## Removing patches using the NPM

---

### Application

Use this procedure to remove patches using the Network Patch Manager (NPM).

### Prerequisites

This procedure has the following prerequisites:

- Ensure all ACT category patches are deactivated before they are removed. Refer to procedure [Deactivating patches using the NPM on page 2345](#) if required.
- Ensure the patch to be removed is not on hold.
- To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

### Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2357](#)
- [Using the NPM GUI on page 2360](#)

#### Using the NPM CLUI

##### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

**At the NPM CLUI**

- 2** Perform a query to list patches that can be removed and to list devices that patches can be removed from by typing

```
npm> q patchlist
```

and pressing the Enter key.

- 3** Remove one or more patches from one or more devices by typing

```
npm> remove <patches> [in <devices>]
```

and pressing the Enter key.

where

**patches**

is a list of one or more patch IDs you want to remove using the following syntax

```
<patchid> [<patchid>...<patchid>]
```

or

```
SET <predefined set definition>
```

**devices**

is a list of one or more device IDs from which you want to remove the patches using the following syntax (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and removes them)

```
<deviceid> [<deviceid>...<deviceid>]
```

or

```
SET <predefined set definition>
```

**Example**

```
npm> remove ACT02GAX in GWC-8-UNIT-1
```

- 4** When prompted, press the Enter key.
- 5** Generate a device query report to verify the patches are removed by typing

```
npm> q device
```

and pressing the Enter key.

- 6 Enter the device name in the format **<deviceid>** that you input in step 3.  
  
A device report of known patch activity for the particular device associated with the <device id> is returned.
- 7 Verify from the report that the desired patches are removed.  
  
**Note:** If the patches do not successfully remove, abort the patching procedure and contact your next level of support.
- 8 If you removed patches from any of the following devices, you need to restart the device in order to disable the patches on the device:
  - Patching Server Element (PSE)
  - Integrated Element Management System (IEMS)
  - Integrated EMS security components (IEMSCSS\_DS and IEMSCSS)
  - CS 2000 SAM21 Manager (SAM21EM)
  - Succession Element Sub-network Manager (SESM)
  - QoS Collector Application (QCA)
  - Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
  - Core Element Manager (COREM)
  - Core and Billing Manager (CBM)
  - Client Session Monitor (CSMONITOR)
  - Key Manager (PKMGR\_SERVER)
  - Network Patch Manager (NPM)

To restart a device, refer to procedure [Restarting a device using the NPM on page 2364](#) if required.
- 9 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

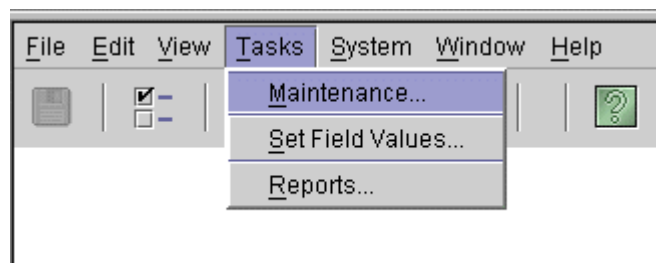
## Using the NPM GUI

### *At your workstation*

- 1 Access the NPM GUI. Refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#) if required.

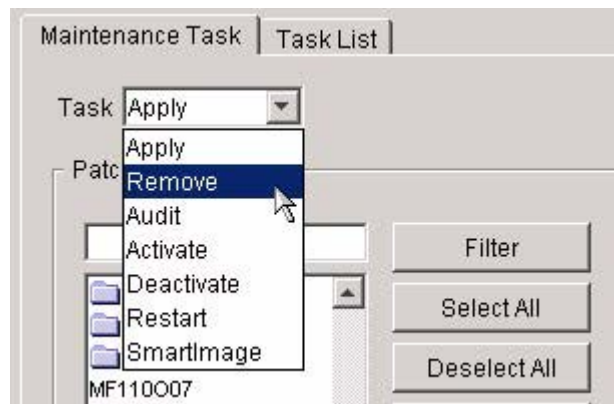
### *At the NPM GUI*

- 2 On the Tasks menu, click **Maintenance....**



The Maintenance window is displayed.

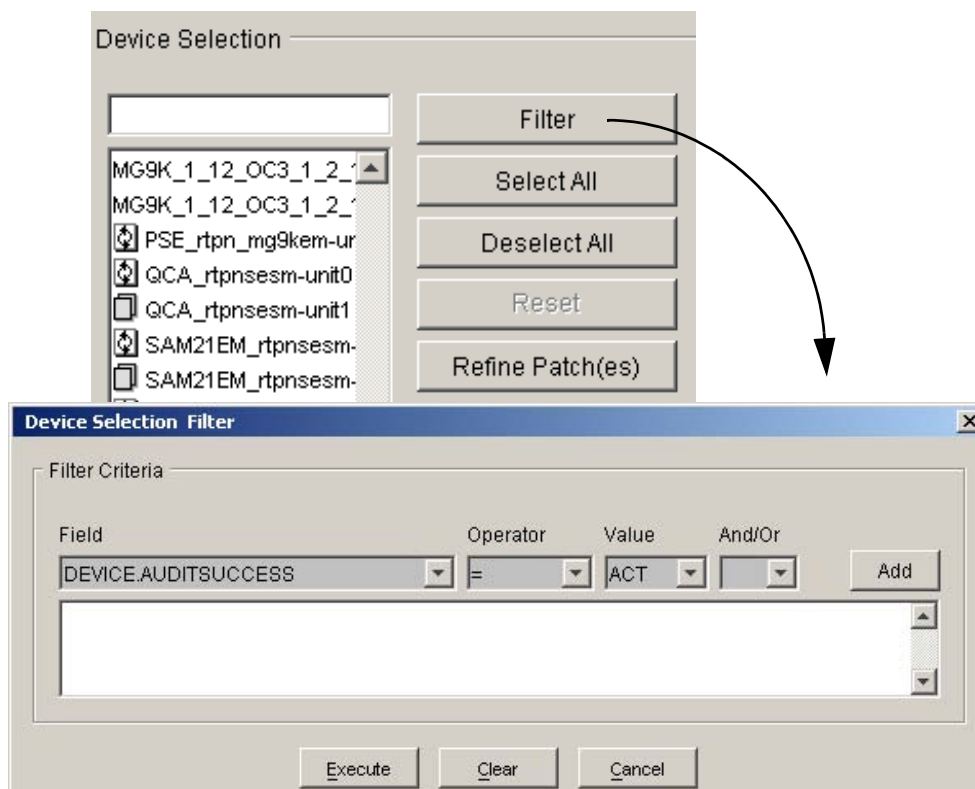
- 3 In the Task list, click **Remove**.



- 4 In the Device Selection list, select the devices you want to remove patches from. Click **Refine Patch(es)** to display a list of patches to which devices belong.

**Note:** The Refine Patch(es) button will not work on device sets.

- 5 To limit the devices displayed in the Device Selection list, click **Filter** to configure a filtering criteria.



- 6 The list of patches shows only the patches applicable to the selected devices. Click **Select All** to select the refined list of patches.

- 7 Click **Execute** to begin the patch removal process.  
The results of the PreRemove phase are displayed.

| SpApp                    | Patch    | Device              | Result | Reason | Detail                           |
|--------------------------|----------|---------------------|--------|--------|----------------------------------|
| <input type="checkbox"/> | SF264091 | SESM_rtpnsesm-unit1 | Pass   | Passed | Remove pre-conditions satisfied. |
| <input type="checkbox"/> | SF263091 | SESM_rtpnsesm-unit1 | Pass   | Passed | Remove pre-conditions satisfied. |
| <input type="checkbox"/> | SF262091 | SESM_rtpnsesm-unit1 | Pass   | Passed | Remove pre-conditions satisfied. |
| <input type="checkbox"/> | SF261091 | SESM_rtpnsesm-unit1 | Pass   | Passed | Remove pre-conditions satisfied. |
| <input type="checkbox"/> | SF260091 | SESM_rtpnsesm-unit1 | Pass   | Passed | Remove pre-conditions satisfied. |

Buttons: Continue, Display, Details, Save, Cancel

- 8 Review the PreRemove Results, then click **Continue** to proceed.

If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Remove Results window is displayed with results added as each action is completed. Failures from the PreRemove phase are also included in the results..

- 9 Click **Save** to save the results to a file, or click Close.  
**Note:** If the patches do not successfully remove, abort the patching procedure and contact your next level of support.
- 10 If you removed patches from any of the following devices, you need to restart the device in order to disable the patches on the device:
  - Integrated Element Management System (IEMS)
  - Integrated EMS security components (IEMSCSS\_DS and IEMSCSS)
  - Patching Server Element (PSE)
  - CS 2000 SAM21 Manager (SAM21EM)
  - Succession Element Sub-network Manager (SESM)
  - QoS Collector Application (QCA)
  - Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
  - Core Element Manager (CEM)
  - Core and Billing Manager (CBM)
  - Client Session Monitor (CSMONITOR)
  - Network Patch Manager (NPM)

To restart a device, refer to procedure [Restarting a device using the NPM on page 2364](#) if required.
- 11 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.



---

## Restarting a device using the NPM

---

### Application

Use this procedure to restart a device using the Network Patch Manager (NPM).

If you applied or removed patches to or from any of the following devices, you need to restart the device in order to enable or disable the patches on the device:

- Patching Server Element (PSE)
- Integrated Element Management System (IEMS)
- IEMS security components (IEMSCSS\_DS and IEMSCSS)
- CS 2000 SAM21 Manager (SAM21EM)
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
- Core Element Manager (COREM)
- Core and Billing Manager (CBM)
- Client Session Monitor (CSMONITOR)
- Key Manager (PKMGR\_SERVER)
- Network Patch Manager (NPM)

If you applied or removed patches to or from multiple devices, you must restart each device, one at a time, starting with the PSE and ending with the NPM.

In a two-server configuration, a restart is required on devices that have running applications and have either been patched or had patches removed. Patches are automatically enabled or disabled without an additional restart step on devices that have no running applications. To determine which devices require a restart, query two system-defined reports; disabledapplied and enabledremoved.

**Note:** Restart is not supported for the Server Platform Foundation Software (SPFS). Refer to the specific SPFS patch for further instructions on how to enable or disable.

A restart takes the application out of service temporarily, then returns the application to service.

## Prerequisites

This procedure has the following prerequisites:

- You have applied or removed all the patches to or from the device.
- The device you are restarting is not on hold.
- To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

## Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2365](#)
- [Using the NPM GUI on page 2369](#)



### CAUTION

Stop or complete any maintenance activities associated with the patched device before you begin the restart.

## Using the NPM CLUI

### ATTENTION

Restarting the PKGMGR\_SERVER loses the current login session to the NPM. You will need to log in again once the PKGMGR\_SERVER has restarted.

### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

**At the NPM CLUI**

- 2** List the devices that need to be restarted to enable the applied patches or disable the removed patches.

- If you applied patches, enter the following command to list the applied but disabled patches:

```
npm> q disabledapplied
```

- If you removed patches, enter the following command to list the removed but enabled patches:

```
npm> q enabledremoved
```

Note the devices that have applied but disabled patches or removed but enabled patches, and proceed to step [3](#) to restart those devices.

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

| If the device you are working on       | Do                     |
|----------------------------------------|------------------------|
| appears in the list of devices         | <a href="#">step 4</a> |
| does not appear in the list of devices | <a href="#">step 8</a> |

- 4** Restart one or more devices by typing

```
npm> restart <devices>
```

and pressing the Enter key.

where

**devices**

is a list of one or more device IDs you want to restart using the following syntax

```
<deviceid> [<deviceid>...<deviceid>]
```

or

```
SET <predefined set definition>
```

**Example**

```
npm> restart SESM_mws0c0l
```

- 5** When prompted, confirm you want to continue with the device restart by typing

**y**

and pressing the Enter key.

Example response

SpAPP: false

Patch: \*

Device: SESM\_mws0c0ld

Result: true

Reason: Passed

Details: Device SESM\_mws0c0ld passed preRestart.

If you wish to continue with this maintenance request, enter Yes (Y or y). Otherwise, just enter return.

- 6** When prompted, confirm you want to continue with the device restart by typing

**y**

and pressing the Enter key.

Example response

npm>

Patch: \*

Device: SESM\_mws0c0ld

Reason: Passed

Detail: Restart passed on device SESM\_mws0c0ld.

Hit <CR> to continue...

7

**ATTENTION**

Restarting the NPM makes it unavailable until it has successfully restarted. You will need to log in once it has restarted.

When prompted, press the Enter key.

Once a PSE or NPM device has been successfully restarted, Nortel Networks recommends that you perform an audit on the PSE or NPM device to synchronize the NPM database with the updates to the patches on the device. The audit will automatically occur at a specified time, however, to perform an audit manually, refer to procedure [Performing a device audit using the NPM on page 2313](#) if required.

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

## Using the NPM GUI

### ATTENTION

Restarting the PKGMGR\_SERVER can cause the NPM GUI connection to be lost. You may need to re-launch the NPM GUI once the PKGMGR\_SERVER has been restarted.

### At your workstation

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

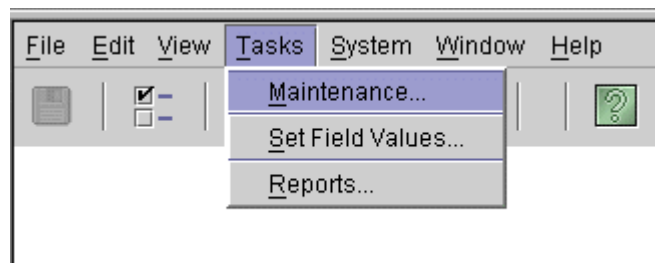
### At the NPM GUI

- 2 On the Tasks menu, click **Reports**. Then click the **Reports List** tab.
- 3 Click the **ENABLEDREMOVED** report and click **Execute**.  
Once the report displays, a restart is required to disable the patches for the listed devices.
- 4 Click the **DISABLEDAPPLIED** report and click **Execute**.  
Once the report displays, a restart is required to enable the patches for the listed devices.
- 5 Use the following table to determine your next step.

| If the device you are working on       | Do                      |
|----------------------------------------|-------------------------|
| appears in the list of devices         | <a href="#">step 7</a>  |
| does not appear in the list of devices | <a href="#">step 14</a> |

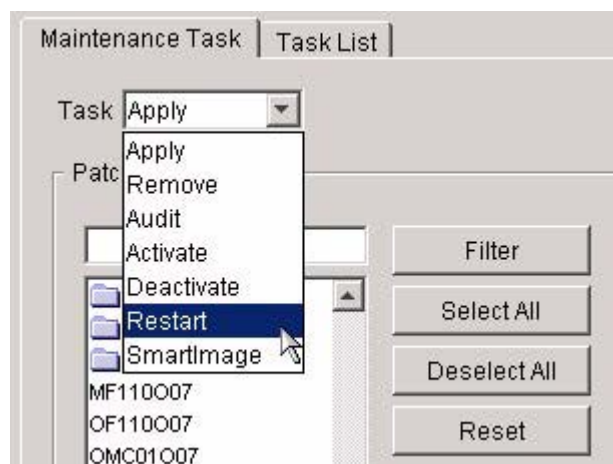
- 6 List the devices that need to be restarted to enable the applied patches or disable the removed patches as follows:
  - a On the Tasks menu, click **Reports** and then click the **Reports List** tab.
  - b Click **ENABLEDREMOVED** and then click **Execute**.  
Once the report displays, a restart is required to disable the patches for the listed devices.
  - c Click **DISABLEDAPPLIED** and then click **Execute**.  
Once the report displays, a restart is required to enable the patches for the listed devices.

- 7 On the Tasks menu, click **Maintenance**.

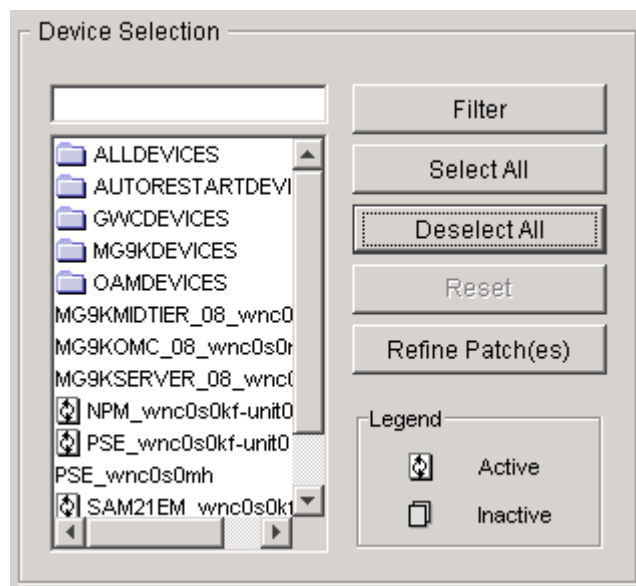


The Maintenance window is displayed.

- 8 In the Task list, click **Restart**.



- 9 In the Device Selection list, select the device, device list, or device set that you want to restart.



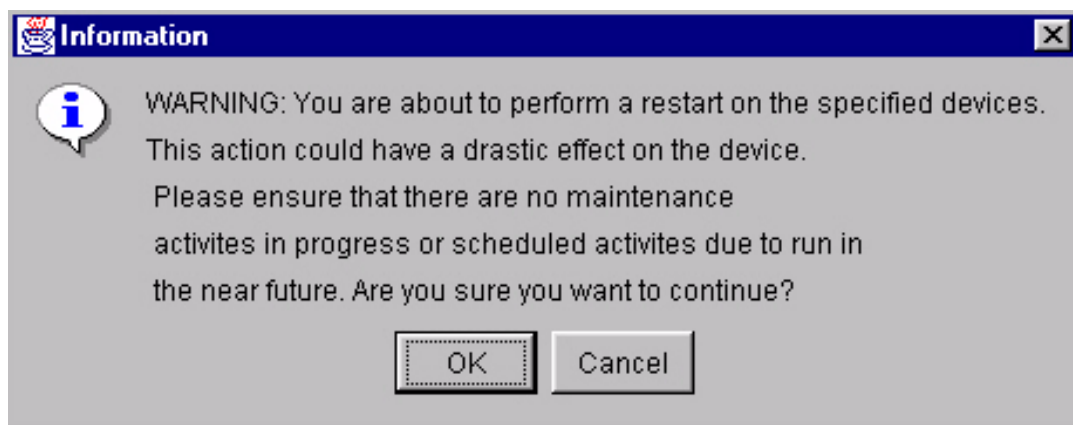
10

#### ATTENTION

Restarting the NPM makes it unavailable until it has successfully restarted. You will need to log in once it has restarted.

Click **Execute** to begin the restart.

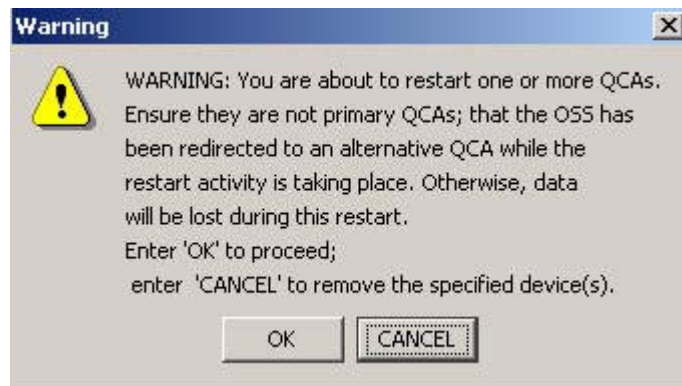
The system returns the following warning.



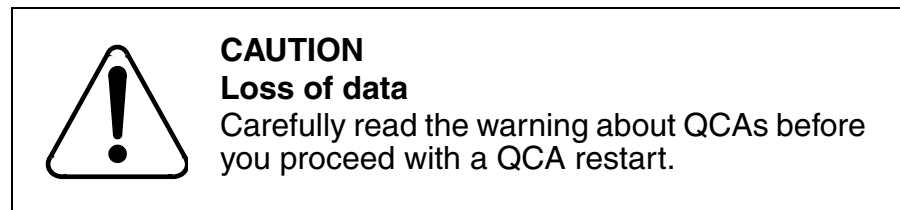
11 Click **OK** to begin the restart.

If you are restarting a QCA device, the system returns the following warning:



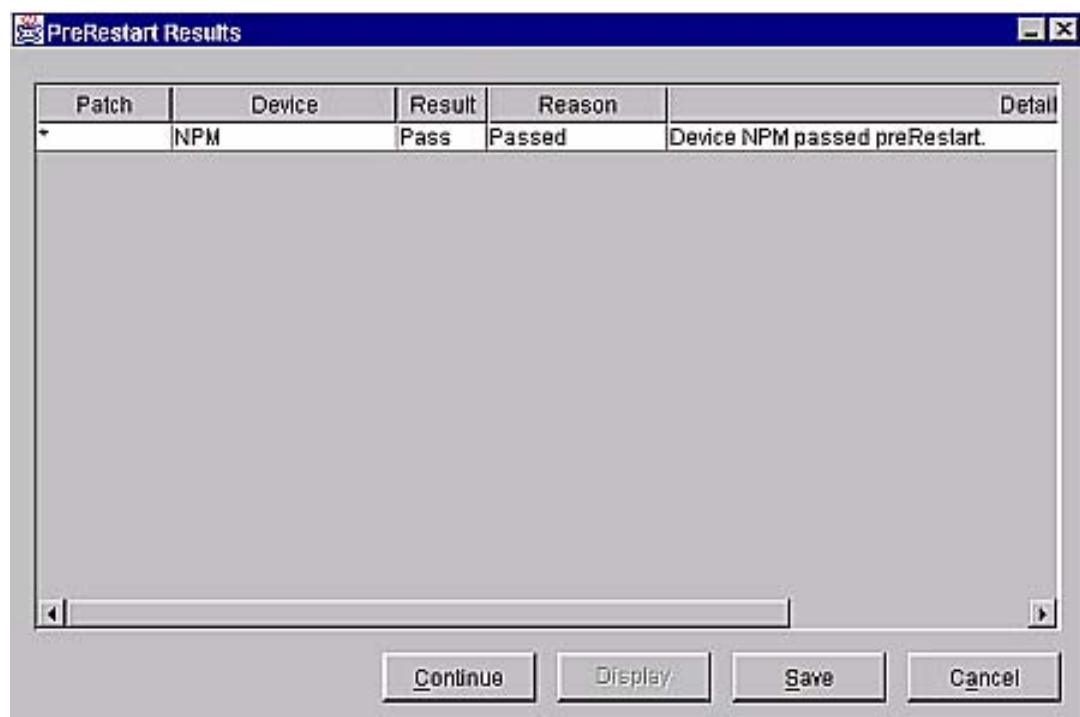


12



If restarting a QCA is acceptable, click **OK** to proceed with the restart, otherwise click Cancel.

The results of the PreRestart phase are displayed.



- 13 Review the PreRestart Results, then click **Continue** to proceed.  
Once the PSE or NPM device has been successfully restarted, Nortel Networks recommends that you perform an audit on the PSE or NPM device to synchronize the NPM database with the updates to the patches on the device. The audit will automatically occur at a specified time, however, to perform an audit manually, refer to procedure [Performing a device audit using the NPM on page 2313](#) if required.
- 14
- 15 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

## Defining NPM patching sets

---

### Application

Use this procedure to define one or more patching sets.

Sets provide a convenient grouping of patches and devices used in routine patching tasks. The sets are dynamic, based on database query statements, and are evaluated at execution time.

The NPM is initially configured with the following defined sets for Patch Selection:

- ALLPATCHES - all patches on the system
- AUTOAPPLY - all patches that can be auto-applied
- NOSPAPP - all patches with no special applications

The NPM is initially configured with the following defined sets for Device Selection:

- ALLDEVICES - all registered devices on the system
- OAMDEVICES - all registered devices that are of device type OAM (PSE, SESM, CS 2000 SAM21 Manager, MG 9000 Manager, QCA, NPM, and SPFS)
- AUTORESTARTDEVICES - all registered devices that are of device type OAM and can be auto-restarted (this excludes QCA)
- MG9KDEVICES - all registered Media Gateway 9000 (MG 9000) devices on the system
- GWCDEVICES - all registered Gateway Controller (GWC) devices on the system

### Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

## Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2375](#)
- [Using the NPM GUI on page 2376](#)

### Using the NPM CLUI

#### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

#### *At the NPM CLUI*

- 2 Define a set by typing

```
npm> newset <type> <setname> <"description">
"where <criteria>"
```

and pressing the Enter key.

where

**type**

is either PATCHSET to define a set of patches, or  
DEVICESET to define a set of devices

**setname**

is the name of the set to be created

**"description"**

is a short description of the set

**criteria**

is the SQL statement that identifies the criteria by which to  
search the NPM database

**Example**

```
npm> newset PATCHSET BR12345PATCH "Patches
for CSR BR12345" "where PATCH.CSR='BR12345' "
```

| To                                          | Command                                                              |
|---------------------------------------------|----------------------------------------------------------------------|
| view the definition of a set                | <b>viewset</b> <setname>                                             |
| view all defined sets                       | <b>viewset</b> all                                                   |
| Execute and display the contents of the set | <b>runset</b> <setname>                                              |
| delete a user-defined set                   | <b>delset</b> <setname>                                              |
|                                             | <b>Note:</b> The system allows you to only delete user-defined sets. |

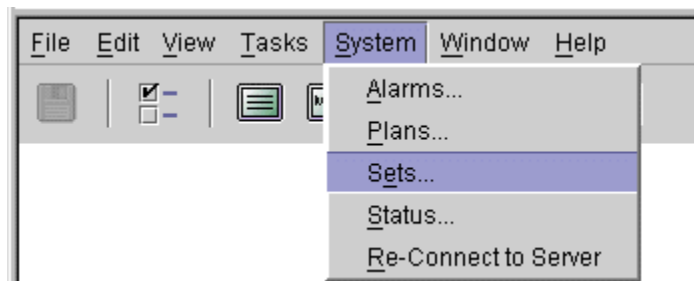
- 3 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

**Using the NPM GUI****At your workstation**

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

**At the NPM GUI**

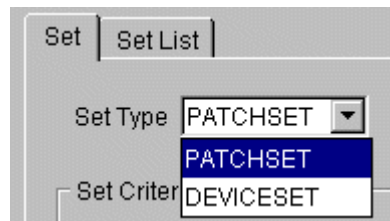
- 2 On the System menu, click **Sets...**



The Sets window is displayed.

- 3 In the Set Type list, select **PATCHSET** to define a set of patches, or **DEVICESET** to define a set of devices.

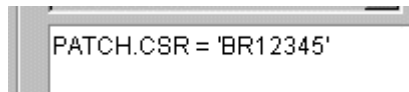
**Note:** You can also edit an existing set definition listed under the Set List tab, that contains similar criteria to the set you want to create, and save it under a new name.



- 4 In the Set Criteria area, specify the criteria for the set using substep [a](#) or [b](#)

- a Type the criteria for the set in the text box.

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

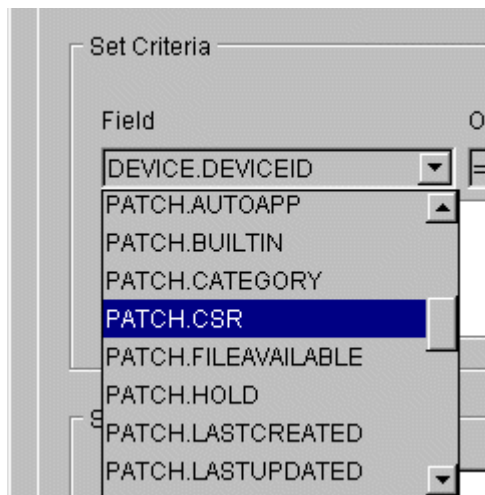


PATCH.CSR = 'BR12345'

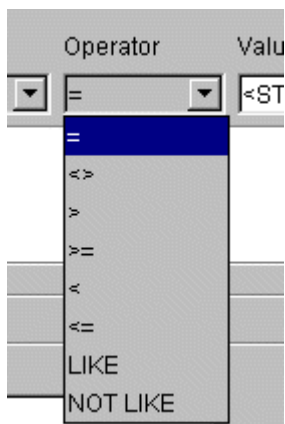
OR

- b Specify the set criteria as follows:

- i In the Field list, select the field of your choice.



- ii In the Operator list, select the operator of your choice.

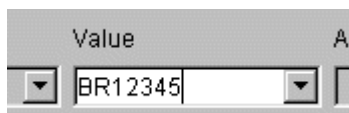


The following table lists the supported operators and their meaning.

| 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 (%) |

- iii In the Value list, select the value of your choice.

**Note:** The data type in the Value list will change depending on the data type selected in the Field list. For alphanumeric data, type the value. For boolean data, select the value.



To combine multiple criteria statements, click **AND** or **OR** in the And/Or list.



- 5 Type a unique name for the set in the Set Name box.

Save Set

Set Name:

Set Description:

- 6 Type a description of the set in the Set Description box if desired.

Save Set

Set Name:

Set Description:

- 7 Click **Save** to save the set.

The new set will appear under the Set List tab once the system has saved it.

| Set            |                                                                            |        |
|----------------|----------------------------------------------------------------------------|--------|
| Set List       |                                                                            |        |
| Set            | Description                                                                | Type   |
| ALLDEVICES     | All registered Devices on the system.                                      | System |
| ALLPATCHES     | All Patches on system.                                                     | System |
| AUTOAPPLY      | All Patches which can be auto-applied.                                     | System |
| AUTORESTART... | All registered devices that are of devicetype OAM and can be AUTO resta... | System |
| GWCDEVICES     | All registered GWC Devices on the system.                                  | System |
| MG9KDEVICES    | All registered MG9K Devices on the system.                                 | System |
| NOSPAPP        | All Patches which have no special applications.                            | System |
| OAMDEVICES     | All registered devices that are of devicetype OAM.                         | System |
| BR12345PATCH   | Patches for CSR BR12345                                                    | User   |

| To                                        | Action                                                                                                                                  |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| view or edit the definition of a set      | select the set from the SetList tab and click <b>Edit</b>                                                                               |
| execute and display the contents of a set | select the set from the SetList tab and click <b>Evaluate</b>                                                                           |
| delete a user-defined set                 | select the set from the SetList tab and click <b>Delete</b><br><br><b>Note:</b> The system allows you to delete only user-defined sets. |

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

---

## Defining NPM patching tasks

---

### Application

Use this procedure to define patching tasks.

A task is a definition of one type of maintenance activity that involves specific devices, and for some types of maintenance activities, can also involve patches. You can define a task for manual or automated execution.

The NPM is initially configured with the following system-defined tasks:

- AUTOAPPLY
- AUTORESTART
- AUDIT
- PFRSGETPATCH
- PFRSGENREPORT
- DELETEREPORTS

### Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

## Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2383](#)
- [Using the NPM GUI on page 2384](#)

### Using the NPM CLUI

#### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

#### *At the NPM CLUI*

- 2 Define a task by typing  

```
npm> newtask <task_name> <task_type>
<task_desc> <task_patchset> <task_deviceset>
```

and pressing the Enter key.

where

**task\_name**

is the name of the task to be created

**task\_type**

is the type of task (APPLYTASK, REMOVETASK, ACTIVATETASK, DEACTIVATETASK, AUDITTASK, RESTARTTASK, or SMARTIMAGETASK)

**task\_desc**

is a description of the task

**task\_patchset**

is the set of patches associated with the task

**Note:** The task\_patchset field is not used with AUDITTASK. For an AUDITTASK, use "" (two double quotes together).

**task\_deviceset**

is the set of devices associated with the task

**Note:** Tasks can only contain patchsets or devicesets, not single patches or devices. You can define a task that applies one patch to one device by putting the patch in a single-member patchset and the device in a single-member deviceset, and then applying the patchset to the deviceset.

Following is an example to apply all NOSPAPP patches to all devices.

```
npm> newtask NOSPAPPALL APPLYTASK "NOSPAPP for
ALLDEVICES" NOSPAPP ALLDEVICES
```

Following is an example to audit all devices.

```
npm> newtask AUDITALL AUDITTASK "Audit all
devices" "" ALLDEVICES
```

| To                            | Command                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------|
| view the definition of a task | <b>viewtask</b> <taskname>                                                                             |
| view all defined tasks        | <b>viewtask</b> all                                                                                    |
| execute a task                | <b>runtask</b> <taskname>                                                                              |
| delete a user-defined task    | <b>deltask</b> <taskname><br><br><b>Note:</b> The system allows you to only delete user-defined tasks. |

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

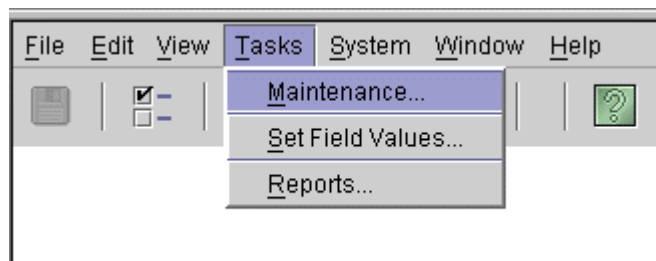
## Using the NPM GUI

### *At your workstation*

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

### *At the NPM GUI*

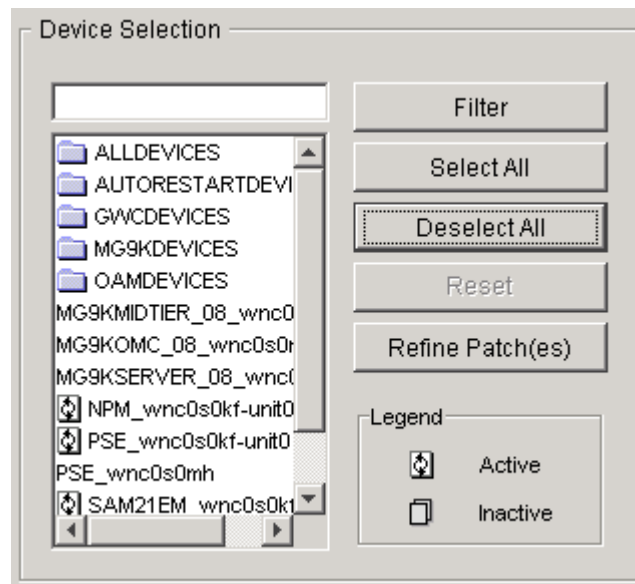
- 2 On the Tasks menu, click **Maintenance....**



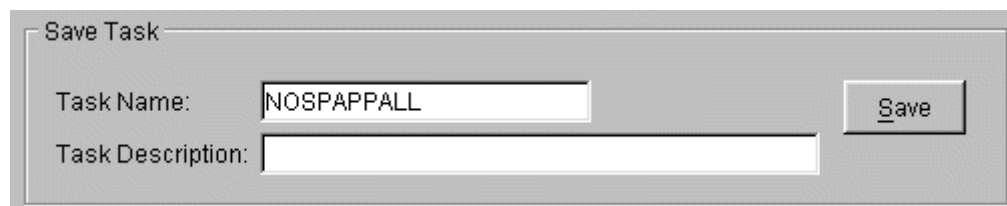
The Maintenance window is displayed.



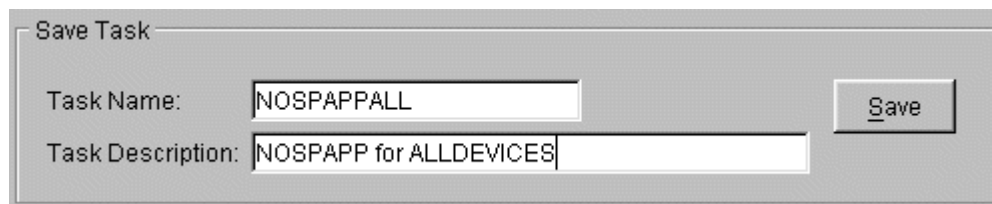
- 5 In the Device Selection list, select the device set you want to associate with the task.



- 6 Type a unique name for the task in the Task Name box.



- 7 Optionally, type a description of the task in the Task Description box.



**8** Click **Save** to save the task.

The new task will appear under the Task List tab once the system has saved the task.

| Maintenance Task |                                          | Task List |
|------------------|------------------------------------------|-----------|
| Task             | Description                              | Type      |
| AUTOAPPLY        | Autoapply Task                           | System    |
| AUDIT            | Audit Task                               | System    |
| AUTORESTART      | Autorestart Task                         | System    |
| PFRSGETPATCH     | Patch File Retrieval Task                | System    |
| PFRSGENREPORT    | Report Generation Task                   | System    |
| DELETEREPORTS    | Delete Reports Associated with NPM Tasks | System    |
| NOSPAPPALL       | NOSPAPP for ALLDEVICES                   | User      |

| To                            | Action                                                                                                                                |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| view the definition of a task | select the task from the TaskList tab and click <b>View</b>                                                                           |
| execute a task                | select the set from the TaskList tab and click <b>Execute</b>                                                                         |
| delete a user-defined task    | select the set from the TaskList tab and click <b>Delete</b><br><b>Note:</b> The system allows you to only delete user-defined tasks. |

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



---

## Setting field values using the NPM

---

### Application

Use this procedure to set field values using the Network Patch Manager (NPM).

The NPM allows the exclusion and inclusion of patches or devices from manual or automated patching tasks. This is accomplished by setting database field values using the “assign” command. An example of when this option can be used is when a new patch is applied to a single device for a test period, without applying the patch to the remaining devices. After the test period, the patch is then applied to the remaining devices.

### Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

### Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2388](#)
- [Using the NPM GUI on page 2390](#)

#### Using the NPM CLUI

##### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

##### *At the NPM CLUI*

- 2 Assign field values by typing

```
npm> assign <pd_option> <val_field> <val_value>
 <val_idset> <val_set>
```

and pressing the Enter key.

where

##### **pd\_option**

identifies what is being assigned (PATCH or DEVICE)

**val\_field**

is the field to be assigned (PATCH.HOLD or DEVICE.HOLD)

**val\_value**

is the new value for the field (Y or N)

**val\_idset**

identifies if you are assigning a single patch or device or a set of patches or devices (ID or SET)

**val\_set**

is the patch, device, or set to be assigned

**Example**

```
npm> assign PATCH PATCH.HOLD Y ID WMB00G07
```

Using the table that follows, determine the Field and Value to select.

**Field and Value combinations**

| Field       | Value | Result                                                                                               |
|-------------|-------|------------------------------------------------------------------------------------------------------|
| PATCH.HOLD  | N     | The patch will be applied to the remaining devices. This is typically after the test period is over. |
| PATCH.HOLD  | Y     | The patch will be excluded from manual or automated patching activities.                             |
| DEVICE.HOLD | N     | The device will be included in patching tasks. This is typically after the test period is over.      |
| DEVICE.HOLD | Y     | The device will be excluded from manual or automated patching activities.                            |

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

## Using the NPM GUI

### At your workstation

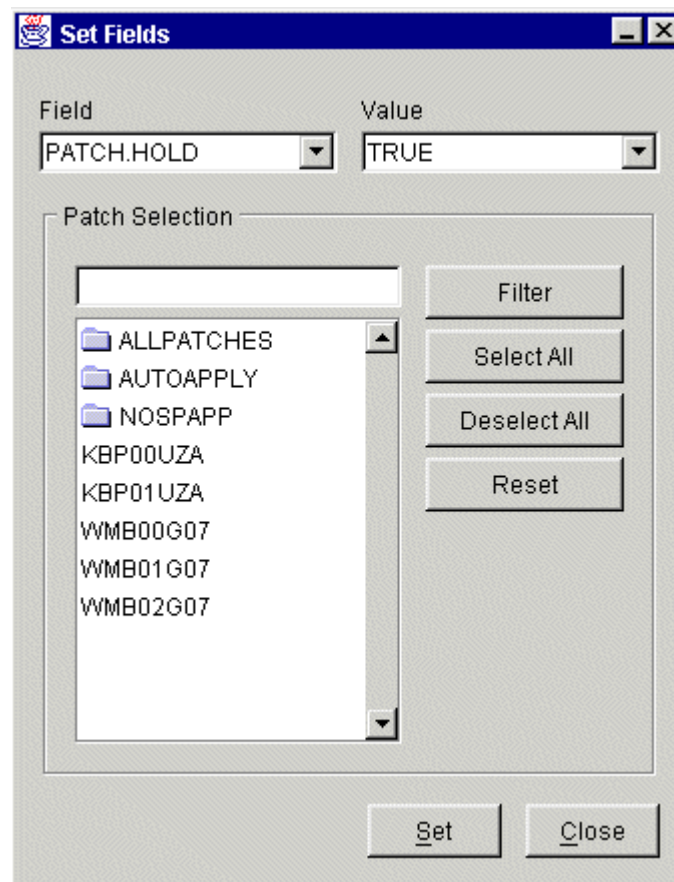
- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

### At the NPM GUI

- 2 On the Tasks menu, click **Set Field Values....**



The Set Field window is displayed.

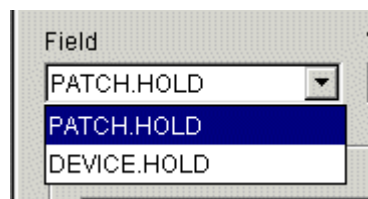


3 Using the table below, determine the Field and Value to select.

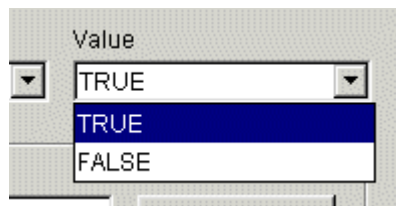
**Field and Value combinations**

| Field       | Value | Result                                                                                               |
|-------------|-------|------------------------------------------------------------------------------------------------------|
| PATCH.HOLD  | FALSE | The patch will be applied to the remaining devices. This is typically after the test period is over. |
| PATCH.HOLD  | TRUE  | The patch will be excluded from manual or automated patching activities.                             |
| DEVICE.HOLD | FALSE | The device will be included in patching tasks. This is typically after the test period is over.      |
| DEVICE.HOLD | TRUE  | The device will be excluded from manual or automated patching activities.                            |

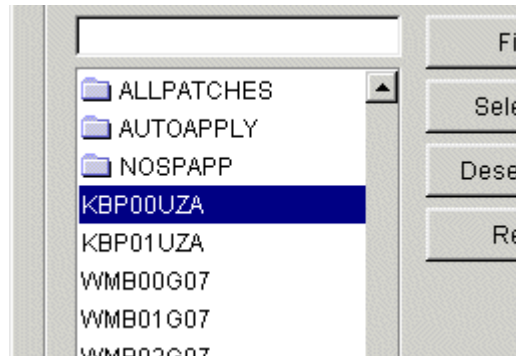
4 In the Field list, click **PATCH.HOLD** or **DEVICE.HOLD**.



5 In the Value list, click **TRUE** or **FALSE**.



- 6 In the Patch Selection list (if you clicked PATCH.HOLD), select one or more patches, or in the Device Selection list (if you clicked DEVICE.HOLD), select one or more devices.



- 7 Click **Set** to apply the changes.  
The system displays a confirmation message at the bottom of the Network Patch Manager window.
- 08:06:40 2002-05-28 INFO: Field PATCH.HOLD set to true
- 8 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

## Defining NPM patching reports

---

### Application

Use this procedure to define a patching report

The reporting feature of the Network Patch Manager (NPM) allows you to select information from the database and display it. Report criteria determines what is displayed.

The NPM is initially configured with the following system-defined reports:

- **ACTLIST** This report contains RPS activation patch information.
- **CALCLIST** This report is an RPS patch calculation report.
- **DEVICE** This report contains information about a specific device. This report has prompts.
- **DEVICELIST** This report contains information about patchable devices on the system.
- **DISABLEDAPPLIED** This report contains patches that are applied but disabled.
- **DISABLEDREMOVED** This report contains patches that are disabled and removed.
- **ENABLEDAPPLIED** This report contains patches that are applied and enabled.
- **ENABLEDREMOVED** This report contains patches that are applied but removed.
- **FULLDEVICELIST** This report contains information about every device on the system.
- **LOADLIST** This report is an RPS device load report.
- **PATCH** This report contains information about a specific patch. This report has prompts.
- **PATCHES\_SINCE** This report contains patch activity since a specific date (prompt report).
- **PATCHINFO** This report contains full information about a specific patch. This report has prompts.
- **PATCHLIST** This report contains information about patches and their relationships on the system.
- **DEVICE\_ACTIVITY** This report displays all devices and their activity states.

- **DEVICE\_ACTLEVEL** This report displays the number of patches activated in each device.
- **DEVICE\_APPLEVEL** This report displays the number of patches applied to each device.
- **INVALID\_LOADNAME** This report displays devices with invalid loads. An audit is required (see procedure [Performing a device audit using the NPM on page 2313](#), if required).
- **DEVICEINFO** This reports lists the devices in the office, the date the device registered, the loadname in the device, and the date the load was discovered in the device.
- **LASTAPPLYACTION** This report displays the patch, device, status, and description of why the apply attempt failed for this patch-device relationship.
- **PFRSSETTINGS** This report displays the PFRS dropbox IP address, userid, and if the delete patches is turned on, the status.
- **SYSTEMPLANSETTINGS** This report displays all the system plans defined for the office as well as the tasks, enable status, and schedule for each plan.
- **OFFICEINFOSETTINGS** This report displays office information, which at this time, only includes the GWC auto-imaging enabled setting.
- **GWCLOADIMAGEREPORT** This report displays the imaged load, the patches contained in the load, the time the image was taken, as well as a list of patches available in the office that are not contained in the image.

## Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

## Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2395](#)
- [Using the NPM GUI on page 2397](#)

## Using the NPM CLUI

### At your workstation

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

### At the NPM CLUI

- 2 Create the report by typing

```
npm> newreport <name> <desc> <fields> where
<criteria>
```

and pressing the Enter key.

where

**name**

is the name of the report you want to create

**desc**

is a short description of the report

**fields**

is the name of one or more fields, separated by a space, you want to include in the report

Use the command **viewtabs** to obtain a list of all the fields in the database that you can use in a report.

**criteria**

is the SQL statement that identifies the criteria by which to search the NPM database

### Example

```
npm> newreport DEVHOLDFALSE "All devices with
HOLD=FALSE" "DEVICE.DEVICEID DEVICE.HOLD
where DEVICE.HOLD='FALSE' "
```

| To                              | Command                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------|
| view the definition of a report | <b>viewreport &lt;reportname&gt;</b>                                                                           |
| view all defined reports        | <b>viewreport all</b>                                                                                          |
| generate a report               | <b>runreport &lt;reportname&gt;</b>                                                                            |
| delete a user-defined report    | <b>delreport &lt;reportname&gt;</b><br><b>Note:</b> The system allows you to only delete user-defined reports. |



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

## Using the NPM GUI

### At your workstation

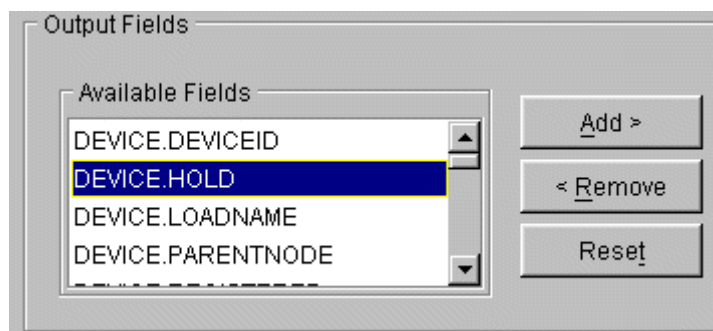
- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

### At the NPM GUI

- 2 On the Tasks menu, click **Reports....**



- 3 Specify the fields to be included in the new report as follows:  
**Note:** You can also edit an existing report listed under the Report List tab, that contains similar criteria to the report you want to create, and save it under a new name.
  - a In the Available Fields list, select a field of your choice.

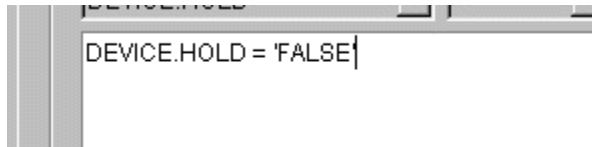


- b Click **Add** to add the field to the Selected Fields list.
  - c Repeat Steps [3a](#) and [3b](#) for each field, then proceed to step [4](#).

- 4 In the **Report Criteria** area, specify the criteria for the report using substep [a](#) or [b](#)

- a Type the criteria for the report in the text box.

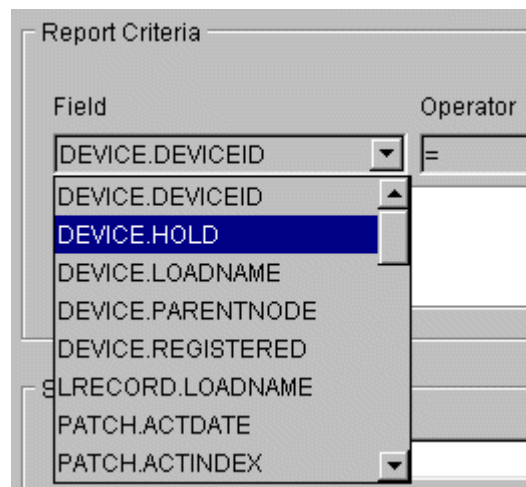
**Note:** Insert parenthesis “( )” to define precedence for multiple criteria statements.



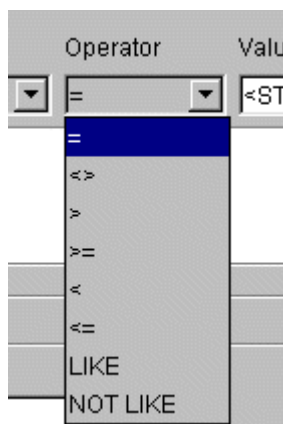
OR

- b Specify the report criteria as follows:

- i In the Field list, select the field of your choice.



- ii In the Operator list, select the operator of your choice.

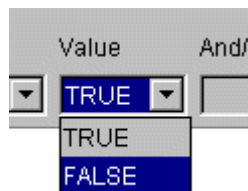


The table below lists the supported operators and their meaning.

| 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 (%) |

iii In the Value list, select the value of your choice

**Note:** The data type in the Value list will change depending on the data type selected in the Field list. For alphanumeric data, type the value. For boolean data, select the value.



To combine multiple criteria statements, click **AND** or **OR** in the And/Or list.

- 5 Type a unique name for the report in the Report Name box.
- 6 Type a description of the report in the Report Description box if desired.

7 Click **Save** to save the report.

The new report will appear under the Report List tab once the system has saved it as shown below.

| Report           | Description                                                      | Type   |
|------------------|------------------------------------------------------------------|--------|
| ACTLIST          | RPS activation patch information.                                | System |
| CALCLIST         | RPS Patch Calculation Report.                                    | System |
| DEVICE           | Information about a specific Device (prompt).                    | System |
| DEVICELIST       | Information about patchable Device(s) on the system.             | System |
| DEVICE_ACTIVITY  | All devices and their activity states                            | System |
| DEVICE_ACTLEVEL  | Displays how many patches are activated in each device.          | System |
| DEVICE_APPLEVEL  | Displays how many patches are applied to each device.            | System |
| DISABLEDAPPLIED  | Patches that are applied and disabled.                           | System |
| DISABLEDREMOVED  | Patches that are removed and disabled.                           | System |
| ENABLEDAPPLIED   | Patches that are applied and enabled.                            | System |
| ENABLEDREMOVED   | Patches that are removed and enabled.                            | System |
| FULLDEVICELIST   | Information about every Device(s) on the system.                 | System |
| INVALID_LOADNAME | Device(s) with invalid loads. Audit required.                    | System |
| LOADLIST         | RPS Device Load Report.                                          | System |
| PATCH            | Information about a specific patch (prompt).                     | System |
| PATCHES_SINCE    | Patch Activity since a specific date (prompt).                   | System |
| PATCHINFO        | Full information about a specific patch (prompt).                | System |
| PATCHLIST        | Information about patches and their relationships on the system. | System |
| DEVICEHOLD       | Devices on hold                                                  | User   |

| To                                      | Action                                                                  |
|-----------------------------------------|-------------------------------------------------------------------------|
| view or edit the definition of a report | select the report from the ReportList tab and click <b>Edit</b>         |
| generate a report                       | select the report from the ReportList tab and click <b>Execute</b>      |
| delete a user-defined report            | select the report from the ReportList tab and click <b>Delete</b>       |
|                                         | <b>Note:</b> The system allows you to only delete user-defined reports. |

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

---

## Defining NPM patching plans

---

### Application

Use this procedure to define a plan.

A plan is a list of one or more tasks that are to be executed according to a specific schedule. The schedule can specify either a one time execution at a given time or a repeated execution according to a frequency definition. A plan can include the following tasks: apply, remove, audit, and reports.

The NPM is initially configured with the following system-defined plans:

- **SYSTEMPLAN** This plan is initially defined with the **AUTOAPPLY** and **AUTORESTART** tasks.
- **REPORTCLEANUP** This plan is initially defined with the **DELETEREPORTS** task.
- **GETPATCH** This plan is initially defined with the **PFRSGETPATCH** task.
- **GENREPORT** This plan is initially defined with the **PFRSGENREPORT** task.

**Note 1:** It is recommended to not have the patching autoapply task run at the same time as a line, trunk, V5.2 (International only), or CS2K data audit when an audit is scheduled.

**Note 2:** The **AUTORESTART** task does not attempt to restart a device if any patches applicable to that device contain an auto restart record of "N". In addition, the **AUTORESTART** task does not attempt to restart the SPFS, as restart is not supported for the SPFS.

The NPM supports a maximum of eight plans, therefore, four plans can be defined in addition to the four system-defined plans.

You can also modify a plan, which includes enabling or disabling the plan, adding or deleting a task or report to or from the plan, modify the schedule of the plan and its description. If required, refer to procedure [Modifying NPM patching plans on page 2409](#).

### Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group **succssn** and secondary user group **esmadm**. If required, refer to procedure "Setting up local user accounts on an SPFS-based server" in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure "Configuring user

settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

## Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2402](#)
- [Using the NPM GUI on page 2404](#)

### Using the NPM CLUI

#### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

#### *At the NPM CLUI*

- 2 Define a plan by typing

```
npm> newplan <plan_name> <plan_freq>
<date_time> <max_time> <plan_desc>
```

and pressing the Enter key.

where

**plan\_name**

is the name of the plan

**plan\_freq**

is how often the plan must execute (Once, Hourly, Daily, Weekly, or Monthly)

**date\_time**

is the date and time the plan is to be executed in mm-dd-yy hh:mm format. Plans executed more than once will begin executing at this time of day each interval.

**max\_time**

is the maximum amount of time to execute the plan (No\_Limit, 15\_min, 30\_min, 1\_Hr, 2\_Hr, 4\_Hr, 8\_Hr, or 16Hr)

**plan\_desc**

is a brief description of the plan

**Example**

```
npm> newplan <plan_name> Weekly "07-15-03
16:59" 4_Hr "NPM weekly scheduled routine
activities"
```

- 3** Enable the plan by typing

```
npm> enableplan <plan_name>
```

and pressing the Enter key.

where

**plan\_name**

is the name of the plan

- 4** Add a task or report to the plan by typing

```
npm> modifyplan <plan_name> <tr_option>
<tr_name> add
```

and pressing the Enter key.

where

**plan\_name**

is the name of the plan

**tr\_option**

is TASK or REPORT, which indicates the type of activity being added

**tr\_name**

is the name of the task or report

**Example**

```
npm> modifyplan <plan_name> TASK AUDIT ADD
```

- 5** Repeat step [4](#) for each task or report you want to add to the plan.

| To                            | Command                                                               |
|-------------------------------|-----------------------------------------------------------------------|
| view the definition of a plan | <b>viewplan &lt;plan_name&gt;</b>                                     |
| view all defined plans        | <b>viewplan all</b>                                                   |
| delete a user-defined plan    | <b>delplan &lt;plan_name&gt;</b>                                      |
|                               | <b>Note:</b> The system allows you to only delete user-defined plans. |

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



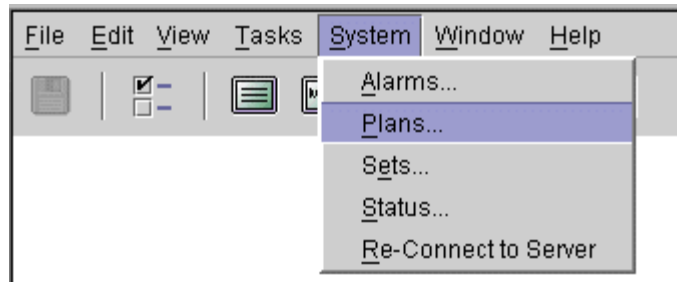
## Using the NPM GUI

### *At your workstation*

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

### *At the NPM GUI*

- 2 On the System menu, click **Plans...**



The Plans window opens.

- 3 Click the **Plans** tab if not already displayed, and click **Reset All**.

Plans | Plan List

Plan Name:

Plan Description:

☐ Enabled

Task / Report Selection

Available Tasks/Reports

- Tasks
- AUTOAPPLY
- AUDIT
- AUTORESTART
- PFRSGETPATCH
- PFRSGENREPORT

Selected Tasks/Reports

- Tasks
- Reports

Frequency: Once | Date: 06/07/2005 | Time: 00:00 | Time Limit: No\_Limit

Save | **Reset All** | Close

- 4 In the Plan Name box, type a unique name for the plan, and in the Plan Description box, type a description of the plan (optional).

Plans | Plan List

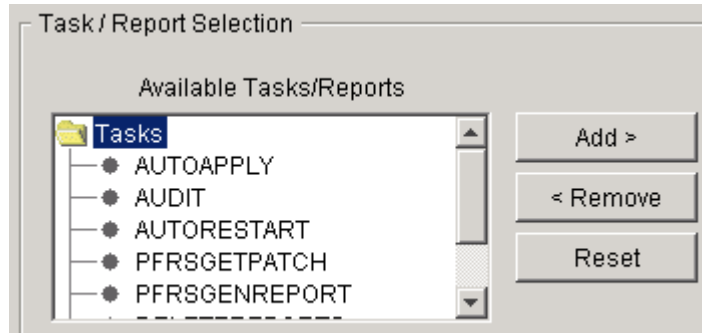
Plan Name:

Plan Description:

- 5 Click the **Enabled** check box.

☒ Enabled

- 6 Add tasks or reports to the plan as follows:
- a In the Available Tasks/Reports list, double click on the **Tasks** or **Reports** folder to display the available tasks or reports.



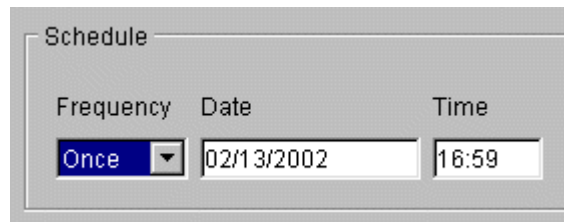
- b Click the task or report you want to add to the plan.
- Note:** Only add reports that do not require any user input when they are run in the event a user is not present at the time the plan runs. This includes pre-defined reports and user-defined reports. The pre-defined reports that require user input are as follows:
- DEVICE
  - PATCH
  - PATCHES\_SINCE
  - PATCHINFO
- c Click **Add** to add the task or report to the Selected Tasks/Reports list.
- Note:** The order in which the tasks and reports appear in the Selected Tasks/Reports list, is the order in which they will execute. The tasks in a plan are executed sequentially.
- d Repeat step [6a](#) through [6c](#) for each task or report you want to add to the plan.
- Note:** You can use the Shift key to select multiple tasks or reports consecutively, or the Ctrl key to select multiple tasks or reports non-consecutively.

**7** Specify the execution schedule under Schedule are as follows:

- a** In the Frequency list, select the frequency option of your choice.

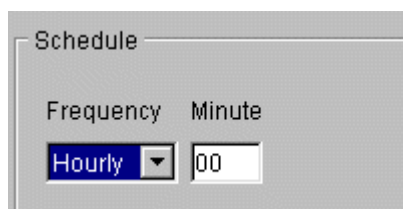
When you select a frequency option, the related scheduling fields are displayed. An example of each frequency option and its related fields follows.

**Once option**



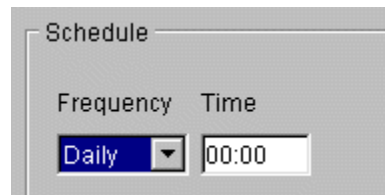
The screenshot shows a dialog box titled "Schedule". It contains three fields: "Frequency" with a dropdown menu set to "Once", "Date" with a text box containing "02/13/2002", and "Time" with a text box containing "16:59".

**Hourly option**



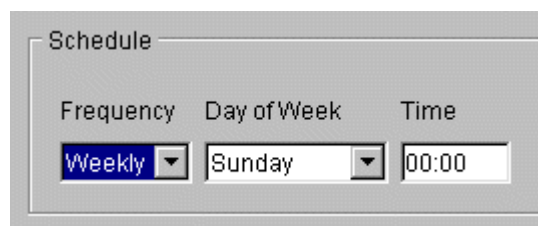
The screenshot shows a dialog box titled "Schedule". It contains two fields: "Frequency" with a dropdown menu set to "Hourly", and "Minute" with a text box containing "00".

**Daily option**



The screenshot shows a dialog box titled "Schedule". It contains two fields: "Frequency" with a dropdown menu set to "Daily", and "Time" with a text box containing "00:00".

**Weekly option**



The screenshot shows a dialog box titled "Schedule". It contains three fields: "Frequency" with a dropdown menu set to "Weekly", "Day of Week" with a dropdown menu set to "Sunday", and "Time" with a text box containing "00:00".

- b** Enter the appropriate scheduling information for the frequency option you selected.
- c** In the Time Limit list, select the time limit of your choice. The time limit defines how long the plan will be allowed to run.

**8** Click **Save** to save the plan.

The new plan will appear on the Plan List tab once the NPM has saved the plan.

| Plans Plan List |                                     |           |              |                   |                               |
|-----------------|-------------------------------------|-----------|--------------|-------------------|-------------------------------|
| Plan            | Enabled                             | Frequency | Date/Time    | Tasks/Reports     | Description                   |
| SYSTEMPLAN      | <input type="checkbox"/>            | Daily     | 00:00        | TASK:AUTOAPPL...  | NPM System scheduled routi    |
| REPORTCLEANUP   | <input type="checkbox"/>            | Daily     | 00:00        | TASK:DELETEREP... | Delete reports associated w   |
| GETPATCH        | <input type="checkbox"/>            | Daily     | 23:00        | TASK:PFRSGETP...  | Patch file retrieval          |
| GENREPORT       | <input type="checkbox"/>            | Daily     | 10:00        | TASK:PFRSGENR...  | PFRS Inform list report gener |
| NEWPLAN         | <input checked="" type="checkbox"/> | Weekly    | Sunday 00:00 | TASK:AUDIT        | Weekly routine activities     |

| To                            | Action                                                                                                                                     |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| view the definition of a plan | select the plan from the PlanList tab and click <b>View</b>                                                                                |
| execute a plan                | select the plan from the PlanList tab and click <b>Execute</b>                                                                             |
| delete a user-defined plan    | select the plan from the PlanList tab and click <b>Delete</b><br><br><b>Note:</b> The system allows you to only delete user-defined plans. |

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

---

## Modifying NPM patching plans

---

### Application

Use this procedure to make one or more of the following modifications to a plan using the Network Patch Manager (NPM):

- enable or disable the execution of a plan
- add or delete a task or report to or from a plan
- modify the schedule of a plan
- modify the description of a plan

**Note:** You cannot rename a plan, but you can save it under a new name and delete the original plan.

A plan is a list of one or more tasks that are to be executed according to a specific schedule. The schedule can specify either a one time execution at a given time or repeated execution according to a frequency definition. A plan can include the following tasks: apply, remove, audit, and reports.

The NPM is initially configured with the following system-defined plans:

- **SYSTEMPLAN** This plan is initially defined with the **AUTOAPPLY** and **AUTORESTART** tasks.
- **REPORTCLEANUP** This plan is initially defined with the **DELETEREPORTS** task.
- **GETPATCH** This plan is initially defined with the **PFRSGETPATCH** task.
- **GENREPORT** This plan is initially defined with the **PFRSGENREPORT** task.

The system-defined plans cannot be renamed, but they can be modified or deleted.

**Note 1:** It is recommended to not have the patching autoapply task run at the same time as a line, trunk, V5.2 (International only), or CS2K data audit when an audit is scheduled.

**Note 2:** The **AUTORESTART** task does not attempt to restart a device if any patches applicable to that device contain an auto restart record of "N". In addition, the **AUTORESTART** task does not attempt to restart the SPFS, as restart is not supported for the SPFS.

The NPM supports a maximum of eight plans, therefore, four plans can be defined in addition to the four system-defined plans.

## Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

## Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2410](#)
- [Using the NPM GUI on page 2414](#)

### Using the NPM CLUI

#### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

#### *At the NPM CLUI*

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

| If you want to                                   | Do                     |
|--------------------------------------------------|------------------------|
| enable the execution of a scheduled plan         | step <a href="#">3</a> |
| disable the execution of a scheduled plan        | step <a href="#">4</a> |
| add or delete a task or report to or from a plan | step <a href="#">5</a> |
| modify the schedule and description of a plan    | step <a href="#">6</a> |

**3** Enable the execution of a scheduled plan by typing

```
npm> enableplan <plan_name>
```

and pressing the Enter key.

where

**plan\_name**

is the name of the plan

**Note:** If the start time for the plan has already passed, this step will fail. To correct this, modify the plan schedule to change the start time (see step [6](#)). Then perform this step again.

Proceed to step [7](#).

**4** Disable the execution of a scheduled plan as follows:**a** Disable the execution of the scheduled plan by typing

```
npm> disable <plan_name>
```

and pressing the Enter key.

where

**plan\_name**

is the name of the plan

**b** Determine whether any tasks are running by typing

```
npm> qrunning
```

and pressing the Enter key.

---

| If                                                                     | Do                     |
|------------------------------------------------------------------------|------------------------|
| a task is running                                                      | step <a href="#">c</a> |
| the system response is "No maintenance commands are currently running" | step <a href="#">d</a> |

---

**c** Allow any non-completed tasks to finish.**d** Proceed to step [7](#).



**5** Add or delete a task or report to or from a plan by typing

```
npm> modifyplan <plan_name> <tr_option>
 <tr_name> <add_delete>
```

and pressing the Enter key.

where

**plan\_name**

is the name of the plan

**tr\_option**

is TASK or REPORT, which indicates whether the type of activity being added or deleted to or from the plan is a Task or Report

**tr\_name**

is the name of the task or report being added or deleted

**add\_delete**

is ADD or DELETE, which indicates whether the task or report is being added or deleted to or from the plan

**Example**

```
npm> modifyplan TASK AUDIT ADD
```

Proceed to step [7](#).

- 6 Modify the schedule and description of a plan by typing

```
npm> updsched <plan_name> <plan_freq>
<date_time> <max_time> <plan_desc>
```

and pressing the Enter key.

where

**plan\_name**

is the name of the plan

**plan\_freq**

is Once, Hourly, Daily, Weekly, or Monthly, which indicates how often the plan must execute

**date\_time**

is the date and time the plan is to be executed in mm-dd-yy hh:mm format. Plans executed more than once will begin executing on the day and time each interval.

**max\_time**

is No\_Limit, 15\_min, 30\_min, 1\_Hr, 2\_Hr, 4\_Hr, 8\_Hr, or 16Hr, which indicates the maximum amount of time to execute the plan

**plan\_desc**

is a brief description of the plan

**Example**

```
npm> updsched Weekly "02-15-02 16:59" 4_Hr
"NPM System weekly scheduled routine
activities"
```

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

| If                             | Do                     |
|--------------------------------|------------------------|
| you have further modifications | step <a href="#">2</a> |
| otherwise                      | step <a href="#">8</a> |

- 8 Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

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

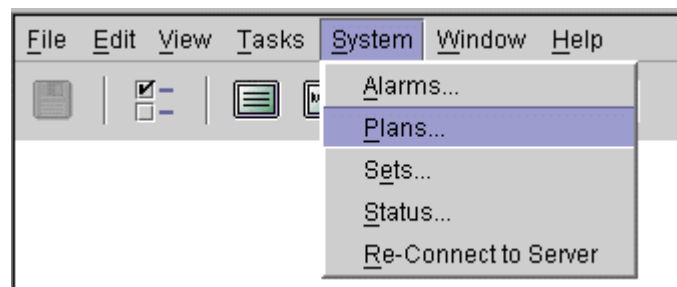
## Using the NPM GUI

### At your workstation

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

### At the NPM GUI

- 2 On the System menu, click **Plans...**



The Plans window opens.

- 3 Click the **Plan List** tab.
- 4 In the Plans List tab, select the plan you want to modify.

| Plans         |                          |           |           |                   |                               |
|---------------|--------------------------|-----------|-----------|-------------------|-------------------------------|
| Plan List     |                          |           |           |                   |                               |
| Plan          | Enabled                  | Frequency | Date/Time | Tasks/Reports     | Description                   |
| SYSTEMPLAN    | <input type="checkbox"/> | Daily     | 00:00     | TASK:AUTOAPPL...  | NPM System scheduled rout     |
| REPORTCLEANUP | <input type="checkbox"/> | Daily     | 00:00     | TASK:DELETEREP... | Delete reports associated w   |
| GETPATCH      | <input type="checkbox"/> | Daily     | 23:00     | TASK:PFRSGETP...  | Patch file retrieval          |
| GENREPORT     | <input type="checkbox"/> | Daily     | 10:00     | TASK:PFRSGENR...  | PFRS Inform list report gener |

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

| If you want to                                   | Do                      |
|--------------------------------------------------|-------------------------|
| enable the execution of a scheduled plan         | step <a href="#">6</a>  |
| disable the execution of a scheduled plan        | step <a href="#">7</a>  |
| modify the description of a plan                 | step <a href="#">8</a>  |
| add or delete a task or report to or from a plan | step <a href="#">9</a>  |
| modify the schedule of a plan                    | step <a href="#">12</a> |

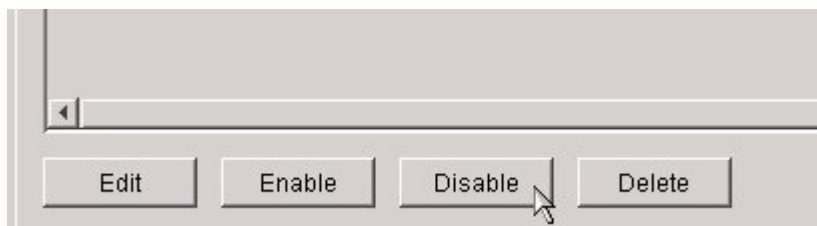
- 6 Click **Enable** to enable the execution of the plan.



Proceed to step [14](#).

- 7 Disable the execution of the plan as follows:

- a Click **Disable**.



- b On the View menu, click **Tasks Window** to determine whether any tasks are running.



The Tasks window opens.

| If the Tasks window                      | Do                     |
|------------------------------------------|------------------------|
| shows that one or more tasks are running | step <a href="#">c</a> |
| shows completed or no tasks              | step <a href="#">d</a> |

**c** Allow any non-completed tasks to finish.

**d** Click **Close** to close the Tasks window.

Proceed to step [14](#).

**8** Modify the description of the plan as follows:

**a** Click **Edit**.



**b** In the Plan Description box, type a new description of the plan.

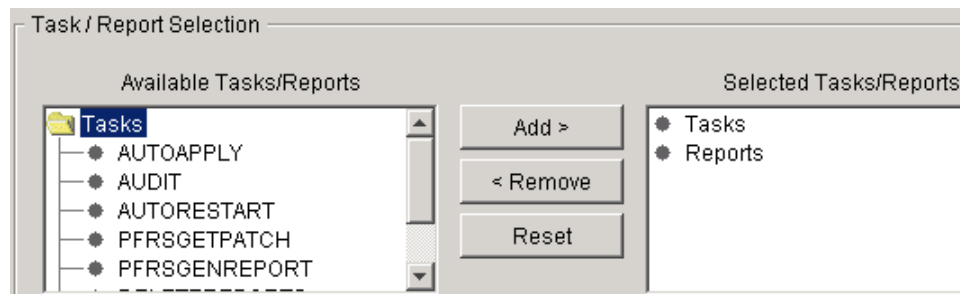
 A screenshot of a software window titled 'Plans'. It has two tabs: 'Plans' and 'Plan List'. The 'Plan List' tab is selected. Below the tabs, there are two input fields. The first is labeled 'Plan Name:' and contains the text 'NEWPLAN'. The second is labeled 'Plan Description:' and contains the text 'Weekly routine activities'.

Proceed to step [13](#).

**9** Use the following table to determine your next step.

| If you want to                        | Do                      |
|---------------------------------------|-------------------------|
| add tasks or reports to the plan      | step <a href="#">10</a> |
| delete tasks or reports from the plan | step <a href="#">11</a> |

- 10 Add tasks or reports to the plan as follows:
- In the Available Tasks/Reports list, double-click on the **Tasks** or **Reports** folder to display the available tasks or reports.



- Select the task or report you want to add to the plan.

**Note:** Do not add reports that require user input when they execute in the event a user is not present at the time those reports execute. This includes system-defined reports and user-defined reports. The system-defined reports that require user input, and that you must not add, are as follows:

- DEVICE
- PATCH
- PATCHES\_SINCE
- PATCHINFO

- Click **Add** to add the task or report to the Selected Tasks/Reports list.

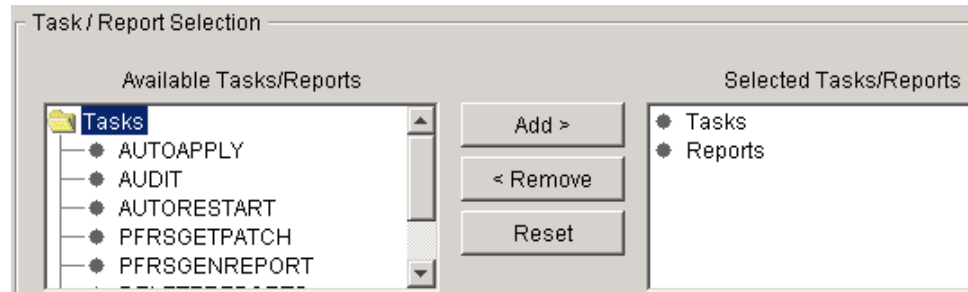
**Note:** The order in which the tasks and reports appear in the Selected Tasks/Reports list, is the order in which they will execute. The tasks in a plan are executed sequentially.

- Repeat steps [10a](#) through [10c](#) for each task or report you want to add to the plan.

**Note:** You can use the Shift key to select multiple tasks or reports consecutively, or the Ctrl key to select multiple tasks or reports non-consecutively.

Proceed to step [13](#).

- 11 Delete tasks or reports from the plan as follows:
- In the Selected Tasks/Reports list, double-click on the **Tasks** or **Reports** folder to display the selected tasks or reports.



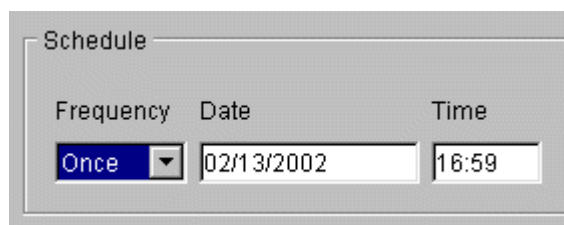
- Click the task or report you want to delete from the plan.
- Click **Remove** to delete the task or report from the Selected Tasks/Reports list.
- Repeat steps [11a](#) through [11c](#) for each task or report you want to remove from the plan.

**Note:** You can use the Shift key to select multiple tasks or reports consecutively, or the Ctrl key to select multiple tasks or reports non-consecutively.

Proceed to step [13](#).

- 12 Under Schedule, update the plan schedule if required, as follows:
- In the Frequency list, select the frequency option of your choice.
- When you select a frequency option, the related scheduling fields are displayed. An example of each frequency option and its related fields follows.

### Once option



### Hourly option

Schedule

Frequency Minute

Hourly 00

### Daily option

Schedule

Frequency Time

Daily 00:00

### Weekly option

Schedule

Frequency Day of Week Time

Weekly Sunday 00:00

- b Enter the appropriate scheduling information for the frequency option you selected.
  - c In the Time Limit list, select the time limit of your choice. The time limit defines how long the plan will be allowed to run.
- 13** Click **Save** to save the plan.

The modified plan will appear on the Plan List tab once the NPM has saved the plan.

| Plans Plan List |                                     |           |              |                   |                               |
|-----------------|-------------------------------------|-----------|--------------|-------------------|-------------------------------|
| Plan            | Enabled                             | Frequency | Date/Time    | Tasks/Reports     | Description                   |
| SYSTEMPLAN      | <input type="checkbox"/>            | Daily     | 00:00        | TASK:AUTOAPPL...  | NPM System scheduled routi    |
| REPORTCLEANUP   | <input type="checkbox"/>            | Daily     | 00:00        | TASK:DELETEREP... | Delete reports associated w   |
| GETPATCH        | <input type="checkbox"/>            | Daily     | 23:00        | TASK:PFRSGETP...  | Patch file retrieval          |
| GENREPORT       | <input type="checkbox"/>            | Daily     | 10:00        | TASK:PFRSGENR...  | PFRS Inform list report gener |
| NEWPLAN         | <input checked="" type="checkbox"/> | Weekly    | Sunday 00:00 | TASK:AUDIT        | Weekly routine activities     |



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

| <b>If</b>                      | <b>Do</b>               |
|--------------------------------|-------------------------|
| you have further modifications | step <a href="#">5</a>  |
| otherwise                      | step <a href="#">15</a> |

- 15** Click **Close** to close the Plans window.
- 16** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

## Prioritizing or aborting a patching maintenance request using the NPM

---

### Application

Use this procedure to prioritize or abort a patching maintenance request.

### Prerequisites

To use the NPM for patching activities, your user account must be assigned to both the primary user group succssn and secondary user group esmadm. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP solution-level Security and Administration*, NN10402-600, or procedure “Configuring user settings” in *IEMS Security and Administration*, NN10336-611, for centrally-managed user accounts.

### Action

Use one of the following methods to complete this procedure.

- [Using the NPM CLUI on page 2421](#)
- [Using the NPM GUI on page 2422](#)

#### Using the NPM CLUI

##### *At your workstation*

- 1 Access the NPM CLUI. If required, refer to procedure [Accessing the Network Patch Manager CLUI on page 2284](#).

##### *At the NPM CLUI*

- 2 List the maintenance requests that are either in progress or in the queue by typing

```
npm> qrunning
```

and pressing the Enter key.

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

| If you want to                   | Do                     |
|----------------------------------|------------------------|
| prioritize a maintenance request | step <a href="#">4</a> |
| abort a maintenance request      | step <a href="#">5</a> |

- 4 Move the desired maintenance request to the top of the processing queue by typing  
`npm> priority <task ID>`  
and pressing the Enter key.  
where  
**task ID**  
is the number next to the task  
The task moves to the top of the queue for processing.  
Proceed to step 6.
- 5 Abort the desired maintenance request by typing  
`npm> abtk <task ID>`  
and pressing the Enter key.  
where  
**task ID**  
is the number next to the task  
The system aborts the task.
- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

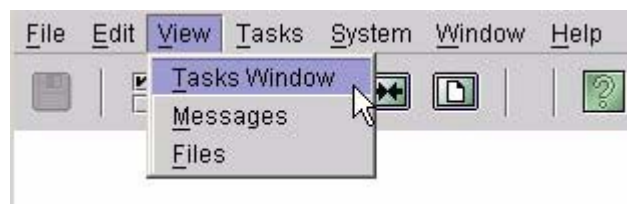
## Using the NPM GUI

### *At your workstation*

- 1 Access the NPM GUI. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

### *At the NPM GUI*

- 2 On the View menu, click **Tasks Window**.

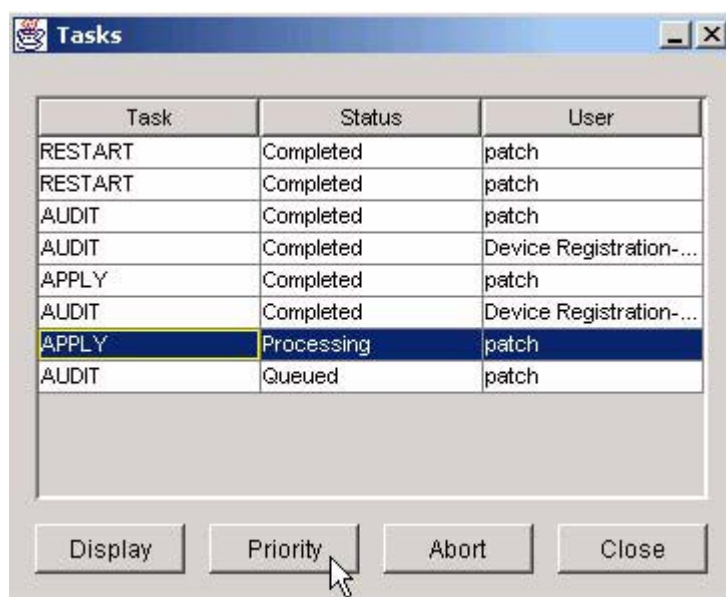


The **Tasks** window displays.

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

| If you want to                            | Do                     |
|-------------------------------------------|------------------------|
| prioritize a patching maintenance request | step <a href="#">4</a> |
| abort a patching maintenance request      | step <a href="#">5</a> |

- 4 Select the queued task to move to the top of the processing queue, and click **Priority**.



The task moves to the top of the queue for processing.

Proceed to step [6](#).

- 5 Select the queued task you want to abort, and click **Abort**.  
The system aborts the task.
- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

## Manually activating patches

### ATTENTION

Ensure that the passwords for the patch activation have been provided by Nortel's Software Delivery team. If you need assistance with missing passwords or other password related issues, please contact your Nortel Account Manager.

After completing an SN09FF network upgrade a group of patches requires special consideration. These patches require manual activation in the sequence specified in the Manual Activation Patch Order table for the different processor types. Two limited patches require application rather than activation.

Only activate the patches associated with the DRUs installed in the network. The following table contains the SN09FF DRUs and associated patches that require manual activation. The patch IDs of patches listed in the table are appended with a suffix to identify whether they are for a PowerPC (ppc) or BRISC-based processor. The [Manual patch activation procedure](#) describes how to determine which DRUs are in the network.

### SN09FF DRUs and Associated Patches

| DRU     | Associated Patches                                                                                                                                       |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| CCM     | ZIG62, TWH76, SPL51, SPL70, SPL55, SPL57, SPL83, SPL60, SPL89, DDR69, MSP53, MSP57, SPL78, SPL86, MSP01, MSP59, CFZ46, CFZ50, CKD52, CFZ51, CFZ54, MSP59 |
| WT      | AHN13, ZAT94, PTA39, PTA77, PTA78, PTA88                                                                                                                 |
| MSH     | TWH77, SPL79, CKD50                                                                                                                                      |
| CNA     | SPL94, SPL66, MSP08                                                                                                                                      |
| ESU13BB | XIX39 (limited patch)                                                                                                                                    |
| ESI13BB | XIX41 (limited patch)                                                                                                                                    |

Refer to the *Post-Release Software Manager (PRSM) Reference Guide*, 297-8991-540 located in the DMS or TDM documentation collections for procedures to apply patches using the PRSM tool.

## Prerequisites

Before manually activating the patches referenced in this procedure, ensure that:

- the entire SN09FF upgrade has been completed
- the patches requiring activation have been applied through PRSM
- SOC CS2C0005 is enabled if the network supports:
  - SIP Lines: International Support
  - Enhanced Network Centrex and RES services
- ensure that the passwords and list of patches for the patch activation have been provided by Nortel's Software Delivery team. Contact your Nortel Account Manager for any password related issues.
- limited patches XIX39 and XIX41 have been downloaded if the network supports the MG9000 ABI I/F to SMU feature

## Manual patch activation

The following tables list the required activation sequence. Only activate the patches that apply to your network and processor type. Nortel Software Delivery provides a listing of patches that require passwords for activation. Start with the first patch in the applicable table that applies to your network and continue sequentially to the next patch in the table until all required patches have been activated in the proper sequence.

Use the patch IDs in one of the following tables:

- For core platforms using PowerPC-based processors, use the table [Manual Activation Patch Order for a PowerPC-based processor on page 2425](#).
- For core platforms using BRISC-based processors, use the table [Manual Activation Patch Order for a BRISC-based processor on page 2427](#).

### Manual Activation Patch Order for a PowerPC-based processor

|   | Patch ID | DRU | Password | Billable |
|---|----------|-----|----------|----------|
| 1 | ZIG62P9E | CCM | Y        |          |
| 2 | AHN13P9P | WT  | Y        |          |
| 3 | TWH76P9E | CCM |          |          |
| 4 | TWH77P9M | MSH | Y        |          |

**Manual Activation Patch Order for a PowerPC-based processor**

|    | Patch ID | DRU | Password | Billable |
|----|----------|-----|----------|----------|
| 5  | SPL94P9F | CNA | Y        |          |
| 6  | SPL51P9E | CCM | Y        |          |
| 7  | SPL66P9F | CNA | Y        |          |
| 8  | SPL70P9E | CCM | Y        |          |
| 9  | MSP08P9F | CCM | Y        |          |
| 10 | SPL55P9E | CCM | Y        |          |
| 11 | SPL57P9E | CCM | Y        |          |
| 12 | SPL83P9E | CCM | Y        |          |
| 13 | SPL60P9E | CCM | Y        |          |
| 14 | SPL89P9E | CCM | Y        |          |
| 15 | DDR69P9E | CCM |          |          |
| 16 | MSP53P9E | CCM | Y        |          |
| 17 | MSP57P9E | CCM |          |          |
| 18 | SPL78P9E | CCM | Y        |          |
| 19 | SPL79P9M | MSH | Y        |          |
| 20 | SPL86P9E | CCM | Y        |          |
| 21 | MSP01P9E | CCM |          |          |
| 22 | MSP59P9E | CCM |          |          |
| 23 | ZAT94P9P | WT  | Y        | Y        |
| 24 | PTA39P9P | WT  | Y        |          |
| 25 | CKD50P9M | MSH |          | Y        |
| 26 | CFZ46P9E | CCM |          | Y        |
| 27 | CFZ50P9E | CCM |          | Y        |

**Manual Activation Patch Order for a PowerPC-based processor**

|    | Patch ID | DRU | Password | Billable |
|----|----------|-----|----------|----------|
| 28 | CKD52P9E | CCM | Y        | Y        |
| 29 | CFZ51P9E | CCM | Y        | Y        |
| 30 | CFZ54P9E | CCM |          | Y        |
| 31 | PTA77P9P | WT  | Y        |          |
| 32 | PTA78P9P | WT  |          |          |
| 33 | PTA88P9P | WT  | Y        |          |
| 34 | MSP59    | CCM |          |          |

**Manual Activation Patch Order for a BRISC-based processor**

|    | Patch ID | DRU | Password | Billable |
|----|----------|-----|----------|----------|
| 1  | ZIG62B9E | CCM | Y        |          |
| 2  | AHN13B9P | WT  | Y        |          |
| 3  | TWH76B9E | CCM |          |          |
| 4  | TWH77B9M | MSH | Y        |          |
| 5  | SPL94B9F | CNA | Y        |          |
| 6  | SPL51B9E | CCM | Y        |          |
| 7  | SPL66B9F | CNA | Y        |          |
| 8  | SPL70B9E | CCM | Y        |          |
| 9  | MSP08B9F | CCM | Y        |          |
| 10 | SPL55B9E | CCM | Y        |          |
| 11 | SPL57B9E | CCM | Y        |          |
| 12 | SPL83B9E | CCM | Y        |          |
| 13 | SPL60B9E | CCM | Y        |          |
| 14 | SPL89B9E | CCM | Y        |          |



**Manual Activation Patch Order for a BRISC-based processor**

|    | Patch ID | DRU | Password | Billable |
|----|----------|-----|----------|----------|
| 15 | DDR69B9E | CCM |          |          |
| 16 | MSP53B9E | CCM | Y        |          |
| 17 | MSP57B9E | CCM |          |          |
| 18 | SPL78B9E | CCM | Y        |          |
| 19 | SPL79B9M | MSH | Y        |          |
| 20 | SPL86B9E | CCM | Y        |          |
| 21 | MSP01B9E | CCM |          |          |
| 22 | MSP59B9E | CCM |          |          |
| 23 | ZAT94B9P | WT  | Y        | Y        |
| 24 | PTA39B9P | WT  | Y        |          |
| 25 | CKD50B9M | MSH |          | Y        |
| 26 | CFZ46B9E | CCM |          | Y        |
| 27 | CFZ50B9E | CCM |          | Y        |
| 28 | CKD52B9E | CCM | Y        | Y        |
| 29 | CFZ51B9E | CCM | Y        | Y        |
| 30 | CFZ54B9E | CCM |          | Y        |
| 31 | PTA77B9P | WT  | Y        |          |
| 32 | PTA78B9P | WT  |          |          |
| 33 | PTA88B9P | WT  | Y        |          |
| 34 | MSP59    | CCM |          |          |

Perform the following procedure for each patch that requires manual activation.

## Manual patch activation procedure

### *At the CI level of the MAP display*

- 1 Determine the DRUs installed on the network by typing:

**IMAGENAME**

#### *SAMPLE OUTPUT*

XANA1 BCS 57 BN built on 2005-SEP-03 at 10:54:00 using psnnc09bs  
PRODUCT: SNNCS.009  
LOAD: SN000.009  
LAYER: BAS.23.0.BN  
LAYER: TL.22.0.BN  
LAYER: SHR.22.0.BS  
LAYER: CCM.22.0.BS  
LAYER: CNA.22.0.BS  
LAYER: UCS.22.0.BS  
LAYER: TOPSC.22.0.BS  
LAYER: CNATOPS.22.0.BS  
LAYER: BCTOPS.22.0.BS  
LAYER: MSH.22.0.BS  
LAYER: SNNCSH.09.0.BS

- 2 The DRU name appears immediately after “LAYER:” Compare the DRUs to those listed in the [SN09FF DRUs and Associated Patches](#) table to determine which patches require activation.

For example, the sample output in this procedure would require only activating the patches associated with the following DRUs: CCM, MSH, and CNA

Likewise, according to the sample output, the following DRUs would not require activation: WT and GWC.

**Note:** In this example, the two limited patches associated with DRUs ESU13BB and ESI13BB would not require application

- 3 Access the PRSM tool by typing

**PRSM**

- 4 Manually activate each patch that requires activation (those with DRUs identified in the network) according to the sequence listed in the table for your processor type by typing:

**ASSIGN ACTIVE Y IN PRSASET <patchid>**

*Examples for PowerPC*

**ASSIGN ACTIVE Y IN PRSASET ZIG62P9E**

**ASSIGN ACTIVE Y IN PRSASET AHN13P9P**

- 5 Based on the DRU listing in the *imagename* output from [step 1](#), determine if limited patches require application.

---

| <b>If ESU13BB or ESI13BB are</b> | <b>Do</b>              |
|----------------------------------|------------------------|
| in the output                    | <a href="#">step 6</a> |
| not in the output                | <a href="#">step 7</a> |

---

- 6 Using patch application procedures in the Post-Release Software Manager (PRSM) Reference Guide apply the appropriate limited patches:
- XIX39 (ESU13BB)
  - XIX41 (ESI13BB)
- 7 Procedure is complete

---

## Adding a maintenance interface for Session Server-Lines

---

### Application

Use this procedure to add a maintenance interface (OMI) field in the CS 2000 Management Tools for the Session Server-Lines component. This field is used when testing SIP lines using the LMM application.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.  
  
In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.  
  
For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).
- 2 Access the bin directory by typing:  
  
**cd /opt/nortel/NTsesm/admin/bin**  
  
and pressing the Enter key.
- 3 Enter the configuration CLUI by typing  
  
**configure**  
  
and pressing the Enter key.

#### *Example response*

```
SESM configuration
 1 - SESM common configuration (IP addresses,
Market, CM CLI)
 2 - SESM database tools
 3 - SESM related applications configuration
(MG9K, LMM, CICM, CS2KSS)
 4 - SESM provisioning configuration
 5 - SESM logging configuration (syslog, sesm
debug log)
 6 - view sesm configuration settings
 7 - SESM refresh properties
```

8 - GWC hardware and profile compatibility  
inspect tool (For Upgrade to SESM SN10)

X - exit

**4** Enter

**3**

and press the Enter key.

Example response

SESM Related Applications Configuration

1 - SESM MG9K configuration

2 - SESM LMM CM CLLI registration

3 - SESM CICM EM configuration

4 - SESM CS2KSS Provisioning Manager Server  
configuration

X - exit

select-

**5** Enter

**4**

and press the Enter key.

Example response

SESM-CS2KSS configuration

OPI - Provisioning Manager Interface  
configuration

Enter OPI transport protocol to EM server (  
http/https - default: https)

[1] - http

[2] - https

[x] - exit

select-

**6** Enter

**2**

and press the Enter key.

Example response

Using default transport protocol - https

Enter the IP address / Name of the primary CS2KSS prov server (default: 47.142.128.36) :

The primary CS2KSS prov server IP address is the same as the logical IP address of primary Session Manager server.

- 7** Accept the current value by pressing the Enter key.

Example response

Enter the primary CS2KSS prov server http port (default is 8443):

- 8** Accept the current value by pressing the Enter key.

Example response

Enter the IP address / Name of the secondary CS2KSS prov server (default: 47.142.128.36) :

The secondary CS2KSS prov server IP address is the same as the logical IP address of secondary Session Manager server.

- 9** Accept the current value by pressing the Enter key.

Example response

Enter the secondary CS2KSS prov server http port (default is 8443):

- 10** Accept the current value by pressing the Enter key.

Example response

Enter the OPI administrator user name (default: admin):

- 11** Enter the OPI administrator user name and press the Enter key.

The OPI administrator user name and password must match the MCP provisioning manager user name and password.

Example response

Enter the OPI administrator password:

- 12** Enter the OPI administrator password and press the Enter key.

Example response

Re-enter the OPI administrator password:

- 13** Enter the OPI administrator password again and press the Enter key.

Example response

OMI - Provisioning Manager Interface configuration

```
Enter OMI transport protocol to EM server (
http/https - default: https)
```

```
[1] - http
[2] - https
[x] - exit
```

```
select -
```

**14** Enter

**2**

and press the Enter key.

Example response

```
Using default transport protocol - https
Enter the IP address / Name of the primary
CS2KSS mtc server (default: none) :
```

**15** Type in the IP address for the CS2KSS mtc server and press the Enter key.

Example response

```
Enter the primary CS2KSS mtc server https port
(default is 12121):
```

**Note:** For this procedure, the OMI ip address is the same as the OPI ip address. Additionally, the primary OPI and OMI ip address are the same as the secondary OPI and OMI ip address. This may not apply in all cases, depending on your configuration.

**16** Accept the current value by pressing the Enter key.

Example response

```
Using default port.
Enter the IP address / Name of the secondary
CS2KSS mtc server (default: 47.142.128.36) :
```

**17** Accept the current value by pressing the Enter key.

Example response

```
Enter the secondary CS2KSS mtc server http port
(default is 12121):
```

**18** Accept the current value by pressing the Enter key.

Example response

```
Enter the OMI administrator user name (default:
admin):
```

- 19** Enter the OMI administrator user name and press the Enter key.  
The OMI administrator user name and password must match the MCP provisioning manager user name and password.

Example response

Enter the OMI administrator password:

- 20** Enter the OMI administrator password and press the Enter key.  
Example response

Re-enter the OMI administrator password:

- 21** Enter the OMI administrator password again and press the Enter key.

Example response

OPI - Provisioning Manager configuration

```
Transport protocol to EM server :
https://
Primary CS2KSS Provisioning Manager IP / Name
: 47.142.128.36
Primary CS2KSS Provisioning Manager port
: 8443
Secondary CS2KSS Provisioning Manager IP / Name
: 47.142.128.36
Secondary CS2KSS Provisioning Manager port
: 8443
The administrator user name :
admin
```

OMI - Maintenance Manager configuration

```
Transport protocol to Maintenance Manager
: https://
Primary CS2KSS Maintenance Manager IP / Name
: 47.142.128.36
Primary CS2KSS Maintenance Manager port :
12121
Secondary CS2KSS Maintenance Manager IP / Name
: 47.142.128.36
Secondary CS2KSS Maintenance Manager port
: 12121
The administrator user name :
admin

Is the information correct? (y or n) :
```



- 22 Confirm that the information is correct by typing  
**y**  
and pressing the Enter key.
- 23 Exit the CLUI by typing  
**x**  
repeatedly until you return to the command prompt.
- 24 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

## Cleaning up old data in the NPM database

---

### Application

Use this procedure to clean up the old data in the Network Patch Manager (NPM) database following an upgrade.

#### ATTENTION

This procedure includes stopping and starting the NPM, which has the NPM rediscover the patches on the system when the NPM is brought back into service. This can take several hours depending on office configuration. Therefore, ensure patching tasks are not planned or scheduled in the timeframe you want to perform this procedure.

#### ATTENTION

The createdb command used in this procedure purges any user-defined reports, tasks, sets, plans and alarms, disables any enabled plans such as SYSTEMPLAN, GENREPORT and GETPATCH, releases any patches or devices on hold, and unconfigures the Patch File Receipt System (PFRS). Therefore, you will need to restore these using the database file archived from the old NPM database or manually via the NPM GUI or CLUI.

### Prerequisites

This procedure has the following prerequisites

- You must have root user privileges to perform this procedure.
- You will need to retrieve and place the old\_npm\_db.tar file in the /data/npm directory. This file was created in the procedure [Archiving the NPM database into a file on page 383](#).

## Action

Perform the following steps to complete this procedure.

### *At your workstation*

- 1 Generate and save a patchlist report using the NPM CLUI or GUI.

**Note:** The patchlist report will be useful in the event that the apply time information is required at a later time.

| If you want to use the | Do                      |
|------------------------|-------------------------|
| CLUI                   | <a href="#">step 2</a>  |
| GUI                    | <a href="#">step 14</a> |

- 2 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 3 Change directory to /data/npm by typing

```
cd /data/npm
```

and pressing the Enter key.

- 4 Determine if a tmp directory exists in the npm directory by typing

```
ls -l
```

and pressing the Enter key.

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

| If                     | Do                     |
|------------------------|------------------------|
| a tmp directory exists | <a href="#">step 7</a> |
| otherwise              | <a href="#">step 6</a> |

- 6 Create a tmp directory by typing

```
mkdir tmp
```

and pressing the Enter key.

- 7 Change directory to the tmp directory by typing  
`# cd tmp`  
and pressing the Enter key.
- 8 Generate the patchlist report by typing  
`# npm q patchlist output <filename>.list`  
and pressing the Enter key.  
where  
**filename**  
is the name you want to give to the patchlist report

**Example**`npm q patchlist output aug032004.list`**Example response**

Enter the NPM Succession user id and password.  
Login

- 9 When prompted, enter the NPM user ID.

**Example response**

password

- 10 When prompted, enter the NPM user password.

**Example response**

Redirecting output to: aug032004.list  
System retrieved...  
patchid, category, hold, spapp, stattime,  
status, deviceid  
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03  
08:21:09.540, VA, NCOS8\_1\_7\_OC3\_0\_1\_10  
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02  
14:35:34.538, A, NCOS8\_1\_7\_OC3\_0\_1\_11  
Redirecting output to standard I/O

- 11 Display the file by typing

`# ls`

and pressing the Enter key.

**Example response**

aug032004.list  
local.login  
local.cshrc  
local.profile

- 12 If required, display the contents of the file by typing

```
cat <filename> |more
```

and pressing the Enter key.

where

**filename**

is the name you gave to the patchlist report file

**Example**

```
cat aug032004.list
```

Example response

```
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
```

- 13 Proceed to [step 25](#).

- 14 Access the NPM GUI.

For detailed steps, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

### ***At the NPM GUI***

- 15 On the Tasks menu, click **Reports....**

- 16 Click the **Report List** tab to display the list of defined reports.

- 17 Click on **PATCHLIST**, and then click **Execute** to generate the PATCHLIST report.

The Reports Results window is displayed.

- 18 Click **Save** to save the results of the PATCHLIST report and specify the filename and location to save the report.

The Save window is displayed.

- 19 Enter a name for the saved report in the File name field and then click **Save**.

- 20 Click **Close** to close the Reports Results window.

- 21 Click **Close** to close the Reports window.

- 22 On the Edit menu, Click **Preferences**.

- 23 Click on the **System Preferences** tab.

Copy and paste the data on display including that in the Delete Patches from the Drop Box after Retrieval checkbox.

### ***At your workstation***

- 24** Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure [Logging in to an SPFS-based server on page 323](#).

- 25** Stop the NPM server application by typing
- ```
# servstop NPM
```
- and pressing the Enter key.
- 26** Access the command line interface by typing
- ```
cli
```
- and pressing the Enter key.
- 27** Enter the number next to the “Configuration” option in the menu.
- 28** Enter the number next to the “Succession Element Configuration” option in the menu.
- 29** Enter the number next to the “NPM Application Configuration” option in the menu.
- 30** Enter the number next to the “CreateDB” option in the menu. Allow to complete.
- 31** Exit each menu level of the command line interface to eventually return to the root level by typing
- ```
select - x
```
- and pressing the Enter key.
- 32** Use the following table to determine your next step.
- | If | Do |
|---|-------------------------|
| the old.npm.db.tar file is in the directory /data/npm | step 33 |
| otherwise | step 36 |
- 33** Restore the NPM db using the file created in [Archiving the NPM database into a file on page 383](#) by typing
- ```
cd /data/npm
```

and pressing the Enter key.

```
tar -xvf old_npm_db.tar
```

and pressing the Enter key.

- 34** Start the NPM server application by typing

```
servstart NPM
```

and pressing the Enter key.

- 35** Go to step [41](#).

- 36** Start the NPM server application by typing

```
servstart NPM
```

and pressing the Enter key.

- 37** If any user-defined reports, tasks, sets, plans, or alarms existed prior to this procedure, redefine them using the corresponding procedure.

- for reports, use procedure [Defining NPM patching reports on page 2393](#)
- for tasks, use procedure [Defining NPM patching tasks on page 2382](#)
- for sets, use procedure [Defining NPM patching sets on page 2374](#)
- for plans, use procedure [Defining NPM patching plans on page 2401](#)
- for alarms, use procedure “Defining alarms using the NPM” in document *ATM/IP Fault Management*, NN10408-900.

- 38** If any patches or devices were on hold prior to this procedure, place them back on hold using procedure [Setting field values using the NPM on page 2388](#).

- 39** If any plans such as SYSTEMPLAN, GENREPORT and GETPATCH, were enabled prior to this procedure, re-enable them using procedure [Modifying NPM patching plans on page 2409](#).

- 40** If PFRS was configured prior to this procedure, re-configure it using procedure [Configuring NPM for automatic patch file delivery on page 493](#).

**Note:** If any users were logged in to the NPM GUI prior to this procedure, they must exit and launch the GUI again. A reconnect to the NPM server from the GUI is not sufficient to clean up old data showing up in the GUI.

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



## Performing a rollback of Session Server Trunks software

Complete the steps for the following activity, in the order indicated, to roll back an upgrade activity that has been performed on both units in the node.

**CAUTION****Service interruption**

This is a service affecting activity. Performing this rollback activity causes approximately an hour-long service interruption to all SIP-related call traffic and billing activity.

**CAUTION****Possible loss of customer data**

Ensure that you have a recent backup copy of the SIP Gateway application database available. If a backup version of the database is not available, the first unit to be rolled back must be recommissioned and the SIP Gateway application reprovisioned.

Complete the steps for the following activity:

**Perform a rollback activity**

| Step | Procedure or activity                                                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <p>Locate and have available the DVD-ROM or an ESD downloaded image file of the previous release.</p> <p>Ensure that you have available a recent backup copy of the SIP Gateway application database for the software version rolling back to.</p>                                 |
| 2    | <p>If performing the rollback using an ISO image acquired using ESD, verify that the applicable ISO files are copied to the hard drive of each unit. If necessary, use procedure <a href="#">Extract an ISO image from an Electronic Software Delivery (ESD) on page 1134</a>.</p> |

**Perform a rollback activity**

| Step                                                                | Procedure or activity                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rollback NCGL, reboot, and rollback the application software</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 3                                                                   | Jam the inactive unit.                                                                                                                                                                                                                                                                                                                                                                                                         |
| 4                                                                   | <p>At the active unit CLI complete procedure <a href="#">Drop database synchronization for the SIP Gateway application on page 2464</a>.</p> <p><b>Note:</b> Once executed, this script drops call processing and application database synchronization between the active and inactive units. The SIP Gateway application maintains this non-synchronized state until a manual SwAct is performed, later in the procedure.</p> |
| 5                                                                   | <p>Set the default NCGL bootfile to the load that was running prior to the upgrade. Refer to procedure <a href="#">Rollback an NCGL platform software upgrade on page 2462</a>.</p> <p><b>Note:</b> All applied and committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying and committing patches is not required.</p>                                    |
| 6                                                                   | From the active unit, use procedure <a href="#">Reboot a unit on page 1151</a> to perform a RebootMate of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.                                                                                                                                                                                                                       |
| 7                                                                   | At the inactive unit, roll back the SIP Gateway application software. Complete procedures <a href="#">Upgrade/rollback/reinstall a Session Server - Trunks application on page 1196</a> .                                                                                                                                                                                                                                      |
| 8                                                                   | From the active unit, use procedure <a href="#">Reboot a unit on page 1151</a> to perform a RebootMate of the inactive unit. Monitor the reboot progress from the active unit of the CS 2000 NCGL Platform Manager.                                                                                                                                                                                                            |
| 9                                                                   | If the security certificates were modified, restore the original security certificates from a backup directory using procedure <a href="#">Manual restore of security related files on page 2491</a> . This procedure must be performed on both units.                                                                                                                                                                         |

**Perform a rollback activity**

| Step                                 | Procedure or activity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SwAct to the rolled back unit</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 10                                   | UnJam the inactive unit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 11                                   | Perform a SwAct (Force) of the units by completing procedure <a href="#">Invoke a maintenance SWACT of the Session Server Trunks platform on page 1219</a> , to make the downgraded unit active.                                                                                                                                                                                                                                                                                                                                                         |
| <b>Restore the backup database</b>   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 12                                   | <p>On the newly active, rolled back unit, restore a backup copy of the SIP Gateway application database.</p> <p>If rolling back to an SN08, refer to <a href="#">Restore as part of rollback or abort to SN08 on page 2482</a></p> <p>If rolling back to an SN09 load, refer to <a href="#">Session Server - Trunks restore on page 2485</a>.</p> <p><b>Attention:</b> If a backup version of the database for the software version rolling back to is not available, the unit must be recommissioned and the SIP Gateway application reprovisioned.</p> |
| 13                                   | <p>Restart the SIP Gateway application by locking, suspending, unsuspending, and unlocking the application. Refer to the following for assistance:</p> <ul style="list-style-type: none"> <li>• <a href="#">Lock the SIP Gateway application on page 2465</a></li> <li>• <a href="#">Suspend the SIP Gateway application on page 2468</a></li> <li>• <a href="#">Unsuspend the SIP Gateway application on page 2476</a></li> <li>• <a href="#">Unlock the SIP Gateway application on page 2479</a></li> </ul>                                            |
| 14                                   | <p>As applicable to your site, test the software on the downgraded unit, now active. Testing includes:</p> <ul style="list-style-type: none"> <li>• placing test calls according to your site upgrade guidelines</li> <li>• applying a minimum live traffic soak time for the unit according to your site upgrade guidelines</li> <li>• monitoring logs and alarms. Clear all alarms and verify normal functioning of both units before continuing.</li> </ul>                                                                                           |

**Perform a rollback activity**

| Step                                                                  | Procedure or activity                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15                                                                    | <p>Monitor the system for an appropriate period according to your site guidelines.</p> <p>If all software tests are successful, continue with the next step in this activity.</p> <p>Otherwise, if the active unit (with rolled back load) experiences problems with call processing, stop executing this activity and contact your next level of support or Nortel GNPS.</p> |
| <b>Rollback NCGL, reboot, and rollback application on second unit</b> |                                                                                                                                                                                                                                                                                                                                                                               |
| 16                                                                    | Use procedure <a href="#">Inhibit a system SwAct (Jam) on page 1141</a> to jam the inactive unit.                                                                                                                                                                                                                                                                             |
| 17                                                                    | For the newly inactive unit, set the default NCGL bootfile to the load the unit was running prior to the upgrade. Refer to procedure <a href="#">Rollback an NCGL platform software upgrade on page 2462</a> .                                                                                                                                                                |
| 18                                                                    | From the active unit, use procedure <a href="#">Reboot a unit on page 1151</a> to perform a RebootMate of the inactive unit.                                                                                                                                                                                                                                                  |
| 19                                                                    | On the inactive unit, rollback the SIP Gateway application software using procedure <a href="#">Upgrade/rollback/reinstall a Session Server - Trunks application on page 1196</a> .                                                                                                                                                                                           |
| 20                                                                    | From the active unit, use procedure <a href="#">Reboot a unit on page 1151</a> to perform a RebootMate of the inactive unit. Monitor the reboot progress from the active unit of the CS 2000 NCGL Platform Manager.                                                                                                                                                           |
| 21                                                                    | <p>After the inactive unit reboots, go to the active unit. Verify that the SIP Gateway application databases are synchronizing using procedure <a href="#">Verify synchronization status on page 1215</a>.</p> <p>If they are synchronizing then go to step <a href="#">23</a>.</p> <p>If they are not synchronizing then go to the next step in this activity.</p>           |

**Perform a rollback activity**

| Step                                                             | Procedure or activity                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Monitor logs and alarms, verify synchronization completes</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>22</b>                                                        | <p>Use procedure <a href="#">View the operational status of the NCGL platform on page 1172</a> to check the status of the inactive unit to determine why database synchronization is not taking place by reviewing existing faults and logs.</p> <p>Monitor logs and alarms. Refer to <i>Session Server - Trunks Fault Management</i>, NN10332-911 for assistance. Clear all alarms and verify normal functioning of both units before continuing.</p> |
| <b>23</b>                                                        | <p>Once the databases are in sync, unjam the inactive unit using procedure <a href="#">Enable a system SwAct (Unjam) on page 1217</a>.</p>                                                                                                                                                                                                                                                                                                             |
| <b>24</b>                                                        | <p>Perform a SwAct of the units by completing procedure <a href="#">Invoke a maintenance SWACT of the Session Server Trunks platform on page 1219</a>, to make the downgraded unit active.</p>                                                                                                                                                                                                                                                         |
| <b>25</b>                                                        | <p>Monitor the system for an appropriate period according to your site guidelines before declaring this rollback activity complete.</p> <p>If all software tests are successful, continue with the next step in this activity.</p> <p>Otherwise, if you continue to experience problems with call processing, contact your next level of support or Nortel GNPS.</p>                                                                                   |
| <b>26</b>                                                        | <p>You have completed this rollback activity. If applicable, return to the higher level task flow or procedure that directed you to this procedure.</p>                                                                                                                                                                                                                                                                                                |

## Abort an upgrade

### ATTENTION

This high-level activity assumes that you have not upgraded the second unit in the node. If you have already upgraded both units, then contact your next level of support or Nortel GNPS.

Complete the steps for the following activity, in the order indicated, to abort a upgrade activity in progress.

### Abort an upgrade activity

| Step | Procedure or activity                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Complete procedure <a href="#">Invoke a maintenance SWACT of the Session Server Trunks platform on page 1219</a> to revert call processing to the non-upgraded unit (the unit that is operating with the previous release load).                                                                                                                                                                                                                          |
| 2    | Use procedure <a href="#">Inhibit a system SwAct (Jam) on page 1141</a> to jam the units.                                                                                                                                                                                                                                                                                                                                                                 |
| 3    | Log on to the inactive unit and use procedure <a href="#">Rollback an NCGL platform software upgrade on page 2462</a> to set the default NCGL bootfile to the previous load the unit was running.                                                                                                                                                                                                                                                         |
| 4    | At the active unit, use the CS 2000 NCGL Platform Manager and go to the NCGL Administration page. Perform a FORCED reboot (RebootMate) of the inactive (mate) unit. Refer to procedure <a href="#">Reboot a unit on page 1151</a> for assistance.<br><br><b>Note:</b> All applied and committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying and committing patches is not required. |
| 5    | On the inactive unit CLI, use the DVD-ROM or ISO image from the latest maintenance release of the previous release to downgrade the SIP Gateway application software using procedure <a href="#">Upgrade/rollback/reinstall a Session Server - Trunks application on page 1196</a> .                                                                                                                                                                      |

**Abort an upgrade activity**

| Step | Procedure or activity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6    | After the inactive unit reboots, go to the active unit and verify that the SIP Gateway application databases on both units have synchronized using procedure <a href="#">Verify synchronization status on page 1215</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 7    | Once the databases are in-sync, Unjam the inactive unit using procedure <a href="#">Enable a system SwAct (Unjam) on page 1217</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 8    | Complete procedure <a href="#">Invoke a maintenance SWACT of the Session Server Trunks platform on page 1219</a> to make the downgraded unit active.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 9    | As applicable to your site, test the software on the downgraded unit, now active. Testing includes: <ul style="list-style-type: none"><li>• placing test calls according to your site upgrade guidelines</li><li>• applying a minimum live traffic soak time for the unit according to your site upgrade guidelines</li><li>• monitoring logs and alarms. Clear all alarms and verify normal functioning of both units before continuing.</li></ul>                                                                                                                                                                                                                                                  |
| 10   | <p>Monitor the system for an appropriate period according to your site guidelines before declaring this abort activity a success.</p> <p>If all software tests are successful, continue with the next step in this activity.</p> <p>Otherwise, if the active unit (with downgraded load) experiences problems with call processing, perform the following tasks in order:</p> <ul style="list-style-type: none"><li>• complete procedure <a href="#">Invoke a maintenance SWACT of the Session Server Trunks platform on page 1219</a></li><li>• complete procedure <a href="#">Inhibit a system SwAct (Jam) on page 1141</a></li><li>• contact your next level of support or Nortel GNPS.</li></ul> |
| 11   | You have completed this abort activity. If applicable, return to the higher level task flow or procedure that directed you to this procedure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

---

## Patching the NCGL operating system and installed applications

---

Platform and application patching activities occur when new patches become available that must be installed. Any application or NCGL operating system software not delivered in a standard release or a maintenance release is delivered in a patch file. Patching can also occur when an older patch becomes obsolete and must be removed. Installing some patches may be optional.

A patch is a single file that contains the executables, libraries, data, scripts, dependency information and special instructions necessary to apply and remove the patch. Patching commands, run from the root account, are used to install and uninstall patches. Any patch can be applied on the inactive unit without impact to active call processing. Consult the patch release notes or administrative file for details.

### Patching SIP Gateway application versus patching NCGL

The criteria and methodologies used for patching applications is similar to patching NCGL but the commands and procedures for applying NCGL patches and application patches are different. Patching the NCGL and application cannot occur simultaneously.

### Patching strategy

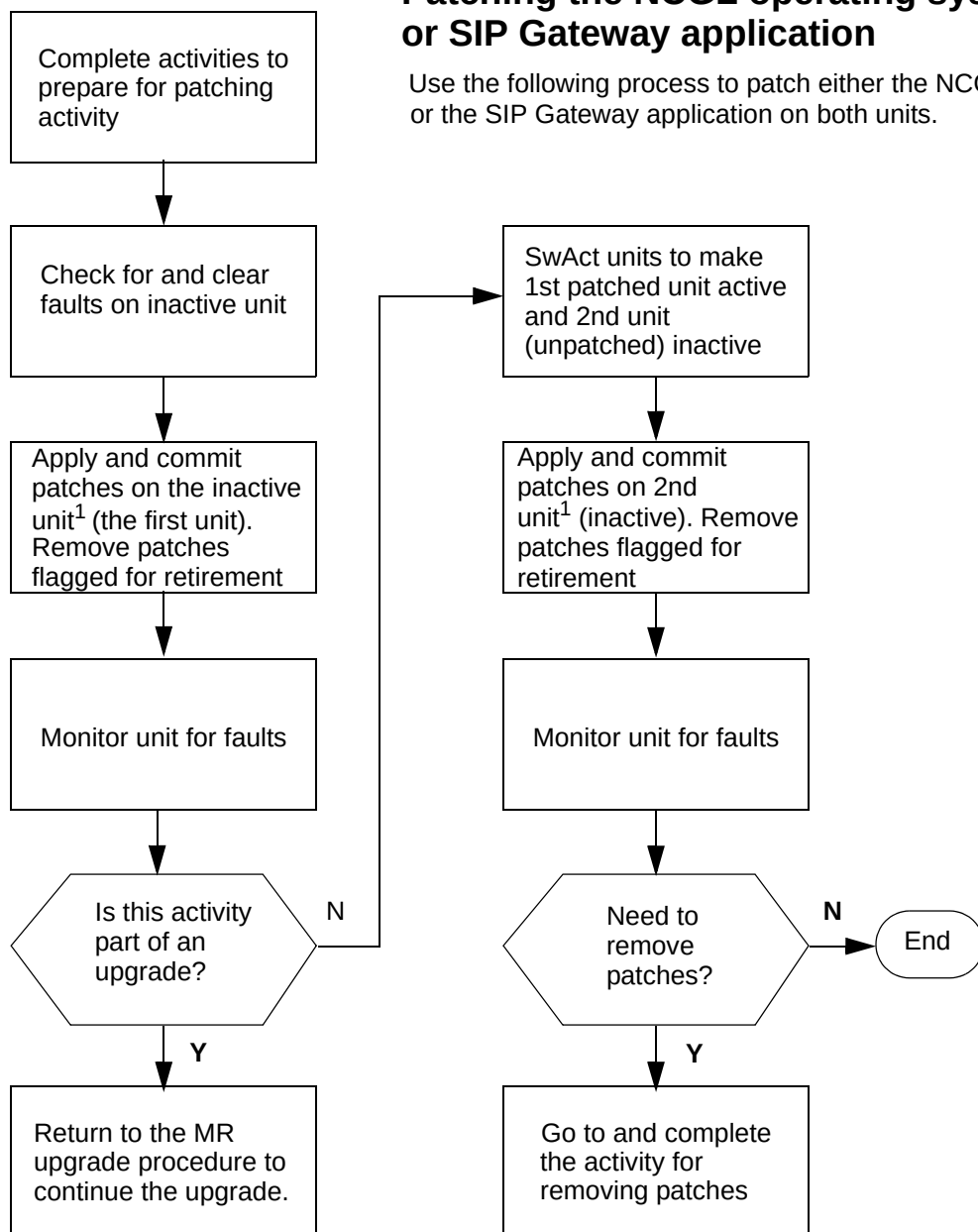
Although most patch files apply to any Nortel customer site, some patch files are created for a particular customer's site-specific installation. Not all patches made available apply to all customer sites. Contact Nortel GNPS customer support if you are concerned about which patches are applicable to your site.

Both units in the Session Server Trunks node must be patched when applying either application or NCGL patches. Each unit is usually patched separately while it is operating in standby mode. When patching the units, apply and commit the patch to the inactive unit first, then check logs and system status before SwActing the units. Check the logs and status for some period of time to ensure there are no patch-related events. After a time designated by your site guidelines, apply and commit the patch the newly inactive (unpatched) unit and check for logs and system status again. Refer to the following activity diagram for a high level view of the patching process.



## Patching the NCGL operating system or SIP Gateway application

Use the following process to patch either the NCGL or the SIP Gateway application on both units.



<sup>1</sup>In some cases, SIP Gateway application patches can or must be applied directly to the active unit and a SwAct may not be necessary. Consult the patch release notes for details.

## Patching limitations

Patches can only be applied using the CLI (command line interface).

## Delivery methods for patch files

Patch files can be released at any time. They can also be made available with a major upgrade or during a maintenance release. Patch files can be acquired in the following ways:

- self administration - <http://www.nortel.com> website by accessing the Technical Support portal and selecting Software Downloads. Search under the Carrier VoIP product family for Next Generation Session Server
- CD-ROM - sent to the customer site for initial installations
- Regional Patch Selector (RPS) - a service where Nortel delivers patches to a customer-based interface server that is accessible from the internet. The patch files are transferred from the customer-based interface server to the Session Server Trunks units by the customer network administrator or other trained personnel.

## Locating existing patch files on the units

NCGL patch files are stored in the /patching/patchholding directory on each unit that is to be patched.

Application patch files are stored in a patch directory under the /opt/swd/incoming directory or /opt/swd/storage, on each unit that is to be patched.

## Preparing for NCGL or application patching activities

### Purpose of this procedure

Use this procedure to prepare for standalone NCGL or application patching activities, outside of any upgrade activity:

### Action

#### Preparing for NCGL patching

- 1 If you are applying patches while performing a maintenance release upgrade, then skip this step.  
Backup the SIP Gateway application database on active unit using procedure [Perform a backup on page 1128](#).
- 2 Acquire patch files from Nortel either using ESD delivery or from a patch or maintenance release DVD-ROM disk.
- 3 Use procedure [View release notes for a release on page 1132](#) to check release notes to identify the required NCGL patches for your load. Also note any patches that are retired and must be removed. Verify if any previously installed patches must first be removed before installing new patches.
- 4 Perform [Acquire patch files on page 1189](#). Store NCGL patch files in /patching/patchholding.
- 5 Complete procedure [Query status of NCGL patches on page 2461](#) to ensure that the NCGL patch files being added or removed from the unit have been copied to the unit's hard drive.
- 6 Obtain SIP Gateway application patches using procedure [Acquiring Session Server Trunks patch files on page 1202](#).
- 7 Refer to *Session Server Trunks Fault Management*, NN10332-911, and use procedures "View Session Server alarms" and "View Session Server logs" to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
- 8 You have completed this activity. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Applying and committing NCGL patches

### Purpose of this procedure

Use the following procedure to patch both of the Session Server units.

This high level activity can be part of a high level maintenance release upgrade activity.

### Action

#### Applying NCGL patches

- 1 Ensure that you have first completed section [Preparing for NCGL or application patching activities on page 2454](#).
- 2 Use procedure [Inhibit a system SwAct \(Jam\) on page 1141](#) to jam the units.
- 3 Complete procedure [Apply and commit an NCGL patch on page 1191](#) on the inactive unit.
- 4 Refer to the *Session Server Trunks Fault Management*, NN10332-911, and use procedures “View Session Server alarms” and “View Session Server logs” to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
- 5 If performing patching as part of an upgrade activity, return to the procedure now.  
  
If this is a patching only activity, continue with the next step in this activity.
- 6 Unjam the inactive unit using procedure [Enable a system SwAct \(Unjam\) on page 1217](#).
- 7 Complete procedure [Invoke a maintenance SWACT of the Session Server Trunks platform on page 1219](#).
- 8 Use procedure [Inhibit a system SwAct \(Jam\) on page 1141](#) to jam the units.
- 9 Repeat procedure [Apply and commit an NCGL patch on page 1191](#) for the second (mate) unit, now the new standby unit.
- 10 Unjam the inactive unit using procedure [Enable a system SwAct \(Unjam\) on page 1217](#).
- 11 Monitor logs and alarms. Clear all alarms and verify normal functioning of both units before continuing.

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

## Removing NCGL patches

### Purpose of this procedure

#### ATTENTION

Under normal operating conditions patches must be removed from both units. Exceptions to this case are when a patch is being tested on a single unit before being committed and installed on the second unit.

Use the following procedure to remove patches from one or both units:

### Action

#### Removing NCGL patches

- 1 Use procedure [Inhibit a system SwAct \(Jam\) on page 1141](#) to jam the units.
- 2 Complete procedure [Remove an NCGL patch on page 2459](#) on the inactive unit.
- 3 Monitor logs and alarms. Clear all alarms and verify normal functioning of both units before continuing.
- 4 Use procedure [Enable a system SwAct \(Unjam\) on page 1217](#) to unjam the units.
- 5 Complete procedure [Invoke a maintenance SWACT of the Session Server Trunks platform on page 1219](#).
- 6 Repeat procedure [Remove an NCGL patch on page 2459](#) for the second (mate) unit, now the new standby unit.
- 7 Monitor logs and alarms. Clear all alarms and verify normal functioning of both units before continuing.
- 8 You have completed this activity. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Removing a Session Server Trunks patch

### Purpose of this procedure

Use this procedure to remove an application patch from one or both Session Server mate units.

### Limitations and restrictions

Both Session Server mate units must be on a NGSS\_09.1 or later release load and that load must be the same in both mate units.

Removing a patch "deactivates" the software changes relating to the patch. However, if autopatching is utilized, the removed patch is a candidate patch to be reapplied during the next autopatch timeframe. If it is appropriate for the patch being removed to not be applied during the next autopatch timeframe, the `ngssdeletepatch` command must be used as outlined below to complete remove the patch from the Session Server.

### Prerequisites

The patch you intend to remove must be applied on the unit(s) in question. Also, the patch file associated with the patch to be removed must be in the `/opt/swd/storage` directory on the unit(s) where the patch is to be removed.

### Action

#### Removing a Session Server Trunks patch

- 1 Log into the active unit and become the root user.
- 2 Decide which unit(s) you wish to remove the patch from and enter the appropriate command as follows:
  - Remove from inactive unit only:  

```
/opt/swd/bin/ngsspatch remove inactive
<patchid.i386>
```
  - Remove from active unit only:  

```
/opt/swd/bin/ngsspatch remove active
<patchid.i386>
```
  - Remove from both active and inactive units:  

```
/opt/swd/bin/ngsspatch remove
inactive/active <patchid.i386>
```

**where**

<patchid.i386> is the name of the patch in the format:  
"session\_server\_i686-<release>.<week#>.<sub-release>  
-<patch#>.i386"

- 3 At this point, if the patch is not applied to either unit, if autopatching is activated, and if it is NOT desired for this patch to be reapplied during the next autopatching timeframe, the patch must be deleted from the Session Server patching system including the <patchid.i386.parcel> file currently in the /opt/swd/storage directory.

If desired, make a copy of the related <patchid.i386.parcel> patch file, copying it to any directory except /opt/swd/incoming or /opt/swd/storage.

Delete the patch by typing

```
/opt/swd/bin/ngssdeletepatch
<patchid.i386.parcel>
```

- 4 This procedure is complete.

---

## Remove an NCGL patch

---

### Purpose of this procedure

Use this procedure to remove patches from the inactive Session Server - Trunks unit.

### Restrictions and Limitations

**ATTENTION**

Remove NCGL patch files only from the inactive unit.

Patching activities must be completed on both units in the node.

### Prerequisites

Verify which patches are to be removed by referring to the patching or maintenance release notes.

### Action

***At the NCGL CLI or IEMS client***

- 1 Log on to the inactive unit and change to the root user.
- 2 Uncommit the patch:  

```
patch_ha -v <patch_version> -o Uncommit
```

where  
**patch\_version**  
is the name of the patch file to be uncommitted
- 3 Remove the patch files and replace them with the files that existed prior to the patch:  

```
patch_ha -v <patch_version> -o Remove
```



- 4 Delete the patch file:  
**patch\_ha -v <patch\_version> -o Delete**
- 5 If necessary, allow the unit to reboot or if requested, perform a reboot using procedure [Reboot a unit on page 1151](#). Otherwise go to the next step.
- 6 Monitor logs and alarms. If errors occur that are related to the patch removal activity, contact your next level of support.  
  
**Note:** Checking unit status entails different activities depending on the what type of software item has been patched and any special patch application requirements. For example, some software subsystem processes require a reboot before a pre-patched version can become active, whereas other subsystem processes restart once patch removal is complete.
- 7 Complete procedure [Invoke a maintenance SWACT of the Session Server Trunks platform on page 1219](#).
- 8 Repeat this procedure for the mate unit.
- 9 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Query status of NCGL patches

---

### Purpose of this procedure

Use this procedure to review the status of patch files and to ensure that a patching file has been installed on both units in the node.

### Restrictions and Limitations

There are no restrictions for performing this procedure.

### Prerequisites

Patch files must first be copied to the unit.

### Action

#### *At the NCGL CLI or IEMS client*

- 1 Log on to either unit and change to the root user.
- 2 Display patch status information:  
**patch\_ha -o QueryAll**  
or  
**patch\_ha -v <patch\_version> -o QueryPatch**  
*where*  
**patch\_version**  
is the name of the patch file to be queried in the format:  
<NCGL\_release\_number>.<week\_number>.<major\_version\_number>.<minor\_version\_number>
- 3 Repeat this procedure on the mate unit.
- 4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Rollback an NCGL platform software upgrade

### Purpose of this procedure

This procedure describes how to rollback an NCGL platform load.

### Limitations and Restrictions

You can only rollback to a previous load if it still exists on the unit disk drive. If not, you must reinstall the load onto the disk drive from DVD-ROM disk or ESD ISO image.

### Prerequisites

#### ATTENTION

This procedure assumes that you are experiencing problems with an upgrade on the first unit and that you have not upgraded the second unit in the node. If you have already upgraded both units with the and are having problems, then refer to section [Performing a rollback of Session Server Trunks software on page 2444](#).

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

- 1 Select Succession Communication Server 2000 NCGL Platform Manager from the launch point menu.

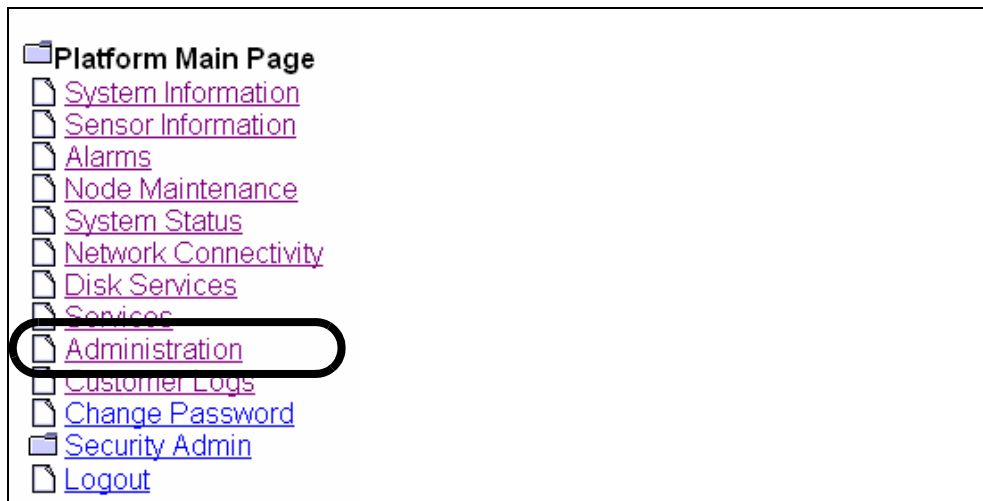
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

*The Platform Main Page menu is displayed.*

- 2 Click the Administration link.



- 3 Select the bootloader version to use and click Set default.

| Bootload Management |                    |        |
|---------------------|--------------------|--------|
| Bootload            | Maintenance        |        |
| 5.36.1.0.0409032059 | Default Bootload   |        |
| 5.26.1.0.0406231534 | <b>Set default</b> | Delete |

- 4 Verify that the default bootloader has been set to the version previous to the upgrade.

| Bootload Management        |                         |        |
|----------------------------|-------------------------|--------|
| Bootload                   | Maintenance             |        |
| 5.36.1.0.0409032059        | Set default             | Delete |
| <b>5.26.1.0.0406231534</b> | <b>Default Bootload</b> |        |

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Additional information

By default, previous bootloads remain stored on disk. For housekeeping purposes, older bootloader versions can be manually removed by clicking the Delete button.

## Drop database synchronization for the SIP Gateway application

### Purpose of this procedure

Use the following procedure to drop application database synchronization between the active and inactive units.

#### ATTENTION

Perform this procedure only as part of the high level activity [Performing a rollback of Session Server Trunks software on page 2444](#).

### Limitations and restrictions

Perform this procedure from the active unit only.

Once this procedure has been executed, the SIP Gateway application database continues in a non-synchronized state until a manual SwAct is performed.



#### CAUTION

##### Possible loss of customer data

Use care when using this procedure. This procedure can cause the loss of customer data.

### Prerequisites

Ensure that you have backed up the SIP Gateway application database on the active unit before executing this procedure.

### Action

#### *At the NCGL CLI or IEMS client*

- 1 Log in to the active unit and change to the root user.
- 2 Drop synchronization:  
`/opt/apps/NGSS_App_Mtc_Deliver/dropSync`
- 3 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Lock the SIP Gateway application

---

### Purpose of this procedure

Use the following procedure to change the administrative status of the SIP Gateway application to Locked.

### Limitations and restrictions

This procedure provides instructions for changing the service status of the SIP Gateway application software only. The NCGL operating status is not affected.

**CAUTION****Service interruption**

This is a service affecting procedure. Locking the SIP Gateway application releases all SIP calls in progress, regardless of call state, and causes an outage of all SIP media communications.

### Prerequisites

There are no prerequisites for this procedure.

### Action

***At the CS 2000 Session Server Manager or IEMS client***

- 1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select Session Server > Maintenance > Application > SIP Gateway.



- 3 In the SIP Gateway panel click the Lock button.

| Unit Number | Activity State | Operational State |
|-------------|----------------|-------------------|
| 0           | Active         | Enabled           |
| 1           | Inactive       | Enabled           |

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

*The system responds:*

This action will release all existing SIP calls and will cause a SERVICE OUTAGE on this Session Server. There are x active calls. Do you wish to continue?

- 4 Click OK to confirm locking the SIP Gateway application.
- 5 Monitor the status of the SIP Gateway application and ensure the Administrative State changes to Locked.

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| Locked               | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh

QueryInfo

**Note:** The status panel is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the Refresh Rate button. Otherwise, manually refresh the page by clicking on the Refresh button.

- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



---

## Suspend the SIP Gateway application

---

### Purpose of this procedure

Use the following procedure to temporarily take the SIP Gateway application out of service. This activity must be performed whenever selected SIP Gateway application provisioning changes are made and the application must be restarted for the changes to take effect.

**Note:** For more detailed information about SIP Gateway application services states and administrative functions, refer to “Interpreting SIP Gateway application states” in the *Session Server - Trunks Security and Administration*, NN10346-611.

### Limitations and restrictions

This procedure can only be performed when the SIP Gateway application is in the following service states:

- the Operational State is Enabled
- the Administrative State is Locked

### Prerequisites

The SIP Gateway application must previously have been locked. If it is not locked or you are uncertain of the state of the application, refer to procedure [Lock the SIP Gateway application on page 2465](#).

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

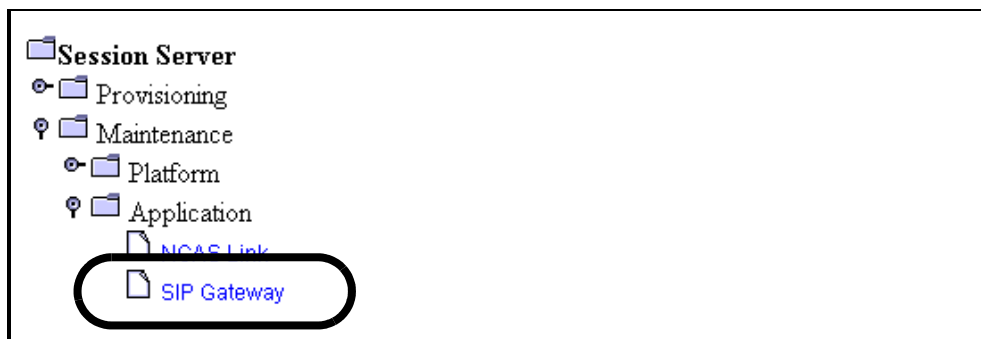
- 1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ❑ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ❑ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu:



- 3 In the SIP Gateway panel click Suspend.

| Session Server Status - Connected to Unit #0 |                |                   |  |
|----------------------------------------------|----------------|-------------------|--|
| Unit Number                                  | Activity State | Operational State |  |
| 0                                            | Active         | Enabled           |  |
| 1                                            | Inactive       | Enabled           |  |

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| Locked               | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

- 4 Monitor the status of the SIP Gateway application in the SIP Gateway Status box:
- the Operational State changes to Disabled
  - the Control Status changes to Suspended

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| Locked               | Disabled          | -                 | Suspended      |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh

QueryInfo

- 5 If applicable, restart the SIP Gateway application by executing procedures [Unsuspend the SIP Gateway application on page 2476](#) and [Unlock the SIP Gateway application on page 2479](#), in the order shown.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## View the operational status of the SIP Gateway application

### Purpose of this procedure

Use the following procedure to view the service status of the SIP Gateway application.

### Limitations and restrictions

This procedure provides instructions for determining the service status of the SIP Gateway application software only. For instructions on determining the status of the platform and operating system, refer to procedure [View the operational status of the NCGL platform on page 1172](#).

### Prerequisites

There are no prerequisites for this procedure.

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

- 1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu.



**3** Monitor the status of the SIP Gateway application from this view:

| Session Server Status - Connected to Unit #1 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Inactive       | Enabled           |
| 1                                            | Active         | Enabled           |

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

Refresh QueryInfo

Last Performed Operation: Refresh

Result: Passed

SIP Cold SwAct

This page updates automatically every 10 seconds!  
Last update: Thu Jun 10 13:04:20 EDT 2004

10 sec Refresh Rate

**Note:** This view is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the Refresh Rate button or manually refresh the page by clicking the Refresh button.

- 4 Refer to section [Interpreting SIP Gateway application status and maintenance fields on page 2474](#) to review the description of the various fields of this view.

**Note:** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section “Interpreting SIP Gateway application states” in *Session Server - Trunks Security and Administration*, NN10346-611.

- 5 The following service affecting actions are available:
- Lock the SIP Gateway application
  - Unlock the SIP Gateway application
  - Suspend the SIP Gateway application
  - Unsuspend the SIP Gateway application
  - Cold SwAct the SIP Gateway application
- 6 To view the number of active calls currently being handled by the application and the synchronization status of the units, click QueryInfo.

|                                                 |
|-------------------------------------------------|
| Last Performed Operation: Query Number of Calls |
| Result: Passed                                  |
| Number Of Active Calls: 0                       |
| SIP Gateway is: In Sync                         |
| SIP Gateway Cold SwAct                          |

- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Interpreting SIP Gateway application status and maintenance fields

Use the following table to assist you in interpreting information displayed in the Status area:

### Node status field descriptions

| Field                      | Description                                                                                                                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit Connection Status Bar | Indicates which unit in the node the CS 2000 Session Server Manager is connected to.                                                                                                                            |
| Unit Number                | Identifies the two units in the node, labeled 0 and 1.                                                                                                                                                          |
| Activity State             | Indicates which unit is Active and which is Inactive (standby). Also acts as an indirect indicator of fault-tolerant status; when both units have an Operational status of Enabled, the node is fault-tolerant. |
| Operational State          | Indicates the service status of each unit, Enabled or Disabled.                                                                                                                                                 |

Use the following table to assist you in interpreting information displayed in the SIP Gateway status area:

### SIP Gateway application Status field descriptions

| Field                | Indication                        |
|----------------------|-----------------------------------|
| Administrative State | Locked, Unlocked, or ShuttingDown |
| Operational State    | Enabled or Disabled               |
| Procedural Status    | Terminating or -                  |
| Control Status       | Suspended or -                    |

Use the following table to assist you in interpreting the SIP Gateway area's CCITT X.731-style and related DMS-style status indicators:

**SIP Gateway Maintenance field descriptions and interpretation of service states**

| Administrative State                              | Operational State | Procedural Status | Control Status | DMS style Service States          |
|---------------------------------------------------|-------------------|-------------------|----------------|-----------------------------------|
| Locked                                            | Disabled          | -                 | Suspended      | Offline (OFFL)                    |
| Locked                                            | Enabled           | -                 | -              | Manual Busy (MANB)                |
| Locked                                            | Enabled           | Terminating       | -              | Manual Busy Transitioning (MANBP) |
| Unlocked                                          | Enabled           | -                 | -              | In Service (INSV)                 |
| Unlocked                                          | Disabled          | -                 | -              | System Busy (SYSB)                |
| Shutting Down                                     | Enabled           | -                 | -              | Going out of service (INSVD)      |
| <b>Note:</b> (-) indicates a status of in-service |                   |                   |                |                                   |



---

## Unsuspend the SIP Gateway application

---

### Purpose of this procedure

Use the following procedure to bring the SIP Gateway application back into service without restarting callP activity.

**Note:** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section “Interpreting SIP Gateway application states” in *Session Server - Trunks Security and Administration*, NN10346-611.

### Limitations and restrictions

This procedure can only be performed when the SIP Gateway application is in the following service states:

- the Operational State is Disabled
- the Administrative State is Locked
- the Control Status is Suspended

### Prerequisites

The SIP Gateway application must previously have been suspended. If it is not suspended or you are uncertain of the state of the application, refer to procedure [Suspend the SIP Gateway application on page 2468](#).

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

- 1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

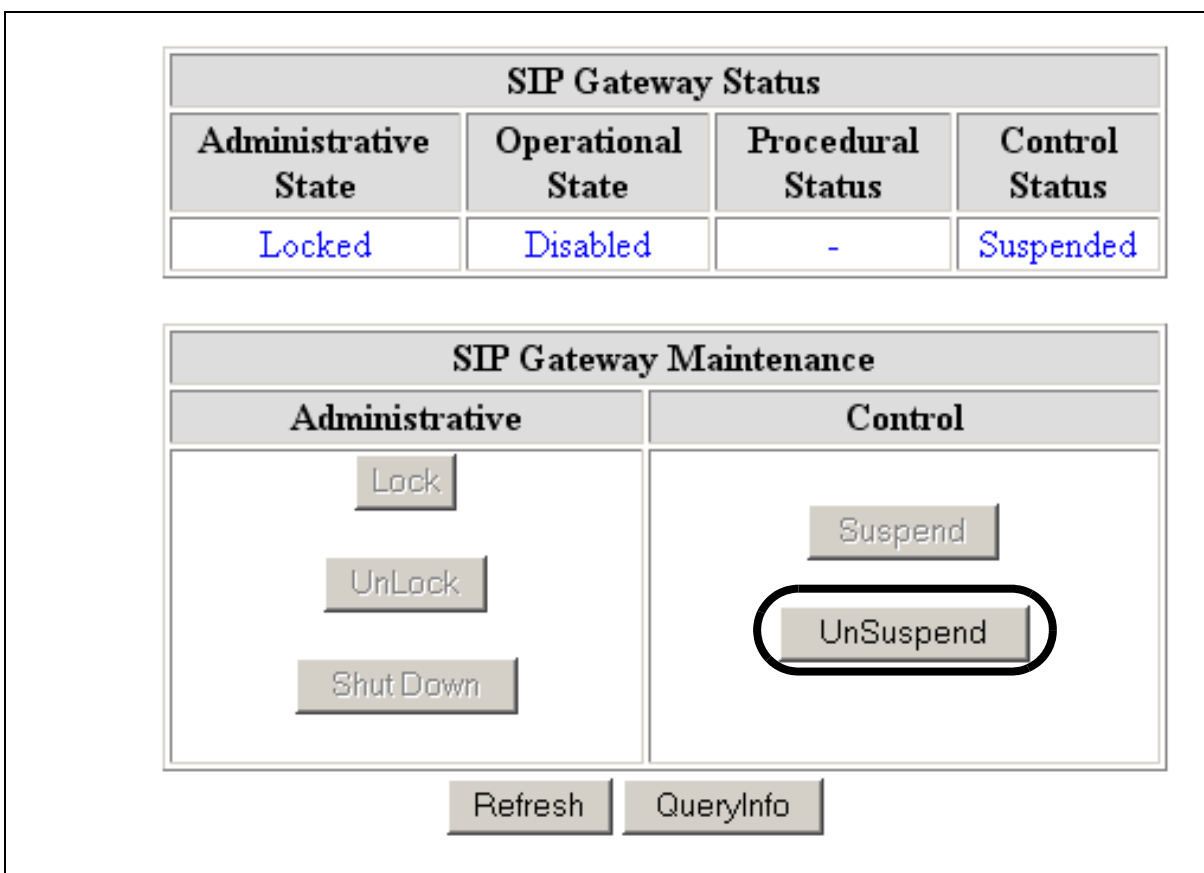
Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu:



- 3 In the SIP Gateway panel click Unsuspend.



- 4 Monitor the status of the SIP Gateway application in the SIP Gateway Status box:
- the Operational State changes to Enabled
  - the Control status changes to -

| Session Server Status - Connected to Unit #0 |                |                   |  |
|----------------------------------------------|----------------|-------------------|--|
| Unit Number                                  | Activity State | Operational State |  |
| 0                                            | Active         | Enabled           |  |
| 1                                            | Inactive       | Enabled           |  |

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| Locked               | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

- 5 If necessary, bring the SIP Gateway application back into service by executing procedure [Unlock the SIP Gateway application on page 2479](#).
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## Unlock the SIP Gateway application

---

### Purpose of this procedure

Use the following procedure to change the administrative status of the SIP Gateway application to Unlocked, bringing the application into service and enabling call processing to begin.

**Note:** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section of *Session Server - Trunks Security and Administration*, NN10346-611.

### Limitations and restrictions

This procedure provides instructions for changing the service status of the SIP Gateway application software only. For instructions on determining the status of the platform and operating system, refer to procedure [View the operational status of the NCGL platform on page 1172](#).

### Prerequisites

The active unit must be in a locked Administrative state. If it is not locked or you are uncertain of the state of the application, refer to procedure [Lock the SIP Gateway application on page 2465](#).

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

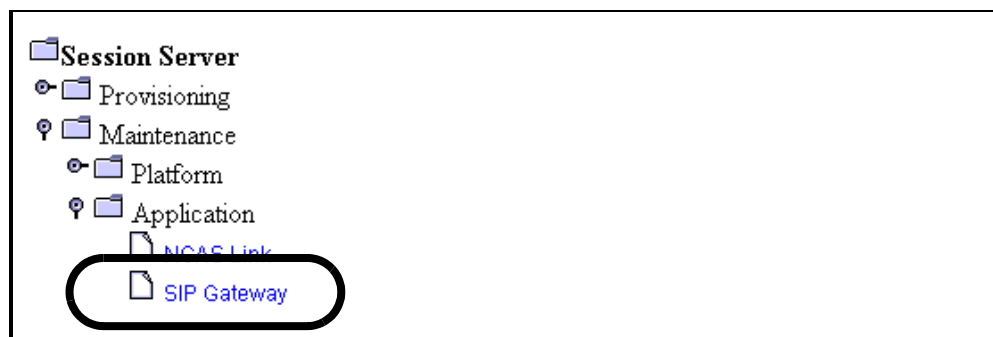
- 1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu:



- 3 In the SIP Gateway panel click Unlock.

| Session Server Status - Connected to Unit #0 |                |                   |  |
|----------------------------------------------|----------------|-------------------|--|
| Unit Number                                  | Activity State | Operational State |  |
| 0                                            | Active         | Enabled           |  |
| 1                                            | Inactive       | Enabled           |  |

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| Locked               | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

- 4 Monitor the status of the SIP Gateway application in the SIP Gateway Status box and ensure the Administrative State changes to Unlocked.

| Unit Number | Activity State | Operational State |
|-------------|----------------|-------------------|
| 0           | Active         | Enabled           |
| 1           | Inactive       | Enabled           |

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |

**Note:** The status panel is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the Refresh Rate button. Otherwise, manually refresh the page by clicking on the Refresh button.

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Restore as part of rollback or abort to SN08

If performing a rollback or abort from an SN09 maintenance release to another SN09 software load, refer to [Session Server - Trunks restore on page 2485](#) instead of this procedure.

### Purpose of this procedure

Use this procedure to restore the database files during a rollback or abort from SN09 to SN08.

### Limitations and Restrictions

**CAUTION****Loss of redundancy**

When performing this procedure the units are operating in simplex and are not fault-tolerant.

### Prerequisites

If the database backup to restore is located on a remote server, then secure copy (scp) access to that remote host is needed.

### Action

***From the remote server where the backup database file is located***

- 1 If the database file is stored on a remote server, then secure copy the database file to the unit:

```
scp solid.db mtc@<ip_address>:
```

where

**ip\_address**

is the IP address of the local unit

*The database file is copied to the /users/mtc directory on the target unit*

***At the NCGL CLI or IEMS client***

- 2 Log in to the unit you are restoring a backup copy of the database to, and change to the root user.
- 3 Move the solid.db file you copied in [step 1](#) from the /users/mtc directory to the /opt/apps/database/solid/backup directory:

```
cd /users/mtc
```

- ```
mv solid.db /opt/apps/database/solid/backup
```
- 4 Change directory to the backup database directory:
- ```
cd /opt/apps/database/solid/backup
```
- 5 Verify that the correct version (based on the file date) of the solid.db database file that you want to restore is located in the directory:
- ```
ls -l /opt/apps/database/solid/backup
```
- 6 Verify that the presence of files solid.ini and solmsg.out files are also in the /opt/apps/database/solid/backup directory.

ATTENTION

The restorebackup.sh script does not run if you do not have the solid.ini and solmsg.out files located in the correct directory.

- 7 If the solid.ini file is not present, copy it into the backup directory:
- ```
cp /opt/apps/database/solid/dbfiles/solid.ini /opt/apps/database/solid/backup/solid.ini
```
- 8 If the solmsg.out file is not present, copy it into the backup directory:
- ```
cp /opt/apps/database/solid/dbfiles/solmsg.out /opt/apps/database/solid/backup/solmsg.out
```
- 9 Change the ownership of all files in the backup directory:
- ```
chown soliddb *
```
- 10 Change the group of all files in the backup directory:
- ```
chgrp adm *
```
- 11 Change the access permissions for all files in the backup directory:
- ```
chmod 600 *
```
- 12 Execute the restore backup script:
- ```
cd /opt/apps/database/solid_install  
./restorebackup.sh
```
- Progress is printed to the terminal. When complete, the database is reverted to when the backup was made.*
- 13 Perform [Manual restore of security related files on page 2491](#).

- 14** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Session Server - Trunks restore

Purpose of this procedure

Use this procedure to restore a backup copy of critical files to a unit.

Limitations and Restrictions

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

Performing a restore of the SIP Gateway application database to the active unit is a service affecting activity and can cause data mismatches at the CS 2000.

Prerequisites

You must have secure file transfer access, such as scp, to the unit from a remote host if the backup file is stored on a remote host.

Backups are also stored locally on each unit in directory
/data/bkresmgr/backup.

Note: Both units must be free of any Session Server Manager patches before the database is restored. This is accomplished by reinstalling the current version of the SIP Gateway application software (performed in step [1](#) below). It is not necessary to remove NCGL patches.

Action

At the NCGL CLI or IEMS client

- 1 If either unit has Session Server Manager patches applied, reinstall the current application software on both units by performing the [Upgrade/rollback/reinstall a Session Server - Trunks application on page 1196](#).

Note: Do not re-apply any Session Server Manager patches after the reinstall.

From the remote server where the backup database file is located

- 2 If the backup is stored on a remote host, copy the backup file to the unit.

Note: Backup files are unit-specific. Ensure the backup file being copied from the remote host is the file that was originally created on the unit.

To use a secure copy, type

```
scp <backupfile> mtc@<ip_address>:<dest_dir>
```

where

backupfile

is a value like unit0.backupfile.2005-04-12_17-10.tgz and is identified by the hostname, date, and time that the backup occurred

ip_address

is the IP address of the unit

dest_dir

is the location to put the backupfile and is either blank to place it in /users/mtc, or a full path such as /data/bkresmgr/restore

The database file is copied to the target unit. If the local workstation is not on the CS LAN, copy the backup file to the server hosting the CS 2000 Management Tools first, and then transfer it between the server hosting the CS 2000 Management Tools and the Session Server - Trunks unit.

At the NCGL CLI or IEMS client

- 3 Log in to the unit and change to the root user.
- 4 If the backup file was not transferred directly to /data/bkresmgr/restore, then move the backup file:

```
mv /users/mtc/<backupfile>  
/data/bkresmgr/restore
```

Note: If restoring a local backup, the backup file is located in /data/bkresmgr/backup.

- 5 Change directory to the restore directory:

```
cd /data/bkresmgr/restore
```

- 6 Uncompress the backup:

```
tar xvzf <backupfile>.tgz
```

A listing of the files is printed to the screen and the files to restore are located in /data/bkresmgr/restore/data/bkresmgr/temp.

- 7 Change directory to the files:
`cd /data/bkresmgr/restore/data/bkresmgr/temp`
- 8 Repeat steps [2](#) through [7](#) on the mate unit.

Jam the inactive unit and suspend call processing

At the CS 2000 Session Server Manager or IEMS client

- 9 Select Session Server > Maintenance > Platform > Node Maintenance from the left side menu.
The Node Maintenance panel opens in the right side.
- 10 Click Jam.
Two Jlnact alarms are raised.
- 11 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu.
The SIP Gateway Maintenance page opens in the right side.
- 12 Click Lock.
- 13 Click Suspend.
- 14 Perform any of the following restore activities and then perform [Unsuspend call processing and Unjam the inactive unit on page 2491](#).
 - [Restore database on page 2487](#)
Note: Restore the database only on the active unit.
 - [Restore system data on page 2489](#)
 - [Restore web files on page 2490](#)
 - [Manual restore of security related files on page 2491](#) — these files are stored in a separate backup file, but restoring them as part of this procedure avoids an additional web server restart

Restore database

Perform these steps only if the database corruption has occurred on both units. The database must be restored on the active unit.

At the NCGL CLI or IEMS client

- 15** Copy the database files:

```
cp -i solid.db
/opt/apps/database/solid/backup/solid.db

cp -i solid.ini
/opt/apps/database/solid/backup/solid.ini

cp -i solmsg.out
/opt/apps/database/solid/backup/solmsg.out
```

- 16** Set the attributes for the files in the backup directory:

```
chown soliddb /opt/apps/database/solid/backup/*
chgrp adm /opt/apps/database/solid/backup/*
chmod 700 /opt/apps/database/solid/backup/*
```

- 17** Restore the backup files:

```
/opt/apps/database/solid_install/restorebackup
.sh
```

The following status is printed to the screen. The database on the inactive unit is synchronized to the restored database on the active unit.

```
Restoring database from backup
Stopping dbwatchdog.sh:          [ OK ]
Stopping soliddb.sh:            [ OK ]
Starting soliddb.sh:             [ OK ]
Solid SQL Editor (teletype) v.04.10.0139
(C) Copyright Solid Information Technology Ltd 1993-2004
Execute SQL statements terminated by a semicolon.
Exit by giving command: exit;
Connected to 'tcp 1315'.
admin command 'hsb set primary alone'
      RC TEXT
      -- ----
      0 HotStandby server set to PRIMARY ALONE.
1 rows fetched.

admin command 'hsb netcopy'
      RC TEXT
      -- ----
      0 Copy started.
1 rows fetched.

SOLID SQL Editor exiting.
Starting dbwatchdog.sh:          [ OK ]
```

- 18** If the database is the only item to restore, then unsuspend, unlock, and unjam the inactive unit. Refer to [Unsuspend call processing and Unjam the inactive unit on page 2491](#) for assistance.

Restore system data

At the NCGL CLI or IEMS client

- 19** Copy the necessary files:
- ```
cd /data/bkresmgr/restore/data/bkresmgr/temp
cp -i hosts /etc
cp -i passwd /etc
cp -i group /etc
cp -i ntp.conf /etc
cp -i shadow /etc
```

- ```
cp -i ifcfg-eth0 /etc/sysconfig/network-scripts
cp -i netnodes /etc/sysconfig
cp -i ssh_host_dsa_key.pub
/opt/base/synch_local/common/etc/ssh
cp -i ssh_host_key.pub
/opt/base/synch_local/common/etc/ssh
cp -i ssh_host_rsa_key.pub
/opt/base/synch_local/common/etc/ssh
```
- 20 Set the permissions on the restored files:
- ```
chmod 755 /etc/hosts
chmod 755 /etc/passwd
chmod 755 /etc/shadow
chmod 755 /etc/group
chmod 755 /etc/sysconfig/netnodes
chmod 755
/etc/sysconfig/network-scripts/ifcfg-eth0
chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_
key.pub
chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_
dsa_key.pub
chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_
rsa_key.pub
```
- 21 Repeat steps [19](#) through [20](#) on the mate unit.

## Restore web files

### *At the NCGL CLI or IEMS client*

- 22 Copy the files:
- ```
cd /data/bkresmgr/restore/data/bkresmgr/temp
cp -i redirect*.jsp
/opt/apps/webint/jakarta-tomcat-4.1.30/webapps
/<tag_name>/jsp
cp -i redirect_apps.php
/usr/local/apache/htdocs
```

- 23 Repeat step [22](#) on the mate unit.

Unsuspend call processing and Unjam the inactive unit

At the CS 2000 Session Server Manager or IEMS client

- 24 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu.
- 25 Click Unsuspend.
- 26 Click Unlock.
- 27 Select Session Server > Maintenance > Platform > Node Maintenance from the left side menu.
- 28 Click Unjam.
- 29 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Manual restore of security related files

Security related files are not stored in the automatically generated backup to guard against compromise of the keys in the event that a backup is stolen or misplaced.

Restored security files must be the same on both units of a node.

Locate the manual backup of security related files and restore the following files:

- /opt/base/share/ssl/certificate.keystore
- /opt/base/share/ssl/gen_cert.txt
- /opt/base/share/ssl/server.crt
- /opt/base/share/ssl/server.key
- /opt/base/share/ssl/trusted.crt

Note: If the unit is running SN09 software, optionally restore the files listed above to a location such as /users/mtc, and then use the cert_mgnt tool with option 3, Import certificates and private key, to restore the files to /opt/base/share/ssl and set the permissions correctly.

- /opt/base/synch_local/common/etc/ssh/ssh_host_dsa_key
- /opt/base/synch_local/common/etc/ssh/ssh_host_key
- /opt/base/synch_local/common/etc/ssh/ssh_host_rsa_key

At the NCGL CLI or IEMS

- 1 Become the root user.
- 2 Change directories to the location where the backup of the security certificates are stored:

```
cd /opt/base/share/ssl/<SNxx_ddmmyyyy>
```

where

SNxx_ddmmyyyy

is the name of the backup directory

Example

```
cd /opt/base/share/ssl/SN09_12102005
```

- 3 Verify the contents of the backup directory:

```
ls -l
```

Sample system response:

```
-rw-r--r--  1 root   root   1858 Dec 10 11:11
certificate.keystore

-rw-r--r--  1 root   root   190 Dec 10 11:11 gen_cert.txt

-rw-r--r--  1 root   root   3249 Dec 10 11:11 server.crt

-rw-----  1 root   root   887 Dec 10 11:11 server.key

-rw-r--r--  1 root   root   1254 Dec 10 11:11 trusted.crt
```

- 4 Determine your next step:

If	Do
the backup directory is empty or contains files other than those shown in the previous example	You are either in the wrong backup directory or you did not properly back up the security certificates. If necessary, contact Nortel GNPS for assistance. This procedure is complete.
the backup directory contains files similar to the display and the running software load is SN09	Run cert_mgnt and choose option 3. This restores the files and sets permissions correctly. This procedure is complete.
the backup directory contains files similar to the example shown in the previous step and the running software load is older than SN09	Continue to step 5 to copy the files and set permissions manually.

- 5 Copy the files to the /opt/base/share/ssl directory:

```
cp * /opt/base/share/ssl
```

ATTENTION

This step overwrites the current security certificates on this unit.

- 6 Change directories to the /opt/base/share/ssl directory:

```
cd /opt/base/share/ssl
```

- 7 Verify the contents of the backup directory were restored:

```
ls -l
```

Sample system response:

```
-rw-r--r-- 1 root root 1858 Dec 10 11:11  
certificate.keystore  
  
-rw-r--r-- 1 root root 190 Dec 10 11:11 gen_cert.txt  
  
-rw-r--r-- 1 root root 3249 Dec 10 11:11 server.crt  
  
-rw----- 1 root root 887 Dec 10 11:11 server.key  
  
-rw-r--r-- 1 root root 1254 Dec 10 11:11 trusted.crt
```

Note: File size values will vary.

- 8 Set the permissions for the restored files:

```
chown root:root *  
chmod 644 server.crt  
chmod 644 gen_cert.txt  
chmod 600 certificate.keystore  
chmod 600 server.key  
chmod 644 trusted.crt
```

- 9 Perform the steps in [Jam the inactive unit and suspend call processing on page 2487](#).

- 10 Enter the following commands to restart the applications that use the restored files:

```
/usr/local/apache/bin/apachectl restart  
/opt/apps/webint/tomcatd restart  
/etc/init.d/sshd restart
```

- 11 Perform the steps in [Unsuspend call processing and Unjam the inactive unit on page 2491](#)
- 12 Repeat this procedure on the mate unit.
- 13 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Downgrading the MG 9000 and MG 9000 Manager from SN09U to SN08 or SN09

When to use this procedure

When it is necessary to downgrade the MG 9000 and MG 9000 Manager from SN09U to SN08 or SN09, perform this downgrade procedure.

Before continuing, consider the following service impacts:

- Earlier releases of the MG 9000 Manager cannot run in tandem with the SN09 MG 9000 Manager.
- Before proceeding with downgrade, clear all alarms.
- If the customer wants to run an SN08 MG 9000 Manager (and thus not an SN09U MG 9000 Manager), both the SPFS and MG 9000 Manager must be at SN08. Different platform version of MG 9000 Manager and SPFS cannot be mixed.
- During a downgrade, the GWC cannot be downgraded until all MG 9000 network elements that subtend it are downgraded.
- If an MG 9000 has been placed within a Community of Interest (COI) to support Internodal ESA, and it is downgraded, an error message appears notifying the user that the downgrade cannot continue until the network element is removed from the COI.
- If NTNY53BA and NTNY53CA Global Line cards (GLC) have been installed in an SN09U MG 9000, any attempt to downgrade to SN08 or SN09 will render the NTNY53BA and NTNY53CA non-functional. The NTNY53BA and NTNY53CA GLC cards must be deprovisioned and removed before attempting the downgrade.

Prerequisites

If the SDM is newly installed, remove the SSH keys on all cards in the MG 9000(s) by performing the following:

- At the MG 9000 Manager, from the NE desktop view menu bar, select Services->Load Server SSH Authentication
- Enter the load server (SDM/CBM) IP address and click Apply.
 - If validation is successful, a dialog box appears with the following message: SSH validation is complete.
 - If validation fails because of an SSH key mismatch or the MG 9000 does not have keys cached for the server, a fingerprint icon appears with an Accept or Reject option.
 - If you click the Accept button, the MG 9000 distributes the new SSH keys to all the cards in the network element, and an SSH validation complete message appears when complete.
 - If you click the Reject button, the MG 9000 discards the new SSH keys. The existing SSH key cache is not changed. If an incorrect load server (SDM/CBM) IP address is provided, an SSH validation failed message appears.

Note 1: This SSH authentication (load server authentication) procedure is only required once on an MG 9000. Unless the SDM/CBM is newly installed, the procedure is NEVER required again, however it must be performed once.

Note 2: The load server authentication process must be performed before downgrading an SN09U MG 9000. If a downgrade is started without performing this load server authentication procedure, the upgrade will likely fail after a partial downgrade. For example, the downgrade could fail on the ABI cards, which are the final step of the downgrade.

Note 3: When the upgrade fails because of a non-authenticated load server, there is no way this issue can be resolved, apart from aborting the upgrade, upgrading the full node to SN09U, performing the authentication procedure, and then performing the downgrade again. This recovery process will take approximately 6 hours and the mg9kuptool cannot be used to perform the downgrade.

Action

Downgrading the MG 9000 from SN09U to SN09 or SN08

- 1 If the cards are currently on version SN09U, perform a downgrade on all the cards on the NE to go back to their SN08 or SN09 version using procedure [Upgrading the MG 9000 from SN08 or SN09 to SN09U using the mg9kuptool without options on page 1593](#). When using the mg9kuptool, select the SN08 or SN09 loads appropriate for each card when configuring the downgrade. Wait for the entire downgrade to complete before proceeding.
- 2 This procedure is complete. Proceed to procedure [Downgrading the t1400 or N240 simplex configuration MG 9000 Manager from SN09U to SN09 or SN08 on page 2498](#) or [Downgrading the N240 HA cluster configuration MG 9000 Manager from SN09U to SN09 or SN08 on page 2506](#).

Downgrading the t1400 or N240 simplex configuration MG 9000 Manager from SN09U to SN09 or SN08

At the MG 9000 Manager server

1

Note: Do not downgrade the MG 9000 Manager before the downgrade is complete of those MG 9000 network elements under the MG 9000 Manager's control.

Telnet to the MG 9000 Mid-tier server and log in as root.

2 Stop the MG 9000 Manager mid-tier application. To stop the application, type

```
> servstop MG9KMIDTIER
```

3 Record the existing configuration settings for the mid-tier server. To view these settings, type

```
> /opt/nortel/mg9kmtr_09_1/bin/mg9kconfig.sh
```

When prompted, enter Y to keep the existing settings and exit from the script.

4 To remove the mid-tier server SN09U software, type

```
> pkgrm NTmg9km91
```

To continue, respond to the two prompts with Y.

5 Telnet to the MG 9000 Manager master server and log in as root.

6 Stop the MG 9000 Manager server application. To stop the application, type

```
> servstop MG9KSERVER
```

7 Record the existing configuration settings for the master server. To view these settings, type

```
> /opt/nortel/mg9ksrv_09_1/bin/mg9kconfig.sh
```

When prompted, enter Y to keep the existing settings and exit from the script.

8 Drop the SN09U tablespace by typing

```
> /opt/nortel/mg9ksrv_09_1/bin/mgems_ora_ts_drop.sh <IP address of SESM>
```

- 9 Restore the SN09 (or SN08) tablespace data from the file that was saved during the SN09U upgrade process by typing

```
>/opt/nortel/mg9ksrv_09_1/bin/mgems_ora_ts_restore.sh -a <app_name> <data_db_file> <log_file> <ora_host>
```

where

<app_name>
is MG9KEM

<data_db_file>
is replaced with the dmp file generated in
/data/mg9kem/persistdata/tsBackup

<log_file>
is replaced with the log file generated in
/data/mg9kem/persistdata/tsBackup

<ora_host>
is the database IP address where you want to restore the database

Note: The tablespace data is written to
/data/mg9kem/persistdata/tsBackup.

- 10 To remove the master server SN09USN09U software, type

```
> pkgrm NTmg9ks91
```

To continue, respond to the prompt with Y.

- 11 Use the information in the following table before proceeding to the next step.

If the command SSPFS_Upgrade.accept has	Do
NOT been entered	step 12a
been entered	step 12b

- 12** Downgrade both the mid-tier server and the master server to the SN09 or SN08 SPFS platform.
- a** Execute the following command on the mid-tier and master server:


```
> /SSPFS_Upgrade.fallback
```

 Go to step [13](#).
 - b** On the mid-tier and server, follow the instructions in procedure “Performing a full system restore on an SSPFS-based server” in *Nortel ATM/IP Solution-level Fault Management*, NN10408-900.

- 13** At the workstation dedicated as the MG 9000 Manager master server, install the master server software using the following steps:

- a** Use the following table to determine the next step.

If the SN08 or SN09 MG 9000 Manager software load is delivered through	Do
CD	step 13b
ESD	step 13d

- b** Login as root (superuser) and insert the MG 9000 Manager software CD into the CD-ROM drive. This server is also running the OpenOrb NamingService.
- c** At the prompt (#), use pkgadd to install the server portion (NTmg9ks<release_number>.pkg) of the software. To directly install the software from the CD-ROM use the following commands to read the CD-ROM and list the contents to read the release number.

Insert the MG 9000 Manager software CD into the CD-ROM drive.

```
# cd /cdrom/cdrom0/
```

```
# ls
```

```
# pkgadd -d
/cdrom/cdrom0/NTmg9ks_<release_number>_xx_0.
pkg
```

where

release number is a value such as 08 or 09

The system responds with the following (in these examples, the responses are based on a downgrade to SN08):

The following packages are available:

```
1 NTmg9ks08      Succession MG 9000 Manager
                  Server(sparc) NTMG9KS_8_09_0
```

Select package (s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]:

Go to step [13e](#).

- d** At the prompt (#), use pkgadd to install the server portion (NTmg9ks<release_number>.pkg) of the software from ESD by typing

Note: For information on retrieving software from ESD, refer to procedure [Preparing MG 9000 Manager software delivered through ESD for an upgrade on page 1104](#).

```
# pkgadd -d
/opt/nortel/NTmg9ks_<release_number>_xx_0.pk
g
```

where

release number is a value such as 08 or 09

The system responds with the following (in these examples, the responses are based on a downgrade to SN08):

The following packages are available:

```
1 NTmg9ks08      Succession MG 9000 Manager
                  Server(sparc) NTMG9KS_8_09_0
```

Select package (s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]:

- e** Enter 1 and press return to begin the server installation process.

Note: If the following message appears, respond Y at the prompt:

```
The following files are already installed on
the system and are being used by another
package: /opt/nortel<attribute change only>
Do you want to install these conflicting
files [y,n,?,q]
```

After the installation is complete, a message appears reporting that the installation was successful.

Note: Verify the installation of <NTmg9ks08> was successful. If there are any errors, contact your next level of support.

- f If applicable, eject the CD-ROM by typing

```
# eject cdrom0
```

Note: This is not necessary if the mid-tier and master server reside on the same server.

- g To configure the master server, type

```
>
/opt/nortel/mg9ksrv_<release_number>/bin/mg9
kconfig.sh
```

where

release number is a value such as 08 or 09

If previous installation settings are detected, enter Y and accept the settings. Otherwise, follow the prompts to enter the settings. Use the data that was recorded in step [7](#).

- h To start the master server, enter the following command:

```
# servstart MG9KSERVER<_release_number>
```

where

release number is a value such as 08. Release number is not required for SN09)

Note: If messages appear indicating that a patch failed to stay up, these messages can be ignored.

- 14** At the workstation dedicated as the MG 9000 Manager mid-tier server, install the mid-tier server software by performing the following steps:

- a Use the following table to determine the next step.

If the SN08 or SN09 MG 9000 Manager software load is delivered through	Do
CD	step 14b
ESD	step 14d

- b Login as root (superuser).

- c At the prompt (#) use pkgadd to install the mid-tier portion (NTmg9km<release_number>.pkg) of the software. If you are directly installing from the CD-ROM use the following command to read the CD-ROM, and list the contents to read the release number:

Insert the MG 9000 Manager software CD into the CD-ROM drive.

```
# cd /cdrom/cdrom0/  
# ls  
# pkgadd -d  
/cdrom/cdrom0/NTmg9km_<release_number>_xx_0.  
pkg
```

where

xx is the release number such as 08 or 09.

The system responds with the following information. In these examples, the responses are based on a downgrade to SN08:

```
The following packages are available:  
1   NTmg9km08 Succession MG 9000 Manager  
Midtier Server (sparc) NTMG9KM_8_09_0
```

```
Select package(s) you wish to process (or  
'all' to process all packages). (default:  
all) [?,??,q]: all
```

Go to step [14e](#).

- d At the prompt (#), use pkgadd to install the mid-tier portion (NTmg9km<release_number>.pkg) of the software from ESD by typing

Note: For information on retrieving software from ESD, refer to procedure [Preparing MG 9000 Manager software delivered through ESD for an upgrade on page 1104](#).

```
# pkgadd -d  
/opt/nortel/NTmg9km_<release_number>_xx_0.pk  
g
```

where

release number is a value such as 08 or 09

The system responds with the following (in these examples, the responses are based on a downgrade to SN08):

```
The following packages are available:
```

```
1 NTmg9km08      Succession MG 9000 Manager
                  Midtier Server(sparc) NTMG9KM_8_09_0
```

```
Select package (s) you wish to process (or
'all' to process all packages). (default:
all) [?,??,q]:
```

- e Enter 1 and press Return to begin the server installation process.

The system responds as follows:

```
Executing checkinstall script.Using </opt> as
the package base directory.Processing package
information.Processing system information.1
package pathname is already properly
installed.
```

Note: If a message appears with a confirmation prompt to overwriting conflicting files, respond Y. If existing files are not overwritten, the MG 9000 Manager mid-tier server upgrade cannot continue.

```
Verifying disk space requirements.Checking
for conflicts with packages already
installed.Checking for setuid/setgid
programs.
```

```
This package contains scripts which will be
executed with super-user permission during
the process of installing this package.
```

```
Do you want to continue with the installation
of <NTmg9km08> [y,n,?]
```

```
# Y
```

- f The installation continues automatically and installs all the mid-tier server files in /opt/nortel/mg9kmtr_08 subdirectory as noted in the system response.

```
Installing Succession MG 9000 Manager Midtier
Server as <NTmg9km08>
```

```
## Installing part 1 of 1.
```

```
.
.
```

```
Configuring system, please wait ...
```

```
Installation of <NTmg9km08> was successful.
The Installation is complete.
```

After the installation is complete, a message appears reporting that the installation was successful.

Note: Verify the installation of <NTmg9km_08_xx_0> was successful. If there are any errors please contact your next level of support.

- g If applicable, eject the CD from the CD-ROM drive.

eject cdrom0

- h To configure the mid-tier server, type

/opt/nortel/mg9kmtr_08/bin/mg9kconfig.sh

If previous installation settings are detected, enter Y and accept these settings. Otherwise follow the prompts to enter the settings. Use the data that was recorded in step 3.

- i Enter the following command to start the mid-tier server.

servstart MG9KMIDTIER_<release number>

where

release number is a value such as 08. Release number is not required for SN09.

Press the Enter key again for the login prompt to appear.

- 15 To apply patches, refer to procedure [Applying patches using the NPM on page 2319](#).
- 16 Remove JAVA applications from cache by performing [Removing an MG 9000 Manager JWS application from cache on page 1101](#). Refer to [Uninstalling the Java client on page 1101](#) if the Java client must be removed from your Windows PC or Sun workstation. If the client software must be reinstalled, perform the GUI client installation procedure based on the platform type used for the client, PC or Sun workstation. Refer to [Installing the MG 9000 Manager Windows PC client software on page 1097](#) or [Installing the MG 9000 Sun client software on page 1099](#).
- 17 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Downgrading the N240 HA cluster configuration MG 9000 Manager from SN09U to SN09 or SN08

At the MG 9000 Manager server

1

Note: Do not downgrade the MG 9000 Manager before the downgrade is complete of those MG 9000 network elements under the MG 9000 Manager's control.

Use the information in the following table to determine the next step.

If the inactive side is currently running	Do

SN08 or SN09	step 9
SN09U	step 2

- 2 Record the existing configuration settings for the master server. To view these settings, type:

```
>/opt/nortel/mg9ksrv_09_1/bin/mg9kconfig.sh
```

When prompted, enter Y to keep the existing settings and exit from the script.

- 3 On the inactive side, remove the master server SN09U software by typing

```
> pkgrm NTmg9ks91
```

To continue, respond to the two prompts with Y.

- 4 Record the existing configuration settings for the mid-tier server. To view these settings, type

```
> /opt/nortel/mg9kmtr_09_1/bin/mg9kconfig.sh
```

When prompted, enter Y to keep the existing settings and exit from the script.

- 5 On the inactive side, remove the mid-tier server SN09U software by typing

```
> pkgrm NTmg9km91
```

To continue, respond to the two prompts with Y.

- 6 On the inactive side, downgrade both the mid-tier server and the master server to the SN08 or SN09 SPFS platform.

Details about downgrading the SPFS platform are provided in procedures “Performing a full system restore on an SPFS-based server” in *Nortel ATM/IP Solution-level Fault Management*, NN10408-900.

- 7 On the inactive side, install the master server software using the following steps:

- a Login as root (superuser) and insert the MG 9000 Manager software CD into the CD-ROM drive. This server is also running the OpenOrb NamingService.

- b At the prompt (#), use pkgadd to install the server portion (NTmg9ks<release_number>.pkg) of the software. To directly install the software from the CD-ROM use the following commands to read the CD-ROM and list the contents to read the release number:

```
# cd /cdrom/cdrom0/
# ls
# pkgadd -d
/cdrom/cdrom0/NTmg9ks<release_number>_xx_0.p
kg
```

where

release number is a value such as 08 or 09

The system responds with the following. In these examples, the responses are based on a downgrade to SN08:

The following packages are available:

```
1 NTmg9ks08      Succession MG 9000 Manager
                  Server(sparc) 08.44
```

```
Select package (s) you wish to process (or
'all' to process all packages). (default:
all) [?,??,q]:
```


- c Enter 1 and press return to begin the server installation process.

Note: If the following message appears respond Y at the prompt:

```
The following files are already installed on
the system and are being used by another
package: /opt/nortel<attribute change only>
Do you want to install these conflicting
files [y,n,?,q]
```

After the installation is complete, a message appears reporting that the installation was successful.

- d The package is processed and the following information is displayed.

```
Processing package instance <NTmg9ks08> from
</NTmg9ks09.pkg>
Succession MG 9000 Manager Server (sparc)
08.44
```

```
Copyright (c) 1998-2003 Nortel Networks All
Rights Reserved
```

Note: Verify the installation of <NTmg9ks08> was successful. If there are any errors please contact your next level of support.

Eject the CD-ROM.

- e To configure the master server, type

```
> /opt/nortel/mg9ksrv_08/bin/mg9kconfig.sh
```

If previous installation settings are detected, enter Y and accept these settings. Otherwise follow the prompts to enter the settings. Use the data that was recorded in step 2.

- 8 On the inactive side, install the mid-tier server software by performing the following steps:

- a Login as root (superuser) and insert the CD containing the MG 9000 Manager software into the CD-ROM drive.

- b At the prompt (#) use pkgadd to install the mid-tier portion (NTmg9km08.pkg) of the software. If you are directly installing from the CD-ROM use the following command to read the CD-ROM, and list the contents to read the release number:

```
# cd /cdrom/cdrom0/
```

```
# ls
```

```
# pkgadd -d /cdrom/cdrom0/NTmg9km08_xx_0.pkg
```

where xx is the release number.

The system responds with the following information.

The following packages are available:

```
1   NTmg9km08 Succession MG 9000 Manager
Midtier Server (sparc) 08.44
```

```
Select package(s) you wish to process (or
'all' to process all packages). (default:
all) [?,??,q]: all
```

- c** Enter 1 and press Return to begin the server installation process.

The system responds as follows:

```
Executing checkinstall script.Using </opt> as
the package base directory.Processing package
information.Processing system information.1
package pathname is already properly
installed.
```

Note: If a message appears with a confirmation prompt to overwriting conflicting files, respond Y. If existing files are not overwritten, the MG 9000 Manager mid-tier server upgrade cannot continue.

```
Verifying disk space requirements.Checking
for conflicts with packages already
installed.Checking for setuid/setgid
programs.
```

```
This package contains scripts which will be
executed with super-user permission during
the process of installing this package.
```

```
Do you want to continue with the installation
of <NTmg9km08> [y,n,?]
```

```
# y
```

Note: Verify the Installation of <NTmg9km08_xx_0> was successful. If there are any errors please contact your next level of support.

- d** The installation continues automatically and installs all the mid-tier server files in /opt/nortel/mg9kmtr_08 subdirectory as noted in the system response.

```
Installing Succession MG 9000 Manager Midtier
Server as <NTmg9km08>
```

```
## Installing part 1 of 1.
```

```
.  
.
.
```

```
Configuring system, please wait ...
```

```
Installation of <NTmg9km08> was successful.  
The Installation is complete.
```

After the installation is complete, a message appears reporting that the installation was successful.

e Eject the CD from the CD-ROM drive.

f To configure the mid-tier server, type

```
# /opt/nortel/mg9kmtr_08/bin/mg9kconfig.sh
```

If previous installation settings are detected, the installation will ask if the previous settings should be accepted.

g If previous installation settings are detected, enter Y and accept these settings. Otherwise follow the prompts to enter the settings. Use the data that was recorded in step [4](#).

9 On the active side, stop the MG 9000 Manager server application. To stop the server, type

```
> servstop MG9KSERVER
```

10 On the active side, stop the MG 9000 Manager mid-tier application. To stop the application, type

```
> servstop MG9KMIDTIER
```

11 On the active side, drop the SN09U tablespace by typing

```
>  
/opt/nortel/mg9ksrv_09_1/bin/mgems_ora_ts_drop  
.sh <IP Address of SESM>
```

- 12 On the active side, restore the SN08 tablespace data from the file that was saved during the SN09U upgrade process by typing

```
>/opt/nortel/mg9ksrv_09_1/bin/mgems_ora_ts_restore.sh -a <app_name> <data_db_file> <log_file> <ora_host>
```

where

<app_name>
is MG9KEM

<data_db_file>
is replaced with the dmp file generated in
/data/mg9kem/persistdata/tsBackup

<log_file>
is replaced with the log file generated in
/data/mg9kem/persistdata/tsBackup

<ora_host>
is the database IP address where you want to restore the database

Refer to procedure [Upgrading MG 9000 Manager software from SN08 or SN09 to SN09U on page 1076](#).

- 13 Telnet to the cluster IP address, login to the active unit and perform a failover of the system by typing

```
> init 0
```

If the other unit is at the OK prompt, enter the following command:

```
> boot
```

- 14 Clone the inactive server. For details, refer to “Cloning the image of one unit in a cluster to the other node” in *ATM/IP Solution-Level Administration and Security*, NN10402-600.

- 15 Remove JAVA applications from cache by performing [Removing an MG 9000 Manager JWS application from cache on page 1101](#). Refer to [Uninstalling the Java client on page 1101](#) if the Java client must be removed from your Windows PC or Sun workstation. If the client software must be reinstalled, perform the GUI client installation procedure based on the platform type used for the client, PC or Sun workstation. Refer to [Installing the MG 9000 Manager Windows PC client software on page 1097](#) or [Installing the MG 9000 Sun client software on page 1099](#).

- 16 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Upgrading the MG 9000 Manager software to a maintenance release

When to use this procedure

Use the following procedure when upgrading the MG 9000 Manager software to a maintenance release (MR).

When an MR is made available to the customer, data on the MG 9000 Manager which is at the SN09 format, must be moved into the MR format to maintain provisioned data.

The MR process is different depending on whether you have a High Availability (HA)-cluster or non-cluster setup.

- non-cluster setup - a simplex configuration with a single N240 server or two T1400s configured to run the MG 9000 Manager software
- HA-cluster setup - a duplex configuration with two N240 servers that share one cluster IP address

Use the MR process that applies to your MG 9000 Manager setup.

Prerequisites

Prior to proceeding with this MR upgrade procedure, perform a backup of the entire Oracle database. Refer to procedure [Performing a backup of oracle data on an SPFS-based server on page 374](#).

Action

Upgrading MG 9000 Manager software to a maintenance release in a non-cluster setup (simplex configuration)

At the MG 9000 Manager

- 1 Upgrade the hardware, if necessary. Ensure the connection from the MG 9000 Manager to the MG 9000 is up.
- 2 To stop the GUI clients, click File->Exit from the GUI to exit.
- 3 Telnet into the server running the MG 9000 Manager mid-tier application and log in as root at the servers during the MR process.
- 4 Stop the mid-tier server by typing

```
# servstop MG9KMIDTIER
```

Process information will be displayed
Shutting MG 9K Midtier Server down ...

- Midtier shutdown complete
- 5 Telnet to the master server and login as root.
 - 6 Stop the master server by typing


```
# servstop MG9KSERVER
```

 Process information will be displayed


```
Shutting MG 9K Server down ...
Server shutdown complete
```
 - 7 If required, upgrade to the MR CVoIP Server Platform Foundation Software Platform software, if any. Refer to procedure [Upgrading SPFS software on page 403](#). Back up the MG 9000 file system and save all data in the /data/mg9kem/persistdata directory. This includes the SPFS load on the servers running the MG 9000 Manager master and mid-tier applications.
 - 8 Login as root to the master server.
 - 9 Remove the old MG 9000 Manager server package by typing


```
> pkgrm NTmg9ks09_1
```

 The following package is currently installed:


```
NTmg9ks09_1    Succession MG 9000 Manager Server
                (sparc) NTMG9KS_09_1_11_0
```

 Do you want to remove this package?
 To continue, respond to the two prompts with a Y.
 - 10 To install and start the MR release MG 9000 Manager server application, telnet into the server running the MG 9000 Manager server application and log in as root.
 - 11 Use the following table to determine the next step.

If installing the master server software from	Do
CD-ROM	step 12
electronic software delivery (ESD)	step 13
 - 12 Add in the MR server package from CD-ROM by typing


```
> pkgadd -d
/cdrom/cdrom0/<MG9K_MR_server_package_name>.pkg
```

```
The following packages are available:
1 NTmg9ks09_1 Succession MG 9000 Manager
    Server (sparc) NTMG9KS_09_1_44_0
Select package(s) you wish to process (or 'all'
to process all packages).
(default: all) [?,??,q]:1
```

Go to step [14](#).

- 13** Add in the MR server package from ESD by typing

```
> pkgadd -d
/opt/nortel/<MG9K_MR_server_package_name>.pkg
```

```
The following packages are available:
1 NTmg9ks09_1 Succession MG 9000 Manager
    Server (sparc) NTMG9KS_09_1_44_0
Select package(s) you wish to process (or 'all'
to process all packages).
(default: all) [?,??,q]:1
```

- 14** To continue, type 1 and press the Enter key.

Respond to the one or two additional prompts with Y.

- 15** Change to the following directory

```
> cd /opt/nortel/mg9ksrv09_1/bin
```

- 16** Configure the MG 9000 Manager server by typing

```
> ./mg9kconfig.sh
```

The system responds with the following message:

```
Setup has detected configuration settings from
a previous installation.
```

```
*****Setup Server As : MASTER
Master Server IP Address : 47.xxx.xx.207
```

```

CS2M IP Address           : 47.xxx.xx.220
Security Authentication Host: 47.xxx.xx.207
Get Northbound logs from IEMS : n
Oracle IP Address         : 47.xxx.xx.220
Image Server              : 47.xxx.xx.207
Image Server User ID      : maint
SuperCore Gige Image Directory: /swd/mg9k
SuperCore IMA Image Directory: /swd/mg9k
SuperCore OC3 Image Directory: /swd/mg9k
ITP Image Directory       : /swd/mg9k
ITX Image Directory       : /swd/mg9k
ABI Image Directory       : /swd/mg9k
DS1 Image Directory       : /swd/mg9k
OM Collector CSV Directory : /data/oms/1
*****
Is the above information correct?
Press the enter key to accept the default (y/n)?
Default:[n]=>y

```

Note: Accept the default values to continue with the upgrade. However, if you want to change the settings at this time, use the prompts to change any values.

- 17 Start the MR MG 9000 Manager server application by typing

```
> servstart MG9KSERVER
```

- 18 To install and start the MR release mid-tier application, telnet into the server running the MG 9000 Manager mid-tier application and log in as root on the MG 9000 mid-tier server.

- 19 Remove the old mid-tier package by typing

```
> pkgrm NTmg9km09_1
```

```

The following packages are available:
1 NTmg9km09_1 Succession MG 9000 Manager
  Midtier Server
  (sparc) NTMG9KM_9_1_44_0

```

Do you want to remove this package? y

To continue, respond to the two prompts with a Y.

- 20 Use the following table to determine the next step.

If installing the mid-tier server software from	Do
CD-ROM	step 21
electronic software delivery (ESD)	step 22

- 21 Add in the MR mid-tier package from the CD-ROM by typing

```
> pkgadd -d
/cdrom/cdrom0/<MG9K_MR_midtier_package_name>.pkg
```

The following packages are available:

```
1 NTmg9km09_1 Succession MG 9000 Manager
    Midtier Server
    (sparc) NTMG9KM_9_1_44_0
```

Select package(s) you wish to process (or 'all' to process all packages).

(default: all) [?,??,q]:1

Go to step [23](#)

- 22 Add in the MR mid-tier package from ESD by typing

```
> pkgadd -d
/opt/nortel/<MG9K_MR_midtier_package_name>.pkg
```

The following packages are available:

```
1 NTmg9km09_1 Succession MG 9000 Manager
    Midtier Server
    (sparc) NTMG9KM_9_1_44_0
```

Select package(s) you wish to process (or 'all' to process all packages).

(default: all) [?,??,q]:1

- 23 To continue, type 1 and press the Enter key.

Respond to the one or two additional prompts with Y.

- 24 Change to the following directory

```
> cd /opt/nortel/mg9kmtr09_1/bin
```

- 25 Configure the mid-tier by typing

```
> ./mg9kconfig.sh
```

Setup has detected configuration settings from a previous installation.

Master Server IP Address : 47.142.84.210

Security Authentication Host : 47.142.84.211

Is the above information correct?

Press the enter key to accept the default (y/n)?

Default: [n] => y

Note: Accept the default values to continue with the upgrade. However, if you want to change the settings at this time, use the prompts to change any values.

- 26 Start the MR mid-tier application by typing
> servstart MG9KMIDTIER
- 27 Install the new MR release GUI client. Refer to procedure [Installing the MG 9000 Sun client software on page 1099](#) for a Sun workstation, or to procedure [Installing the MG 9000 Manager Windows PC client software on page 1097](#) for a Windows PC.
- 28 Reconnect any SN09 third party application that retrieves alarms for delivery to Operations Support System (OSS) fault management systems.
- 29 This procedure is complete. If applicable, return to the higher lever task flow or procedure that directed you to this procedure.

Upgrading MG 9000 Manager software to a maintenance release in an HA-Cluster setup

At the MG 9000 Manager

- 1 Upgrade the hardware, if necessary. Ensure the connection from the MG 9000 Manager to the MG 9000 is up.
- 2 Apply SSPFS MR upgrade, if necessary. Refer to procedure [Upgrading SPFS software on page 403](#).
- 3 To stop the GUI clients, click File->Exit from the GUI to exit.
- 4 Telnet into the active server through the cluster IP address and log in as root.

All MR upgrades are performed on the standby node while the active node is providing service. After the standby node of the cluster is upgraded and configured, perform a failover so the standby node becomes active. After determining that both nodes are functional, the newly active node with the MR update can be cloned to the standby node. This will ensure both nodes or units of the cluster have the same data image.

- 5 Determine which of the cluster nodes is in standby so it can be upgraded with the MR.
- 6 Telnet to the inactive cluster IP address, log in as root and type:

```
# bash
```

The cluster prompt changes showing the unit and the status of the unit.

```
mgem_ha_srv-unit0(inactive):/>
```

- 7 Remove the old MG 9000 Manager server application on standby unit by typing

```
> pkgrm NTmg9ks09_1
```

The following package is currently installed:

```
NTmg9ks09_1    Succession MG 9000 Manager Server  
               (sparc) NTMG9KS_9_1_44_0
```

```
Do you want to remove this package? Y
```

To continue, respond to the two prompts with Y.

- 8** Install the MR release on the standby unit for the MG 9000 Manager server application by using the following table to determine the next step.

If installing the master server software from

Do

CD-ROM

step [9](#)

electronic software delivery (ESD)

step [10](#)

- 9** Add in the MG 9000 Manager server package from CD-ROM by typing

```
> pkgadd -d
/cdrom/cdrom0/<MG9K_MR_server_package_name>.pkg
g
```

The following packages are available:

```
1 NTmg9ks09_1 Succession MG 9000 Manager
    Server(sparc) NTMG9KS_9_1_441_0
```

```
Select package(s) you wish to process (or 'all'
to process all packages).
```

```
(default: all) [?,??,q]:1
```

Go to step [11](#).

- 10** Add in the MG 9000 Manager MR server package from ESD by typing

```
> pkgadd -d
/opt/nortel/<MG9K_MR_server_package_name>.pkg
```

The following packages are available:

```
1 NTmg9ks09_1 Succession MG 9000 Manager
    Server (sparc) NTMG9KM_9_1_44_0
```

```
Select package(s) you wish to process (or 'all'
to process all packages).
```

```
(default: all) [?,??,q]:1
```

- 11** To continue, type 1 and press the Enter key.

Respond to the one or two additional prompts with Y.

12 Configure the MG 9000 Manager server application by typing

```
> /opt/nortel/mg9ksrv_09_1/bin/mg9kconfig.sh
```

The system responds with the following message:

```
*****Se
tup Server As          : MASTER
Master Server IP Address      : 47.xxx.xx.207
CS2M IP Address              : 47.xxx.xx.220
Security Authentication Host: 47.xxx.xx.207
Get Northbound logs from IEMS : n
Oracle IP Address            : 47.xxx.xx.220
Image Server                 : 47.xxx.xx.207
Image Server User ID         : maint
SuperCore Gige Image Directory : /swd/mg9k
SuperCore IMA Image Directory : /swd/mg9k
SuperCore OC3 Image Directory : /swd/mg9k
ITP Image Directory          : /swd/mg9k
ITX Image Directory          : /swd/mg9k
ABI Image Directory          : /swd/mg9k
DS1 Image Directory          : /swd/mg9k
OM Collector CSV Directory   : /data/oms/1
*****
```

Is the above information correct?

Press the enter key to accept the default (y/n)?

Default:[n]=>y

Note: Accept the default values to continue with the upgrade.
However, if you want to change the settings at this time, use the prompts to change any values.

13 To install the MR release MG 9000 Manager mid-tier server application on the standby unit, remove the old mid-tier package by typing

```
> pkgrm NTmg9km09_1
```

The following packages are available:

```
1 NTmg9km09_1 Succession MG 9000 Manager
    Midtier Server
    (sparc) NTMG9KM_9_1_44_0
```

Do you want to remove this package? y

To continue, respond to the two prompts with Y.

- 14 Use the following table to determine the next step.

If installing the mid-tier server software from	Do
CD-ROM	step 15
electronic software delivery (ESD)	step 16

- 15 Add in the MR mid-tier package from CD-ROM by typing

```
> pkgadd -d
/cdrom/cdrom0/<MG9K_MR_midtier_package_name>.pkg
```

The following packages are available:

```
1 NTmg9km09_1 Succession MG 9000 Manager
    Midtier Server
    (sparc) NTMG9KM_9_1_441_0
```

```
Select package(s) you wish to process (or 'all'
to process all packages).
(default: all) [?,?,q]:1
```

Go to step [17](#)

- 16 Add in the MR mid-tier package from ESD by typing

```
> pkgadd -d
/opt/nortel/<MG9K_MR_midtier_package_name>.pkg
```

The following packages are available:

```
1 NTmg9km09 Succession MG 9000 Manager
    Midtier Server
    (sparc) NTMG9KM_9_1_44_0
```

```
Select package(s) you wish to process (or 'all'
to process all packages).
(default: all) [?,?,q]:1
```

- 17 To continue, type 1 and press the Enter key.

Respond to the one or two additional prompts with Y.

18 Configure the mid-tier by typing

```
> /opt/nortel/mg9ksrv_09_1/bin/mg9kconfig.sh
```

```
Setup has detected configuration settings from  
a previous installation.
```

```
*****  
Master Server IP Address      : 47.xxx.xx.209  
Security Authentication Host  : 47.xxx.xx.208  
*****
```

```
Is the above information correct?
```

```
Press the enter key to accept the default (y/n)?
```

```
Default: [n] => y
```

Note: Accept the default values to continue with the upgrade. However, if you want to change the settings at this time, use the prompts to change any values.

19 To create a failover, telnet to the cluster IP address, login into active unit and type

```
> init 0
```

After the failover, telnet to the cluster IP address and login to the newly active unit.

20 Install the new MR release GUI client. Refer to procedure [Installing the MG 9000 Sun client software on page 1099](#) for a Sun workstation, or to procedure [Installing the MG 9000 Manager Windows PC client software on page 1097](#) for a Windows PC. Connect the client by pointing to the virtual IP address of the cluster.**21** Verify the newly active unit recovers by typing the following command while logged into the cluster IP address

```
> servquery -status all
```

22 Launch the MG 9000 Manager client.**23** Reconnect any SN09 third party application that retrieves alarms for delivery to Operations Support System (OSS) fault management systems.**24** When the newly active node with the MR update is fully functional, mirror the newly active node to the standby node so both nodes have the same image. Perform procedure [Cloning the image of one server in a cluster to the other server on page 478](#).**25** This procedure is complete. If applicable, return to the higher lever task flow or procedure that directed you to this procedure.

Rolling back the Ethernet Routing Switch 8600 software for CS-LAN

Introduction

This procedure rolls back software upgrades to Ethernet Routing Switch 8600 (formerly known as the “Passport 8600”) pairs that support the Communication Server LAN (CS-LAN). The rollback uses a phased approach to prevent service interruption.

Note: Refer to procedure [Upgrading the Ethernet Routing Switch 8600 on page 111](#)

ATTENTION

Nortel urges users of this rollback procedure to read thoroughly this Introduction, especially [Important rollback considerations](#) before attempting this procedure.

New in this release

This section highlights the functionality introduced in this release.

- Added steps addressing the Border Control Point, whereby the portal must be shut down gracefully to prevent it from accepting service requests during an Ethernet Routing Switch 8600 upgrade.

Note: The Border Control Point was formerly known as the RTP Media Portal.

Important rollback considerations



CAUTION

Manually entered configuration changes executed since the completion of an Ethernet Routing Switch 8600 upgrade are lost when rolling back to version 3.7.2.2.

Nortel strongly recommends re-entering configuration changes after the completion of the rollback procedure.

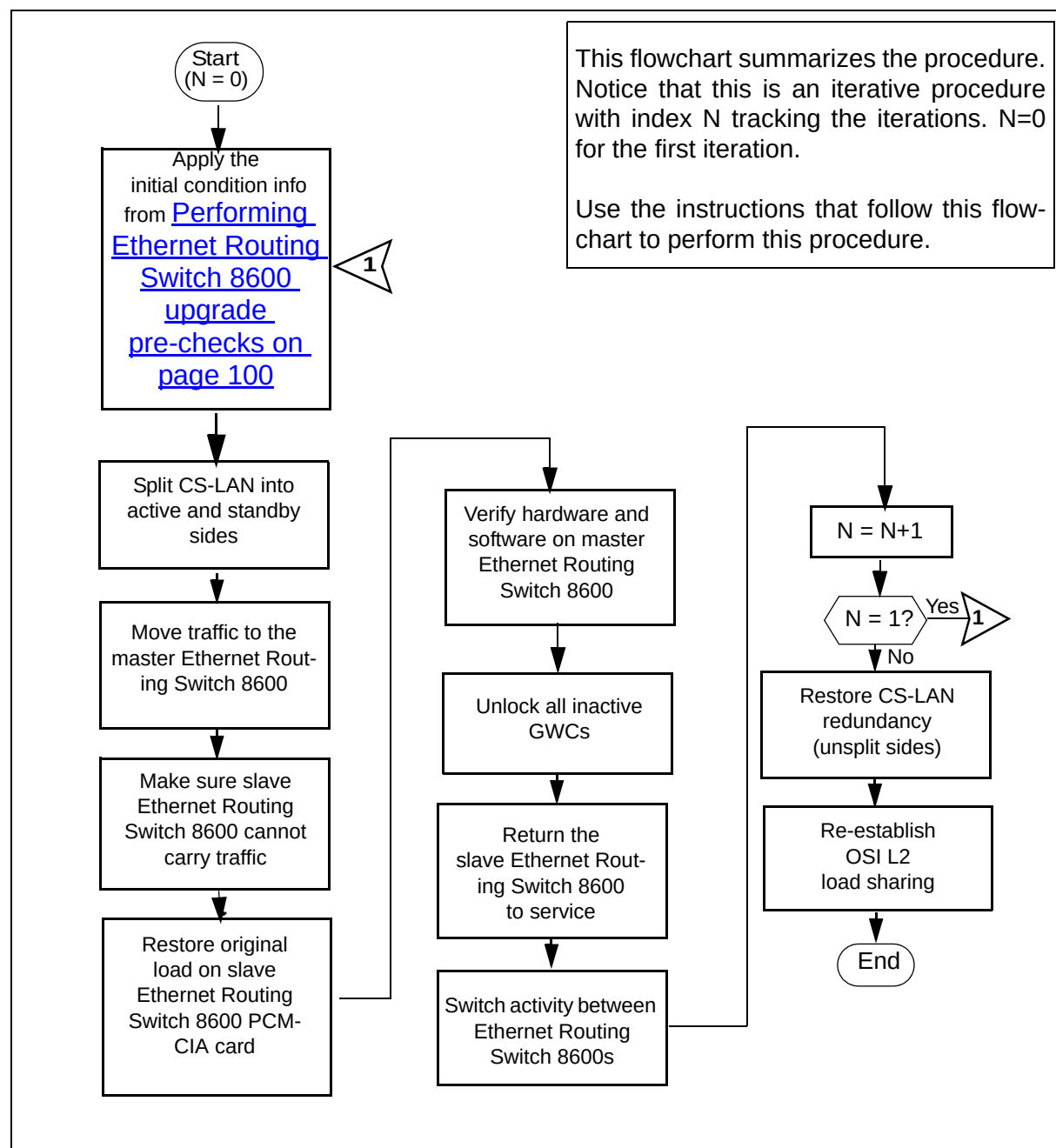
This rollback procedure addresses Ethernet Routing Switch 8600 configurations with dual call processing units (CPU). Therefore, execute all CPU-related commands on the master CPU, except where otherwise noted. Also an Ethernet Routing Switch 8600 must be running with a v3.7.2.2 software load *before* a dual CPU with a high-availability (HA) mode is configured for it.

Note: Also, if rolling back to pre-v3.7.2.2 software version after having attempted a v3.7.2.2 software upgrade for a dual CPU configuration, users must disable the dual CPU HA flag setting *before* the rollback begins.

Also refer to sub-section [Text conventions on page 77](#) for brief descriptions and examples of filenames that appear in commands throughout this procedure. This subsection also includes descriptions for distinguishing between the master and standby CPUs in the command line interface (CLI).

The following flowchart summarizes the Ethernet Routing Switch 8600 rollback procedure.

Rolling back a software upgrade on Ethernet Routing Switch 8600s for the CS-LAN



Procedure

Use this procedure to roll back the software of an Ethernet Routing Switch 8600 to a previous release.

Rolling back software upgrades on Ethernet Routing Switch 8600s Supporting CS-LANs

ATTENTION

This rollback procedure assumes that procedure “Ethernet Routing Switch 8600 software for the CS LAN upgrade” was aborted after some stage of progress. This procedure further assumes that the procedures in “Preparing to upgrade the Ethernet Routing Switch 8600” were completed successfully.

Refer to

- 1 This procedure is iterative (iteration index is N). Use the conventions defined in the following table to complete this procedure.

Iteration	Slave Ethernet Routing Switch 8600	Master Ethernet Routing Switch 8600
First Pass	Chassis N = 0	Chassis X = 1
Second Pass	Chassis N = 1	Chassis X = 0

- 2 Refer to [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#), steps [6](#) through [9](#) and reproduce the

VID (P/V), VRID, OSPF, and PRIO information for Ethernet Routing Switch 8600 Chassis 0 and 1 in the following table.

Ethernet Routing Switch 8600 - Initial conditions

Status					
VID (P/V)	VRID	Chassis 0		Chassis 1	
		OSPF Metric	VRRP PRIO	OSPF Metric	VRRP PRIO
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
Note: Only collect this metric if OSPF is configured on the Ethernet Routing Switch 8600.					

Note: As Ethernet Routing Switch 8600 does not carry call processing traffic in the PT-AAL1 solution, not all the Carrier VoIP componentry in this rollback procedure applies to PT-AAL1.

Therefore, if rolling back the upgrade of the Ethernet Routing Switch 8600 software in a PT-AAL1 solution, skip to [step 96](#).

Splitting the CS-LAN into active and standby sides using the Ethernet Routing Switch 8600 CLI

- 3 Make sure Ethernet Routing Switch 8600 Chassis N is the slave as follows:

- a Enter the following command to set the VRRP priority to 1.

config vlan <vid> ip vrrp <vrid> prio 1

Note: Setting Ethernet Routing Switch 8600 Chassis N <prio> to 1 makes it slave.

- b Enter the following command to set the OSPF priority to 1000.

config vlan <vid> ip ospf metric 1000

- c Repeat sub[step 3a](#) and sub[step 3b](#) for each VLAN provisioned on the router.

- 4 Enter the following command to save the new Ethernet Routing Switch 8600 Chassis N configuration.

sav config

This updates the new Ethernet Routing Switch 8600 configuration so that VRRP settings are maintained after any subsequent reboot.

- 5 Select the next step as follows:

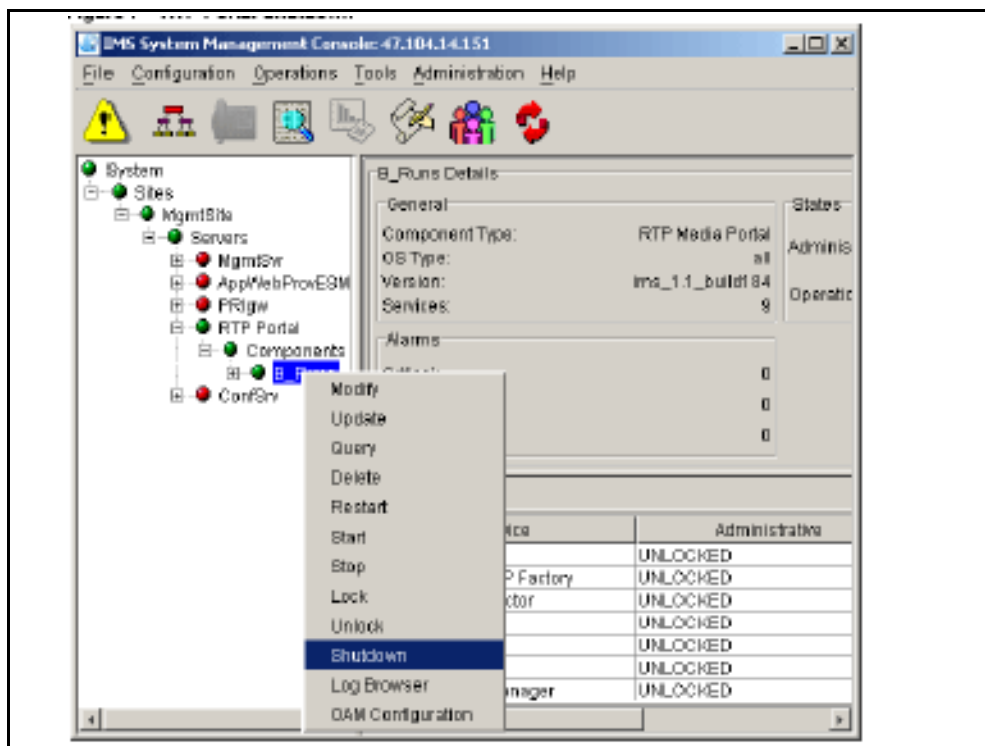
If your configuration includes:	Do
multiple Border Control Points directly connected to the Ethernet Routing Switch 8600	step 6
does not include an Border Control Point	step 9

Shutting down the Border Control Point connected to Chassis N to prevent it from accepting new service requests using the System Management Console

- 6 In the System tree, right click on the target Border Control Point component.

Note: Ensure you are addressing the port that is connected directly to the Ethernet Routing Switch 8600.

- 7 From the pop-up menu, select **Shutdown**.



Note: Alternately, the **Shutdown** command is available from the pull-down Operations menu.

A confirmation window appears.

Shutdown will affect the operations of this component.

Do you want to continue?

- 8 Click **Yes**.

The Border Control Point shuts down gracefully and transitions into a LOCKED state when the last active media session ends. (Refer to the General Information area of the System Management Console.)

- 9 Select the next step as follows:

If your CS-LAN:	Do
includes ATM PVGs directly connected to the Ethernet Routing Switch 8600 (i.e., a non-VR solution)	step 10
includes PVGs connected by Gig Ethernet (GigE)	step 25
does not include PVGs	step 25

If your CS-LAN:

includes ATM interfaces connected to a PVG
15000/7400 chassis running VR or VrAp

Do

[step 25](#)

Note 1: The following steps ([step 10](#) to [step 24](#)) offload PVG traffic from the Ethernet Routing Switch 8600 chassis undergoing a software upgrade. Offloading PVG traffic using these steps minimizes the impact of the software upgrade process on call processing.

Note 2: These steps apply to full-featured Packet Trunking Transit solutions that use Media Gateways 15000/7400 with the CS-LAN.

Determining the PVG IP addresses using the PVG CLI

10 Check the provisioning information for the VSPs, NSTA, and VGS subcomponents as follows:

- a Enter the following command to display media and signaling gateway IP addresses.

d -p nsta/* vgs ctrl/*

The following list provides sample MG and SG IP addresses for a single VSP card provisioned in slot 7.

Nsta	Ctrl	ipAddr	dnsList
7	mg	172.16.201.2	
7	sg	172.16.201.6	

Note: The... **nsta/* vgs ctrl/*** component of this command causes IP addresses for all provisioned VSP cards to be displayed. The example only shows MG and SG IP addresses for a single VSP card provisioned in slot 7.

- b Enter the following command to display the IPmcon IP address.

d -p nsta/* vgs ipmcon

The following list provides a sample IPmcon IP address for a single VSP card provisioned in slot 7:

```

+=====+-----+-----+-----+
| Nsta  |      ipAddr      | udpBa | Response |
|       |                   | se    |          |
+=====+-----+-----+-----+
|       7 | 172.16.201.10   | 49152 |          |

```

Note: The ... *nsta/* vgs ipmcon* component of this command causes IP addresses for all provisioned VSP cards to be displayed. The example only shows IPmcon IP address for a single VSP card provisioned in slot 7.

Verifying that the PVGs are set up redundantly using each Ethernet Routing Switch 8600 CLI

- 11 Enter the following command on each Ethernet Routing Switch 8600 chassis to check the VLAN configuration file.

sho config module vlan

This command outputs all VLANs provisioned on the Ethernet Routing Switch 8600 Chassis. The example that follows shows the output of this command for only one VSP blade:

```

vlan 702 create byport 1 name "PVG40-vsp07-mg"
vlan 702 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 702 ports add 8/1 member portmember
vlan 702 ip create 172.16.201.1/255.255.255.252 mac_offset 5
vlan 706 create byport 1 name "PVG40-vsp07-sg"
vlan 706 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 706 ports add 8/1 member portmember
vlan 706 ip create 172.16.201.5/255.255.255.252 mac_offset 14
vlan 710 create byport 1 name "PVG40-vsp07-media"
vlan 710 ports remove 1/1-1/8,2/1-2/48,4/1-4/48,7/1-7/8,8/2-8/8,10/1-10/8 member portmember
vlan 710 ports add 8/1 member portmember
vlan 710 ip create 172.16.201.9/255.255.255.252 mac_offset 6

```

Note: Both Ethernet Routing Switch 8600s display the identical PVG VLAN configuration. The **vlan ### ports add** entry identifies each VSP ATM Sonet connection. This information is required in [step 17](#).

- 12 Select an Ethernet Routing Switch 8600 chassis (Chassis N or Chassis X) and record the routing table information for all of its VSP VLANs as follows.

Note: Substep c repeats this step for the other chassis.

- a Enter the following command to display IP route information.

sho ip route info ip x.y.z

where

x.y.z

specifies the IP Net address provided at [step 10](#)

The following list provides an example for the command output for one of the Ethernet Routing Switch 8600s:

```
=====
                        Ip Route
=====
      DST          MASK          NEXT      COST  VLAN  PORT  PROT  AGE  TYPE  PRF
-----
  172.16.201.0 255.255.255.252  172.16.201.1    1  702  -/-   LOC   0 DB   0
  172.16.201.4 255.255.255.252  172.16.201.5    1  706  -/-   LOC   0 DB   0
  172.16.201.8 255.255.255.252  172.16.201.9    1  710  -/-   LOC   0 DB   0

2 out of 360 Total Num of Dest Networks,360 Total Num of Route Entries displayed.
=====
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW
```

The following list provides an example for the command output for the other Ethernet Routing Switch 8600 Chassis.

```
=====
                        Ip Route
=====
      DST          MASK          NEXT      COST  VLAN  PORT  PROT  AGE  TYPE  PRF
-----
  172.16.201.0 255.255.255.252  172.30.242.230   20   80  -/-  OSPF   0 IB  120
  172.16.201.4 255.255.255.252  172.30.242.230   20   80  -/-  OSPF   0 IB  120
  172.16.201.8 255.255.255.252  172.30.242.230   20   80  -/-  OSPF   0 IB  120

2 out of 360 Total Num of Dest Networks,360 Total Num of Route Entries displayed.
=====
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW
```

ATTENTION

The routing information under the PROT column heading must indicate either VSP subnet LOC or OSPF.

If both Ethernet Routing Switch 8600s indicate the same status for the same VSP subnet, this is a non-standard condition. Contact your next level of support.

To prevent service interruption, VSP VLANs on Chassis N of the Ethernet Routing Switch 8600 must be OSPF (LOC for Chassis X). See [step 19](#) for detailed steps for forcing compliance to this requirement.

- b** Repeat sub[step a](#) for each VSP VLAN on the selected Ethernet Routing Switch 8600 chassis.
- c** Select the other Ethernet Routing Switch 8600 chassis and repeat sub[step a](#) and sub[step b](#).

Verifying the correct provisioning of each VSP using the PVG CLI

- 13** Check the SPVCAP subcomponent of each VSP VGS Ctrl/<mg,sg> and IPmcon as follows:

- a** Enter the following command to display the provisioning information for each VSP.

d -p -no nsta/* vgs ctrl/* spvcap

The following list shows VSP provisioning information for slot 7. The actual command output lists all VSP information.

```
Nsta/ 7 VGS Ctrl/mediaGateway SpvcAp
  atmServiceCategory = nrtVariableBitRate
  peakCellRate      = 800 cells
  sustainedCellRate= 400 cells
  maximumBurstSize= 100 cells
  retryLimit        = 0
  localAddress      = 45613512123400002F000000010020480D527001
  remoteVpiVci      = 7.2
  addressToCall     = 45613512123400002F000000010020480D008D00

Nsta/ 7 VGS Ctrl/signalingGateway SpvcAp
  atmServiceCategory = nrtVariableBitRate
  peakCellRate      = 450 cells
  sustainedCellRate= 210 cells
  maximumBurstSize= 60 cells
  retryLimit        = 0
  localAddress      = 45613512123400002F000000010020480D527002
  remoteVpiVci      = 7.2
  addressToCall     = 45613512123400002F000000010020480D008D00
```

b Enter the following command to display IPmcon information

d -p -no nsta/* vgs ipmcon spvcap

*The following list shows information for the IPmcon in slot 7.
The actual command output lists information for all IPmcon
sub-components of the NSTA VGS.*

```
Nsta/ 7 VGS IpMcon SpvcAp
  atmServiceCategory = rtVariableBitRate
  peakCellRate       = 336000 cell/s
  sustainedCellRate  = 336000 cell/s
  maximumBurstSize   = 1 cells
  retryLimit         = 0
  localAddress       = 45613512123400002F000000010020480D517000
  remoteVpiVci       = 7.10
  addressToCall      = 45613512123400002F000000010020480D008D00
```

- 14** Confirm that the VSP VGS addressToCall (ATMIF UNI address) for Ctrl/mediaGateway, Ctrl/signaling Gateway, and IpMcon are identical.

Note: If they are not identical, contact your next level of support.

- 15** Enter the following command to check the ATMIF UNI addresses provisioned as primary and alternate by typing:

l atmif/* uni addr/*

A sample of the command output for the ATMIFs present on the PVG shelf follows.

```
Atmif/141 Uni Addr/45613512123400002F000000010020480D008D00, primary
Atmif/151 Uni Addr/45613512123400002F000000010020480D008D00, alternate
Atmif/151 Uni Addr/45613512123400002F000000010020480D009700, primary
```

Note: Make sure the ATMIF UNI provisioning reflects a Primary and Alternate configuration for the same address for each VSP. (Refer to your engineering guidelines for more information.) If they do not match, contact your next level of support.

Verifying the PVG ATM (software) connection to the Ethernet Routing Switch 8600s using the PVG CLI

- 16** Determine which ATMIF the VSP VGS Ctrl/<mg,sg> and IPmcon ATMCON subcomponents point to as follows.
- a** Enter the following command to display the VGS Ctrl/<mg,sg> ATMCON subcomponent for all VSPs.

d nsta/* vgs ctrl/* atmconn

A sample of the command output for a VSP provisioned in slot 7 follows. The actual command output lists all connection states and the ATMIFs they use.

```

+====+====+-----+-----+
|Nsta |Ctrl|      nextHop      |state|
+====+====+-----+-----+
|   7 |mg  |AtmIf/141 Vcc/7.2 Ep|connec|
|   7 |sg  |AtmIf/141 Vcc/7.6 Ep|connec|

```

Note: Make sure the AtmIf information for each VSP is identical to the primary interface information listed in [step 15](#). If they do not match, contact your next level of support.

- b** Enter the following command to display the NSTA VGS IPmcon ATMCON subcomponent for the VSPs.

d nsta/* vgs ipmcon atmcon

A sample of the command output for a VSP provisioned in slot 7 follows. The actual command output lists all connection states and the ATMIFs they use.

```

+====+-----+-----+-----+-----+
| Nsta |      nextHop      |state |Response|
+====+-----+-----+-----+-----+
|   7 |AtmIf/141 Vcc/7.10|connec |        |

```

Note: Make sure the AtmIf information for each VSP is identical to the primary interface information listed in [step 15](#). If they do not match, contact your next level of support.

- 17** Check the physical connections between each PVG ATM interface and their related Ethernet Routing Switch 8600s.

Note: See [step 11](#) for the Ethernet Routing Switch 8600 local route tables for the VSPs to be offloaded and verify the fiber connectivity between the PVGs and Ethernet Routing Switch 8600s. Refer to your engineering guidelines for additional information.

Disabling the ATM interface to the Ethernet Routing Switch 8600 undergoing the software upgrade using the PVG CLI

- 18** Select the next step as follows (refer to [step 12](#)):

If all VSP VLANs for Ethernet Routing Switch 8600 Chassis N are	Do
OSPF (see Note)	step 25
Anything except OSPF	step 19

Note: OSPF routing does not require manual maintenance to reduce the risk of call processing outages, as the link redundancy on PVGs fails over nearly immediately.

- 19** Disable the ATM interface for each VSP as follows.
- a** Enter the following command to identify the ATM interfaces and Sonet layer.

d -p -no lp/* sonet/* sts/0

A sample of the command output for the first Sonet interface on each card follows. The actual command output lists all Sonet interfaces on the PVG.

```
Lp/14 Sonet/1 Sts/0
  applicationFramername    = Atmif/141
  txPathTrace              = ""
  expectedReceivePathTrace = ""
  concatNumber             = 0
  customerIdentifier        = 0
  ifAdminStatus            = up
  ifIndex                  = 6
Lp/15 Sonet/1 Sts/0
  applicationFramername    = Atmif/151
  txPathTrace              = ""
  expectedReceivePathTrace = ""
  concatNumber             = 0
  customerIdentifier        = 0
  ifAdminStatus            = up
  ifIndex                  = 472
```

- b** Enter the following command to lock all Sonet layer connections related to the ATM ports connected to Ethernet

Routing Switch 8600 Chassis N.

lock -force Ip/<slot> sonet/<sonetif>

where

<slot>

is the slot number of the ATMIF blade

<sonetif>

is the Sonet interface on the ATM blade

Note: This command results in Sonet layer Alarms.

c Record all locked Sonet interfaces.

20 Confirm the ATM (software) connection switch over is successful as follows.

a Enter the following command to display the VGS Ctrl/<mg,sg> ATMCON subcomponent for the VSPs.

d nsta/* vgs ctrl/* atmconn

A sample of the command output for the switched ATMCON for the Ctrl/ to the ATMIF in slot 7 follows. This example shows a switchover from AtmIf/141 (see [step 16](#)) to AtmIf151.*

```

+====+====+-----+-----+-----+
|Nsta |Ctrl|           nextHop           |state
+====+====+-----+-----+-----+
|      7|mg  |AtmIf/151 Vcc/7.2 Ep|connec
|      7|sg  |AtmIf/151 Vcc/7.6 Ep|connec

```

b Enter the following command to display the VGS IPmcon ATMCON subcomponent for the VSPs.

d nsta/* vgs ipmcon atmcon

A sample of the command output for the switched ATMCON for the IPmcon in slot 7 follows. This example shows a switchover from AtmIf/141 (see [step 16](#)) to AtmIf/151.

```

+====+-----+-----+-----+-----+
|Nsta |           nextHop           |state |Response
+====+-----+-----+-----+-----+
|      7|AtmIf/151 Vcc/7.10  |connec|

```

Verifying the IP route table for the offloaded VSP VLANs using the Ethernet Routing Switch 8600 CLI

- 21** Enter the following command to display the routing table for both Ethernet Routing Switch 8600s:

sho ip route info ip x.y.z

where

x.y.z

is the IP Net address (see [step 12](#))

Note: The routing information under the PROT column heading should indicate OSPF for all VSP VLANs on Ethernet Routing Switch 8600 Chassis N.

- 22** Select the next step as follows:

If switchover of all VSPs is:	Do
incomplete (not switched over)	step 19
complete (switched over))	step 23

Re-enabling all disabled ATM ports using the PVG CLI

- 23** Enter the following command to unlock all Sonet ports locked at [step 19](#).

unlock Ip/<slot> sonet/<sonetif>

where

<slot>

is the slot number of the ATMIF blade

<sonetif>

is the Sonet interface on the ATM blade

Checking the IP route tables using the Ethernet Routing Switch 8600 CLIs

- 24** Enter the following command to make sure all VSP VLANs remain OSPF on Ethernet Routing Switch 8600 Chassis N and LOC on Ethernet Routing Switch 8600 Chassis X.

sho ip route info ip 172.16.201

The routing information under the PROT column heading must indicate OSPF for all VSP VLANs on Ethernet Routing Switch 8600 Chassis N. If it does not, contact your next level of support.

Making the devices that subtend Ethernet Routing Switch 8600 Chassis N inactive using the CS 2000 Management Tools

- 25** Launch CS 2000 Management Tools from your web browser. If required, refer to procedure [Launching CS 2000 Management Tools and NPM client applications on page 2286](#).

Note: If Java Web Start is not installed on your workstation, you are prompted to install Java Web Start.

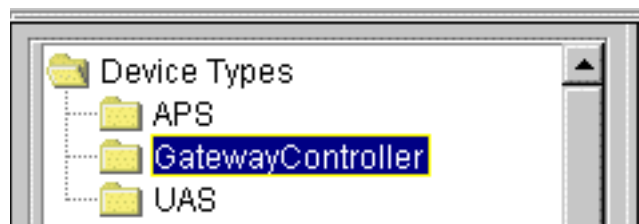
- 26** Click on the CS 2000 Management Tools link.

The Login window appears.

- 27** Access the Maintenance information window for the GWCs as follows:

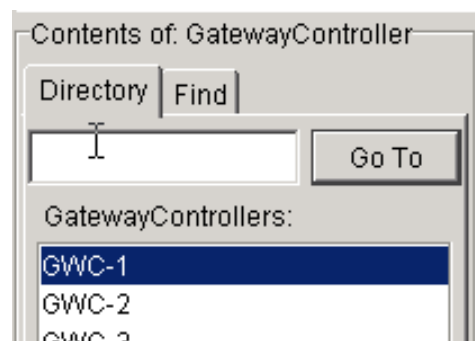
- a** Select GatewayController from the Device Types field of the CS 2000 Management Tools GUI.

The GatewayController folder in the Device Types field is highlighted.



- b** Select the Directory tab on the Contents of: Gateway Controller field.

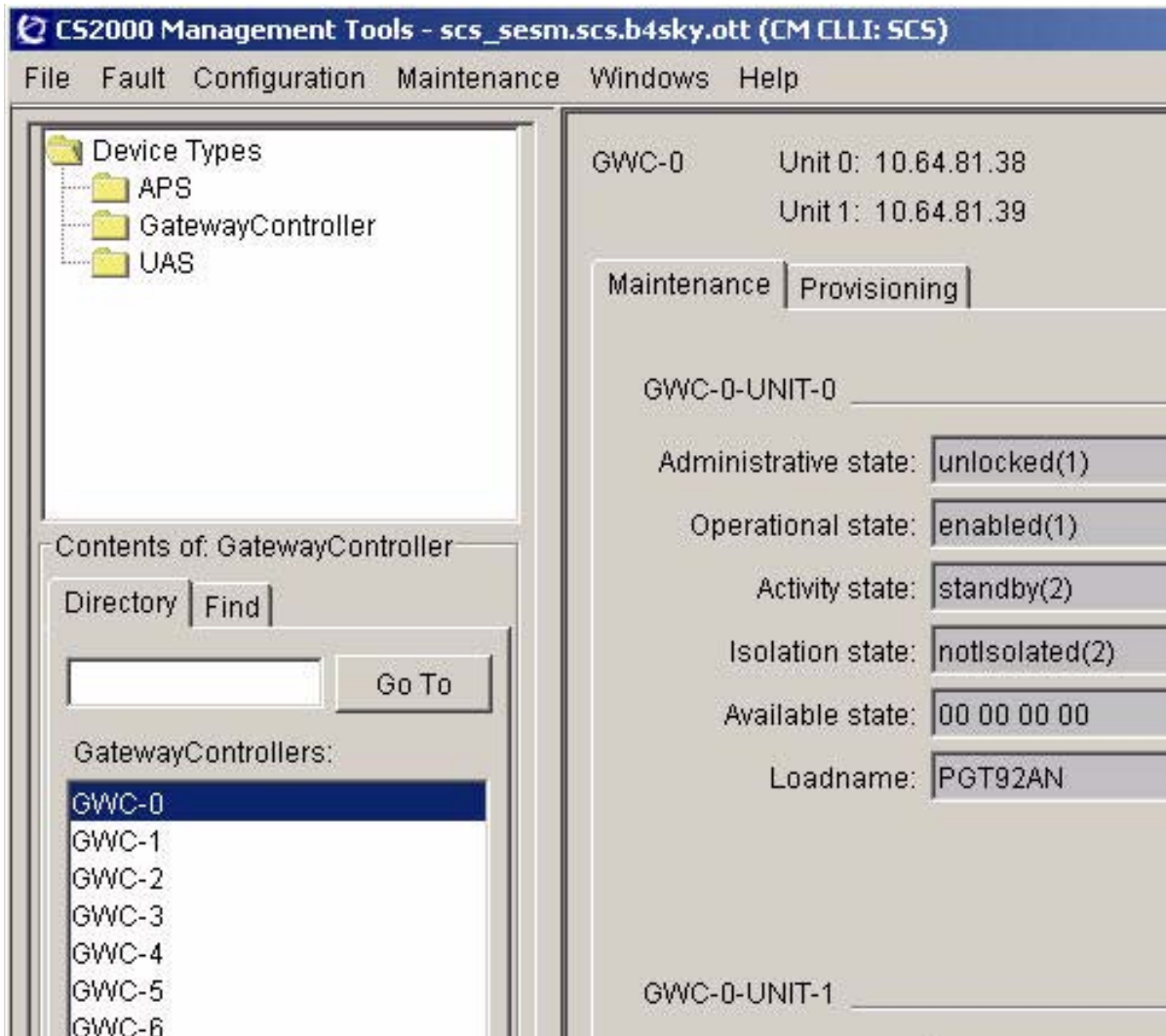
The list of Gateway Controllers appears.



- c** Select the first GWC in the list.

The GWC is highlighted and the related Maintenance or Provisioning information (depending on the active tab) appears in the large right-hand field.

- d Select the Maintenance tab to make sure the Maintenance information is active.



- 28 Make all GWCs inactive on Ethernet Routing Switch 8600 Chassis N.

Note: Recall that the recommendation in [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#) requires that GWC unit 0s subtend Ethernet Routing Switch 8600 Chassis 0. GWC unit 1s subtend Ethernet

Routing Switch 8600 Chassis 1. The following table reiterates the Ethernet Routing Switch 8600 Chassis configurations.

Iteration		Comment
First Pass	N = 1	Chassis 1 Master
Second Pass	N = 2	Chassis 0 Master

- a Check the Activity State field for GWC unit N to determine which unit is active and which is standby.

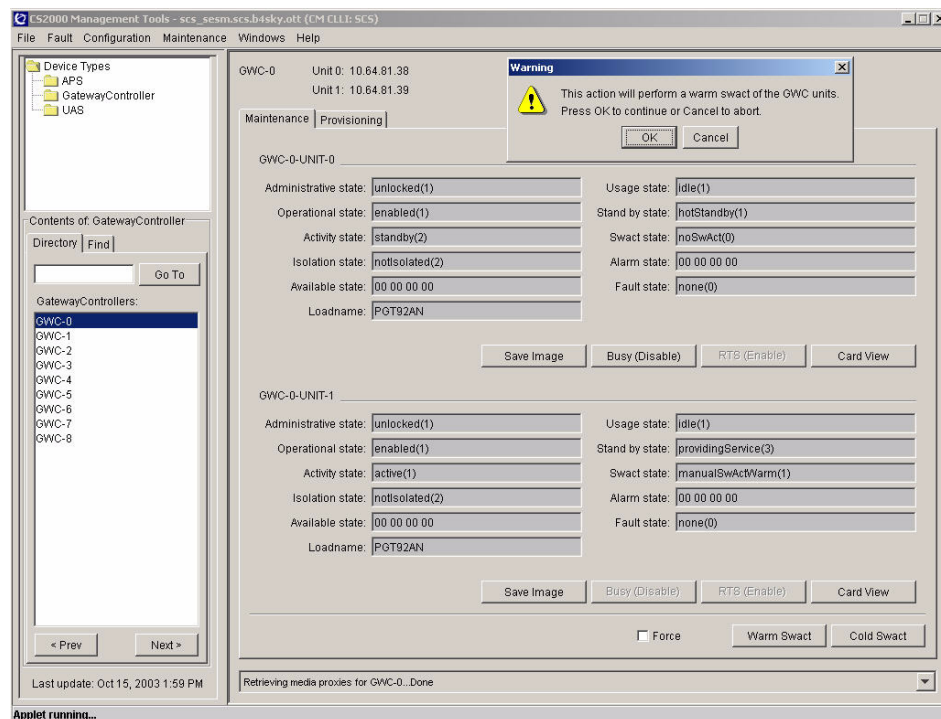
If the Activity State field is	Do
active	sub step 28b
standby, instead of inactive	sub step 28d

Note: For the first iteration, all GWC unit 0s should be standby. For the second iteration, all GWC unit 1s are standby.

- b Click WarmSwact.

A warning window appears.

Press OK to continue or Cancel to abort.



- c Click OK and wait for the activity change to complete.

The selected GWC undergoes a change of activity. The change of activity can take approximately 2 minutes.

- d Select the next GWC in the list and repeat these substeps until the Activity State field for Unit: N Status is inactive for all GWCs in the list.

29 Select the next step as follows:

If the Communication Server uses:

Do

an XA-Core

[step 30](#)

a Compact chassis

[step 32](#)

Disabling the Ethernet link with Ethernet Routing Switch 8600 Chassis N using the XA-Core MAP terminal

- 30** Enter the following command to access the ETHR level of the MAP display.

>MAPCI;MTC;XAC;ETHR

Note: Refer to the IP addresses in table CMIPADDR. Verify that HIOP links 5R and 14R map to the correct arp table on both Ethernet Routing Switches.



- 31** Disable the Ethernet link between the XA-Core and Ethernet Routing Switch 8600 Chassis N. Enter the following command.

bsy <slot> r link force

HIOPs/HCMICs	N = 0	N = 1
<slot>	5	14

- 32** Select the next step as follows:

If you have	Do
a 3PC with a USP Compact	step 33
a 3PC with a standard USP	step 56
an XA-Core	step 65

Preparing the slave USPc blade for locking using the USP Compact (USPc) GUI

33

ATTENTION

Prior to adhering to steps [34](#) to [49](#), ensure that the slave USPc blade is being addressed during the first iteration of the Ethernet Routing Switch 8600 software upgrade.

Refer to your network diagram and determine the USPc blade-to-Ethernet Routing Switch 8600 connectivity. The slave USPc blade must connect to Chassis N of the Ethernet Routing Switch 8600; master USPc blade to Chassis X. (This information coincides with the network element-to-Ethernet Routing Switch 8600 assumptions stated in [step 1](#) of this procedure.)

34 Launch the USPc GUI.

35 Select **Configuration --> platform --> Node**.

The Administration tab of the USPc GUI displays.

The screenshot shows the Administration tab of the USPc GUI. The interface includes a top toolbar with icons for New, Add, Modify, Delete, Lock, Unlock, Load, Offline, Swact, and Restart. Below the toolbar are tabs for Administration, Search, and Graphical View. The main content area is divided into three sections: Provisioning Data, Operational Data, and Boot Data.

Provisioning Data

slot-type	usp-compact			
slot-name	USP1			
slot-description	USP-Compact #1			
shelf	0			
slot	15			
t1-e1-mode	t1			
ext-ip-address	47	131	125	82
ext-subnet-mask	255	255	255	128
ext-gateway	47	131	125	126
front-pec	NTRX51FN			

Operational Data

operational-state	enabled
administrative-state	unlocked
procedural-state	null
availability-state	null
activity-state	inactive
rex-status	

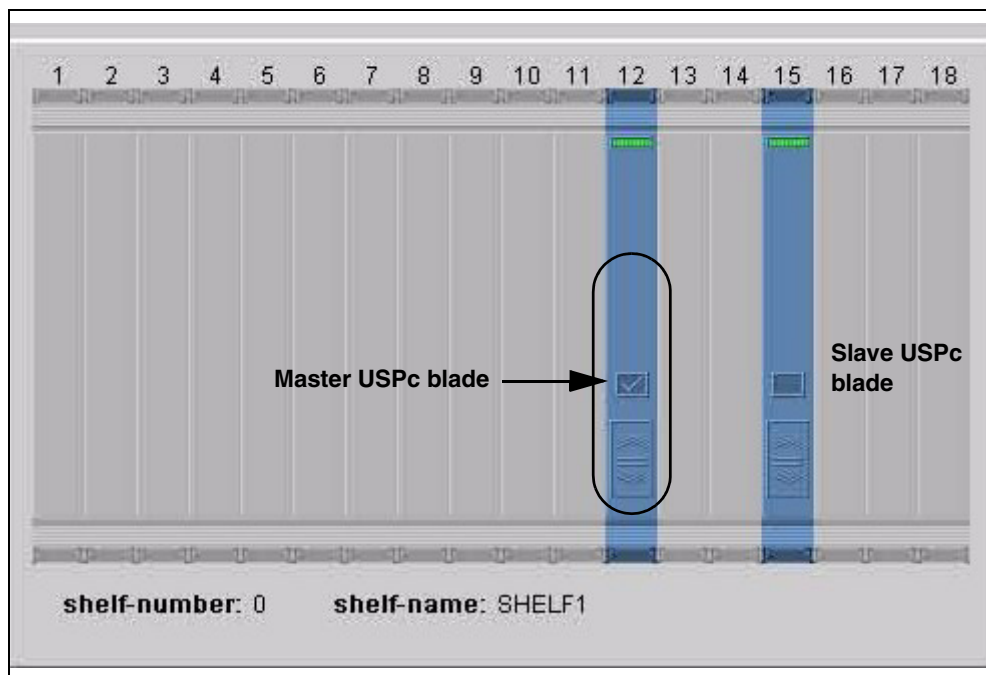
Boot Data

status-message	
running-image	samss7_ppc750_10_00_01_06g
ha-running-image	ss7t1e1ha_ppc8260_10_00_01_06g
running-snapshot	current active
boot image	uspc_10_00_01_06g_base
ha-boot-image	uspc_10_00_01_06g_t1e1ha
boot-snapshot	current active
snapshot-description	current active
snapshot-date	
snapshot-version	

loading complete

- 36** Verify the master and slave USPc blade-to-Ethernet Routing Switch 8600 connectivity by selecting the Graphical View tab.

The following figure displays the Graphical View of the USPc blades.



The icon with a checkmark identifies the master USPc blade. Slot 12 contains the master USPc blade. Slot 15 contains the slave USPc blade.

- 37** Select the next step as follows.

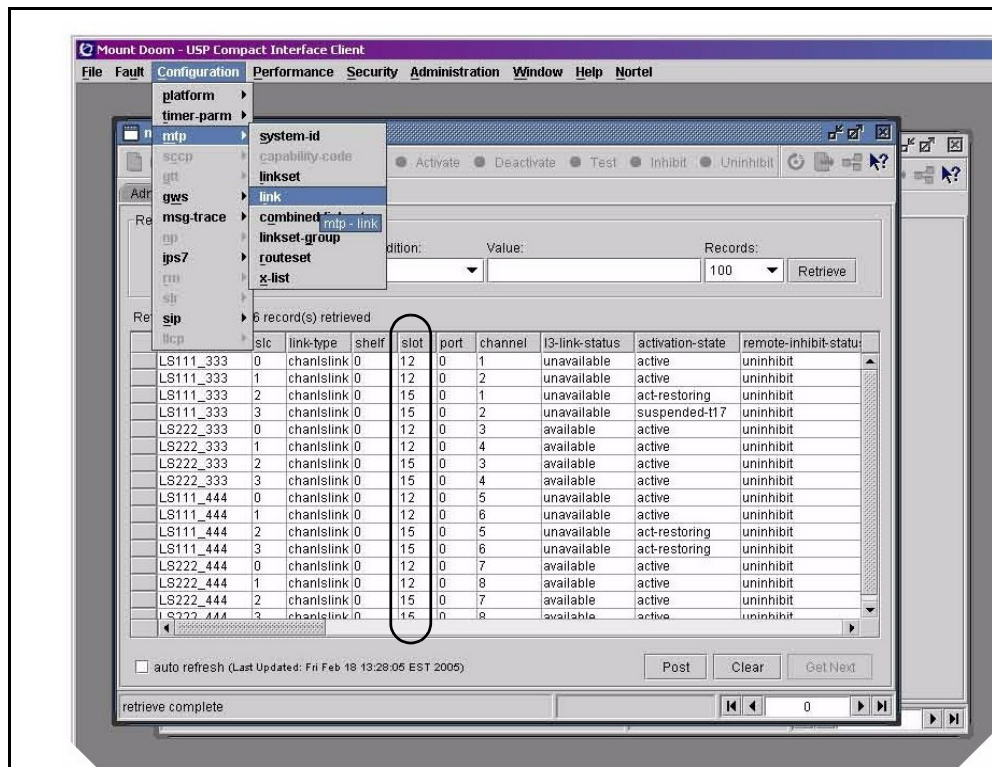
If the slave USPc blade is	Do
not connected to Chassis N of the ERS 8600	step 38
connected to Chassis N of the ERS 8600	step 39

- 38** To perform a SWACT on the two USPc blades, press **Swact**.

- 39** Turn down the paths and the links associated with the slave blade to be unlocked.

Select **Configuration --> MTP --> Links** from the pull-down menu.

The following figure displays.



- 40** Refer to the Slot column to verify the SS7 links against the USPc blades. Select any SS7 links that are against the slave USPc blade.

Click **Inhibit**.

The following prompt displays.

The inhibit command will be executed for all posted records.

Are you sure you want to continue?

- 41** Click **Yes** to execute the command on the selected links.
- 42** Using the same screen, reselect the links. Click **Deactivate**.

The following prompt displays.

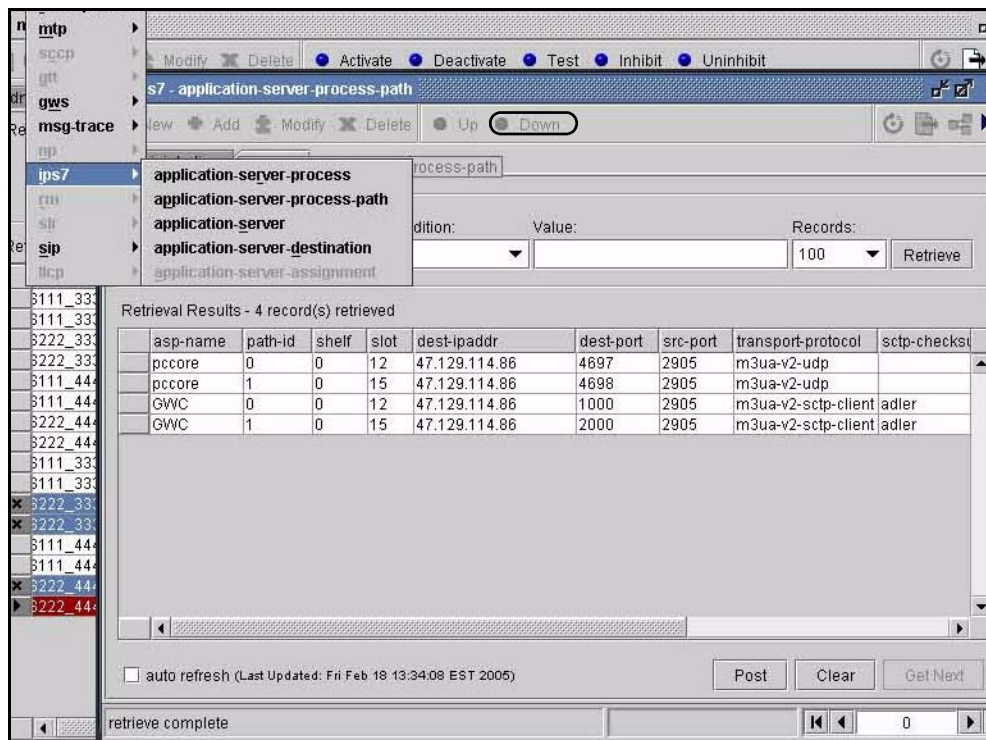
The deactivate command will be executed for all posted records.

Are you sure you want to continue?

- 43** Click **Yes** to execute the command on the selected links.
- 44** Post the IPS7 paths that use the slave USPc blade.

Select **Configuration --> ips7 --> application-server-process-path**.

The following figure displays.



- 45** Select all the IPS7 paths against the slave USPc blade. Click **Down**.

The following prompt displays:

The down command will be executed for all posted records. Are you sure you want to continue?

- 46** Click **Yes** to execute the command on the IPS7 paths on the slave USPc blade.

At this point, the IPS7 paths and SS7 links against the slave USPc blade have been deactivated.

- 47** Lock the slave USPc blade.

Select **Configuration --> platform --> Node**.

The Administration tab, as shown in [step 35](#), redisplays.

- 48** Click **Lock**.

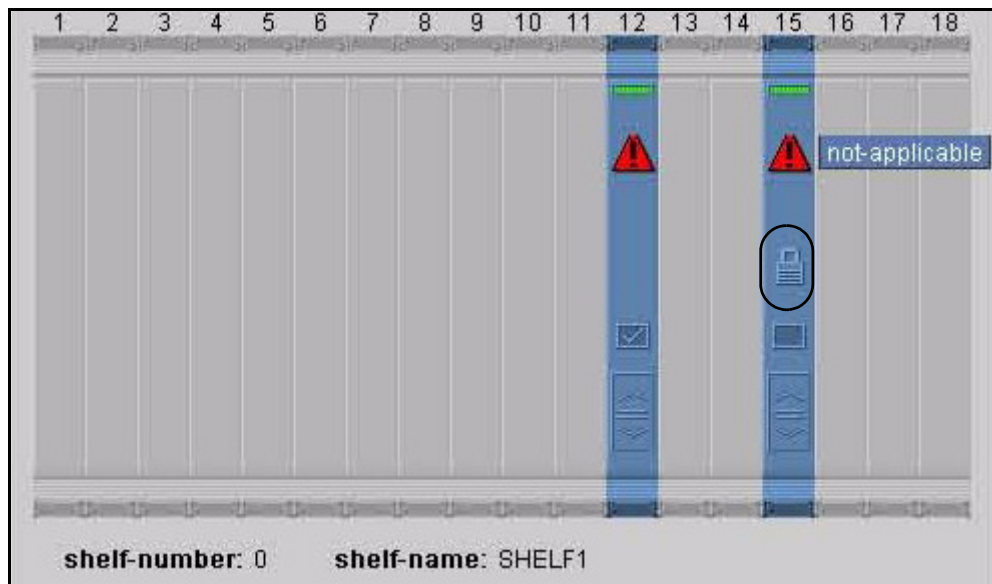
The following prompt displays:

The node lock command will impact the last in-service link from at least 1 linkset which may impact network traffic. Do you want to continue?

- 49** Click **Yes** to lock the USPc blade.

Click the Graphical View tab.

The Graphical View tab shows that the USPc blade has a lock icon next to it, indicating it has been locked.

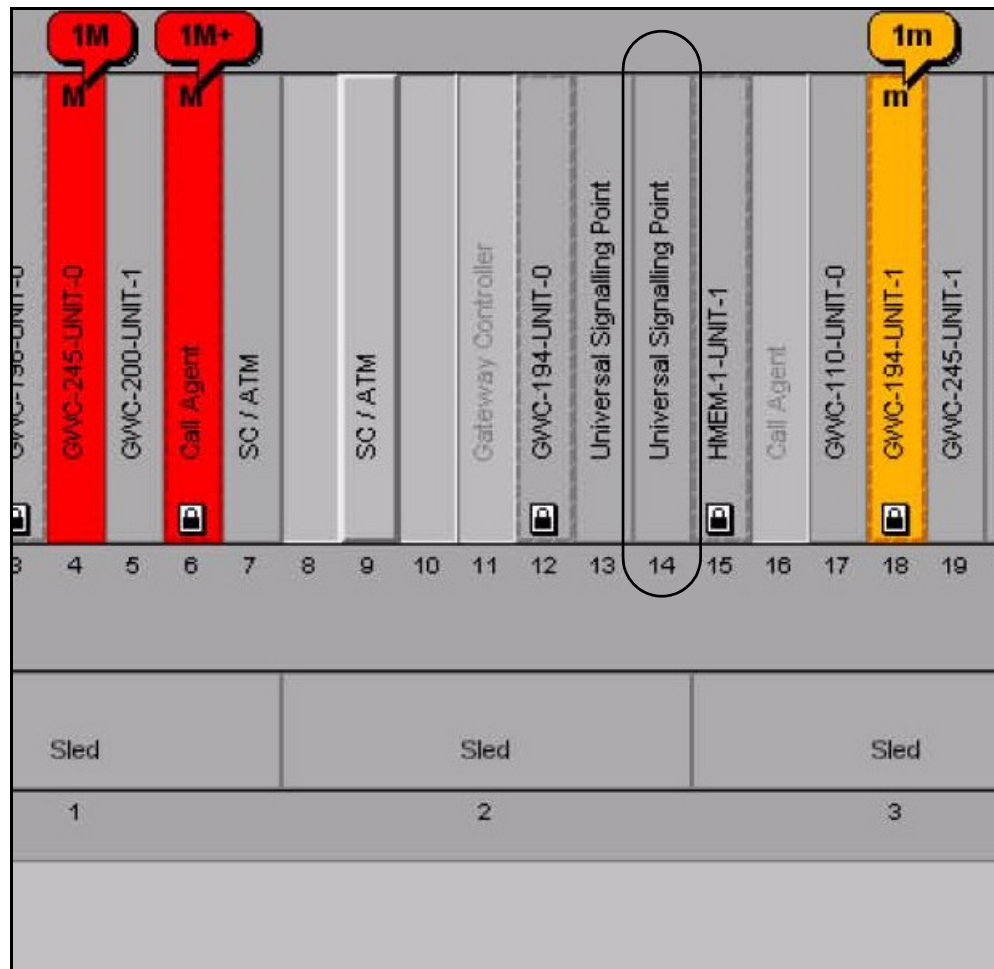


Locking the USPc blade using the SAM21 Manager

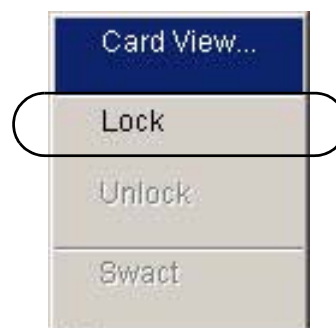
- 50** Access the SAM21 EM GUI.

- 51** Select the shelf by double clicking on its icon.

The following figure shows an example in which the slave USPc blade resides on slot 14.



- 52** Right click on the icon which corresponds to where the slave USPc blade resides.
- A sub-window appears with the Card View and Lock selections enabled.*



53 Click **Lock**.

The slave USPc blade is locked.

Note 1: *This prevents an automatic change of activity from occurring. An automatic SWACT at this point could cause a system outage.*

Note 2: *An alternative method to Lock the blade from the SAM21 EM is to first open the card by double clicking on it. Then click the Lock button towards the upper-right portion from display of the States tab.*

Determining if STORM devices require rotating, demounting and busying**54****ATTENTION**

Before proceeding with the following STORM-related steps, consider if other applications might be affected by the loss of STORM disk volumes.

55 Select the next step as follows

If	Do
STORM uses a Dothill device	step 56
STORM IA (SAM-XTS) device ¹	step 65

1. The SAM-XTS configuration uses dual-homed split multilink trunks (SMLT). Both STORM volumes are recognized by both Ethernet Routing Switch 8600 routers. Therefore, taking down one router in an SAM-XTS configuration does not affect the STORM volume being addressed.

56 Select the next step as follows

If	Do
the volumes on any STORM disk (for example, sd01) are actively mounted in DIRP ¹	step 57
the volumes on the STORM disk are not actively mounted in DIRP ²	step 65

1. Loss of network connectivity between SOS, the call processing application, and the active STORM disk can cause some or all DIRP volumes to be marked "INER-ROR," resulting in permanent loss of data.

2. Regardless of whether DIRP volumes are mounted, the procedure can result in an unavailable STORM disk and associated volumes.

- 57** Refer to your network diagram and verify that the STORM device-to-Ethernet Routing Switch 8600 connectivity in your configuration is set up as follows:
- STORM volumes prefixed with sd00 reside on STORM device 0, which *must* connect to Ethernet Routing Switch 8600 Chassis 0.
 - STORM volumes prefixed with sd01 reside on STORM device 1, which *must* connect to Ethernet Routing Switch 8600 Chassis 1.

Note: This information coincides with the network element-to-Ethernet Routing Switch 8600 assumptions stated in [step 1](#) of this procedure.

If the STORM-to-Ethernet Routing Switch 8600 connections in your configuration do not match these assumptions, adjust the commands in steps [58](#) to [64](#) to address the appropriate STORM device.

- 58** From the Core MAP command line, enter the following command to list all available DIRP subsystems (field SYSSNAME in table DIRPSSYS) for the Core.

>table dirpssys; lis all

- 59** Enter the following command to access the DIRP level in SOS by typing:

>mapci nodisp;mtc;iod;dirp

- 60** Enter the following command to query all volumes associated with the subsystem.

>query <subsystem> all

where:

<subsystem> is from the list of available subsystems executed in [step 58](#).

The following figure shows an example of this command for the dlog subsystem with an active file highlighted.


```

>query dlog all
SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL EMERGENCY
DLOG      1      1      3      7  NONE  ***YES***

REGULAR
FILE(S)   STATE VOLUME   RECCOUNT BLOCK E  V  V_B VLID FNUM FRN#
ACTIVE    AVAIL SD00DLG1      1      1 0 71 NO  8448 000D 1014
STANDBY1  AVAIL SD01DLG1      0      0 0 70 NO  8408 0015 3012

PARALLEL
FILE              STATE VOLUME   BLOCK E  V  V_B VLID FNUM FRN#
              NONE

REGULAR VOLUME(S)
VOL# VOLNAME  STATE          IOC CRD PORT VOL FSEG ROOM VLID FILES
  70 SD01DLG1 READY          N/A N/A N/A   8   10   11 8408 S1
  71 SD00DLG1 READY          N/A N/A N/A   8  112  116 8448 A

REGULAR SPACE
VOL# VOLNAME  STATE          SEGS    EXP UNEXP TOTAL
  70 SD01DLG1 READY          10      1     0    11
  71 SD00DLG1 READY         112      4     0   116

```

- 61** Rotate the active volume for each subsystem if it is located on a STORM blade connected to the router being upgraded for this iteration. Enter the following command to manually rotate all subsystems until the active files reside on STORM volumes connected to the Ethernet Routing Switch 8600 chassis that is not being upgraded for this iteration.

>rotate <subsystem> <variable>

where:

<variable> is *regular*, *parallel*, or *both* (Enter *regular* to rotate regular volumes. Enter *parallel* to rotate parallel volumes. Enter *both* to rotate both volumes.)

Note 1: Parallel is intentionally misspelled.

Note 2: Volumes associated with the slave Ethernet Routing Switch 8600 should *not* be active. Ensure that no volumes are active in each pass which are prefixed with:

sd0N

where N = 0 (first pass)

N = 1 (second pass)

For example, sd00 volumes should not be active during the first pass. Sd01 volumes should not be active during the second pass. (Rotate each subsystem with volumes prefixed with sd0N that are active.)

Note: To minimize risk, rotate and demount the AMA subsystem last. Then restore the AMA subsystem first.

The following figure shows example of input for variable regular.

```
>rotate dlog REGULAR
ACTIVE FILE WILL BE CLOSED IF POSSIBLE (ROTACLOS).
SENDING REQUEST TO SUBSYSTEM
Please confirm ("YES", "Y", "NO", or "N"):
>y
REQUEST SENT TO SUBSYSTEM, CHECK DIRP LOG FOR DETAILS
```

- 62** Repeat [step 61](#) to ensure that all volumes needing rotating have been rotated successfully.

- 63** Enter the following command to demount all DIRP volumes connected to the Ethernet Routing Switch 8600 chassis that is to be upgraded.

>dmnt <subsystem> <volume> <variable>

where:

<volume> is the volume on the STORM (prefixed with sd0N where N is defined in [Note 2](#) of [step 61](#))

<variable> is *regular* or *parallel*

Note 1: The **<variable>** parameter is not required when mounting and demounting regular DIRP volumes.

Note 2: Nortel recommends recording all subsystems, volume, and variable information for each volume being demounted in this step.

- 64** Enter the following command to Busy all STORM volumes connected to the Ethernet Routing Switch 8600 chassis to be upgraded.

>diskadm sd0N; bsy all

where:

sd0N is the STORM volume defined in [Note 2](#) of [step 61](#)

Note 1: Nortel does not recommend using option *bsy all force*.

Note 2: Issuing a bsy all command affects all volumes serviced by that STORM blade, not just those used by DIRP.

- 65 Select the next step as follows:

If the CS-LAN is used with	Do
a Trimodal solution	step 66
an ATM-based solution	step 66
an IP-based solution	step 68

Locking the inactive Shelf Controller (SC) blade connected to Chassis N using the SAM21 Manager

66

ATTENTION

During a SWACT on the SCs, flapping (that is, rapid enabling and disabling of the router port connected to a SC) can result in a temporary loss of Ethernet connectivity. This could cause ongoing failures on the newly active SC following the SWACT.

To prevent the possibility of an outage due to this condition, monitor ongoing or recent logs for Ethernet instability on the router ports that are associated with SCs.

Do **not** SWACT the SCs until all network problems involving flapping are addressed.

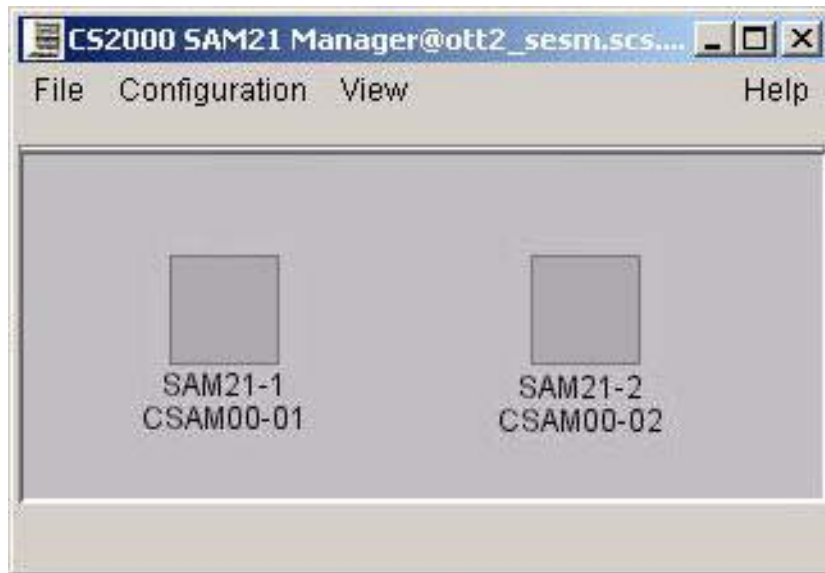
Confirm that SC blade connectivity complies with all topology recommendations.

Note: The recommendation in procedure [Performing Ethernet Routing Switch 8600 upgrade pre-checks on page 100](#) requires SC unit 0s (in slot 7) subtend Ethernet Routing Switch 8600 Chassis 0, and SC unit 1s (in slot 9) subtend Ethernet Routing Switch 8600 Chassis 1. If the SAM21shelf varies from this recommendation, adjust this procedure accordingly.

- 67 Lock the inactive SAM21 SC blade for each SAM21 shelf in turn as follows:

- a Launch the SAM21 Manager.

The SAM21 Manager GUI appears with the related shelf icons displayed.



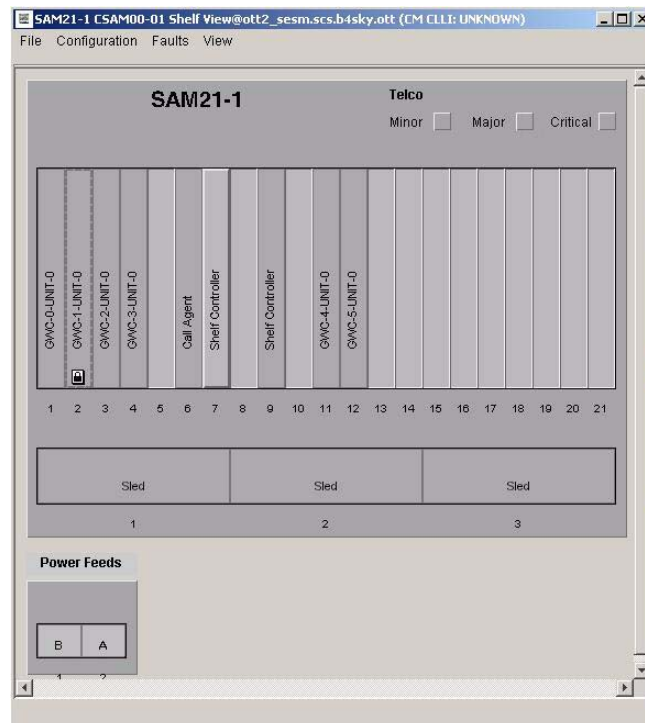
- b** Use the cursor to select the shelf icon for the first SAM21 shelf displayed.

Example

The first shelf in the figure above is SAM21-1 CSAM00-01.

- c** Double-click the selected shelf icon.

The SAM21 Manager shelf view for the selected shelf appears.



- d Right-click on the icon for the SC blade associated with the inactive Ethernet Routing Switch 8600 Chassis.

Note: The SC blade in slot 7 subtends Ethernet Routing Switch 8600 Chassis 0, slot 9 subtends Chassis 1 (see note to [step 66](#)).

A sub-window appears with the Card View and Lock selections enabled.



- e click **Card View**

The SC Card View appears.

The screenshot shows a web-based configuration interface for a Nortel device. At the top, there are tabs: Alarms, Equip, States, Diags, and Provisioning. The 'States' tab is selected. Below the tabs, there are three main sections: Activity, OSI, and History. The Activity section contains a 'Status' dropdown menu currently set to 'Active' and a 'Swact' button. The OSI section contains three dropdown menus: 'Administrative' set to 'Unlocked', 'Operational' set to 'Enabled', and 'Availability' set to 'None'. To the right of the 'Operational' dropdown are 'Lock' and 'Unlock' buttons. The History section is a large empty box with a vertical scrollbar. At the bottom of the interface are 'Save' and 'Clear' buttons.

- f Select the **State** tab and make sure the SC is inactive.
*If the SC state is **Active** , click **SWACT** to change the activity status to Inactive.*
- g Close the **Card View** .
*The **Shelf View** reappears.*
- h Right-click on the icon for the inactive SC blade.
*A sub-window appears with the **Card View** and **Lock** selections enabled.*
- i Click **Lock**.
The inactive SC blade is locked.
Note: This prevents an automatic change of activity from occurring. An automatic SWACT at this point could cause a system outage.
- j Close the **Shelf View**.
The SAM21 Manager view reappears.

k select the next step as follows

If the (inactive) SC cards are	Do
locked on all SAM21 shelves	step 95
not all locked	select the next SAM21 Shelf and go to sub step 67c

Note: Repeat sub[step 67c](#) through sub[step 67j](#) until the inactive SCs are all locked.

68 Select the next step as follows:

If your office is	Do
in a Geographic Survivability environment	step 69 through step 94
not in a Geographic Survivability environment	step 95

Locking the Media Server 2000 (MS 2000) Series node connected to Chassis N using the Integrated Element Management System (IEMS) GUI

69 Launch the IEMS GUI.

Note: Refer to NTP *Integrated EMS Basics*, NN10329-111, for details on logging into the IEMS GUI.

70 Select **Applications ---> Integrated EMS --->Network Elements**.

71 Select the MS 2000 Series node to be locked and right click on its icon.

72 Select the Config and Maintenance Tool from the pop-up menu.
The Config and Maintenance Tool launches.

Note: For details, refer to procedure "Launching the Maintenance and Configuration tool" in section *Configuring and maintaining MS 2000 devices, NTP Integrated EMS Configuration Management*, NN10330-511.

73 From the left side of the Config and Maintenance Tool screen, click **Graceful Lock** to lock the MS 2000 node.

Note: A graceful lock signals to the node that a lock has been requested. The node then stops allocating new audio resources and waits for the last resource to be freed before locking the node. (A forced lock causes the node to immediately free up any resources in use and lock the node.)

- 74 Click **Lock** to gracefully lock short-duration calls from the MS 2000 node.

Note: Since a graceful lock prevents new calls from being originated on the node, existing calls will be taken down on their own. Therefore for calls still active after an extended period of time, *it is up to the discretion of the craftsperson to determine whether to issue a forced lock, or to proceed when the Ethernet Routing Switch 8600 is rebooted.*

Dropping sync on the inactive Call Agent

- 75 Before locking the inactive Call Agent card, enter the following commands to perform a drop synchronization on the inactive Call Agent card from the active Call Agent Manager.

```
> ccamtc
> coremtc
> appl
> dpsync
```

- 76 Select the next step as follows.

If the (active) Call Agent card is	Do
connected to the ERS 8600 Chassis N	step 77
not connected to the ERS 8600 Chassis N	step 84

Use the MAP display to perform a LIMITED_PRESWACT

- 77 At the MAP display, enter the following command to initiate a limited password.

```
> BCSUPDATE; LIMITED_PRESWACT
```

Note 1: If a LIMITED_PRESWACT process fails to complete, LIMITED_PRESWACT stops and displays additional information. When this occurs, use the information to investigate and correct the problem.

Note 2: Complete all LIMITED_PRESWACT steps prior to SWACTing.

The LIMITED_PRESWACT command displays a warning:

*Limited_Preswact should not be used for
BCSUPGRADE SWACTs. Do you wish to continue?
Please confirm ("YES", "Y", "NO", "N"):*

- 78 Enter the following command to confirm.

> Y

A series of steps execute and complete. LIMITED_PRESWACT stops at MATE_RESTART_RELOAD.

```
MATE_RESTART_RELOAD           executing
There are users still logged on the Inactive.
Do you want to continue?
MATE_RESTART_RELOAD           not complete
ACT - Error: Restart aborted. Type
LIMITED_PRESWACT to continue
Investigate and correct if needed.
```

- 79** If the LIMITED_PRESWACT process halts, re-enter the following command to continue.

> LIMITED_PRESWACT

The following warning displays.

```
MATE_RESTART_RELOAD           executing
There are users still logged on the Inactive.
Do you want to continue?
Please confirm ("YES", "Y", "NO", "N"):
```

- 80** Enter the following command to confirm.

> Y

The inactive unit indicates /restart at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated by display of the following message:

```
Total execution time for all complete procedures
00:07:31.362
All LIMITED_PRESWACT steps completed
successfully.
```


Performing a NORESTARTSWACT

- 81** If the active Call Agent card is connected to the Ethernet Routing Switch 8600 to be upgraded, minimize the possibility of an outage by performing a NORESTARTSWACT.

- a** Enter the following command to check the status.

> BCSUPDATE;SWACTCI;STATUSCHECK

The following response displays:

```
SWACTCI:
Checking Nodes Status
STATUSCHECK successful
```

- b** Enter the following command to execute the NORESTARTSWACT.

> NORESTARTSWACT

Progress is printed and the process stops to verify that the inactive Call Agent is not jammed.

```
Beginning SWACT checks:
All the SWACT checks have finished
successfully.
The VR_PRESWACT_TRANSFER step completed
successfully.
All INSV and ISTB series 1 PMs will have execs
loaded after the SWACT.
Device Checking Status:
NOMATCH option is set to OFF <default
setting>.
Device matching during CC WARM SWACT Enabled.
Do you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
>
```

- c** If the only alarm is an APPL simplex alarm, enter the following command to confirm.

> Y

The final progress follows. Activity also switches at the Call Agent Manager.

```
All Pre_SWACT checks completed. Starting Warm
SWACT now.
**** The cursor will not be returned. ****
```

```
**** unless a critical failure occurs.****  
**** Now monitoring Warm SWACT messages.****
```

```
Pre-initialization done  
Communication established  
Exchange of data with the mate done  
Transfer of data done (FASPECT)  
Data estimation done
```

- d** The telnet session to the active and inactive call processing applications are lost. Re-establish the connection. Refer to section Interface set in Call Agent Upgrades for this procedure.

Performing a POSTSWACT

- 82** At the MAP display, enter the following command to run a Postswact through completion.
> BCSUPDATE;POSTSWACT
- 83** When prompted at the CA_SYNC step, enter the following command to leave the switch out of sync.
> N

Locking the inactive Call Agent card**84****CAUTION**

Possible service interruption

DO NOT ATTEMPT TO LOCK THE ACTIVE CALL AGENT CARD.

Locking the active unit causes a complete service outage.

To lock the inactive Call Agent, follow these steps:

- a Access the SAM21 EM GUI.
- b Select the SAM21 shelf by double clicking on its icon.
- c From the Shelf View, right click on the card that corresponds to the inactive Call Agent card.
- d Select the **Lock** option from the context menu.

Note: Lock is also available from the States tab of the Card View window.

- e Wait for the Lock icon to appear on the selected card.

Demounting the active DIRP volumes off of SD01

- 85** At the MAP display, enter the following command to access the DIRP level.

>MAPCI NODISP;MTC;IOD;DIRP

- 86** Enter the following commands to query the subsystem to determine which files are active and which are standby.

>QUERY JF FILES

>QUERY DLOG FILES

- 87** Enter the following commands to demount all volumes on SD01 for the subsystems that are not active.

>DMNT DLOG SD01DLG0

>DMNT DLOG SD01DLG1

>DMNT DLOG SD01DLOG2

- 88** Enter the following commands to rotate the subsystems to a standby volume on SD00.

>ROTATE JF

>ROTATE DLOG

- 89 Enter the following commands to query the subsystem again to verify that the active files are on SD00.

>QUERY JF FILES**>QUERY DLOG FILES**

- 90 Enter the following commands to demount any remaining volumes on SD01.

>DMNT JF SD01JF**>DMNT DLOG SD01DLG3**

- 91 Enter the following commands to query the subsystem again to verify that no volumes on SD01 are used.

>QUERY JF FILES**>QUERY DLOG FILES**

The display should indicate that the JF and DLOG subsystems are not using any volumes on SD01.

- 92 Repeat [step 86](#) for any additional DIRP subsystems.

- 93 Enter the following command to quit the DIRP level.

>QUIT ALL

Busying all STORM disk volumes on SD01 to ensure that the call processing application does not attempt to access the STORM unit

- 94 At the MAP display, enter the following command to busy all disk volumes on device SD01.

>DISKADM SD01;BSY ALL

If the devices do not pass, determine which application has open files. Perform maintenance on those applications so that the application closes the files.

Note: Refer to NTP Upgrading the STORM, NN10066-461, for details.

Making devices subtending Chassis X of Ethernet Routing Switch 8600 active (Chassis N devices inactive) using the Ethernet Routing Switch 8600 CLI

- 95 Enter the following command to recheck the address resolution protocol information.

sho ip arp info

The IP ARP file appears. Verify that active units subtend the Ethernet Routing Switch 8600 Chassis X (inactive units subtend Chassis N)

Note 1: *For more information IR ARP information, select option Documentation under Ethernet Routing Switch 8600 Routing Switch on the Nortel website, or contact your next level of support.*

Note 2: *If any units do not meet this requirement, repeat [step 28](#). If the problem persists, contact your next level of support.*

Restoring the original software load on Ethernet Routing Switch 8600 Chassis N using the Ethernet Routing Switch 8600 CLI

96 Select the next step as follows

If your CS-LAN:

is a dual CPU configuration

is a single CPU configuration

Do

[step 97](#)

[step 102](#)

97

ATTENTION

Before addressing any commands with a peer option, ensure that the DNS entries were created previously for each CPU. For details on creating DNS entries, refer to the v3.7.X.X Release Notes.

Due to the implementation of DNS, the peer command option is not available unless you add the peer IP address in a new file called flash/etc/hosts.

You must create this file. No default file exists. Use a simple text editor to create it, similar to the text editor provided by the Ethernet Routing Switch 8600.

For an Ethernet Routing Switch 8600 with a dual-CPU configuration, TFTP the upgrade software to the flash on the master CPU. Then copy it to the standby CPU.

In the following substeps, both commands must be executed on the master CPU.

Note: The Ethernet Routing Switch 8600 automatically copies files to the flash card using the same name as the current file. When entering the copy command if a destination name is not specified, then the system uses the same name as the source filename. Therefore, it is not necessary to enter a new filename for the backup version of this file in [step 97a](#) through [step 97e](#).

a TFTP the new software image file.

Enter the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	copy <a.b.c.d>:/swd/pp8600/XXX/<newload> /flash/
	copy /flash/<newload> peer:/flash/
CBM	copy <a.b.c.d>:/pp8600/XXX/<newload> /flash/
	copy /flash/<newload> peer:/flash/

where <a.b.c.d> is the IP address of the TFTP server, and <newload> is the name of the new software image file

b TFTP the new boot monitor image file.

Enter the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	copy <a.b.c.d>:/swd/pp8600/XXX/<newboot> /flash/
	copy /flash/<newboot> peer:/flash/
CBM	copy <a.b.c.d>:/pp8600/XXX/<newboot> /flash/
	copy /flash/<newboot> peer:/flash/

where <newboot> is the name of the new boot monitor image file

The boot flash image and software image is backed up to the PCMCIA card on the Ethernet Routing Switch 8600 Chassis N.

Note 1: If either file transfer fails, verify TFTP server IP address and connectivity with Ethernet Routing Switch 8600 Chassis N. Confirm Ethernet Routing Switch 8600 TFTP flag is set to true by typing:
config bootconfig flags info

If the **tftpd** flag is set to false, reset the flag to true by typing:
config bootconfig flags tftpd true

Confirm the flag is now set to true, then retry the transfer.
If the problem persists, contact your next level of support.

Note 2: If the transfer completes but the file is corrupted, verify original file and PCMCIA card and transfer the file again. If the problem persists, contact your next level of support.

Note 3: Compare file parameters such as file size to check for possible corruption.

- c** **Only** if Chassis N of Ethernet Routing Switch 8600 uses an ATM blade, TFTP the ATM Flash image to the Flash card on the Ethernet Routing Switch 8600 Chassis N.

Enter the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	copy <a.b.c.d>:/swd/pp8600/XXX/<newATM> /flash/
	copy /flash/<newATM> peer:/flash/
CBM	copy <a.b.c.d>:/pp8600/XXX/<newATM> /flash/
	copy /flash/<newATM> peer:/flash/

where

<newATM>

is the name of the new ATM file

Otherwise go to [step 98](#).

Note: Notes 1 and 2 from sub[step 97b](#) apply.

- d** If the Ethernet Routing Switch 8600 uses DES, TFTP the file.

Enter the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	copy <a.b.c.d>:/swd/pp8600/XXX/<newDES> /flash/
	copy /flash/<newDES> peer:/flash/

If using a(n)	Type
CBM	copy <a.b.c.d>:/pp8600/XXX/<newDES> /flash/
	copy /flash/<newDES> peer:/flash/

where **<newDES>** is the name of the new DES file

- e** If the Ethernet Routing Switch 8600 uses 3DES, TFTP the file.

Type the following commands depending on your core manager platform.

If using a(n)	Type
SDM/CS 2000 Core Manager	copy <a.b.c.d>:/swd/pp8600/XXX/<new3DES> /flash/
	copy /flash/<new3DES> peer:/flash/
CBM	copy <a.b.c.d>:/pp8600/XXX/<new3DES> /flash
	copy /flash/<new3DES> peer:/flash/

where **<new3DES>** is the name of the new 3DES file

- 98** Verify that the software has been copied to the master and standby CPUs.

- a** Enter the following command for the master CPU.

dir

- b** At the prompt of the master CPU, enter the following command for the standby CPU.

peer telnet

dir

- 99** Enter the following command to exit the standby CPU.

exit

- 100** Prepare to boot both CPUs. Select the next substep as follows.

If your CS-LAN**Do**

is a dual CPU configuration

[step 100a](#)

is a single CPU configuration

[step 100b](#)

a

WARNING

Failure to observe this step can result in loss of configuration.

Enter the following command to disable the flag setting before saving the bootconfig file.

```
config bootconfig flags ha-cpu false
```

- b** Specify the new load as the primary load from which to boot by typing

```
config bootconfig choice primary image-file  
/flash/<oldload>
```

where

<oldload>

is the name of the current software image file

Note: There is a mandatory space between **image-file** and **/flash** in the syntax this substep.

- c** Enter the following command to save the bootconfig file.

```
sav bootconfig
```

This prepares Ethernet Routing Switch 8600 Chassis N to reboot.

101

WARNING

When booting the dual CPUs, do not wait for the standby CPU to complete the boot process before booting the master CPU. Waiting results in different images on each CPU. While in the high-availability (HA) mode, booting the master CPU and the standby CPU with different software images can crash the standby CPU.

Boot both CPUs in rapid sequential order, booting the standby CPU first and immediately booting the master CPU next.

- a** In the standby CPU session, enter the following command to boot the standby CPU.

peer telnet

boot /flash/<p80b_OLDLOAD>

where

<p80b_OLDLOAD>

is the name of the current boot monitor image file, for example p80b3722.img

- b**

ATTENTION

This command upgrades the primary-image file (including the ATM-image if present) and boot monitor at the same time.

ATTENTION

Do not interrupt the reboot process. The CPU card can be damaged if the reboot is interrupted incorrectly.

Immediately boot the master CPU. In the master CPU session, enter the following command to boot the master CPU.

Go to [step 106](#).

**boot /flash/<oldboot> [config
/pcmcia/<cfgbkup>]**

- c** Ensure the bootconfig file is properly configured on the /flash (primary) and /pcmcia (secondary). Use the following table to determine your next step.

If your CS-LAN:	Do
is a dual CPU configuration	step 101d
is a single CPU configuration	step 101e

- d** For CS-LANs with a dual CPU configuration, type
sav boot

```
sav config backup /pcmcia/config.cfg standby  
/pcmcia/config.cfg
```

```
sav bootconfig backup /pcmcia/boot.cfg  
standby /pcmcia/boot.cfg
```

Go to [step 102](#).

- e For CS-LANs with a single CPU configuration to save to primary (/flash) and secondary (/pcmcia), type

```
sav config backup /pcmcia/config.cfg
```

```
sav bootconfig backup /pcmcia/boot.cfg
```

- 102** Prepare to reboot Ethernet Routing Switch 8600 Chassis N as follows:

- a Enter the following command to if the original software has already been deleted from the Ethernet Routing Switch 8600.

```
copy /pcmcia/<oldload> /flash/
```

- b Enter the following command if the original boot monitor file has already been deleted from the Ethernet Routing Switch 8600.

```
copy /pcmcia/<oldboot> /flash/
```

- c If an ATM blade exists and the original ATM image file has already been deleted from the Ethernet Routing Switch 8600, enter the following command

```
copy /pcmcia/<oldatm> /flash/
```

- d If the Ethernet Routing Switch 8600 uses DES, enter the following command to TFTP the file.

```
copy /pcmcia/<oldDES> /flash/
```

where

```
<oldDES>
```

is the name of the original DES file

- e If the Ethernet Routing Switch 8600 uses 3DES, enter the following command to TFTP the file.

```
copy /pcmcia/<old3DES> /flash
```

where

```
<old3DES>
```

is the name of the original 3DES file

- f Enter the following command to set the primary image file to the saved load.

**config bootconfig choice primary image-file
/flash/<oldload>**

Note: There is a mandatory space between **image-file** and **/flash** in the syntax this substep.

- g Enter the following command to set the primary config file to the saved configuration.

**config bootconfig choice primary config-file
/pcmcia/<cfgbkup>**

Note: Configure the primary config file to ensure that the original configuration was not changed during the upgrade process.

- h Enter the following command to save the bootconfig file.

sav bootconfig

103

ATTENTION

This command automatically upgrades the primary-image file (including the ATM-image if present) and boot monitor at the same time.



Enter the following command to roll back Ethernet Routing Switch 8600 Chassis N software upgrade.

boot /flash/<oldboot>

The Ethernet Routing Switch 8600 reboots loading the original software image. The reboot takes approximately 15 to 20 seconds. Serial connectivity is maintained during the reboot.

Note: If the reboot is unsuccessful make sure the path is correct and try again. If the problem persists contact your next level of support.

- 104 If using an XA-core, skip to [step 109](#).

105 Select the next step as follows**If the STORM disk is on****Do**

a Dothill device

[step 106](#)a STORM IA (SAM-XTS) device¹[step 109](#)

1. The SAM-XTS configuration uses dual-homed split multilink trunks (SMLT). Both STORM volumes are recognized by both Ethernet Routing Switch 8600 routers. Therefore, taking down one router in an SAM-XTS configuration does not affect the STORM volume being addressed.

106 Select the next step as follows.**If****Do**the volumes on any STORM disk (for example, sd01) are actively mounted in DIRP¹[step 107](#)the volumes on the STORM disk are not actively mounted in DIRP²[step 109](#)

1. Loss of network connectivity between SOS, the call processing application, and the active STORM disk can cause some or all DIRP volumes to be marked "INER-ROR," resulting in permanent loss of data.

2. Regardless of whether DIRP volumes are mounted, the procedure can result in an unavailable STORM disk and associated volumes.

107 Enter the following command to return to service all disk volumes connected to the Ethernet Routing Switch 8600 chassis that was upgraded.**>diskadm sd0N; rts all**

where

sd0Nis the STORM volume defined in [Note 2](#) of [step 61](#)**108** Enter the following command to individually remount all volumes in DIRP. (Ensure you are at the nodisp;mtc;iod;dirp level of the MAPCI for this step.)**>mnt <subsystem> <volume> <variable>**

Note 1: The <variable> parameter is not required when mounting and demounting regular DIRP volumes.

Note 2: Nortel recommends recording all subsystems, volume, and variable information for each volume remounted in this step.

Verifying all hardware and software on the master Ethernet Routing Switch 8600 using the Ethernet Routing Switch 8600 CLI

- 109** Confirm master Ethernet Routing Switch 8600 is operating correctly as follows:

Note: Refer to [step 3](#) of [Upgrading Ethernet Routing Switch 8600 software for the CS-LAN](#) for more information

- a** Enter the following command to check the configuration.

sho config

Output similar to the following appears.

```
#<output date and time info>
#boxtype : Passport-8010
#software version : W.X.Y.Z
#monitor version : W.X.Y.Z/NNN
#<output continues>
```

where W.X.Y.Z provides release information and the NNN can be ignored.

Review the configuration file (showing network topology and configuration) and correct any incorrect configurations.

Note: Software version is the load or image version.
Monitor version is the bootflash version.

- b** Enter the following command to check the address resolution protocol information by typing:

sho ip arp info

Review the IP ARP file and correct any MAC address problems.

- c** Select the next step as follows:

If rolling back with an	Do
Trimodal solution	step 110
ATM solution	step 110
IP solution	step 112

Unlocking the inactive SCs using the SAM21 Manager

- 110** Launch the SAM21 Manager.

The SAM21 EM GUI appears. Padlock icons identify locked SC blades.

- 111** From the SAM21 Manager shelf view, right click on each of the locked SC blades in turn and do the following:
- a** Select **Unlock** from the drop-down menu that appears.
 - b** Repeat sub^{step 111a} until all locked SC blades are unlocked.
- 112** Select the next step as follows:

If the USP Compact is:	Do
used	step 113
not used	step 149

Performing the following additional steps (for USP Compact only) using the SAM21 Manager

- 113** Re-access the SAM21 EM. Unlock the slave USPc.

Note 1: Unlocking the slave USPc from the SAM21 EM enables the USPc GUI.

Note 2: An alternative method to Unlock the blade from the SAM21 EM is to first open the card by double clicking on it. Then click the Unlock button towards the upper-right portion from display of the States tab.

Performing the following additional steps using the USPc GUI

- 114** Re-access the USPc GUI, waiting to ensure that the inactive blade is enabled and locked.

Note: Re-accessing the USPc GUI can take several minutes.

- 115** Select **Configuration --> platform --> Node**.

The Administration tab of the USPc GUI displays.

The screenshot shows the Administration tab of the USPc GUI. The interface includes a toolbar at the top with buttons for New, Add, Modify, Delete, Lock, Unlock (highlighted with a red circle), Load, Offline, Swact, and Restart. Below the toolbar are tabs for Administration, Search, and Graphical View. The main content area is divided into three sections: Provisioning Data, Operational Data, and Boot Data.

Provisioning Data

slot-type	usp-compact			
slot-name	USP1			
slot-description	USP-Compact #1			
shelf	0			
slot	15			
t1-e1-mode	t1			
ext-ip-address	47	131	125	82
ext-subnet-mask	255	255	255	128
ext-gateway	47	131	125	126
front-pec	NTRX51FN			

Operational Data

operational-state	enabled
administrative-state	unlocked
procedural-state	null
availability-state	null
activity-state	inactive
rex-status	

Boot Data

status-message	
running-image	samss7_ppc750_10_00_01_06g
ha-running-image	ss7t1e1ha_ppc8260_10_00_01_06g
running-snapshot	current active
boot image	uspc_10_00_01_06g_base
ha-boot-image	uspc_10_00_01_06g_t1e1ha
boot-snapshot	current active
snapshot-description	current active
snapshot-date	
snapshot-version	

At the bottom of the window, there is a status bar showing "loading complete" and a navigation bar with buttons for back, forward, and search.

116 Unlock the slave USPc blade.

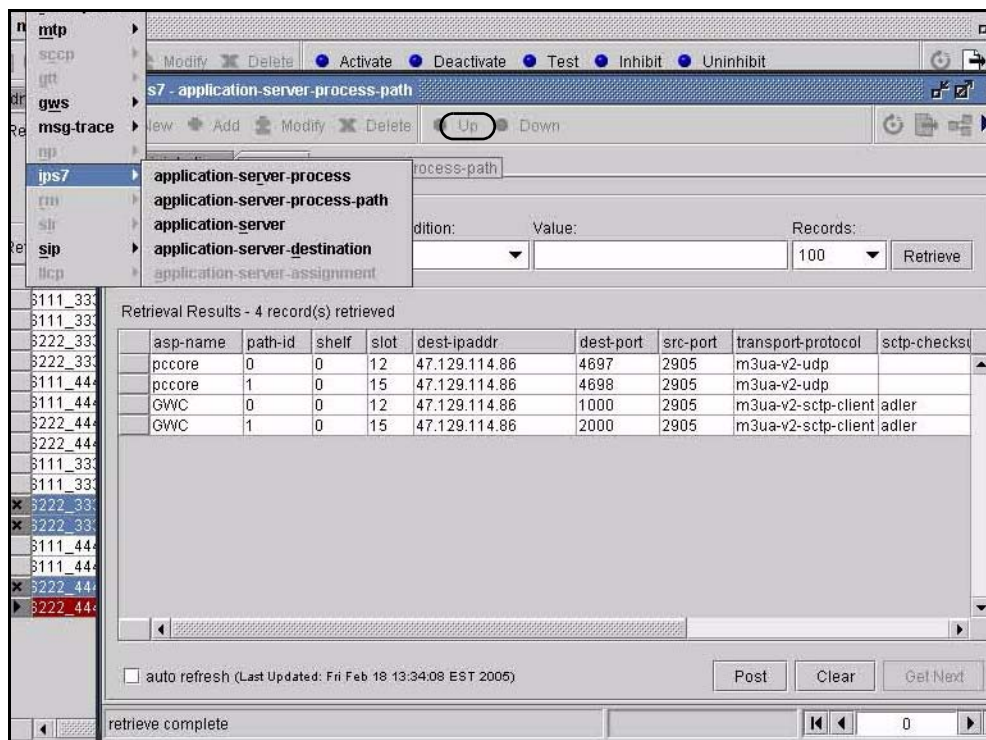
Click **Unlock**.

117 Reactivate the IPS7 paths and the SS7 links associated with the slave USPc blade.

118 Post the IPS7 paths that use the slave USPc blade.

From the menu, select **Configuration --> ips7 --> application-server-process-path** from the pull-down menu.

The following figure displays.



- 119** Select all the IPS7 paths against the slave USPc blade. Click the Up button in the upper-right portion of the screen.

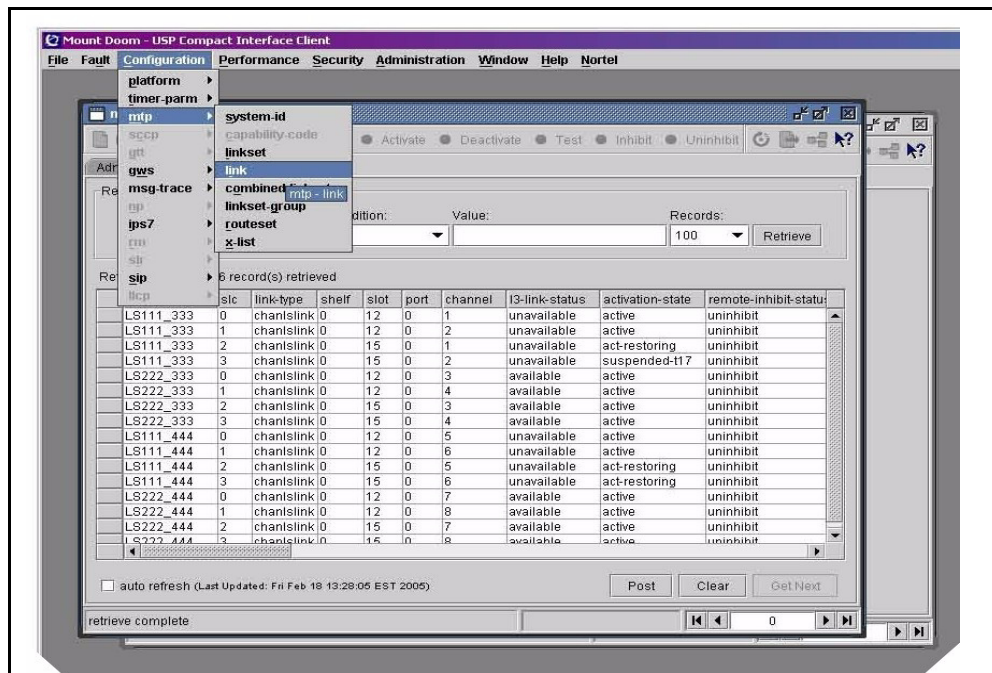
The following prompt displays:

The up command will be executed for all posted records. Are you sure you want to continue?

- 120** Click **Yes** to execute the command on the IPS7 paths on the slave USPc blade.
- 121** Reactivate the SS7 links and the paths associated with the slave USPc blade.

From the Administration tab, select **Configuration --> MTP --> Links** from the pull-down menu.

The following figure appears.



122 Select any SS7 links displayed in the form that are against the slave blade. Click the **Activate** button towards the upper-middle portion of the screen.

123 Click **Yes** to execute the command on the selected links.

124 Using the same screen, reselect the links. Click **Uninhibit** in the upper-right portion of the screen.

125 Click **Yes** to execute the command on the selected links.

126 If desired, perform an optional SWACT on the USPc blades to restore initial mastership states.

To perform a SWACT, redisplay the Administration tab, as shown in [step 115](#). Click **Swact**.

127 Select the next step as follows:

If your office is

Do

in a Geographic Survivability environment

[step 128](#) through
[step 148](#)

not in a Geographic Survivability environment

[step 150](#)

Unlocking the inactive Call Agent card using the SAM21 Manager

- 128** Re-access the SAM21 EM. Unlock the locked inactive Call Agent card.

Note: An alternative method to Unlock the blade from the SAM21 EM is to first open the card by double clicking on it. Then click the Unlock button towards the upper-right portion from display of the States tab.

- 129** Wait for the lock icon to disappear.
- 130** At the Call Agent Manager, verify that the call processing application loads successfully and waits for synchronization.

Performing a LIMITED_PRESWACT on the inactive Call Agent Use the MAP display

- 131** If the switch is in sync, enter the following commands to perform a drop synchronization from the ccamtc apply level.

```
> ccamtc
> coremtc
> appl
> dpsync
```

- 132** At the MAP display, enter the following command to perform a limited PRESWACT.

```
> BCSUPDATE; LIMITED_PRESWACT
```

Note 1: If a LIMITED_PRESWACT process fails to complete, LIMITED_PRESWACT stops and displays additional information. When this occurs, use the information to investigate and correct the problem.

Note 2: All LIMITED_PRESWACT steps must be completed prior to swacting.

The LIMITED_PRESWACT command displays a warning:

```
Limited_Preswact should not be used for
BCSUPGRADE SWACTs. Do you wish to continue?
Please confirm ("YES", "Y", "NO", "N"):
```

- 133** Enter the following command to confirm.

```
> Y
```

- 134** If the LIMITED_PRESWACT process halts, re-enter the following command to continue.

```
> LIMITED_PRESWACT
```

The inactive unit indicates /restart at the Call Agent Manager. Several more steps execute and complete at the MAP. Successful completion is indicated by display of the following message:

*Total execution time for all complete procedures
00:07:31.362
All LIMITED_PRESWACT steps completed
successfully.*

135 Select the next step as follows

If the (inactive) Call Agent card is	Do
not connected to the ERS 8600 being upgraded	step 136
connected to the ERS 8600 being upgraded	step 150

Performing a NORESTARTSWACT

136 If the active Call Agent card is connected to the Ethernet Routing Switch 8600 to be upgraded, minimize the possibility of an outage by performing a NORESTARTSWACT.

- a** Enter the following command to check the status.

> BCSUPDATE:SWACTCI;STATUSCHECK

The following response displays:

*SWACTCI:
Checking Nodes Status
STATUSCHECK successful*

- b** Enter the following command to execute the NORESTARTSWACT.

> NORESTARTSWACT

Progress is printed and the process stops to verify that the inactive Call Agent is not jammed.

*Beginning SWACT checks:
All the SWACT checks have finished
successfully.
The VR_PRESWACT_TRANSFER step completed
successfully.
All INSV and ISTB series 1 PMs will have execs
loaded after the SWACT.
Device Checking Status:
NOMATCH option is set to OFF <default
setting>.
Device matching during CC WARM SWACT Enabled.*

*Do you wish to continue?
Please confirm ("YES", "Y", "NO", or "N"):
>*

- c** If the only alarm is an APPL simplex alarm, enter the following command to confirm.

> Y

The final progress follows. Activity also switches at the Call Agent Manager.

All Pre_SWACT checks completed. Starting Warm SWACT now.

***** The cursor will not be returned. ****
**** unless a critical failure occurs. ****
**** Now monitoring Warm SWACT messages. *****

*Pre-initialization done
Communication established
Exchange of data with the mate done
Transfer of data done (FASPECT)
Data estimation done*

- d** The telnet session to the active and inactive call processing applications are lost. Re-establish the connection. Refer to the Interface set in section Call Agent Upgrades for this procedure.

Performing a POSTSWACT

- 137** At the MAP display, enter the following command to run a Postswact through completion.

> BCSUPDATE;POSTSWACT

- 138** When prompted at the CA_SYNC step, enter the following command to confirm.

> Y

Verifying availability of NFS mounts on STORM

- 139** At the Call Agent Manager, enter the following command to query the NFS mounts to ensure that they are accessible on STORM 1.

> ccamtc

> coremtc

> sys

> querynfs

- 140** From the resulting screen display, verify that all mounts are accessible.
- 141** Select the next step as follows.

If all mounts	Do
are accessible	step 142
are not accessible	Refer to procedure “Verify NFS Availability” in NTP <i>Upgrading the STORM</i> , NN10066-461.

Returning to service disk volumes on SD0X

- 142** Enter the following command to return to service all disk volumes connected to the Ethernet Routing Switch 8600 chassis that were upgraded.

>diskadm sd0N; rts all

where:

sd0N is the STORM volume defined in [Note 2](#) of [step 61](#)

Mounting DIRP volumes

- 143** Enter the following command to individually remount all volumes in DIRP. (Ensure you are at the nodisp;mtc;iod;dirp level of the MAPCI for this step.)

>mnt <subsystem> <volume> <variable>

Note 1: The <variable> parameter is not required when mounting and demounting regular DIRP volumes.

Note 2: Nortel recommends recording all subsystems, volume, and variable information for each volume remounted in this step.

Unlock the MS 2000 node using the IEMS GUI

- 144** Launch the IEMS GUI.

Note: Refer to NTP *Integrated EMS Basics*, NN10329-111, for details on logging into the IEMS GUI.

- 145** Select **Applications ---> Integrated EMS --->Network Elements**.

- 146** Select the MS 2000 Series node to be unlocked and right click on its icon.

- 147** Select the Config and Maintenance Tool from the pop-up menu.
The Config and Maintenance Tool launches.

148 From the left side of the Config and Maintenance Tool screen, click the **Unlock** button under the Lock State options to unlock the MS 2000 node.

149 Select the next step as follows:

If the Communication Server uses:

Do

an XA-Core

[step 150](#)

a Compact chassis

[step 152](#)

Enabling the Ethernet link with Ethernet Routing Switch 8600 Chassis N using the XA-Core MAP terminal

150 Enter the following command to access the ETHR level of the MAP display.

MAPCI;XAC;MTC;ETHR

151 Enable the Ethernet link between the XA-Core and Ethernet Routing Switch 8600 Chassis N. Enter the following command:

rts <slot> r link



HIOPs/HCMICs

N = 0

N = 1

<slot>

5

14

Resetting the VRRP priority settings and OSPF cost metrics and swap the Ethernet Routing Switch 8600 master/slave status using the Ethernet Routing Switch 8600 CLI

152 Make sure Ethernet Routing Switch 8600 Chassis N is in service as follows:

a Enter the following command to check the IP route information.

sho ip route info

The IP route information file appears. Review the file and verify that the route information is correct.

b Enter the following command to check the IP VRRP information.

sho ip vrrp info

The IP vrrp information file appears. Review the file and verify that the information is correct.

- 153** Reset the VRRP priority and OSPF metrics for Chassis N as follows:

a type:

config vlan <vid> ip vrrp <vrid> prio <setting>

Note: See [step 2](#) for <vid> and <vrid> values for Chassis N.

The VRRP priority metric is reset to its operational value.

b type:

config vlan <vid> ip ospf metric <value>

Note: See [step 2](#) for the OSPF metric for <value>.

The OSPF metrics reset to their original value.

- c** Enter the following command to save the new Ethernet Routing Switch 8600 configuration.

sav config

This updates the new Ethernet Routing Switch 8600 configuration so that VRRP settings are maintained after any subsequent reboot.

- 154** Enter the following command to swap the Ethernet Routing Switch 8600 master/slave status on Chassis X.

config vlan <vid> ip vrrp <vrid> priority <prio>

where <prio> is priority information that determines which Ethernet Routing Switch 8600 is master and which one is slave.

Note 1: Refer to [step 2](#) for the applicable <vid>, <vrid>, and <prio> values.

Note 2: The Ethernet Routing Switch 8600 <prio> is higher for the master Ethernet Routing Switch 8600 chassis than for slave.

The master Ethernet Routing Switch 8600 becomes the new slave Ethernet Routing Switch 8600 (the old slave Ethernet Routing Switch 8600 becomes the new master).

- 155** Increment the iteration index ($N = N+1$) and select the next step as follows:

If	Do
$N = 1$	step 3 (second pass)
$N = 2$	step 156

Note: In the second iteration (where $N = 1$), when repeating [step 3](#) through [step 155](#), use Chassis X in place of Chassis N. Ethernet Routing Switch 8600 Chassis 1 (identified as Chassis N) is the slave and Ethernet Routing Switch 8600 Chassis 0 (identified as Chassis X) is the master.

- 156** The procedure is complete.

Using FTP

Application

This procedure is used for the command-line utility file transfer protocol (FTP) to perform the following tasks:

- transfer a file from a remote device, such as a server or another workstation, to your workstation
- transfer a file from your workstation to a remote device, such as a server or another workstation

Prerequisites

This procedure has the following prerequisites:

- You must know the name of the file.
- You must know the IP address of the remote device.
- You must know how to log in to the remote device, and be in possession of both userid and password.
- You must know the name of the directory on your workstation.

Action

Perform each of the following procedures as necessary.

Transferring a file to your workstation

At your workstation

- 1 Open a command prompt window.
- 2 Make sure you are located in the directory that will receive the files. If necessary, use the `cd` command to change directories.
- 3 Start an FTP session by typing

```
# ftp <device_ip_address>
```

and pressing the Enter key.
where
device_ip_address
is the IP address of the remote device where the files reside
- 4 When prompted, enter your user ID and password.

- 5 Change the transfer mode to binary by typing
`ftp> bin`
and pressing the Enter key.
- 6 List the directories on the remote device by typing
`ftp> ls`
and pressing the Enter key.
- 7 Locate the directory that contains the files you want to receive.
If necessary use the `cd` command to change directories.
- 8 List the contents of the directory by typing
`ftp> ls -l`
and pressing the Enter key.
- 9 Locate the file you want to receive.
- 10 Copy the file to your workstation by typing
`ftp> get <file_name>`
and pressing the Enter key.
where
file_name
is the name of the file
- 11 End the FTP session by typing
`ftp> bye`
and pressing the Enter key.
- 12 List the contents of the directory to ensure the files successfully transferred to your workstation by typing
`# ls -l`
and pressing the Enter key.
You have completed this procedure.

Transferring a file from your workstation

At your workstation

- 1 Make sure you have located the directory that contains the file.
If necessary, use the `cd` command to change directories.
- 2 Open a command prompt window.

- 3 List the contents of the directory by typing
`ftp> ls -l`
and pressing the Enter key.
- 4 Make sure the directory contains the file you want to copy.
- 5 Start an FTP session by typing
`# ftp <device_ip_address>`
and pressing the Enter key.
where
device_ip_address
is the IP address of the remote device
- 6 When prompted, enter your user ID and password.
- 7 Change the transfer mode to binary by typing
`ftp> bin`
and pressing the Enter key.
- 8 List the directories on the remote device by typing
`ftp> ls`
and pressing the Enter key.
- 9 Locate the directory that contains the files. If necessary use the `cd` command to change directories.
- 10 List the contents of the directory by typing
`ftp> ls -l`
and pressing the Enter key.
- 11 Copy the file to the remote device by typing
`ftp> put<file_name>`
and pressing the Enter key.
where
file_name
is the name of the file
- 12 List the contents of the directory to ensure the files successfully transferred to the device by typing
`# ls -l`
and pressing the Enter key.

- 13** End the FTP session by typing
ftp> **bye**
and pressing the Enter key.
You have completed this procedure