Copyright © 2006, Nortel Networks

Upgrading the Core and Billing Manager 850: Application Installation and Upgrade Guide

Introduction

Software for the Core and Billing Manager are delivered in the form of software packages and software patches. The software packages are delivered either on CD-ROM or by way of the electronic software delivery (ESD) method through a high-speed internet connection. Patches can also be delivered either on CD-ROM or through ESD. Starting with release CBM009, however, the Network Patch Manager (NPM) residing on SSPFS is used to deliver software patches. The upgrade to CBM009 software load incorporates NPM configuration on the CBM.

This document contains the procedures for upgrading the CBM 850 cluster to a new software release, for applying or removing software packages to or from the CBM 850 cluster, and for patching the CBM 850 cluster.

What's new in Upgrading the Core and Billing Manager 850 in SN09

Features changes

The following feature-related changes have been made in the documentation:

- The OMDD enhancements and robustness feature required changes in the procedure, Installing optional software on a CBM 850
- The CBM-NPM patching convergence feature required changes to Upgrading the CBM 850 procedure and the addition of NPM-related procedures

Other changes

There are no other changes in this release.

Upgrading the CBM 850

Upgrading the CBM 850 involves upgrading both the SSPFS platform and software, and upgrading the CBM 850 software. The SSPFS upgrade consists of two processes; upgrading the Solaris operating system and upgrading the SSPFS software. The CBM upgrade also consists of two processes; preparing the CBM upgrade media and applying and patching the new CBM software. The CBM upgrade is automatically initiated during the SSPFS upgrade.

Guide to the CBM 850 upgrade procedures

The following table provides a list of the procedures used to perform a CBM 850 upgrade.

Procedure
Upgrading the CBM 850 on page 4

Software package application

Although many software packages are applied to a CBM 850 node during CBM installation, some software packages require manual configuration and must be applied to the CBM 850 at a different time. Such packages can be installed through the apply level of the cbmmtc user interface.

You may also remove software packages that have been installed on the CBM 850, through the packages level of the cbmmtc user interface. When a software package is removed, file systems associated with that package are not removed from the system and cannot be removed automatically. The data within those file systems are removed.

Viewing software transaction history and logs on the CBM 850

Through the history level, the cbmmtc user interface also allows you to view additional details about the package transactions, either package installations, package configurations, or package removals, that you have performed. This additional detail includes a log file and the results of the individual operations that were performed.

Querying the system for package information using Queryloads

The SIM Queryloads tool provides an interface used for gathering information about software application packages installed on the system. The tool can also be used to obtain software package baseline information. Information can be presented either as a formatted report or as raw extensible markup language (XML) data.

Guide to the software package application procedures

The following table provides a list of the procedures you can perform to install software application packages.

Procedure
Installing optional software on a CBM 850 on page 208
Removing software packages from a CBM 850 on page 245
Viewing software transaction history and logs on the CBM 850 on page 251
Using the Queryloads tool to display patches and packages applied on the CBM 850 on page 253

Patch Management

Beginning with release SN09, software patches are applied and managed through the Network Patch Manager (NPM). The NPM is packaged with SSPFS. The NPM is equipped to manage patches both manually through a command line interface or graphical user interface (GUI) and through scheduled automatic application. Any patching failures raise alarms within the NPM. The NPM treats the servers in a CBM 850 cluster individually as separate devices and ensures that only one device is restarted at a time.

Note: In a Succession Carrier Voice over IP network, the Integrated EMS hosts the NPM. In a TDM network, the CBM 850 hosts the NPM. If you are unsure as to where the NPM resides in your network, contact your next level of support.

Guide to the NPM patching procedures

The following table provides a list of the patching procedures you can perform.

Procedure
Applying patches to a CBM on page 82
Removing patches from a CBM on page 83

Upgrading the CBM 850

This procedure contains the steps required for upgrading the Core and Billing Manager 850 to release (I)SN09. The procedure supports upgrades from either release (I)SN07 or (I)SN08.

Upgrade strategy

Upgrading the CBM 850 involves upgrading both the SPFS platform and software and upgrading the CBM 850 software. The SPFS upgrade consists of two processes:

- upgrading the Solaris operating system
- upgrading the SPFS software

The CBM upgrade also consists of two processes:

- preparing the CBM upgrade media
- 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. As a consequence, the out-of-service time for the CBM 850 cluster is limited to the duration of this CBM 850 cluster swact.

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 during the upgrade, the inactive node can still assume control.

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. A clone is required to return both nodes to the previous SPFS and CBM 850 release.

Procedures

Upgrading the CBM 850 consists of the following tasks:

Preparing to upgrade the CBM 850

ATTENTION
Before starting the upgrade procedure, ensure that no other users are logged on to the system. The presence of other users logged on to the system can have adverse affects on the upgrade process and could cause the upgrade to fail.

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use the following table as a checklist, and place a check (√) in the √ column as you complete each procedure.

(I)SN09 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
On the INACTIVE node			
1	Verify the state of the cluster.		Perform the procedure Verifying the state of a cluster on page 34
On the ACTIVE node			
2	Ensure that adequate backup space is available on the core for the duration of the scheduled maintenance window if you have not done so already. During the CBM 850 upgrade, the billing application will briefly go into backup.		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.
3	Ensure that you have the appropriate software media, either CD-ROM or an ISO image for ESD application.		If you are updating the CBM 850 cluster using ESD, ensure that the CBM iso.gz.tape image is located in the /swd/sdm directory, on the ACTIVE node of the CBM 850 cluster. If necessary, perform the procedure,Transferring a compressed ISO image to a CBM server on page 59.

(I)SN09 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
4	Ensure that the SN07/SN08 CBM 850 system is patch-current.		Either perform the procedure established by your company for ensuring that the system is patch-current or perform the procedure Ensuring that the CBM 850 running an SN07 or SN08 load is patch-current on page 20.
5	Prior to the upgrade, verify that these file systems on your inactive node have at least the minimum amount of available space. / = 1550000 kilobytes (757 Mb) To display the available space in kilobytes, type df / /opt = 1800000 kilobytes (879 Mb) To display the available space in kilobytes, type df /opt /var = 1200000 kilobytes (586 Mb) To display the available space in kilobytes, type df /var		If required, refer to procedure “Verifying disk utilization on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.
6	Ensure that no SBA alarms are currently raised.		Check for alarms using procedure “SBA alarm troubleshooting” in *Core and Billing Manager 850 Fault Management*, NN10351-911
7	Ensure that all CBM software applications are in-service or are off-line.		At the command line, enter the following command: **`appctrl -q all`** If the status of any application listed is not either in-service or off-line, return the application to service using the CBMMTC maintenance interface.

(I)SN09 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
8	Perform a full system backup on the current load.		Perform Performing a backup of file systems on an SSPFS-based server on page 78

(I)SN09 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
9	Ensure that all SN09 CBM patches are transferred to the CBM patch dropbox (NPM dropbox) prior to starting the upgrade procedure. ***Important:*** In SN09, the CBM patch manager is changing to the Network Patch Manager (NPM). Moving to NPM will change how the sort and filter capabilities work to access CBM patches on Nortel.com. Due to the increased amount of detail, it is strongly advised to take advantage of the Patch Audit Inform Calculator or the Pre-Upgrade Calculator tools. Both are located under the Tools tab of the Core and Billing Manager Product heading.		Perform the following steps: 1. Go to http://www.nortel.com 2. In the Support and Training tab pull-down, click Software Downloads. 3. In the Find Products window, click Find by: Families 4. In the Product Families window, click DMS. 5. In the DMS: General Availability list, click Software under Core and Billing Manager (CBM). 6. Click Pre Upgrade Patch Calculator. You will be required to provide a login ID and password for this activity. 7. Click Pre Upgrade Patch Calculator Readme [readme] for instructions. 8. Click Patch Audit for Inform Lists. 9. Click Patch Audit User Guide [readme] for instructions. 10. Click Patch Audit Application. 11. Enter path and filename of the inform list from site (or use Browse to find the file). 12. Determine where the dropbox for the patches will be on your CBM. 13. In the sorted patch list that displays, click each patch, and then follow the instructions shown to copy the patch to your PC. You will be required to provide a login ID and password for this activity. 14. FTP the patches you copied to your PC to the patch dropbox on your CBM.

(I)SN09 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
10	Ensure that all SN09 SPFS patches are transferred to the CBM patch dropbox (NPM dropbox) prior to starting the upgrade procedure.		Perform the following steps: 1. Go to http://www.nortel.com 2. In the Support and Training tab pull-down, click Software Downloads. 3. In the Find Products window, click Find by: Families 4. In the Product Families window, click Succession. 5. In the Succession: General Availability list, click Tools under Succession Communication Server 2000. 6. Click Pre Upgrade Patch Calculator. You will be required to provide a login ID and password for this activity. 7. Click Pre Upgrade Patch Calculator Readme [readme] for instructions. 8. Click Patch Audit for Inform Lists. 9. Click Patch Audit User Guide [readme] for instructions. 10. Click Patch Audit Application. 11. Enter path and filename of the inform list from site (or use Browse to find the file). 12. After all patches are downloaded, ftp the patches to the patch dropbox on your CBM.

(I)SN09 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
11	Copy the SPFS and CBM patches to the CBM active node. ***Important:*** Execute this step only if the NPM server will reside on the CBM after the CBM is upgraded to release SN09.		Perform Obtaining the NPM patch files for a CBM before a CBM upgrade on page 29 You have completed the steps in the CBM 850 upgrade preparation checklist. Proceed to (I)SN09 CBM 850 upgrade checklist on page 12

Upgrading the CBM 850

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use the following table as a checklist, and place a check (√) in the √ column as you complete each procedure.

(I)SN09 CBM 850 upgrade checklist

	Activities	√	Procedures
On the INACTIVE node			
1	Start the SPFS platform and software upgrade.		Perform Upgrading SSPFS software on page 38
2	Select the CBM 850 upgrade media.		Perform the procedure, Selecting the CBM upgrade media on page 21.
3	Confirm the CBM media upgrade selection.		Perform the procedure, Confirming the upgrade media selection on page 23

(I)SN09 CBM 850 upgrade checklist

	Activities	√	Procedures
4	Observe the CBM upgrade sequence		When the CBM upgrade portion begins, observe the following sequence of events on the Inactive console: a. Verification occurs 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. b. The upgrade program checks for any Major or Critical alarms on either node and notifies you with information about any alarms that have been found. ***Important:*** If problems are encountered at this point of the upgrade, it is recommended that you enter a maintenance shell and correct the error(s). Once you have corrected the errors and exit from the maintenance shell, the system will check the status of the alarms that you have addressed. c. The CBM program examines the upgrade environment and prepares the system for the CBM upgrade. d. Any required CBM packages are applied. e. The SWIM tool upgrades the value-added software currently running on the CBM. f. Any patches that are present on the CBM ISO image are applied. g. Additional tasks are performed, such as preserving logs, preparing data formatting, removing the old release from the upgrade environment, creating load baseline information, and checking the system for alarms.

(I)SN09 CBM 850 upgrade checklist

	Activities	√	Procedures
5	Observe the completion of the CBM setup program and automatic resumption of the SPFS upgrade script.		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. ***Important:*** If you are using SPFS and CBM CDROMs for the upgrade, you are prompted to reinsert an SPFS upgrade CDROM disk into the DVD drive. After inserting the CDROM 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: ***Note:*** 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. a. An activation of the new SN09 boot environment occurs. b. A message may display about how to manually reset the boot device in the event the pending reboot fails c. Two reboots occur automatically. After the first reboot, you must press the return key. ***Note:*** The first reboot takes considerably longer than a normal node reboot.

(I)SN09 CBM 850 upgrade checklist

	Activities	√	Procedures
6	Determine whether you wish to complete the upgrade.		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 25. If you do not want to complete the upgrade because of problems with the upgrade, perform procedure Executing a fallback during an SSPFS-based server upgrade on page 74. (See “Executing a fallback during an SSPFS-based server upgrade” in *ATM/IP Fault Management*, NN10408-900).
7	Complete the upgrade.		Go to Completing the CBM 850 upgrade on page 16.

Completing the CBM 850 upgrade

Perform the activities listed in the table that follows. Each activity references the procedure that contains the detailed steps.

Use the following table as a checklist, and place a check (√) in the √ column as you complete each procedure.

(I)SN09 CBM 850 upgrade completion checklist

	Activities	√	Procedures
On the INACTIVE node			
1	Install any SPFS MNCLs.		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	Configure the Patching Server Element (PSE) on the CBM.		Perform Configuring PSE on a CBM on page 84 ***Important:*** In a Succession Carrier Voice over IP network, the Integrated EMS hosts the NPM. In a TDM network, the CBM 850 hosts the NPM. If you are unsure as to where the NPM resides in your network, contact your next level of support. If you need to configure the NPM on the CBM 850 in your TDM network, perform Configuring NPM on an SSPFS server on page 86
3	Apply any SPFS and CBM patches for the new software release.		If upgrading a CBM on a TDM network, perform the procedure, Patching the inactive node of a cluster during an upgrade on page 102. If upgrading a CBM in a Succession Carrier Voice over IP network, perform the procedure, Applying patches using the NPM on page 125
On the ACTIVE node			
4	Ensure that no SBA alarms are currently raised.		To check for alarms use procedure “SBA alarm troubleshooting” in *Core and Billing Manager 850 Fault Management,* NN10351-911.

(I)SN09 CBM 850 upgrade completion checklist

	Activities	√	Procedures
5	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 SBADVDWRITE" in *Core and Billing Manager 850 Accounting,* NN10363-811.
6	Swact the nodes to bring up services on the upgraded node making it the active node.		Perform a swact of the nodes by entering the following command on the active node: `init 6` When the swact completes, continue with the next step.
7	Determine whether both the SPFS and CBM upgrades are successful up to this point.		Perform procedure Performing an active CBM 850 upgrade post-swact sanity check on page 27

(I)SN09 CBM 850 upgrade completion checklist

	Activities	√	Procedures
8	Start the NPM server. ***Important:*** Execute this step only if the NPM server resides on the CBM.		Enter the following command: **servstart NPM** If you want to enable automatic patch delivery on the CBM, perform Configuring NPM for automatic patch file delivery on page 106. If you are not enabling automatic patch delivery on the CBM, perform Obtaining the latest NPM patch files for a CBM after a CBM upgrade on page 32
9	Choose either to accept the new environment permanently or to roll back to the state prior to the upgrade and lose all upgrade work.		Perform procedure Confirming the upgrade on an SSPFS-based server on page 195
10	Clone the image of the upgraded server onto the other server. ***Important:*** Only perform this procedure at this point if you accepted the upgraded environment.		Perform procedure Cloning the image of one server in a cluster to the other server on page 197
11	If you have decided to accept the new environment permanently, perform a full system backup on the new load.		Perform Performing a backup of file systems on an SSPFS-based server on page 78

(I)SN09 CBM 850 upgrade completion checklist

	Activities	√	Procedures
12	If you have decided to accept the new environment permanently, upgrade and configure client-side application software on the required workstations in your network.		For upgrading purposes, see Installing optional software on a CBM 850 on page 208 (“Installing Optional Software on a CBM 850” in *Upgrading the Core and Billing Manager 850*, NN10347-461). For configuration procedures, see *Core and Billing Manager 850 Configuration Management,* NN10353-511 and *Core and Billing Manager 850 Accounting*, NN10363-811 for the procedures to use.
13	You have completed upgrading this CBM 850 cluster.		If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Ensuring that the CBM 850 running an SN07 or SN08 load is patch-current

ATTENTION
Perform this procedure only on a CBM 850 that is running software load SN07 or SN08.

At your workstation

1 Launch your web browser.

2 Go to http://www.nortel.com

3 In the Support and Training tab pull-down, click Software Downloads.

4 In the Find Products window, click Find by: Families.

5 In the Product Families window, click Succession.

6 In the Succession: General Availability list, click Software under Core and Billing Manager (CBM).

7 Click Filter and Sort.

8 In the Filter and sort category pull-down lists, select the appropriate order code that maps to the “from side” release for the specific upgrade. For example, if you are upgrading from CBM07, filter on CBM00070.

9 In the sorted patch list that displays, click each patch, and then follow the instructions shown to copy the patch to the appropriate directory on your system for the patches.

10 Ensure that the /swd/fixes/incoming directory exists. To create the directory, type:

```
mkdir /swd/fixes/incoming
```

11 Ftp the patches from the intermediate location to the /swd/fixes/incoming directory on the active node of the CBM 850.

12 Apply the patches on the CBM 850 by logging in to the active node of the CBM 850 as the root user and then issuing the following command:

```
patchctrl -d /swd/fixes/incoming
```

13 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 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,

the following banner and prompt displays:

```
=======================================================
         CBM Upgrade Media Setup
=======================================================
Verify SSPFS Boot Environment (est. 2 sec) ... Completed. Verify
Remote Node communication (est. 3 sec) ... Completed.
Please select the software delivery method that is being used
for the CBM load?
- enter 'esd' if Electronic Software Delivery is being used
- enter 'cdrom' if CDROM is being used
- enter 'shell' to suspend the upgrade and enter a Maintenance
Shell.
- enter 'fallback' to cancel the entire UPGRADE procedure

choice (esd | cdrom | shell | fallback):
```

2 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 **cdrom** 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 3 in (I)SN09 CBM 850 upgrade checklist on page 12.
you entered cdrom	Return to step 3 in (I)SN09 CBM 850 upgrade checklist on page 12.
you entered shell	See step 3 for a description of the system response and the next action you can perform.
you entered fallback	See step 4 for a description of the system response and the next action you can perform.

3 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. 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.

4 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 Executing a fallback during an SSPFS-based server upgrade on page 74. (See “Executing a fallback during an SSPFS-based server upgrade” in *ATM/IP Fault Management*, NN10408-900).
you entered no	When you enter no, the system will repeat the last action it performed before you selected to fallback.

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

Confirming the upgrade media selection

At your workstation

1 Use the following table to determine your next step.

If	Do
you are using CDROM for the upgrade	step 2
you are using ESD for the upgrade	step 3

2 If you are using CD-ROM as the software delivery method for the upgrade, the system prompts you to insert the CBM CD disk into the CDROM drive. After you have inserted the CD 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 4 in (I)SN09 CBM 850 upgrade checklist on page 12
you entered shell	Perform Selecting the CBM upgrade media on page 21 starting at step 3
you entered fallback	Perform Selecting the CBM upgrade media on page 21 starting at step 4
you entered media	The system prompts you to select the software delivery method to be used for the upgrade. Perform Selecting the CBM upgrade media on page 21

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 4
only one ESD image is found in the /swd/sdm directory	step 5

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 5
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 Selecting the CBM upgrade media on page 21 starting at step 3 for the system response.
you entered fallback	The system cancels the entire upgrade procedure. Refer to Selecting the CBM upgrade media on page 21 starting at step 4 for the system response.
you entered media	The system prompts you to select the software delivery method. If you select the cdrom delivery method in response, see step 2 for a description of the system response and the action you can perform.

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

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 using the root user ID and password.

3 Verify that your system is running the SN09 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
```

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.

Example response

```
=== Executing "sspfs_soft"

SSPFS version: 09.0 Build: 200508421 Server
Profile: cbm850

==="sspfs_soft" completed successfully
```

d Note the SPFS version.

If the SPFS version is	Do
09.*x*	step 4
anything else	contact your next level of support

4 Exit from the Command Line Interface:

```
x
```

```
x
```

5 Enter the following command to determine whether the inactive node is in a ClusterIndicatorSTBY (standby) state:

```
ubmstat
```

Re-run this command until the inactive node is shown to be in the standby state.

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.

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.

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

Performing an active CBM 850 upgrade post-swact 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 SN09 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
```

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.

Example response

```
=== Executing "sspfs_soft"

SSPFS version: 09.0 Build: 200508421 Server
Profile: cbm850

==="sspfs_soft" completed successfully
```

d Note the SPFS version.

If the SPFS version is	Do
09.*x*	step 4
anything else	contact your next level of support

4 Exit from the Command Line Interface:

```
x
```

```
x
```

5 Enter the following command to determine whether the active node is in a ClusterIndicatorACTIVE state:

```
ubmstat
```

Re-run this command until the active node is shown to be in the active state.

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.

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.

8 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.

9 Enter the following command to determine whether any CBM faults exist:

```
querycbm flt
```

Re-run this command until any faults are cleared.

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

Obtaining the NPM patch files for a CBM 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 Change the permissions on the newly-created directory:

```
chmod 777 /data/npm_patches
```

6 Access the newly-created directory:

```
cd /data/npm_patches
```

7 Log in to the CBM drop box through FTP:

```
ftp <drop box>
```

where

drop box
is the IP address of the unit that patches were downloaded to in step 9 of the (I)SN09 CBM 850 upgrade preparation checklist on page 6

8 When prompted, enter your user ID and password for the CBM drop box.

9 Obtain a list of files and directories on the CBM drop box:

```
ls
```

10 Set the transfer mode to binary:

```
bin
```

11 Change directory to the directory that contains the patches and transfer all of the patches from the CBM drop box to the CBM:

```
cd <dirrectory containing patches>
prompt off
mget *
```

12 Exit from ftp:

```
quit
```

13 Verify that the patches are in the /data/npm_patches directory on the CBM:

```
ls
```

14 Change permissions for the patch files in the directory:

```
chmod 777 *
```

15 You have completed this procedure. Return to step 11 of (I)SN09 CBM 850 upgrade preparation checklist on page 6.

Obtaining the latest NPM patch files for a CBM after 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 Change directory to /data/npm_patches:

```
cd /data/npm_patches
```

5 Create a patchlist file:

```
ls *.* > patchlist
```

6 Access the NPM command line interface (CLUI):

```
npm
```

7 When prompted, enter your user ID and password.

Note: The user name and password must be obtained from the NPM admin personnel.

8 Retrieve the patch files for the NPM to process:

```
getpatch patchlist
```

9 Exit out of the NPM tool to continue the upgrade:

```
quit
```

10 You have completed this procedure. Return to step 8 of (I)SN09 CBM 850 upgrade completion checklist on page 16.

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.

ATTENTION

Perform this procedure to determine the state of the cluster rather than rely on the presence of the ClusterOutOfSync file in the root directory. The ClusterOutOfSync file does not give the definitive state of the cluster.

When a cluster node is out of sync, log SPFS310 is generated.

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 Faut 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 login session to the inactive server, using one of the following methods:

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

2 Log in to the server using telnet (unsecure) as follows:

a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the inactive server

b When prompted, enter your user ID and password.

c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d When prompted, enter the root password.

Note: Ensure you are on the right server by typing ubmstat. You must be on the inactive server and the response must be *ClusterIndicatorSTBY*.

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.

Note: Ensure you are on the right server by typing ubmstat. You must be on the inactive server and the response must be *ClusterIndicatorSTBY*.

4 Determine your next action based on the system response to the **ubmstat** command.

If	Do
the system response is `ClusterIndicatorSTBY`	step 6

If	Do
otherwise	step 5

5 Log out of the active server and return to step 1 to log in to the inactive server.

6 Verify the status of replicated disk volumes by typing

```
# udstat
```

and pressing the Enter key.

If	Do
the system response for each 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)SN07/(I)SN08 response to the CheckConfiguration command and the (I)SN09 response. In (I)SN09, the system returns an additional response if the verification passes and the cluster nodes are in sync. This response is not returned in (I)SN07 or (I)SN08. This discrepancy is normal.

8 Reboot the inactive server by typing

```
# init 6
```

and pressing the Enter key.

If	Do
you identified a problem	Contact your next level of support.
otherwise	the cluster is in a good state and you can proceed to step 9

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

Upgrading SSPFS software

Application

Use this procedure to upgrade the Succession Server Platform Foundation Software (SSPFS) on a Sun Netra t1400 or Sun Netra 240 from (I)SN07 or (I)SN08 to the (I)SN09 release.

The SSPFS must be upgraded prior to upgrading the software for any one of the following components that reside on an SSPFS-based server.

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Media Gateway 9000 Manager
- Core and Billing Manager (CBM)

Prerequisites

This procedure has the following prerequisites:

- If upgrading from CD, ensure you have SSPFS Disk 1, SSPFS Disk 2, and SSPFS Disk 3 for the (I)SN09 release.
- 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.
- If upgrading an SSPFS-based server hosting the CBM, ensure the CBM ISO image is in the /swd/sdm directory. If required, refer to procedure Transferring and mounting an ISO image to an SPFS-based server on page 63.

  Note: The CBM upgrade is automatically initiated during the SSPFS upgrade process.

- 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.
- Nortel recommends verifying that the SSPFS console ports are accessible for Nortel Support in advance of starting this upgrade. Remote access using a terminal server or modem (in accordance

with customer security policies) is preferred to local access using a VT-100 terminal or emulation.

CAUTION

After having completed this procedure, but before attempting to execute procedure Upgrade the ABS software on the CS 2000 Management Tools server, manually modify the USP FTP home directory settings in the SSPFS file. Modifying these settings prevents the USP ABS from failure during booting.

In the SSPFS file /opt/proftpd/etc/proftpd.conf, change all instances of /opt/usp back to /data/usp.

Note: Assume the install directory of the previous release is /data/usp.

Action

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

- Upgrading SSPFS software using CDROM disks on page 39
- Upgrading SSPFS software using ESD on page 47

Upgrading SSPFS software using CDROM disks

ATTENTION
In a two-server configuration, perform the steps that follow on the inactive server.

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.

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.

At the server

2 Insert SSPFS 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 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.

4 Ensure the /opt filesystem has a minimum of 1800000 kilobytes of available disk space for the software by typing

```
# df -k /opt
```

and pressing the Enter key.

Example response

```
# df -k /opt
Filesystem            kbytes    used   avail  capacity Mounted on
/dev/md/dsk/d11       5138022  1782579 3355443    35%     /opt
```

The value under the avail column is the amount of available kilobytes.

5 Ensure the /var filesystem has a minimum of 1200000 kilobytes of available disk space for the software by typing

```
# df -k /var
```

and pressing the Enter key.

Example response

```
# df -k /var
Filesystem            kbytes    used   avail  capacity Mounted on
/dev/md/dsk/d8        2097152   314573 1782579    11%     /var
```

The value under the avail column is the amount of available kilobytes.

6 Ensure the /tmp filesystem has a minimum of 200000 kilobytes of available disk space for the software by typing

df -k /tmp

and pressing the Enter key.

Example response

```
# df -k /tmp
Filesystem            kbytes  used    avail   capacity  Mounted on
swap                  524288   304    523984     1%       /tmp
```

The value under the avail column is the amount of available kilobytes.

7 Ensure the root (/) filesystem has a minimum of 1550000 kilobytes of available disk space for the software by typing

df -k /

and pressing the Enter key.

Example response

```
# df -k /
Filesystem            kbytes  used    avail   capacity  Mounted on
/dev/md/dsk/d2         4089446 1782579 2306867    44%       /
```

The value under the avail column is the amount of available kilobytes.

8 Ensure you are at the root directory level by typing

cd /

and pressing the Enter key.

9 Run the pre-upgrade script by typing

/cdrom/cdrom0/s0/pre_upgrade

and pressing the Enter key.

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.

10 Execute the sync command to write all filesystem changes to disk by typing

```
# /usr/bin/sync
```

and pressing the Enter key.

11 Start the upgrade process by typing

```
# /liveupgrade.ksh
```

and pressing the Enter key.

Example response

```
CDROM image files do not exist in /Upgrade,
Perform CDROM install?
Type yes to continue, no, or exit to abort:
```

12 Confirm you want to continue with the CDROM install by typing

```
yes
```

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/c1t0d0s1> the
boot device for the logical device
</dev/md/dsk/d2>? (yes or no)
```

13 Accept the specified device as the boot device by typing

```
yes
```

and pressing the Enter key.

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: During the execution of this step, the system displays a warning message stating that <n> packages failed to install properly on boot environment SN09. This message is expected and does not indicate a problem. This message is only displayed during an SN07 to SN09 upgrade. It is not displayed during an SN08 to SN09 upgrade.

Once this step completes, the system ejects SSPFS Disk 1 and prompts you to insert the next disk. The next disk is either SSPFS Disk 2 if upgrading from SN07, or SSPFS Disk 3 if upgrading from SN08 as SSPFS Disk 2 is not required for SN08.

14 Use the following table to determine your next step.

If you are upgrading from	Do
SN07	step 15
SN08	step 17

At the server

15 Remove SSPFS Disk 1 from the CDROM drive, and insert SSPFS Disk 2.

At the server console

16 When ready, indicate you want to proceed by typing

```
# ok
```

and pressing the Enter key

The execution of this step takes approximately 35 minutes to complete on a Netra t1400, and 25 minutes on a Netra 240. The execution time can vary depending on system configuration.

Note: During the execution of this step, the system displays a warning message stating that <n> packages failed to install properly on boot environment SN09. This message is expected and does not indicate a problem.

Once this step completes, the system ejects SSPFS Disk 2 and prompts you to insert SSPFS Disk 3.

At the server

17 Remove the SSPFS Disk from the CDROM drive, and insert SSPFS Disk 3.

Note: If upgrading from SN07, you will be removing SSPFS Disk 2, and if upgrading from SN08, you will be removing SSPFS Disk 1 as SSPFS Disk 2 is not required for SN08.

At the server console

18 When ready, indicate you want to proceed by typing

```
# ok
```

and pressing the Enter key

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 SN09. This message is expected and does not indicate a problem. This message is only displayed during an SN07 to SN09 upgrade. It is not displayed during an SN08 to SN09 upgrade.

Note 2: During the execution of this step, you can receive the following warning:

```
Installation of 114332-15 failed:
Attempt to apply a patch that's already been
applied
```

No action is necessary if you receive this warning. It only means that the patch has already been applied.

19 Use the following table to determine your next step.

If	Do
you are upgrading an SSPFS-based server that is hosting the CBM	continue with Upgrading the CBM 850 on page 12 to upgrade the CBM and the remainder of SSPFS
otherwise	step 20

20 Wait until the upgraded server fully reboots, which consists of two reboots.

On simplex SSPFS-based servers hosting the CMT, IEMS, or both, data migration starts once the server has rebooted. Data migration can take approximately 2 hours to complete.

21 Use the following table to determine your next step.

If	Do
the server you are upgrading starts data migration	step 22
otherwise	step 23

22 Wait until data migration completes and the prompt returns before you proceed.

Note: Data migration is complete when the prompt returns.

23 Log back 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.

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.

24 Use the following table to determine your next step.

If	Do
the SSPFS-based server is hosting the IEMS	step 25
otherwise	step 28

25 Use the following table to determine your next step.

If	Do
you are upgrading a simplex server	step 26
otherwise	step 28

26 Use the following table to determine your next step.

If	Do
you are upgrading from SN08	step 27
otherwise	step 28

27 Disable the health monitors and ensure WEBSERVICES is started by typing

`cfgsplxck disable`

and pressing the Enter key.

Example response

```
NOTE: Disabling health monitor...Success.

NOTE: Starting WEBSERVICES...Success.
```

28 Remove SSPFS Disk 3 from the CDROM drive.

29 Perform the steps under Verifying the SSPFS software load on page 57 to complete this procedure.

Upgrading SSPFS software using ESD

At the server console

1 Log in to the SSPFS-based 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.

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 Ensure the /opt filesystem has a minimum of 1800000 kilobytes of available disk space for the ESD software by typing

```
# df -k /opt
```

and pressing the Enter key.

Example response

```
# df -k /opt
Filesystem            kbytes    used   avail  capacity Mounted on
/dev/md/dsk/d11       5138022  1782579 3355443    35%     /opt
```

The value under the avail column is the amount of available kilobytes.

4 Ensure the /var filesystem has a minimum of 1200000 kilobytes of available disk space for the ESD software by typing

```
# df -k /var
```

and pressing the Enter key.

Example response

```
# df -k /var
Filesystem            kbytes    used   avail  capacity Mounted on
/dev/md/dsk/d8        2097152   314573 1782579    11%     /var
```

The value under the avail column is the amount of available kilobytes.

5 Ensure the /tmp filesystem has a minimum of 200000 kilobytes of available disk space for the ESD software by typing

```
# df -k /tmp
```

and pressing the Enter key.

Example response

```
# df -k /tmp
Filesystem            kbytes  used    avail   capacity  Mounted on
swap                  524288   304    523984     1%       /tmp
```

The value under the avail column is the amount of available kilobytes.

6 Ensure the root (/) filesystem has a minimum of 1550000 kilobytes of available disk space for the ESD software by typing

```
# df -k /
```

and pressing the Enter key.

Example response

```
# df -k /
Filesystem            kbytes  used    avail   capacity  Mounted on
/dev/md/dsk/d2         4089446 1782579 2306867    44%       /
```

The value under the avail column is the amount of available kilobytes.

7 Change to the /opt directory by typing

```
# cd /opt
```

and pressing the Enter key.

8 Establish an FTP session to the repository server where the ESD software is located by typing

```
# ftp <repository_server>
```

and pressing the Enter key.

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

9 Log in to the repository server.

10 Change directory to where the SSPFS iso files are located on the repository server by typing

```
ftp> cd <esd_directory>
```

and pressing the Enter key.

where

esd_directory
is the directory that contains the SSPFS iso files, for example, SPFS0090.90.R.NCL.NAP.VAULT.1.D

11 List the contents of the directory by typing

```
ftp> ls
```

and pressing the Enter key.

Example response

```
platform_disk_1.iso
platform_disk_2.iso
platform_disk_3.iso
```

12 Change the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

13 Transfer the platform_disk_1.iso image to the SSPFS-based server by typing

```
ftp> get platform_disk_1.iso
```

and pressing the Enter key.

14 End the FTP session by typing

```
ftp> bye
```

and pressing the Enter key.

15 Access the command line interface to mount the iso image by typing

```
# cli
```

and pressing the Enter key.

16 Enter the number next to the Other option in the menu.

17 Enter the number next to the mount_image option in the menu.

18 Use the following table to determine your next step.

If the response is	Do
`Enter full path To ISO image`	step 20
`ISO Image Already Mounted`	step 19

19 Enter the number next to the umount_image option in the menu, and retry step 17.

If you are repeating this step, and the umount-image or mount_image command is unsuccessful a second time, contact your next level of support.

20 When prompted, enter the full path name of the iso image on the server by typing

```
/opt/platform_disk_1.iso
```

and pressing the Enter key.

Note: Do not attempt to change directories to the /tmpmnt directory until the mount command is complete.

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 un-mount 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 21

If the response is	Do
`Provided full path to ISO image does not exist`	Verify the location and name of the iso image and retry step 19.
`Error creating the image device location`	This response indicates an operating system error with the loopback file driver. Retry step 19, and if it 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. Repeat the procedure starting at step 7. If it fails a second time, contact your next level of support.

21 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.

22 Run the pre-upgrade script by typing

`# /tmpmnt/pre_upgrade`

and pressing the Enter key.

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.

23 Execute the sync command to write all filesystem changes to disk by typing

`# /usr/bin/sync`

and pressing the Enter key.

24

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 by typing

```
# cli
```

and pressing the Enter key.

25 Enter the number next to the Other option in the menu.

26 Enter the number next to the umount_image option in the menu.

27 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.

28 Move the platform_disk_1.iso image by typing

```
# mv /opt/platform_disk_1.iso /Upgrade/
```

and pressing the Enter key.

29 Change to the Upgrade directory by typing

```
# cd /Upgrade/
```

and pressing the Enter key.

30 Establish an FTP session to the repository server where the ESD software is located by typing

```
# ftp <repository_server>
```

and pressing the Enter key.

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

31 Log in to the repository server.

32 Change directory to where the SSPFS iso files are located on the repository server by typing

```
ftp> cd <esd_directory>
```

and pressing the Enter key.

where

esd_directory
is the directory that contains the SSPFS iso files, for example, SPFS0090.90.R.NCL.NAP.VAULT.1.D

33 Change the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

34 Transfer the platform_disk_2.iso image to the SSPFS-based server by typing

```
ftp> get platform_disk_2.iso
```

and pressing the Enter key.

35 Transfer the platform_disk_3.iso image to the SSPFS-based server by typing

```
ftp> get platform_disk_3.iso
```

and pressing the Enter key.

36 End the FTP session by typing

```
ftp> bye
```

and pressing the Enter key.

37 Ensure you are in the root directory by typing

```
# cd /
```

and pressing the Enter key.

38 Run the SSPFS upgrade script by typing

```
# /liveupgrade.ksh
```

and pressing the Enter key.

Example response

```
CDROM image files exist in /Upgrade, Perform ESD
install?
Type yes to continue, no for cdrom install, or
exit to abort:
```

39 Confirm you want to continue with the ESD install by typing

yes

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/c1t0d0s1> as the
system boot device.
Is the physical device </dev/dsk/c1t0d0s1> the
boot device for the logical device
</dev/md/dsk/d2>? (yes or no)
```

40 Accept the specified device as the boot device by typing

yes

and pressing the Enter key.

Note: The warnings that display are expected and can be ignored.

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.

Note: During the execution of this step, the system displays a warning message stating that <n> packages failed to install properly on boot environment SN09. This message is expected and does not indicate a problem. This message is only displayed during an SN07 to SN09 upgrade. It is not displayed during an SN08 to SN09 upgrade.

41 Use the following table to determine your next step.

If	Do
you are upgrading an SSPFS-based server that is hosting the CBM	continue with Upgrading the CBM 850 on page 12 to upgrade the CBM and the remainder of SSPFS
otherwise	step 42

42 Wait until the upgraded server fully reboots, which consists of two reboots.

On simplex SSPFS-based servers hosting the CMT, IEMS, or both, data migration starts once the server has rebooted. Data migration can take approximately 2 hours to complete.

43 Use the following table to determine your next step.

If	Do
the server you are upgrading starts data migration	step 44
otherwise	step 45

44 Wait until data migration completes and the prompt returns before you proceed.

Note: Data migration is complete when the prompt returns.

45 Log back 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.

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.

46 Use the following table to determine your next step.

If	Do
the SSPFS-based server is hosting the IEMS	step 47
otherwise	step 50

47 Use the following table to determine your next step.

If	Do
you are upgrading a simplex server	step 48
otherwise	step 50

48 Use the following table to determine your next step.

If	Do
you are upgrading from SN08	step 49
otherwise	step 50

49 Disable the health monitors and ensure WEBSERVICES is started by typing

`cfgsplxck disable`

and pressing the Enter key.

Example response

```
NOTE: Disabling health monitor...Success.
NOTE: Starting WEBSERVICES...Success.
```

50 Perform the steps under Verifying the SSPFS software load on page 57 to complete this procedure.

Verifying the SSPFS software load

At the server console

1 Verify that your system is running the SN09 version of the SSPFS through the command line interface 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 Note the SSPFS version.

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 Use the following table to determine your next step.

If	Do
the SSPFS version you noted is 09.0	step 7
any other version	stop and contact your next level of support

7 Verify the status of replicated disk volumes by typing

```
# udstat
```

and pressing the Enter key.

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`.

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

Transferring a compressed ISO image to a CBM server

Application

Use this procedure to transfer a compressed 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

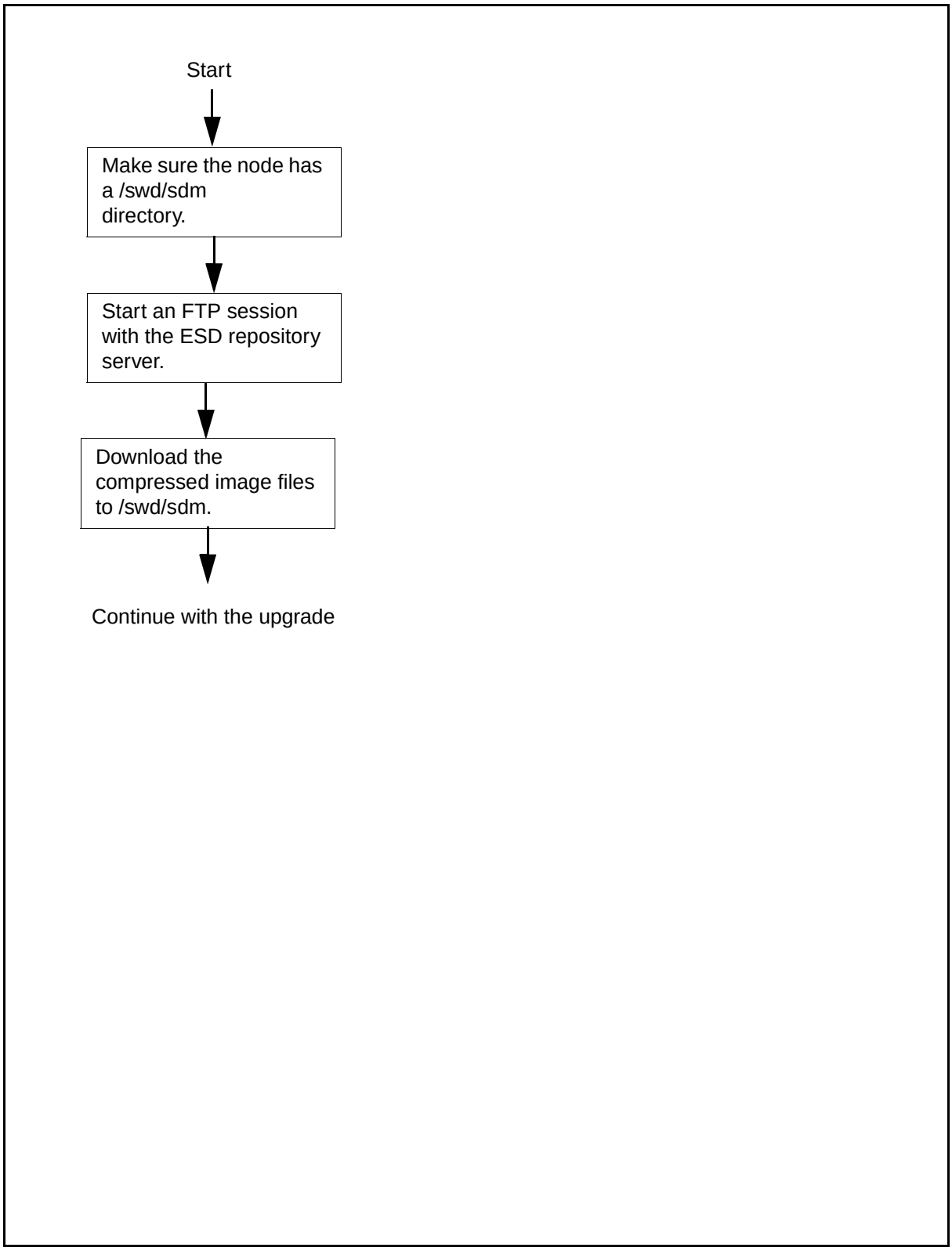
This procedure has the following prerequisites:

- 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 name or IP address of the CBM server.
- You must know the root password to 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 transfer a compressed ISO image to a CBM server



Transferring a compressed ISO image to a CBM server

At your workstation

1 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.

2 Change to the data directory by typing

```
# cd /swd
```

and pressing the Enter key.

3 List the directories in /data by typing

```
# ls -d sdm
```

and pressing the Enter key.

4 Use the following table to determine your next step.

If the response is	Do
`No such file or directory`	step 5
`sdm`	step 6

5 Create the directory by typing

```
# mkdir sdm
```

and pressing the Enter key.

6 Change to the sdm directory by typing

```
# cd sdm
```

and pressing the Enter key.

7 Start an FTP session with the ESD repository server by typing

```
# ftp <ESD_repository_server_ip>
```

and pressing the Enter key.

where

<ESD_repository_server_ip>
is the machine owned by the operating company that was selected to be the destination for ESD software.

8 List the directories on the ESD repository server by typing

```
ftp> ls
```

and pressing the Enter key.

9 Change directory to the drop box directory by typing

`ftp> cd <dropbox_directory>`

and pressing the Enter key.

where

<dropbox_directory>
is the name of the your dropbox directory.

10 List the contents of the drop box by typing

`ftp> ls -l`

and pressing the Enter key.

11 Change the transfer mode to binary by typing

`ftp> bin`

and pressing the Enter key.

12 Transfer the ESD software load to the CBM server by typing

`ftp> get <iso_image>`

and pressing the Enter key.

where

<iso_image>
is the full name of the image file

13 End the FTP session by typing

`ftp> bye`

and pressing the Enter key.

14 Make sure the files successfully transferred to the CBM server. List the files in /swd/sdm by typing

`# ls -l /swd/sdm`

and pressing the Enter key.

15 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 to an SPFS-based server

Application

Use this procedure to perform the following tasks:

- transfer an uncompressed .ISO image file from your ESD load repository server to the SPFS-based server
- mount the image on the SPFS-based server

Nortel delivers compressed software loads through Electronic Software Delivery (ESD) to a local ESD load repository server. Administrators uncompress the loads, which are then available as International Standard of Organization (ISO) 9660-compliant images for transfer to an SPFS-based server.

Prerequisites

This procedure has the following prerequisites:

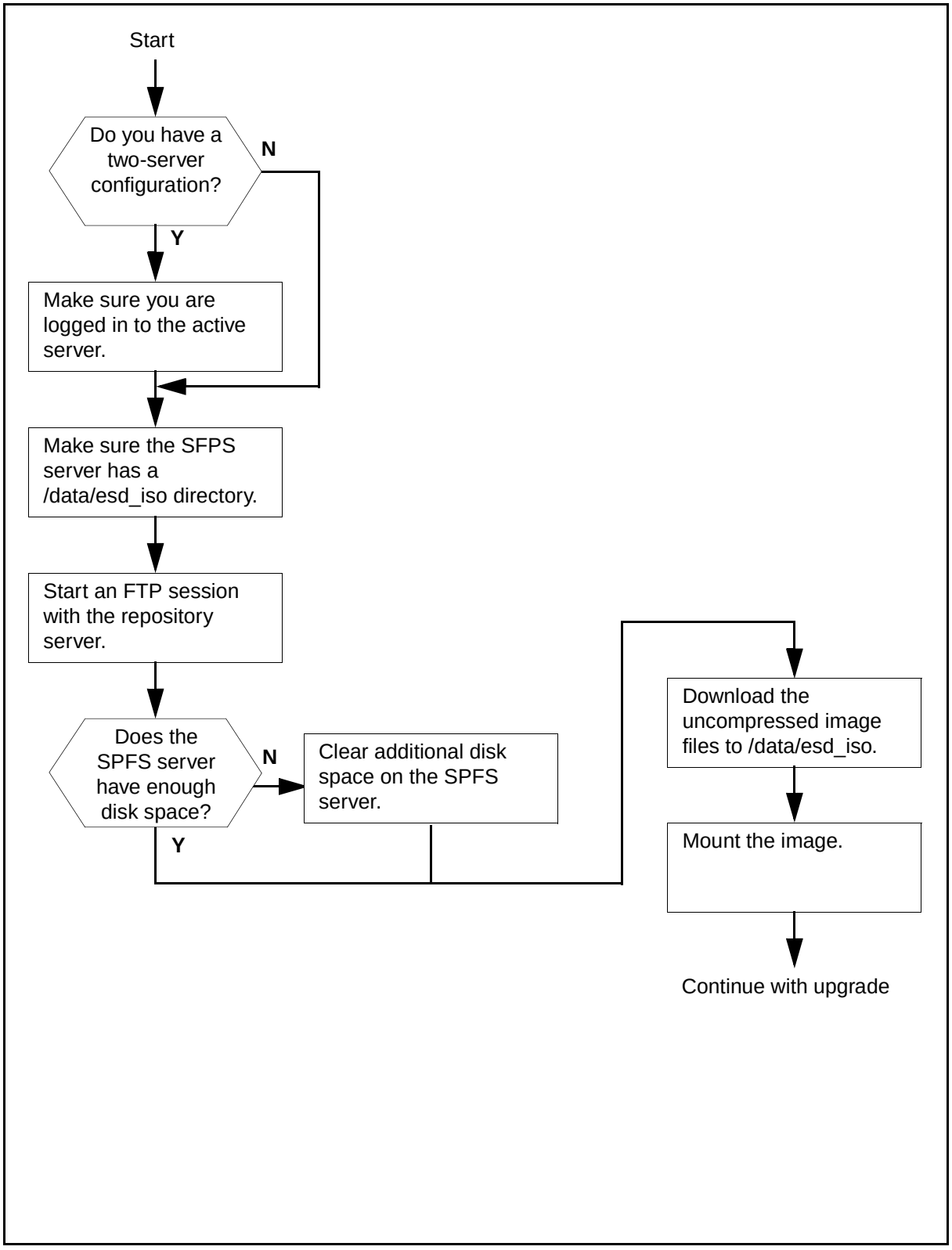
- The image file must be uncompressed and available on your ESD load repository server.
- You must know the name or IP address of the load repository server and the location of the dropbox directory on the server.
- You must know the name or IP address of the SPFS-based server.
- You must know the root 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



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 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 and press the Enter key.

9 Use the following table to determine your next step.

If	Do
you have a two-server configuration	step 10
otherwise	step 13

10 Make sure you are on the active server by typing

\# **ubmstat**

and pressing the Enter key.

11 Use the following table to determine your next step.

If the response is	Do
ClusterIndicatorSTBY	step 12
ClusterIndicatorACT	step 13

12 You are logged on to the inactive server. Log out of this server and return to step 1 to log in to the active server.

13 Make sure the server has the correct directories. Use the following table as reference.

Component	Directory path
ERS 8600	/swd
GWC	/gwc
All other components	/data/esd_iso

Change to the directory for your component by typing

```
# cd <directory>
```

and pressing the Enter key.

where

directory
is /swd, /gwc, or /data/esd_iso

14 Use the following table to determine your next step.

If the response	Do
indicates no such directory exists	step 15
displays the name of the directory	step 16

15 Create the directory by typing

```
# mkdir <directory>
```

and pressing the Enter key.

where

directory
is /swd, /gwc, or /data/esd_iso

16 Display the available disk space in the directory by typing

```
# df -k <directory>
```

and pressing the Enter key.

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
```

17 Record the amount of available disk space. You will need the information later in this procedure.

18 Change directory by typing

```
# cd <directory>
```

and pressing the Enter key.

where

directory
is /swd, /gwc, or /data/esd_iso

19 Start an FTP session with the ESD repository server by typing

```
# ftp <ESD_repository_server_ip>
```

and pressing the Enter key.

where

ESD_repository_server_ip
is the machine owned by the operating company that was selected to be the destination for ESD software.

20 List the directories on the ESD repository server by typing

```
ftp> ls
```

and pressing the Enter key.

21 Change directory to the drop box directory by typing

`ftp> cd <dropbox_directory>`

and pressing the Enter key.

where

dropbox_directory
is the name of the your dropbox directory.

22 List the contents of the drop box by typing

`ftp> ls -l`

and pressing the Enter key.

23 Locate the uncompressed image file you want to transfer, and identify the size of the file.

24 Compare the size of the uncompressed image file with the amount of available space you recorded in step 17.

25 Use the following table to determine your next step.

If	Do
the server has enough available disk space	step 27
otherwise	step 26

26 Clear additional disk space following local office policy, before you continue with this procedure. If necessary, contact your next level of support.

27 Change the transfer mode to binary by typing

`ftp> bin`

and pressing the Enter key.

28 Transfer the ESD software load to the SPFS-based server by typing

`ftp> get <iso_image>`

and pressing the Enter key.

where

iso_image
is the full name of the image file

Note: Do not transfer any file with a .tar.gz extension.

29 End the FTP session by typing

```
ftp> bye
```

and pressing the Enter key.

30 List the contents of the directory to ensure the files successfully transferred to the server by typing

```
# ls -l
```

and pressing the Enter key.

You are now ready to mount the iso image on the server.

31 Perform the steps under Mounting an ISO image on an SPFS-based server on page 70 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 ISO image, 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 14

2 Use the following table to determine your next step.

If	Do
you are mounting the APS iso image	step 14
otherwise	step 3

3 Establish a login session to the inactive server using one of the following methods:

If using	Do
telnet (unsecure)	step 4
ssh (secure)	step 9

4 Log in to the inactive server using telnet by typing

> **telnet <server>**

and pressing the Enter key.

where

server
is the physical IP address of the inactive server

5 When prompted, enter your user ID and password.

6 Change to the root user by typing

$ **su -**

and pressing the Enter key.

7 When prompted, enter the root password.

8 Go to step 11.

9 Log in to the inactive server using ssh 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.

10 When prompted, enter the root password.

11 Make sure you are on the inactive server by typing

ubmstat

and pressing the Enter key.

12 Use the following table to determine your next step.

If the response is	Do
ClusterIndicatorSTBY	step 14
ClusterIndicatorACT	step 13

13 You are logged on to the active server. Log out of this server and return to step 3 to log in to the inactive server.

14 Start the command line interface by typing

```
# cli
```

and pressing the Enter key.

15 Enter the number next to the Other option in the menu.

16 Enter the number next to the mount_image option in the menu.

17 Use the following table to determine your next step.

If the system response is	Do
`Enter full path to ISO image`	step 19
`ISO image Already Mounted`	step 18

18 Enter the number next to the umount_image option in the menu and retry step 16.

Note: If either command is unsuccessful a second time, contact your next level of support.

19 When prompted, enter the full path name of the iso image on the server by typing

```
# <directory_path>/<iso_image>
```

and pressing the Enter key.

where

directory_path
is /swd, /gwc, or /data/esd_iso

iso_image
is the full name of the ISO image file

Note: Do not attempt to change directories to the /tmpmnt directory until the mount command is complete.

20 Use the following table to determine your next step.

If the response	Do
is a warning to unmount the image before removing the image file	step 21
indicates the path you provided does not exist	Verify the location and name of the image and retry step 18.
indicates an error creating the image device location	Retry step 18. An operating system error with the loopback file driver occurred. If the command fails a second time, contact your next level of support.
indicates an error mounting the file	Repeat the steps under Transferring an ISO image to an SPFS-based server on page 65. The ISO image is corrupt or the /tmpmnt directory has been deleted. If the procedure fails a second time, contact your next level of support.

21 Exit each menu level of the command line interface by typing

`select - x`

and pressing the Enter key.

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

Executing a fallback during an SSPFS-based server upgrade

Application

Use this procedure to roll back (fall back) to the state prior to the upgrade.

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 74
- Two-server configuration on page 75

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 Billing Manager (CBM) or MG 9000 Element Manager	step 5
CS 2000 Management Tools or Integrated Element Management System (IEMS)	step 4

4 Restore the oracle data on the server. If required, refer to procedure “Restoring the oracle data on an SSPFS-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 server server that has the new software on it through the console (port A) using the root user ID and password if not already logged in.

2 Rollback to the state prior to the upgrade by typing

```
# /SSPFS_Upgrade.fallback
```

and pressing the Enter key.

3 Use the following table to determine your next step.

If your server is hosting the	Do
Core Billing Manager (CBM)	step 7
CS 2000 Management Tools, Media Gateway 9000 Manager, or Integrated Element Management System (IEMS)	step 4

4 Connect to the console port of the other server that has the previous software on it.

5 Boot the server by typing

```
OK boot
```

and pressing the Enter key.

6 Log in using the root user ID and password.

7 Verify both servers are present by typing

GetRunningClusterNodeNames

and pressing the Enter key.

If the system response returns	Do
one server	step 8
two servers	step 9

8 Wait for one minute and repeat step 7. If after the second time, only one server is displayed, contact your next level of support before proceeding with this fallback.

9 Verify the status of replicated disk volumes by typing

udstat

and pressing the Enter key.

If	Do
all the file systems are ACTIVE normal UP clean	step 10
otherwise	contact your next level of support

10

If	Do
server is hosting the MG 9000 EM Server	step 17

11

If	Do
server is hosting the IEMS or CS2M	refer to procedure “Restoring the oracle data on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600

12

If	Do
server is hosting the NPM	step 13
otherwise	step 17

13 Download the NPM database file (old_npm_db.tar) made in step 44 of Saving user-defined NPM data using the NPM in NN10440-450 to the /data/npm directory on the NPM server if not already carried out.

14 Telnet to server running previous software and su to root where NPM is resident and erase existing NPM database by typing:

```
# cd /data/npm/database
# rm -Rf*
```

15 Now stage the old NPM database by typing:

```
# cd /data/npm
# tar-xvf old_npm_db.tar
```

16 servstart NPM

17 Clone the image of the active server onto the other server. If required, refer to procedure Cloning the image of one server in a cluster to the other server on page 197.

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

Performing a backup of file systems on an SSPFS-based server

Application

Use this procedure to perform a backup of the file systems on a Succession Server Platform Foundation Software (SSPFS)-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 9000 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

Prerequisites

This procedure has the following prerequisites:

- 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

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 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.

At the server

1 Insert the blank tape DVD into the drive. In a two-server configuration, insert the blank DVD into the active server.

At your workstation

2 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 SSPFS-based server on which you are performing the backup

In a two-server configuration, enter the physical IP address of the active server.

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.

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.

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 8

7 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

8 Back up the file systems by typing

```
# /opt/nortel/sspfs/bks/bkfullsys
```

and pressing the Enter key.

Example response:

```
Backup Completed Successfully
```

Note: If you are using DVD, the system will prompt you to insert another blank disk if more than one is needed.

9 Use the following table to determine your next step.

If you are using	Do
a tape for backup	step 10
a DVD for backup	step 12

10 List the contents of the tape by typing

```
# gtar -tvMf /dev/rmt/0
```

and pressing the Enter key.

11 Eject and remove the tape from the drive, label it, write-protect it, and store it in a safe place.

Proceed to step step 19.

12 Insert the backup DVD into the drive. If the backup resides on multiple DVDs, insert the first backup DVD.

13 List the contents of the DVD by typing

```
# gtar -tvMf /cdrom/*bkfullsys*/*.tar
```

and pressing the Enter key.

If you	Do
receive a prompt to prepare another volume	step 14
do not receive a prompt to prepare another volume	step 16

14 Press the Return key.

15 Stop the gtar process by pressing the Ctrl and C keys.

16 Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

17 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.

18 Remove the DVD from the drive, label it, and store it in a safe place.

If the backup	Do
resides multiple DVDs	Insert the next backup DVD in the disk drive and go to step 13.
resides on a single DVD	step 19

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

Applying patches to a CBM

Purpose

This procedure enables you to apply a patch to a CBM.

Procedure

Applying a patch to a CBM

At your workstation:

1 Use the following table to determine your next step:

If	Do
you have not configured PSE	Perform Configuring PSE on a CBM on page 84
you have configured PSE	step 2

2 Use the following table to determine your next step:

If	Do
you have not configured NPM	Perform Configuring NPM on an SSPFS server on page 86
you have configured NPM	step 3

3 Perform Applying patches using the NPM on page 125

4 You have completed this procedure.

Removing patches from a CBM

Purpose

This procedure enables you to remove a patch from a CBM.

Procedure

Removing a patch from a CBM

At your workstation:

1 Use the following table to determine your next step:

If	Do
you have not configured PSE	Perform Configuring PSE on a CBM on page 84
you have configured PSE	step 2

2 Use the following table to determine your next step:

If	Do
you have not configured NPM	Perform Configuring NPM on an SSPFS server on page 86
you have configured NPM	step 3

3 Perform Removing patches using the NPM on page 134

4 You have completed this procedure.

Configuring PSE on a CBM

Purpose

This procedure enables you to configure the Patching Server Element (PSE) on a Core and Billing Manager.

Procedures

ATTENTION
Instructions for entering commands in these procedures do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Configuring PSE on a CBM

At your workstation:

1 Log in to the CBM:

```
telnet <server>
```

where

server
is the IP address or host name of the CBM

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
```

6 Enter the number next to the Configuration option in the menu.

7 Enter the number next to the Succession Element Configuration option in the menu.

8 Enter the number next to the PSE Application Configuration option in the menu.

9 Enter the number next to the Configure_PSE (Configure the Patching Server Element) option in the menu.

10 Enter the NPM hostname or IP address of the server where the NPM resides.

Note: If the NPM is installed on a server in a cluster (two-server configuration), enter the host name or IP address of the cluster.

11 If the hostname or IP address is acceptable, enter y.

12 When prompted, enter x to exit each level until you exit the command line interface.

13 Start the PSE:

```
pse start
```

14 You have completed this procedure.

Configuring NPM on an SSPFS server

Purpose

This procedure enables you to configure the Network Patch Manager (NPM) on an SSPFS server.

Procedures

ATTENTION
Instructions for entering commands in these procedures do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Configuring NPM on an SSPFS server

At your workstation:

1 Log in to the SSPFS server:

```
telnet <server>
```

where

server
is the IP address or host name of the SSPFS 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
```

6 Enter the number next to the Configuration option in the menu.

7 Enter the number next to the Succession Element Configuration option in the menu.

8 Enter the number next to the NPM Application Configuration option in the menu.

9 Enter the number next to the ConfigureNpm (Configure the Network Patch Manager) option in the menu.

10 If you are ready to proceed with NPM application configuration, enter y.

11 When prompted, enter x to exit each level until you exit the command line interface.

12 Start the NPM server:

```
servstart NPM
```

13 You have completed this procedure.

Setting up local user accounts on an SSPFS-based server

Application

Use this procedure to add local user accounts on a Succession Server Platform Foundation Software (SSPFS)-based server and assign them to user groups. Also use this procedure to assign existing user accounts to user groups. For information on user groups, see Additional information on page 91.

If you choose to centrally manage your user accounts, refer to procedure “Adding new users” in *IEMS Security and Administration*, NN10336-611.

If you want to launch the ping and traceroute operations that are performed remotely on SSPFS-based platforms from a centralized GUI on Integrated Element Management System (IEMS), refer to procedures “Running a ping test on the GWC network element or SSPFS platform” and “Running a traceroute test on the GWC network element or SSPFS platform” in *IEMS Basics*, NN10329-111.

ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

Prerequisites

To perform this procedure, you need to have the root user ID and password to log in to the server.

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 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 SSFPS-based server

Note: In a two-server configuration, log in to the active server using its physical IP address.

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If you are	Do
adding a new user	step 6
assigning an existing user to secondary user groups	step 11

6 Add the user to the primary user group *succssn* by typing

```
# useradd -g succssn <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

7 Create a password for the user you just added by typing

```
# passwd -r files <userid>
```

and pressing the Enter key.

where

userid
is the user name you added in the previous step

8 When prompted, enter a password of at least three characters.

Note: It is not recommended to set a password with an empty value. Use a minimum of three characters.

9 When prompted, enter the password again for verification.

10 Proceed to step 13.

11 Determine which groups the user currently belongs to by typing

```
# groups <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

12 Note the user groups the user currently belongs to.

13 Assign the user to one or more secondary user groups by typing

```
# usermod -g succssn -G <groupA,groupB,...>
<userid>
```

and pressing the Enter key.

where

groupA, groupB,...
are the secondary user groups (see table Secondary user groups on page 91) and any other user groups you noted in step 12 to which the user already belonged

Include a comma between groups, but no space.

userid
is a variable for the user name

Example input for a user who can perform line and trunk maintenance operations

```
# usermod -g succssn -G lnmtc,trkmtc johndoe
```

Note: The usermod command overwrites any previous user groups. Therefore, anytime you enter this command, specify all the user groups for the user.

You have completed this procedure.

Additional information

Users of the Nortel OAM&P client applications must belong to the primary user group *succssn* for login access. Users must also belong to one or more secondary user groups listed in the table below, which specify the operations a user is authorized to perform.

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm	secadm
trkrw	lnrw	mgcrw	mgrw	emsrw	secrw
trksprov	lnsprov	mgcspro v	mgsprov	emsspro v	secmtc
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc	secro
trkro	lnro	mgcro	mgro	emsro	

A secondary user group consists of

- a user group domain
- a user group operation

User group domain

A user group domain defines the range of applications to which a user group applies. The user group domains are listed in the following table:

Domain	Application mapping
trk	trunks, trunk-based services, small trunking gateways (port level), carrier-based services
ln	line services, line cards, small line gateways (port level)

Domain	Application mapping
mgc	CS2K, CS3K, USP, GWC, SAM21, IMS, 3PC, Storm, CS 2000 SAM21 Manager, CS 2000 GWC Manager
mg	small and large gateways such as UAS, line gateways, trunk gateways
ems	SDM, MDM, MDP, KDC, device manager, NPM

User group operation

A user group operation dictates the operations a user can perform using the Nortel OAM&P client applications. The user group operations are listed in the following table:

Operation	User role mapping
adm (administration)	Can reconfigure, access all functions, setup fundamental configuration, commission (add, delete, rehome), base frames and systems (SAM21 frames, call servers, large gateways), and run service-impacting diagnostics. The adm user can also do rw, sprov, mtc, and ro user operations.
rw (read/write)	Can view and change configuration and status, commission and reconfigure elements (GWCs, cards, shelves). The rw user can also do sprov, mtc, and ro user operations.
mtc (maintenance)	Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do sprov and ro user operations.
sprov (subscriber provisioning)	Can view status and configuration and change provisioning data, but cannot change maintenance state or do base component configuration. The sprov user can also do ro user operations.
ro (read-only)	Can view status and configuration, but cannot make changes.

When assigning users to secondary user groups, use the tables that follow, which provide a mapping between commands and secondary user groups. The list of the available tables is as follow:

Note: The mappings of commands to secondary user groups in the tables in this section do not apply to Multiservice Data Manager (MDM) when installed on a SSPFS-based server.

Node provisioning operations (Sheet 1 of 2)

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Disassociate a media gateway (MG) from a gateway controller (GWC)		x			
Associate an MG with a GWC		x			
Change the provisioning data for an MG		x			
Query site info					x
Query a GWC					x
Query an MG					x
change MG GWCEM data		x			
Get policy enforcement point (PEP) server data					x
Query a GWC PEP connection					x
Get dynamic quality of service (DQoS) policies data					x
Add or change a network address translations (NAT) device		x			
Query a NATdevice					x
Add, change, delete a media proxy (MP)		x			
Add, change, delete resource usage (RU)		x			
Query RU					x
Add, change, delete limited bandwidth links (LBL)		x			
Query LBL					x
Display call agent identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			

Node provisioning operations (Sheet 2 of 2)

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
View alarms, cards, subnet, shelf, mate shelf, mate card					x
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			
Perform a swact			x		
Firmware flash			x		
Assign/unassign services		x			

Audit operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Configure audit	x				
Run audit	x				
Get audit description					x
Get audit configuration					x
Get list of registered audits					x
Retrieve audit report					x
Take action on problem	x				

Carrier provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Add carrier		x			
Delete carrier		x			
Get endpoint					x
Get carrier					x
Get carrier by filter					x

Alarm operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
View/filter alarms					x

Internet transparency operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add, delete, change SPC	x				
Query SPCs					x
Set network VCAC	x				
Add, delete, change a network zone	x				
Query one or all network zones					x
addMPGroup	x	x			
changeMPGroup	x	x			
queryMPGroup	x	x	x	x	x
deleteMPGroup	x	x			

Internet transparency operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
addVPN	x	x			
deleteVPN	x	x			
queryVPN	x	x	x	x	x

Trunk provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Get tuple					x
Get tuple range					x
Add tuple		x			
Replace tuple		x			
Delete tuple		x			

Trunk maintenance operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Post by trunk CLLI					x
Maintenance by trunk CLLI			x		
Post by gateway					x
Maintenance by gateway			x		
Post by carrier					x
Maintenance by carrier			x		
D-channel Post by trunk CLLI					x
D-channel maintenance by trunk CLLI			x		

Trunk maintenance operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
ICOT			x		
Set Auto Refresh					x

ADSL provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Get subscriber					x
Add subscriber				x	
Add cross connection				x	
Modify subscriber				x	
Modify cross connection				x	
Delete subscriber				x	
Delete cross connection				x	

Line provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
ECHO, QX75, QBB, QBERT, QCM, QCOUNTS, QCPUGNO, QDCH, QDN, QDNA, QGRP, QHLR, QIT, QLEN, QLRN, QLT, QMODEL, QMSB, QPHF, QPRIO, QSCONN, QSCUGNO, QSIMR, QSL, QTOPSPOS, QTP, QWUCR					x

Line provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
QCUST, QDNSU, QDNWRK, QHA, QHASU, QHU, QLENWRK, QLOAD, QMADN, QNCOS, QPDN	x				
All other supported commands for line provisioning				x	

Line maintenance operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Validate line using DN CLLI					x
Validate line using TID CLLI					x
Get line post info					x
Busy line			x		
Return line to service			x		
Force release line			x		
Installation busy line			x		
Cancel deload			x		
Get CM CLLI					x
Get endpoint state					x
GetGwlp					x
run all TL1 line test commands			x		

V5.2 provisioning operations

Command	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
Add, delete, modify V5.2 interface		x					x			
View all V5.2 interfaces					x					x
View signalling channel information entry, update list (V5Prov)					x					x
Add, modify, delete signalling channel information entry (V5Prov)		x					x			
View ringing cadence mapping, update list (V5Ring)					x					x
Add, modify, delete ringing cadence mapping (V5Ring)		x					x			
View signalling characteristic profile, update list (V5Sig)					x					x
Add, delete, modify signalling characteristic profile (V5Sig)		x					x			
View carrier-to-interface and interface-to-carrier mappings					x					x

Patching operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
apply, remove, activate, deactivate, auditd, restart, and smartimage from the NPM GUI or CLUI	x				
Software image from MG 9000 Manager GUI		x			

Automated upgrade operations

Command	User group									
	emsadm	emsrw	emsmtc	emssprov	emkro	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Access and run the GWC uprade CLUI			x					x		
Access and run the SC uprade CLUI			x					x		

Ping and traceroute operations

Command	User group		
	emsadm	emsrw	emsmtc
Launch remote ping	x	x	x
Launch remote traceroute	x	x	x
Note: These operations are for remote operations performed on SSPFS platforms but launched from a centralized GUI on IEMS			

Patching the inactive node of a cluster during an upgrade

Application

Use this procedure to patch the inactive node of a cluster during an upgrade. A cluster refers to a Sun Netra 240 server pair.

ATTENTION
Only use this procedure when directed to do so and when the NPM resides on the network element to be patched. If the NPM does not reside on the server, use procedure Applying patches using the NPM on page 125.

Prerequisites

The patches must first be transferred to the Network Patch Manager (NPM) database. Either contact your network administrator to determine if this has been done, or transfer them now on the active node using procedure Transferring patches delivered on CD to the NPM database on page 119 if you receive patches on CD, or procedure Transferring patches delivered through ESD to the NPM database on page 177 if you receive patches through ESD.

Note 1: If you are performing this procedure on a CBM when the NPM is hosted by the CBM, ensure that all of the CBM and SPFS patches are included in the directory /data/npm_patches on the CBM. If the patches are not already in this directory, perform Obtaining the NPM patch files for a CBM before a CBM upgrade on page 29

Note 2: If you are performing this procedure on a CBM when the NPM is not hosted by the CBM, patches must first be transferred to the NPM database. Either contact your network administrator to determine if this has been done, or transfer them now on the active node using procedure Transferring patches delivered on CD to the NPM database on page 119 if you receive patches on CD, or procedure Transferring patches delivered through ESD to the NPM database on page 177 if you receive patches through ESD.

Action

Perform the following steps to complete this procedure.

ATTENTION
Perform the steps that follow on the inactive 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 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.

Note: Ensure you are on the inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the active server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorSTBY*, which indicates you are on the inactive server.

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.

Note: Ensure you are on the inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the active server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorSTBY*, which indicates you are on the inactive server.

4 Use the following table to determine your next step.

If	Do
the server is hosting the CBM	step 5
otherwise	step 7

5 Patch the inactive node by typing

`# patchUpToDate -directory <directory_name>`

and pressing the Enter key.

where

directory_name
is **/data/npm_patches**

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]
```

6 Proceed to step 8.

7 Patch the inactive node 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]
```

8 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.

Example response:

```
PSE [1 of 1]: There are 3 patches to be applied.
   Applying KAA00O07 [1 of 3] to PSE.
   Applying KAA01O07 [2 of 3] to PSE.
   Applying KAA02O07 [3 of 3] to PSE.
Determining whether any devices need to be
restarted.
```

9 If prompted, indicate whether you want a restart to occur on each of the listed devices.

Note: A restart enables the patches on the device. Typing `no` and pressing the Enter key, causes processing to continue without performing a restart.

10 If prompted, indicate whether you want a system reboot to occur.

Note: Typing `no` and pressing the Enter key causes processing to continue without performing a system reboot.

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.

11 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 167.

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

password
is the password associated with 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     : Patch file retrieval
Status          : SCHED
Enabled         : Y
```

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
```

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.

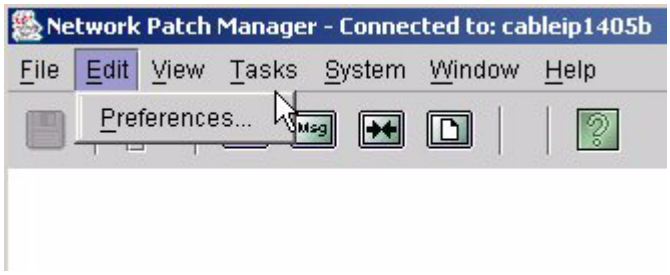
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 183.

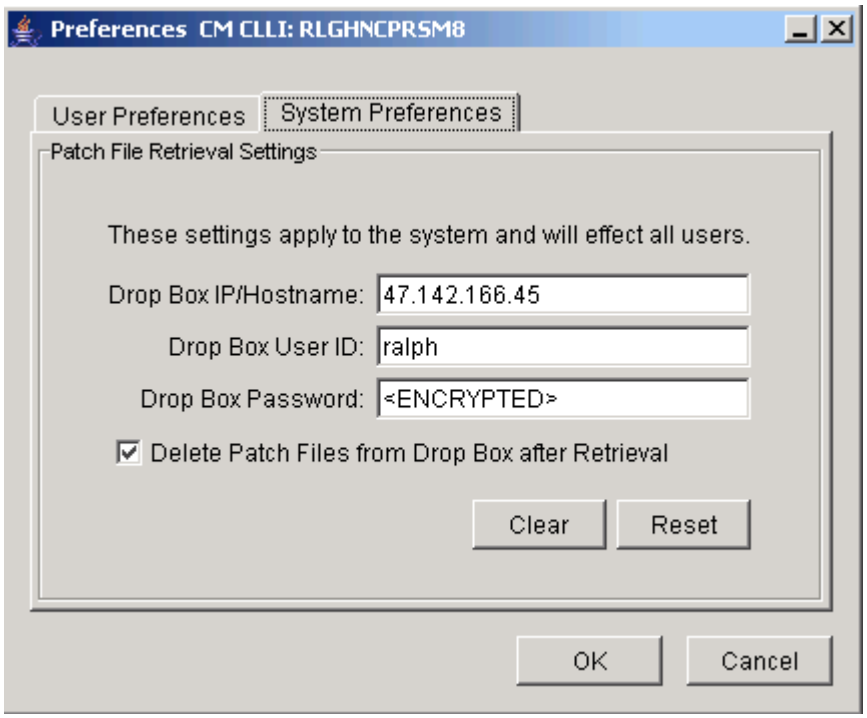
At the NPM GUI

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.

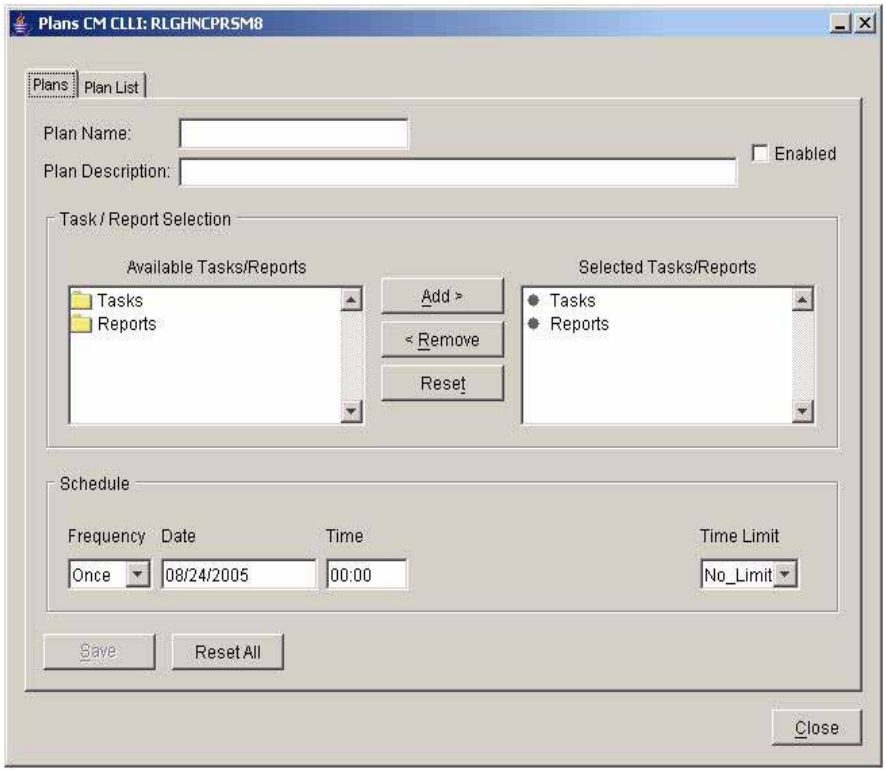
Note: The user ID must have read, write, and overwrite privileges in the FTP user's default directory on this server.

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.

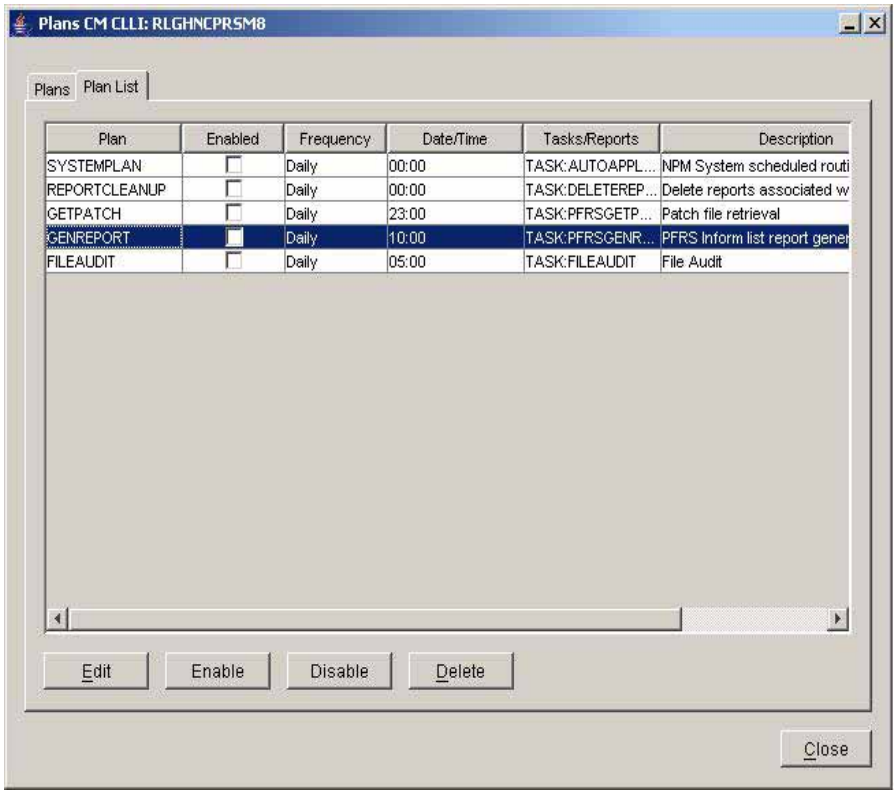
8 Click **OK** to complete the PFRS configuration.

9 On the System menu, select **Plans....**



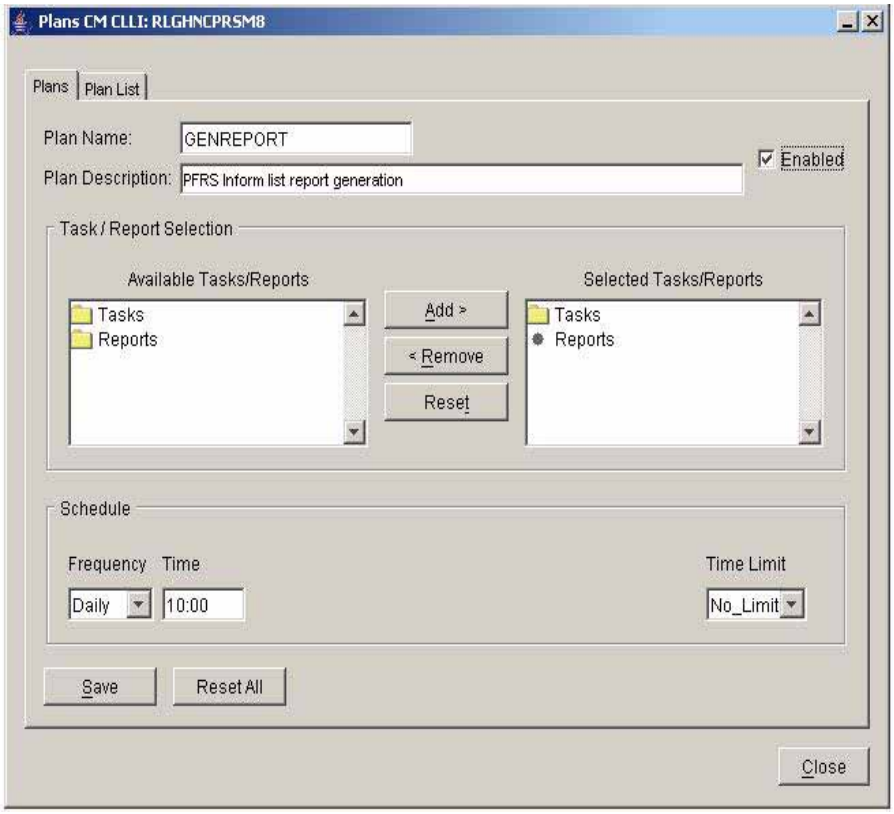
The Plans window is displayed.

10 Click **Plan List** tab.



The Plan List window is displayed.

11 Select the GENREPORT task and click Edit.



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.

Starting the PSE server application on an SSPFS-based server

Application

Use this procedure to start the Patching Server Element (PSE) server application on a Succession Server Platform Foundation Software (SSPFS)-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 SSPFS-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 SSPFS-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.

Starting the NPM server application

Application

Use this procedure to start the Network Patch Manager (NPM) server application on a Succession Server Platform Foundation Software (SSPFS)-based server.

Prerequisites

You need root user privileges to perform this procedure, and CORBA must be running in order for the NPM to come up.

Action

Perform the following steps to complete this procedure.

> **ATTENTION**
> In a two-server configuration, perform the steps that follow on the Active server.

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 SSPFS-based server where the NPM server application resides

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 NPM server application by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

If the NPM server application is	Do
not running	step 6
running	you have completed this procedure

6 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

7 Verify the NPM server application is running by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

You have completed this procedure.

Transferring patches delivered on CD to the NPM database

Application

Use this procedure to manually transfer patches to the Network Patch Manager (NPM) database and retrieve them for processing. Use this procedure if the patches were delivered on CD.

> ***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

You must be assigned to user group emsadm to perform patching activities using the NPM. If required, refer to procedure "Setting up local user accounts on an SSPFS-based server" in *ATM/IP solution-level Security and Administration*, NN10402-600.

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 SSPFS-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 SSPFS-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.

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.

At the server

4 Insert the CD that contains the patches into the drive of the SSPFS-based server where the NPM resides. In a two-server configuration, insert the CD into the drive of the active server.

At your workstation

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 that are on the CD in the temporary directory by typing

```
# find /cdrom -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

If the NPM server application is	Do
running	step 11

10 Start the NPM server application by typing

servstart NPM

and pressing the Enter key.

11 Access the NPM command line user interface (CLUI) by typing

npm

and pressing the Enter key.

12 When prompted, enter your user ID and password.

Note: Do not change directories.

13 Retrieve the patch files copied from the CD by typing

```
npm> getpatch current.patchlist
```

and pressing the Enter key.

Note 1: The following error message may be received when executing this step:

```
Error: Patch file
/data/npm/patch_upgrade/lex83o9s.ptchoamp
cannot be verified. Copying to golden
directory.
```

This is acceptable behavior because the (I)SN07 load cannot verify the (I)SN09 patch. Ignore this error.

Note 2: The golden directory mentioned in the previous note is /data/npm/Au. The files are successfully placed here when the getpatch is done, even though it appears to fail.

14 Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

15 Eject the CD from the drive. Change to the root directory level by typing

```
# cd /
```

and pressing the Enter key.

16 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.

17 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 7
otherwise	close the cdrom tray and proceed to the next step

18 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). You can apply patches using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

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. Refer to procedure Transferring patches delivered on CD to the NPM database on page 119 if your patches are delivered on CD or Transferring patches delivered through ESD to the NPM database on page 177 if your patches are delivered through ESD.

You must be assigned to user group emsadm to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600, for locally-managed user accounts, or procedure “Configuring user settings” in *Integrated EMS 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 155.

Action

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

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 167.

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
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
- Core Element Manager
- Network Patch Manager (NPM)
- Client Session Monitor (CSMON)
- Core and Billing Manager (CBM)

To restart a device, refer to procedure Restarting a device using the NPM on page 169 if required.

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

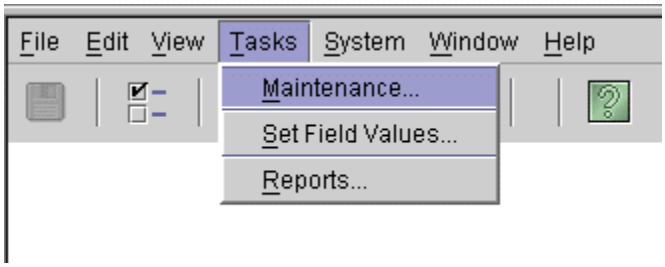
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 183.

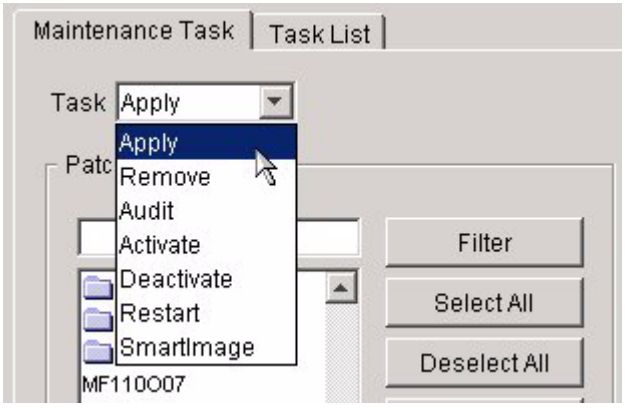
At the NPM GUI

2 On the Tasks menu, click **Maintenance**.

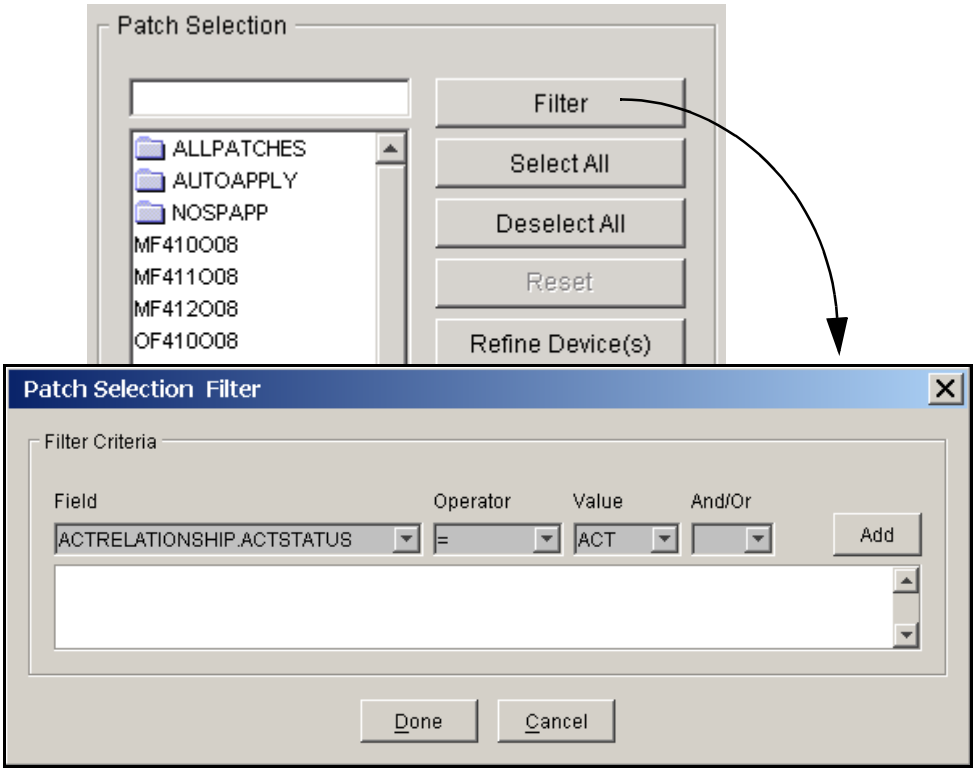


The Maintenance window is displayed.

3 In the Task list, click **Apply**.

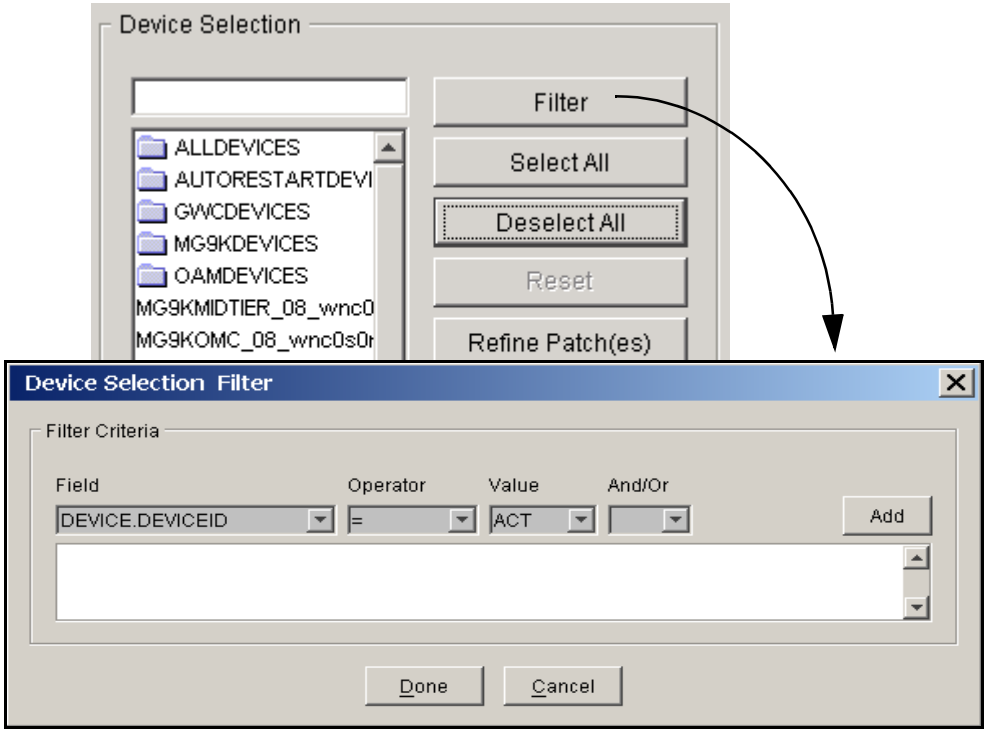


4 In the Patch Selection list, select the patch files or patch sets you want to apply, then click Refine Device(s) to display a list of devices to which the patches apply.



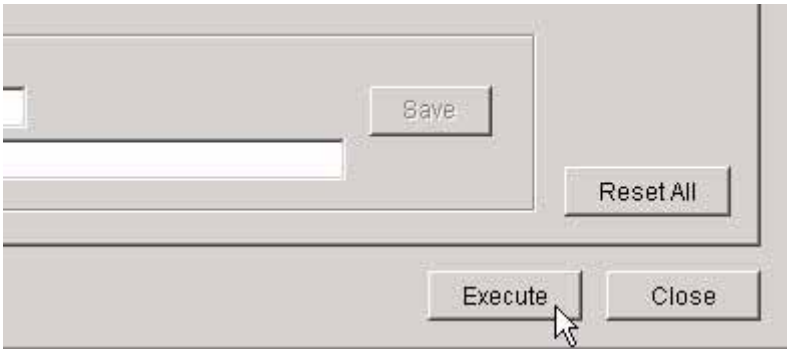
5 To limit the patches displayed in the Patch Selection list, click **Filter** to configure a filtering criteria.

6 In the Device Selection list, select the devices or device sets to which you want to apply the patches.

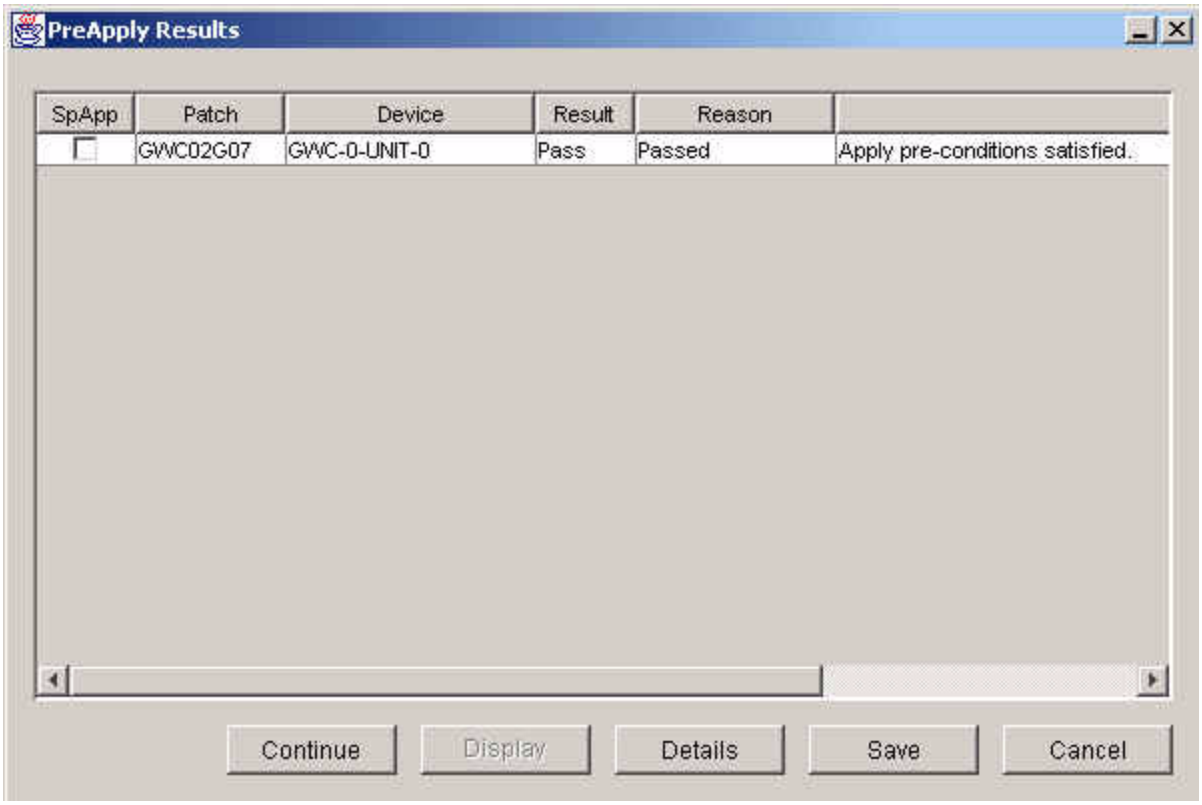


7 To limit the devices displayed in the Device Selection list, click **Filter** to configure a filtering criteria.

8 Click **Execute** to begin the patching process.



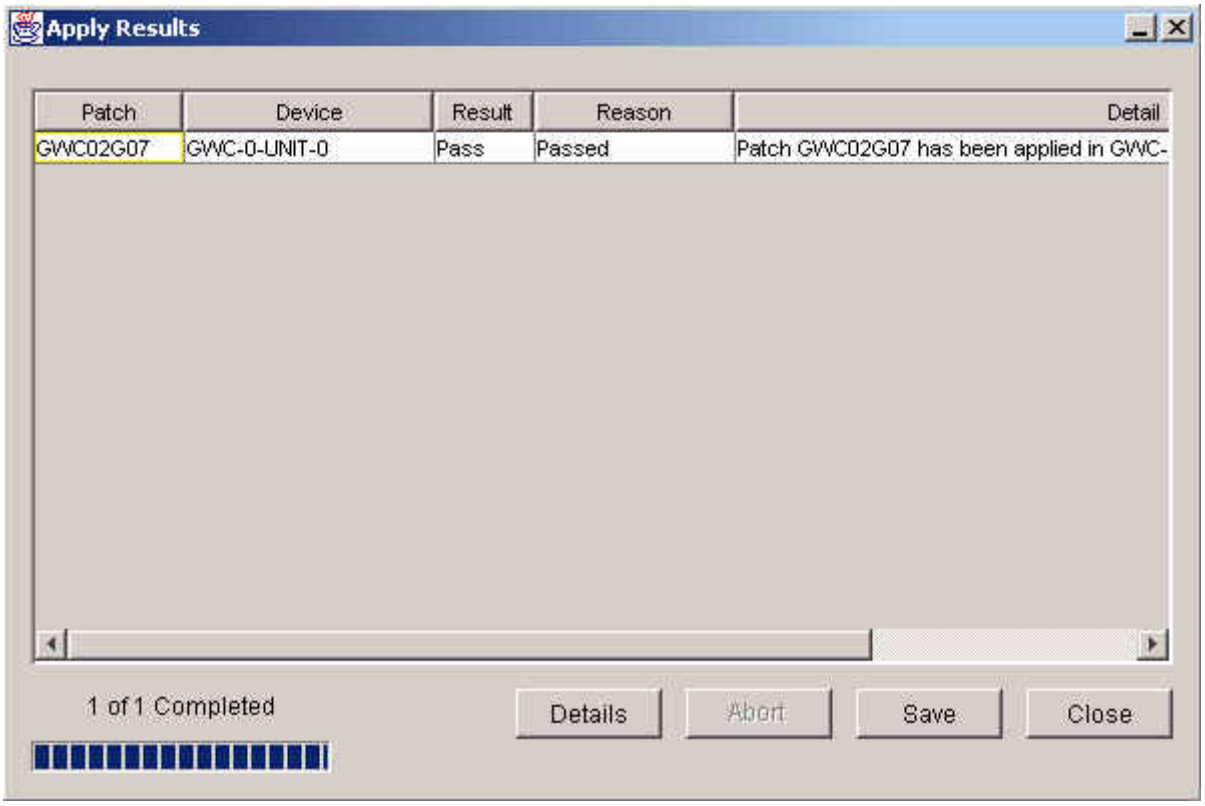
The results of the PreApply phase are displayed.



9 Review the PreApply Results, then click **Continue** to proceed.

If 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
- Succession Element Sub-network Manager
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager components (MG9KEMSERVER and MG9KMIDTIER)
- Core Element Manager
- Network Patch Manager (NPM)
- Client Session Monitor (CSMON)
- Core and Billing Manager (CBM)

To restart a device, refer to procedure Restarting a device using the NPM on page 169 if required.

12 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). You can remove patches using one of the following two NPM interfaces:

- Using the NPM CLUI on page 134
- Using the NPM GUI on page 137

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 143 if required.
- Ensure the patch to be removed is not on hold.
- You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-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 steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. If required, efer to procedure Accessing the Network Patch Manager CLUI on page 167.

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 (CEM)
- Core and Billing Manager (CBM)
- Client Session Monitor (CSMON)
- Network Patch Manager (NPM)

To restart a device, refer to procedure Restarting a device using the NPM on page 169 if required.

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

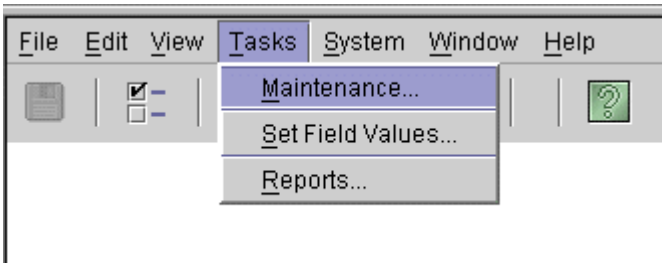
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 183 if required.

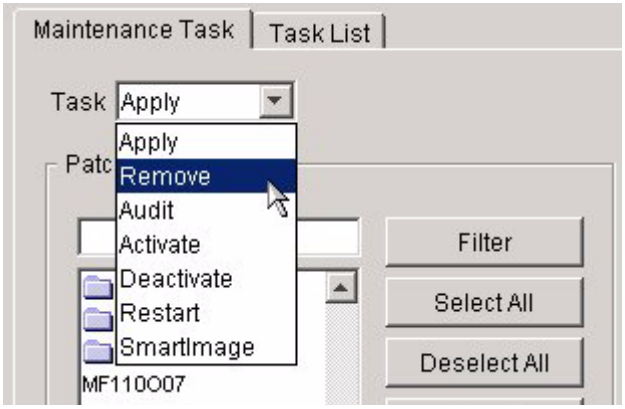
At the NPM GUI

2 On the Tasks menu, click **Maintenance...**.



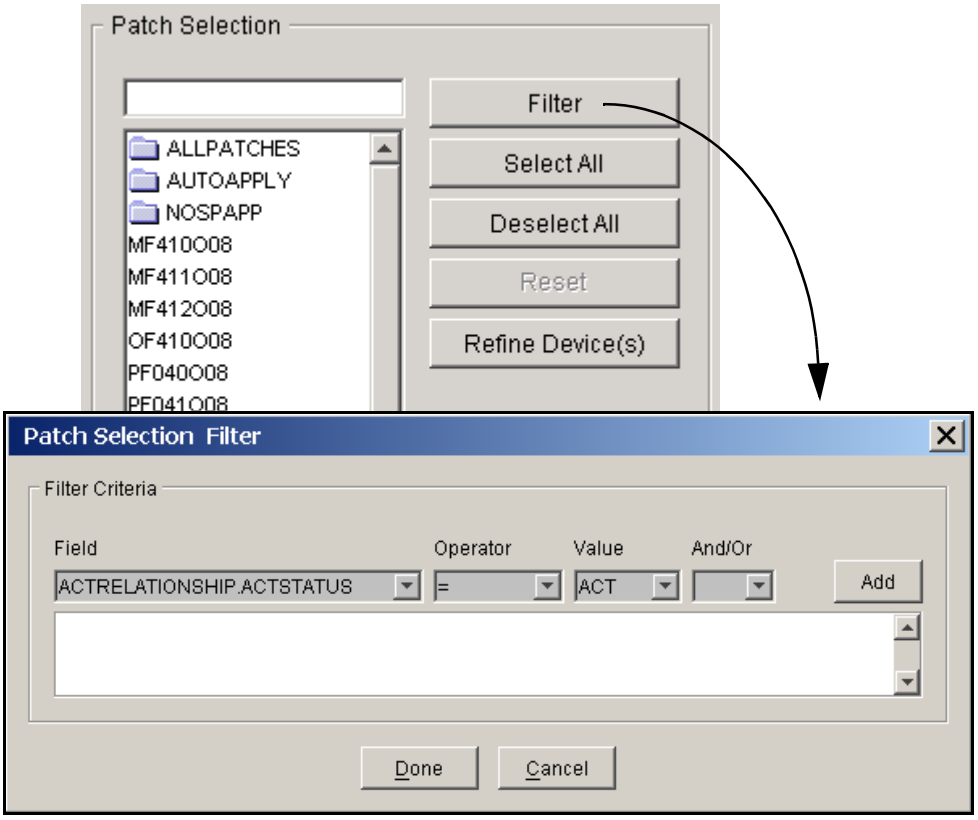
The Maintenance window is displayed.

3 In the Task list, click **Remove**.



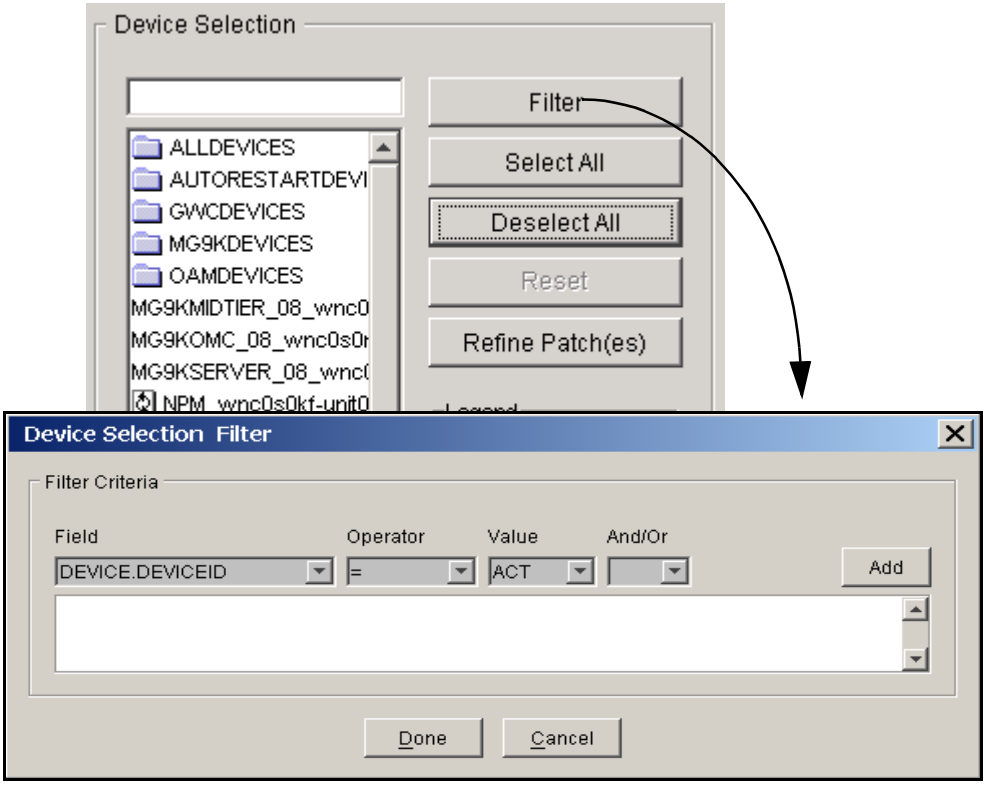
4 In the Patch Selection list, select the patch files or patch sets you want to remove, then click **Refine Device(s)** to display a list of devices to which the patches apply.

To limit the patches displayed in the Patch Selection list, click **Filter** to configure a filtering criteria.

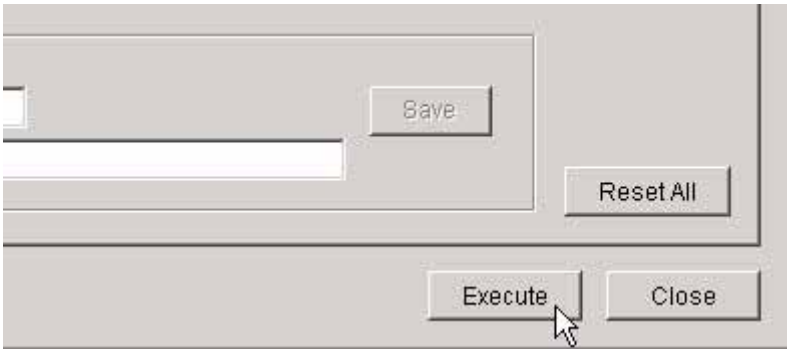


5 In the Device Selection list, select the devices or device sets from which you want to remove the patches.

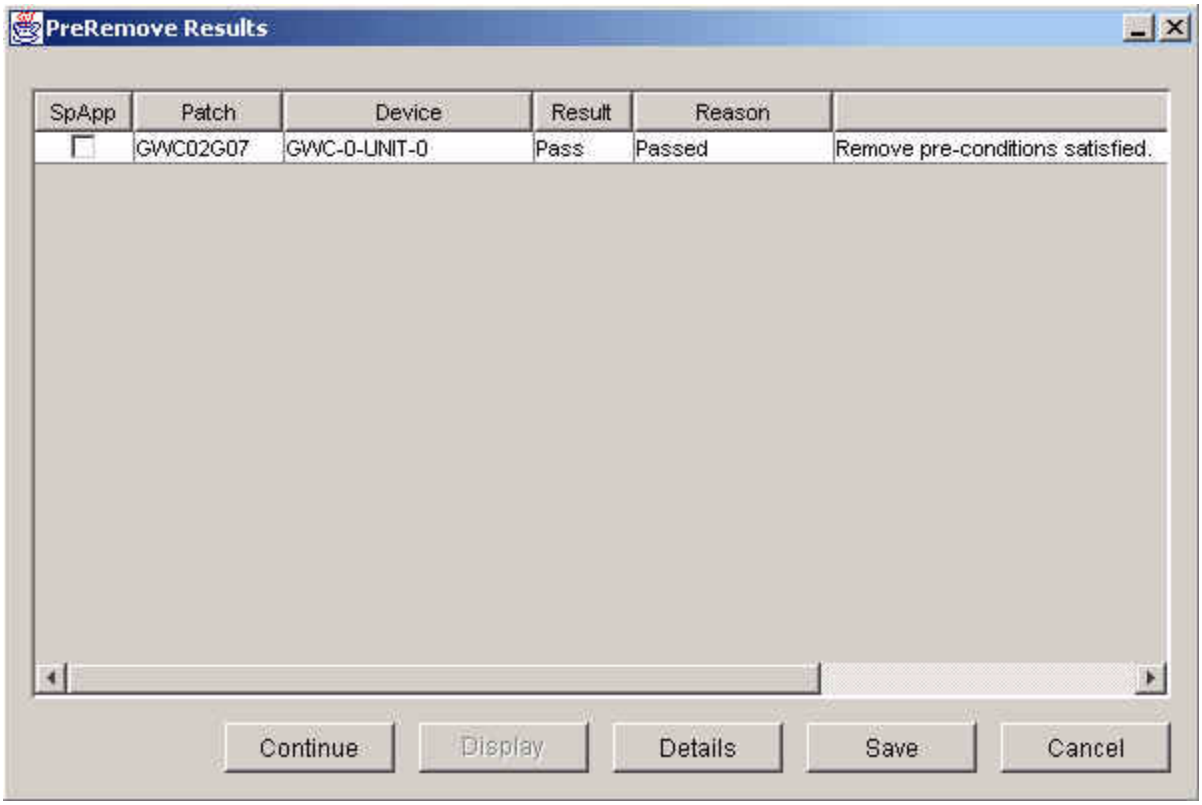
To limit the devices displayed in the Device Selection list, click **Filter** to configure a filtering criteria.



6 Click **Execute** to begin the patch removal process.



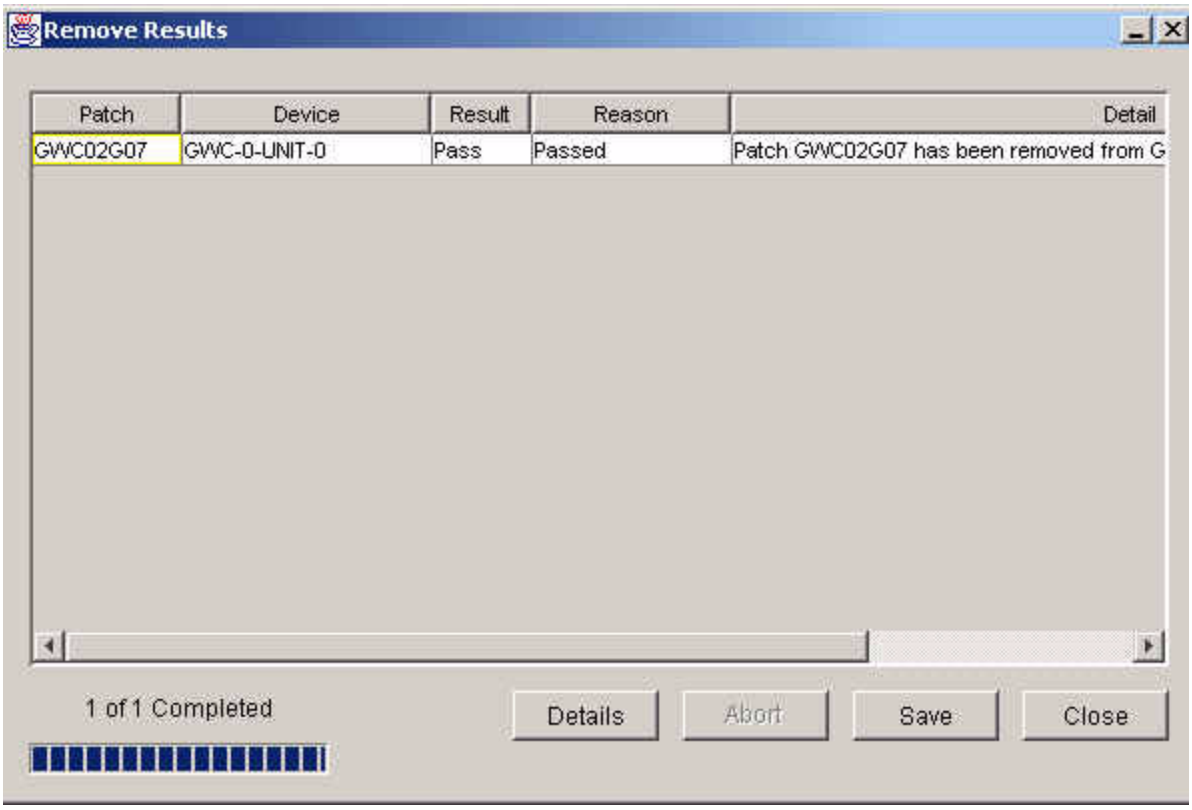
The results of the PreRemove phase are displayed.



7 Review the PreRemove 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 Remove Results window is displayed with results added as each action is completed. Failures from the PreRemove phase are also included in the results.



8 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.

9 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 (CSMON)
- Network Patch Manager (NPM)

To restart a device, refer to procedure Restarting a device using the NPM on page 169 if required.

10 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). You can deactivate patches using one of the following two NPM interfaces:

- Using the NPM CLUI on page 144
- Using the NPM GUI on page 145

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.

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-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 steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 167.

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

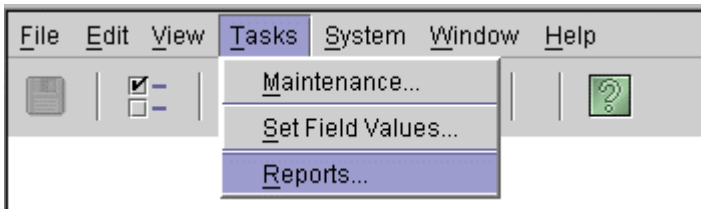
At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 183.

At the NPM GUI

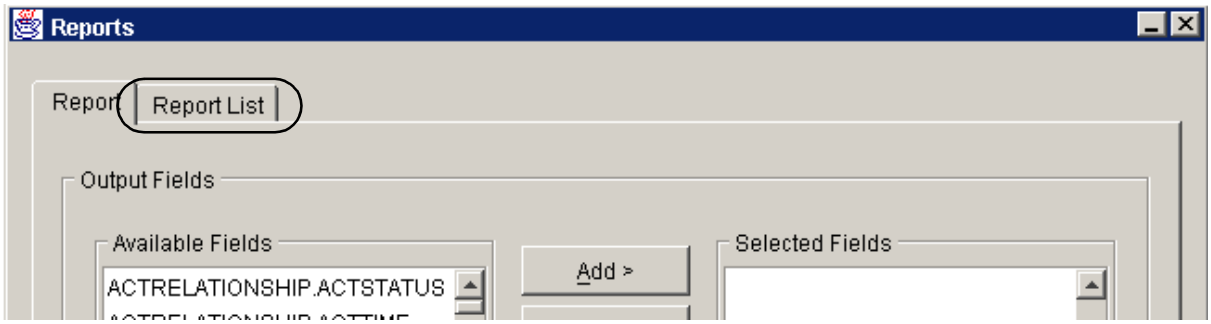
2 Query the NPM for a list of patches that are activated as follows:

a On the Tasks menu, click **Reports...**.

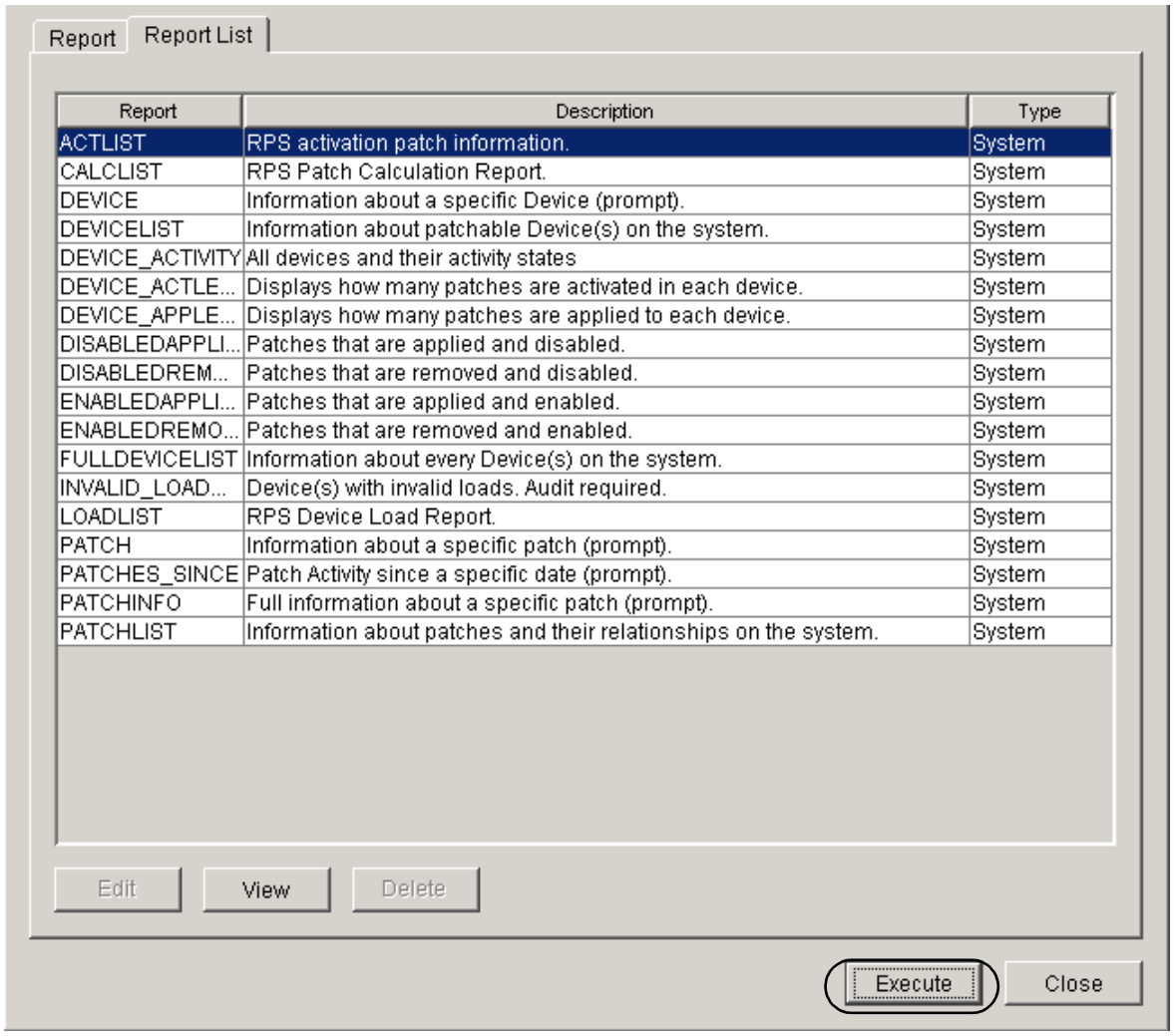


The Reports window is displayed.

b Click the **Report List** tab.

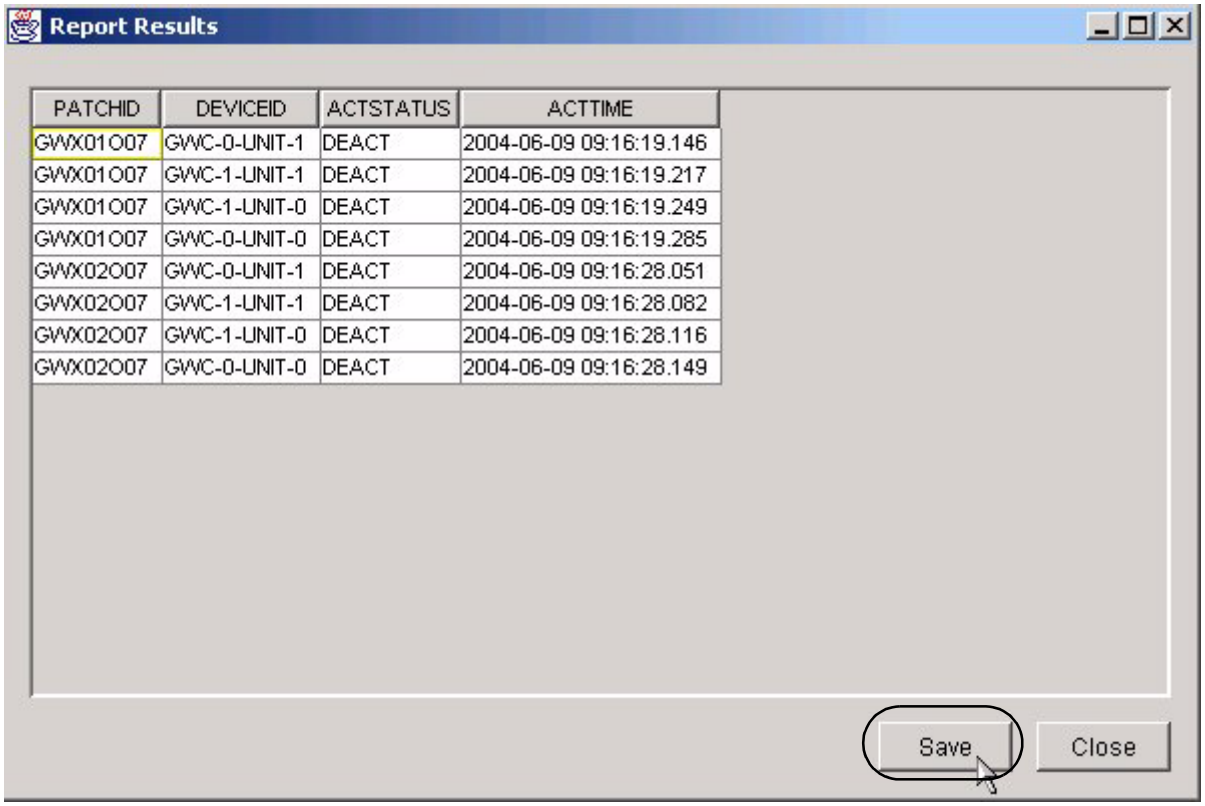


c Click the **ACTLIST** entry in the Report field, then click **Execute**.



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.

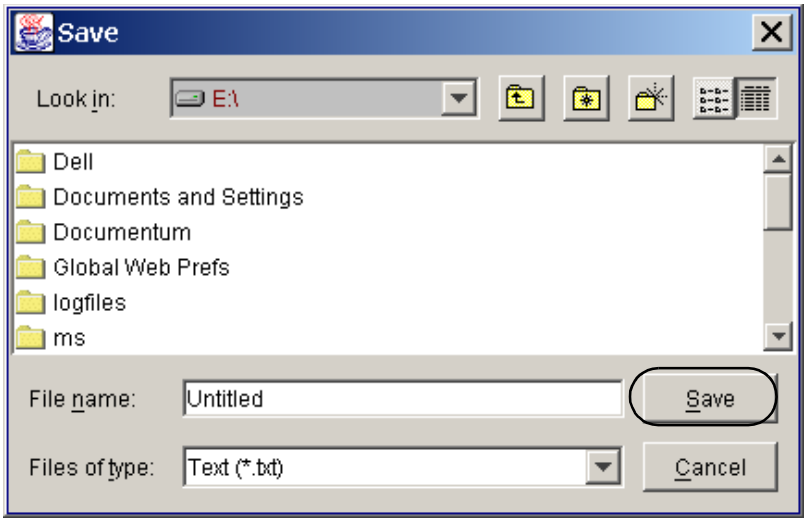
Note: If there are no patches to deactivate, the system returns a dialog box indicating that the report has “empty results”.



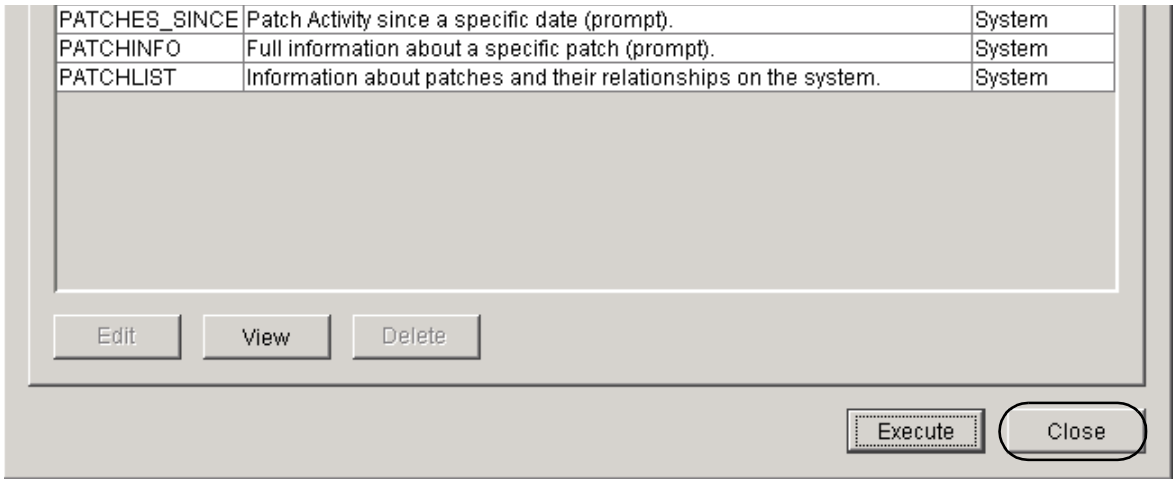
e If necessary, save a copy of the report to a text file as follows:

i Click **Save**.

ii Type a file name in the File name: box, and click **Save**.

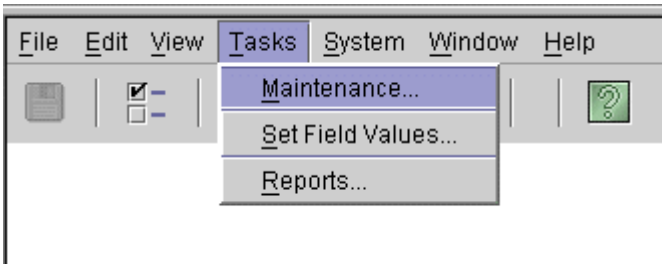


f Click **Close** to close the Reports window.



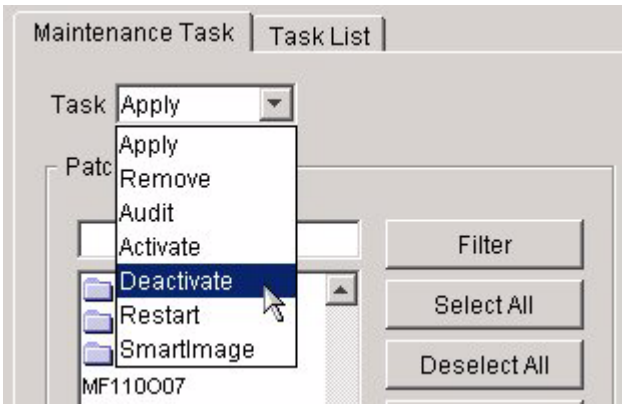
3 Deactivate one or more patches for one or more devices as follows:

a On the Tasks menu, click **Maintenance...**.



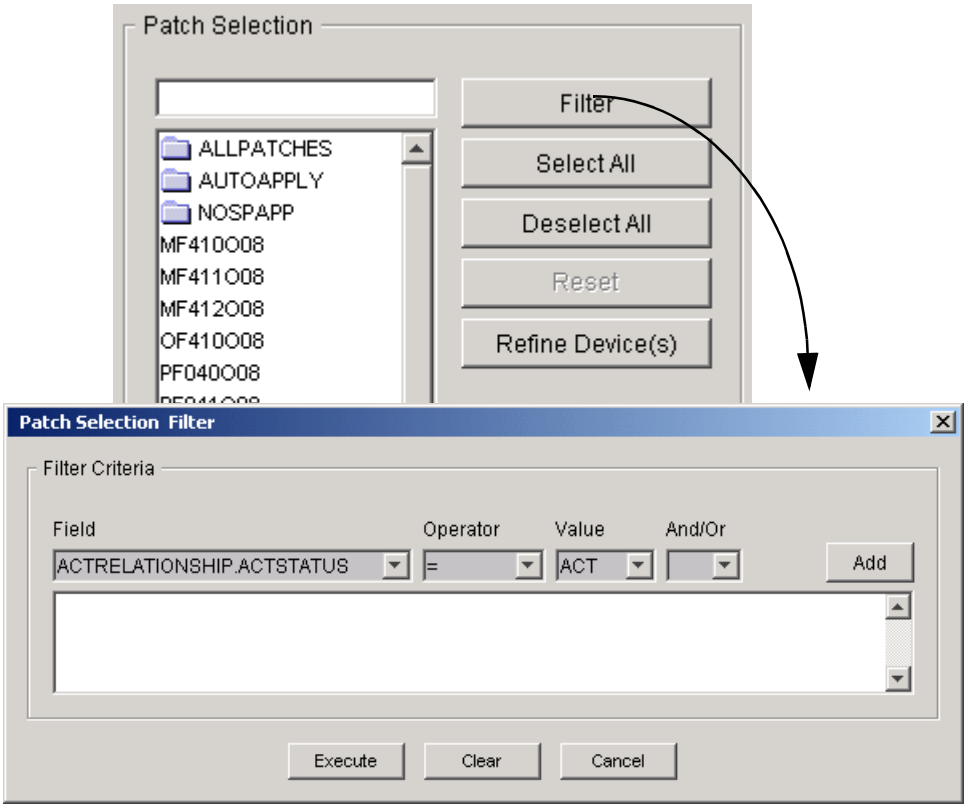
The Maintenance window is displayed.

b In the Task list, click **Deactivate**.



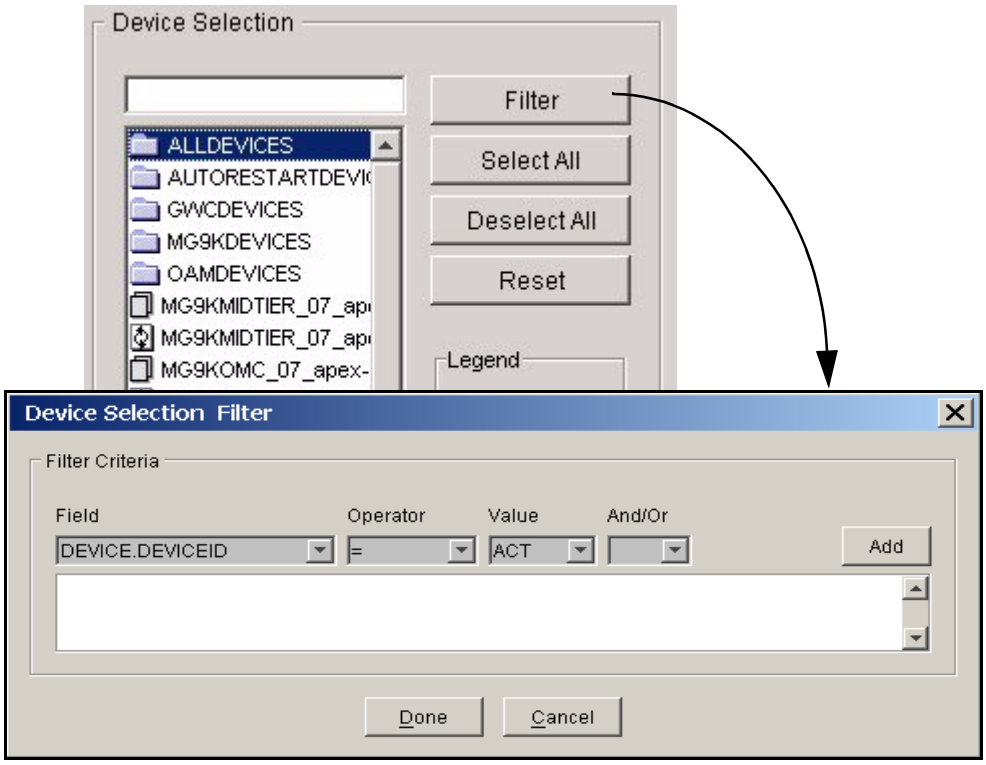
c In the Patch Selection list, select the patch files or patch sets you want to deactivate, then click **Refine Device(s)** to display a list of devices to which the patches apply.

To limit the patches displayed in the Patch Selection list, click **Filter** to configure a filtering criteria.

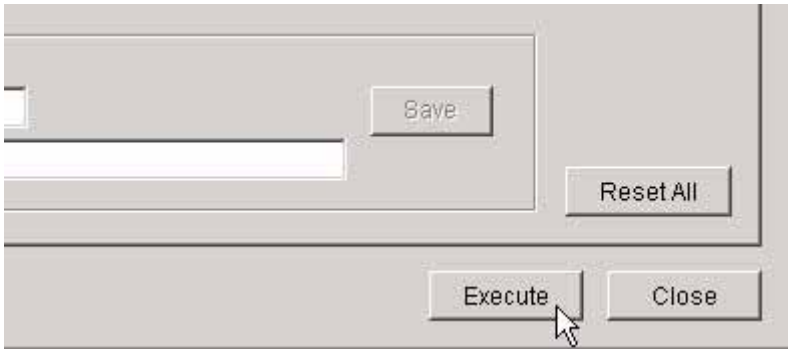


d In the Device Selection list, select the devices or device sets that have the applied patches you want to deactivate.

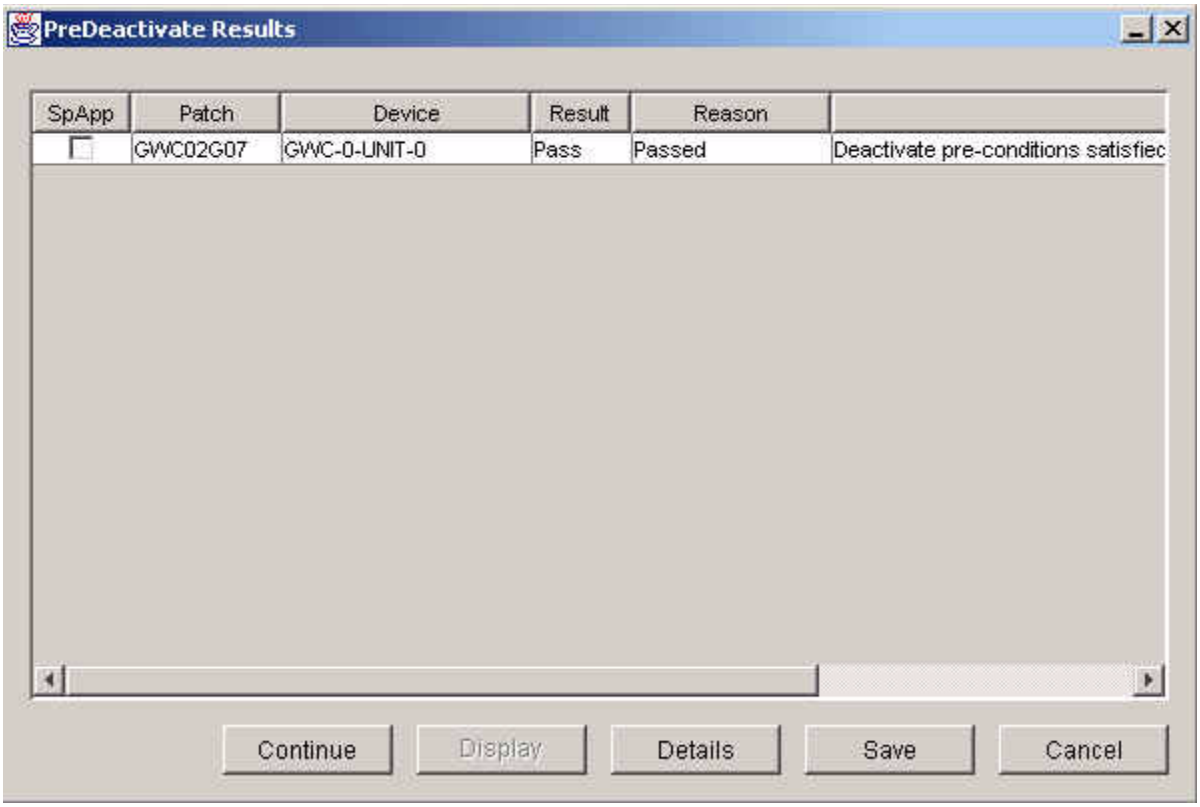
To limit the devices displayed in the Device Selection list, click **Filter** to configure a filtering criteria.



e Click **Execute** to begin the patch deactivation process.

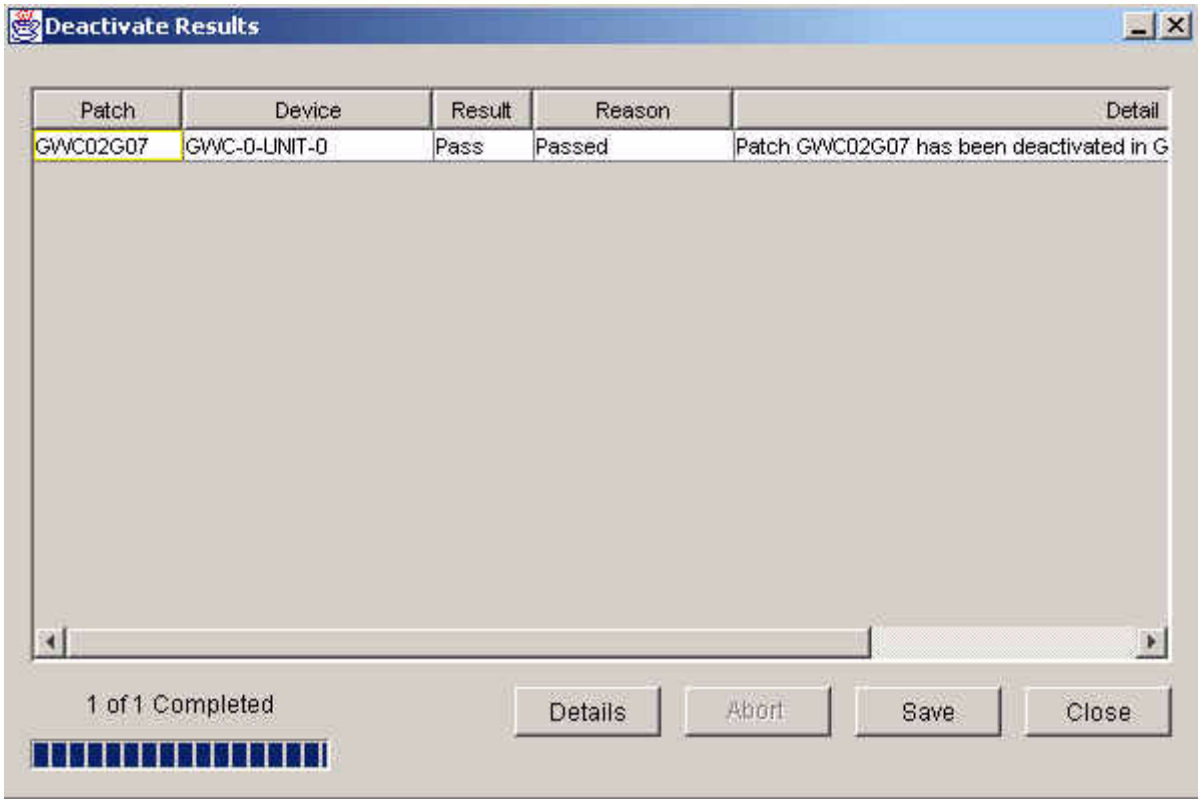


The results of the Pre-deactivate phase are displayed.



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.

Performing a device audit using the NPM

Application

Use this procedure to perform a device audit using the Network Patch Manager (NPM). You can perform a device audit using one of the following two NPM interfaces:

- Using the NPM CLUI on page 155
- Using the NPM GUI on page 156

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 procedure Transferring patches delivered on CD to the NPM database on page 119.

ATTENTION
It is recommended that you perform an audit on devices prior to patching.

Prerequisites

You must be assigned to user group emsadm to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-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 steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 167.

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.

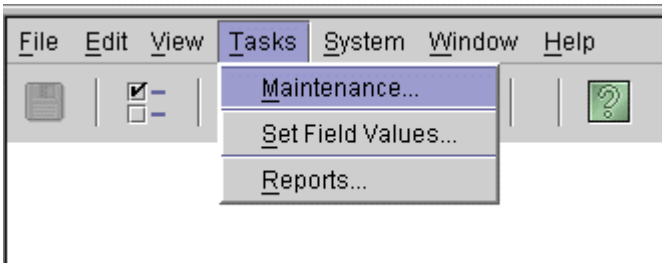
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 183.

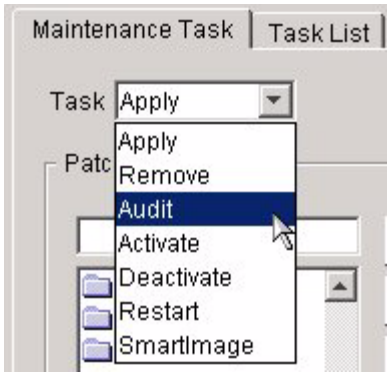
At the NPM GUI

2 On the Tasks menu, click **Maintenance...**.

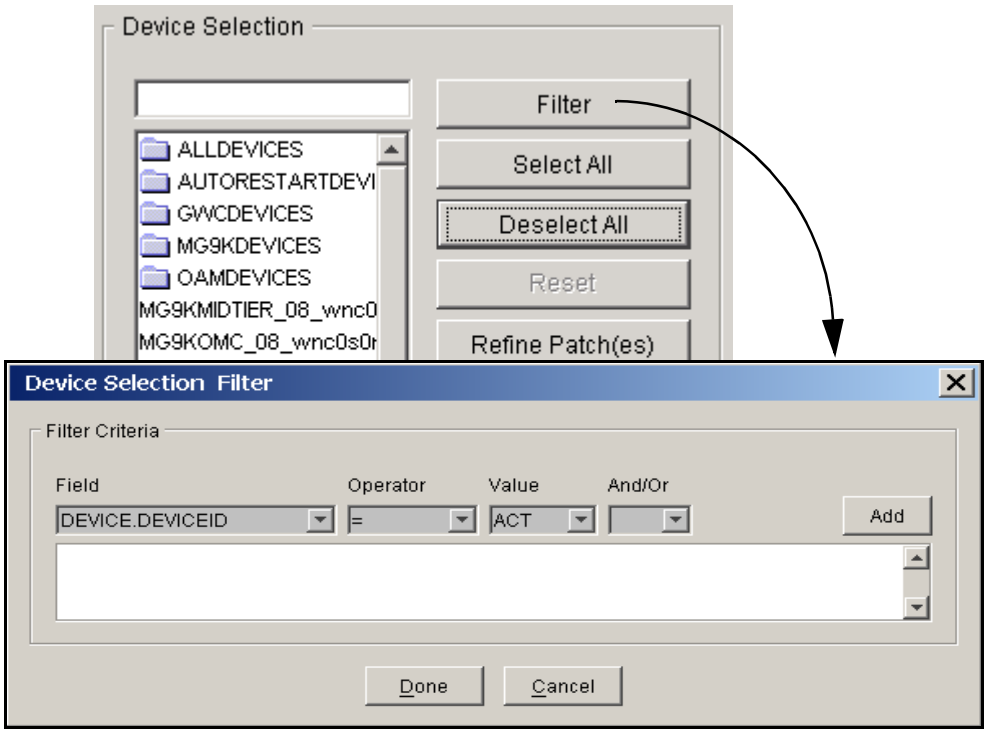


The Maintenance window is displayed.

3 In the Task list, click **Audit**.

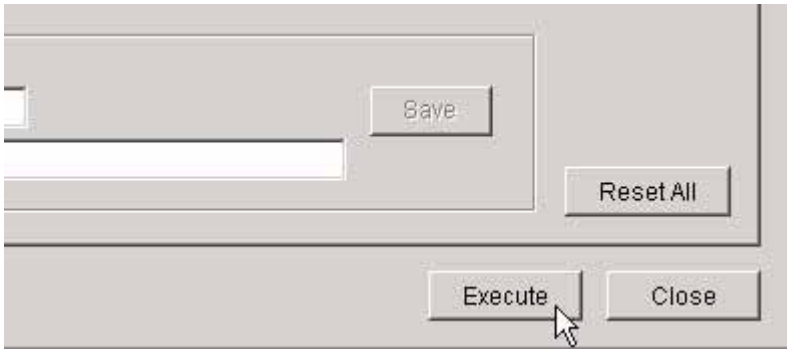


4 In the Device Selection list, select the devices or device sets that you want to audit.

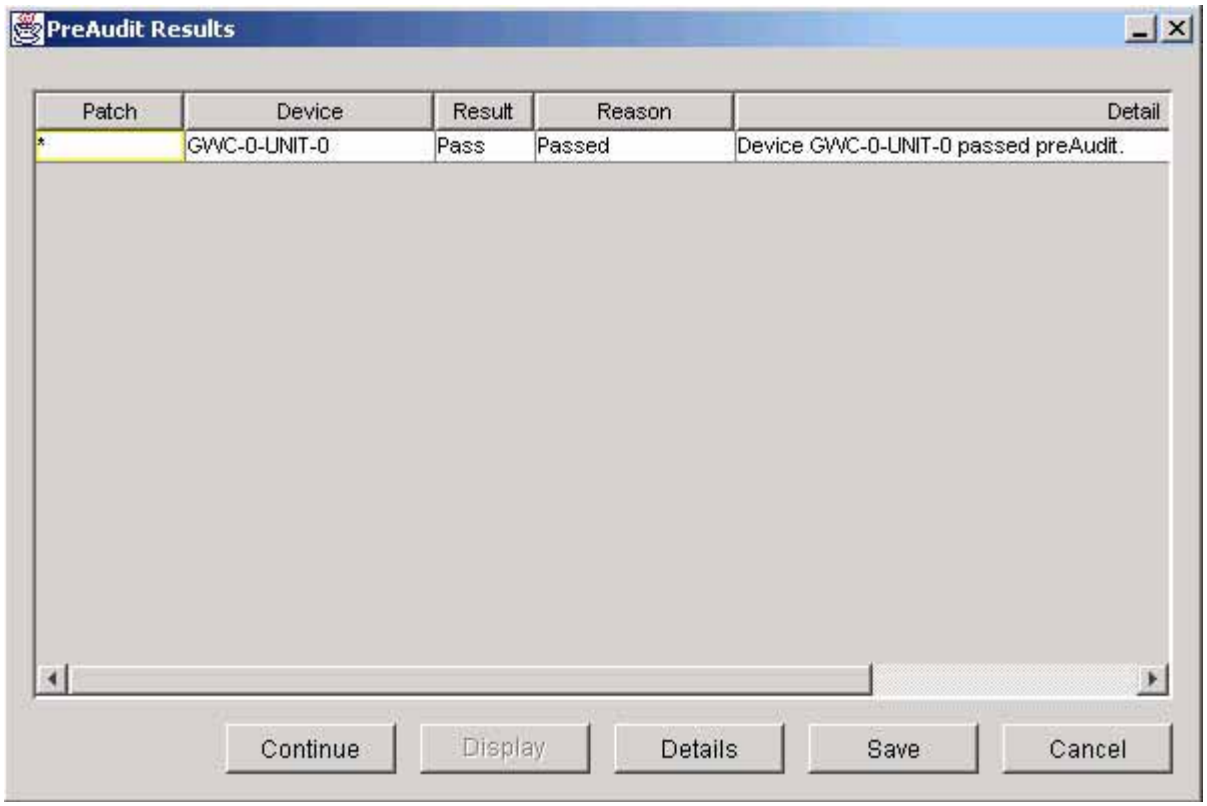


5 To limit the devices displayed in the Device Selection list, click **Filter** to configure a filtering criteria.

6 Click **Execute** to begin the audit process.



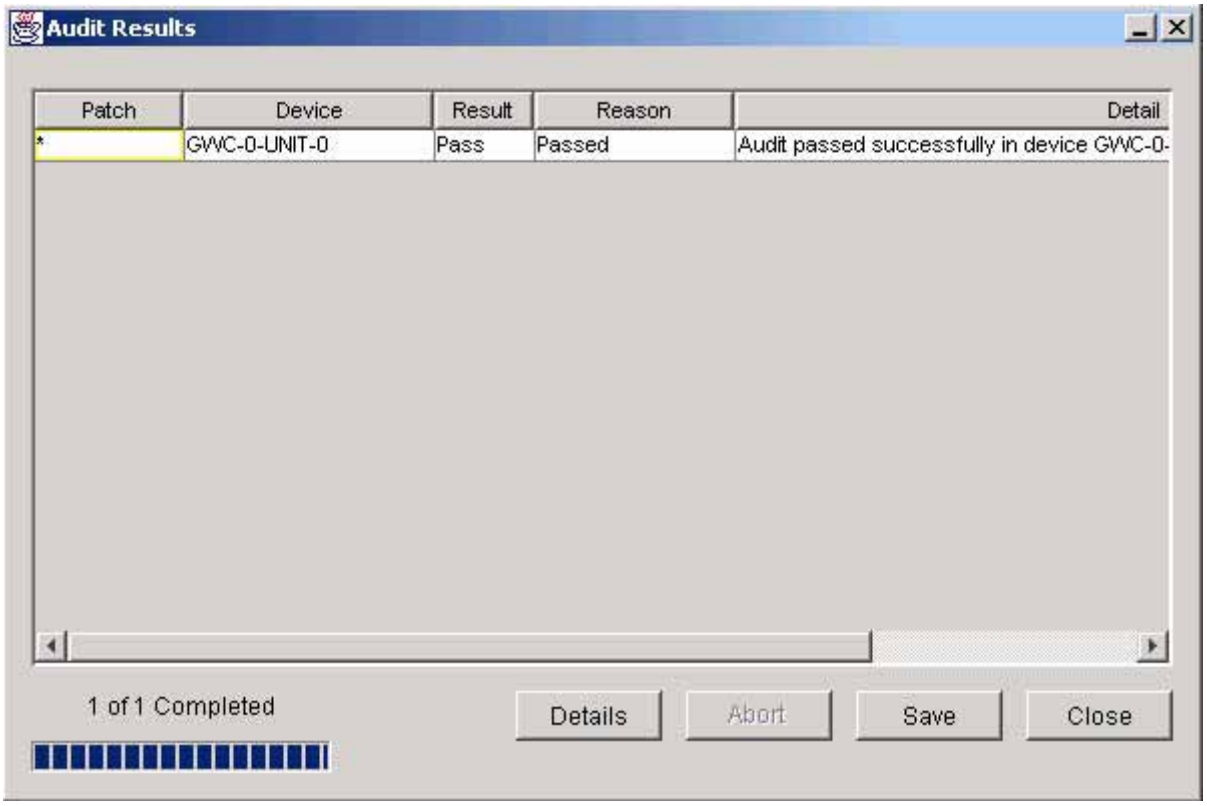
The results of the PreAudit phase are displayed.



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.

Defining NPM patching reports

Application

Use this procedure to define a patching report using one of the following two Network Patch Manager (NPM) interfaces:

- Using the NPM CLUI on page 162
- Using the NPM GUI on page 163

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 155, 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 Thsi 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

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-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 steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. If required, refer to procedure Accessing the Network Patch Manager CLUI on page 167.

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

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	**viewreport <reportname>**
view all defined reports	**viewreport all**
generate a report	**runreport <reportname>**
delete a user-defined report	**delreport <reportname>** ***Note:*** 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.

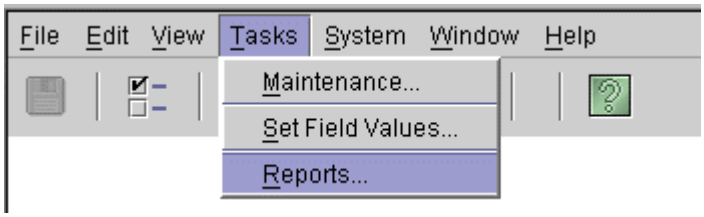
Using the NPM GUI

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 183.

At the NPM GUI

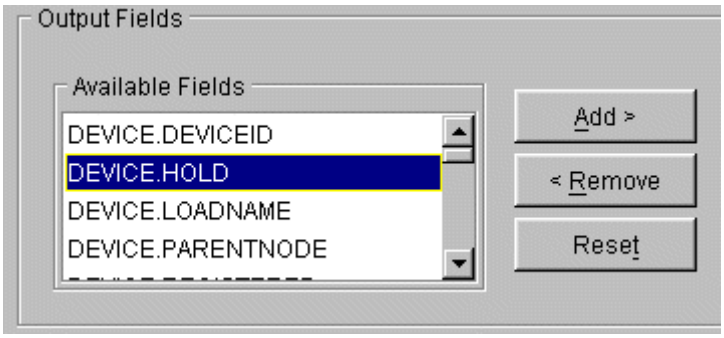
2 On the Tasks menu, click **Reports...**.



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.



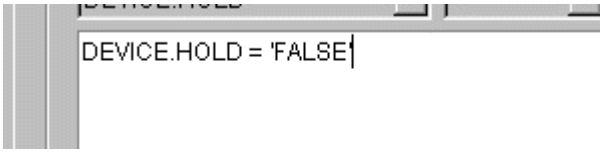
b Click **Add** to add the field to the Selected Fields list.

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.

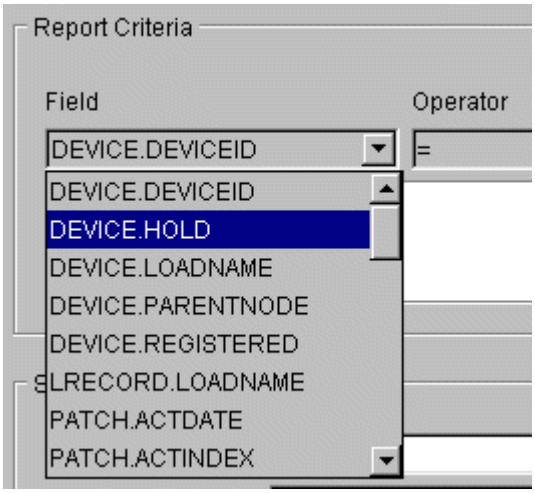
Note: Insert parenthesis "()" to define precedence for multiple criteria statements.



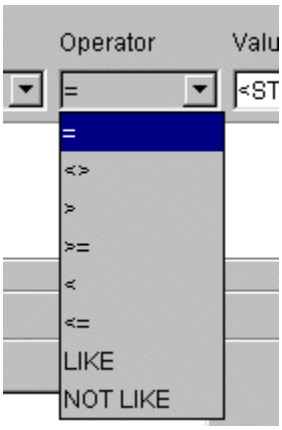
OR

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.

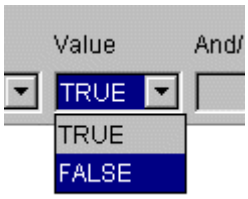


The table below lists the supported operators and their meaning.

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.



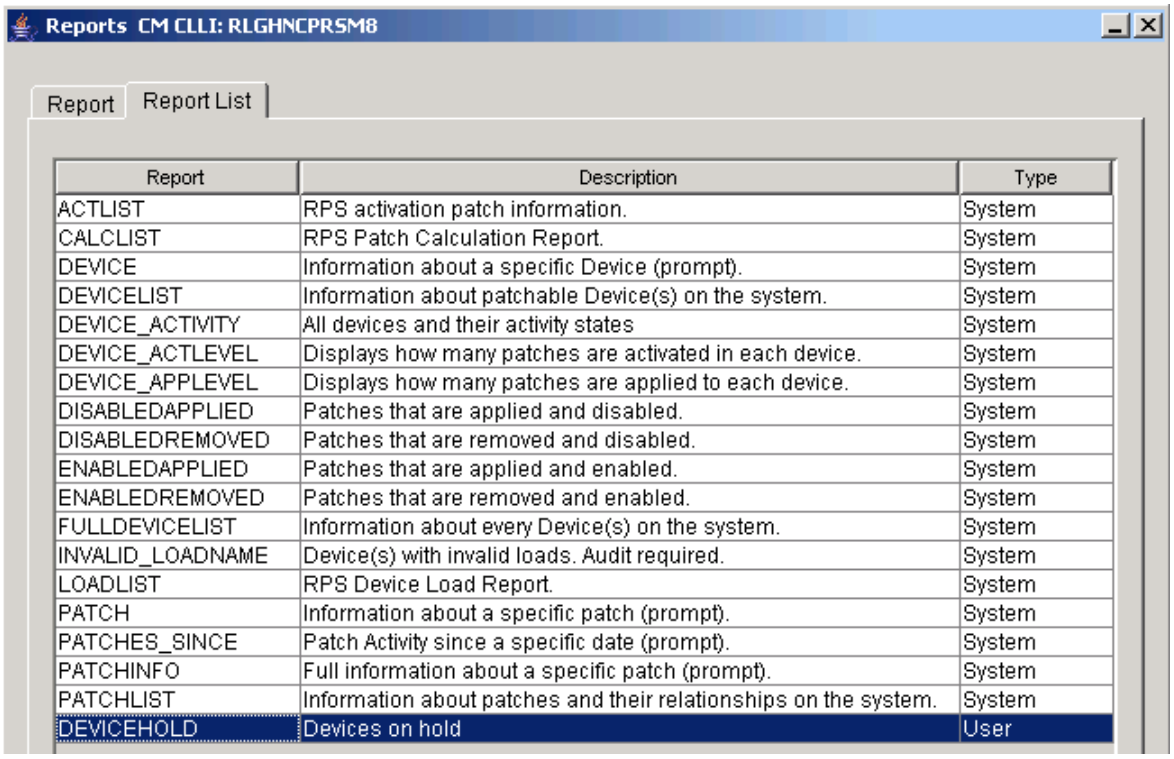
To combine multiple criteria statements, click **AND** or **OR** in the And/Or list.

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.



To	Action
view or edit the definition of a report	select the report from the ReportList tab and click **Edit**
generate a report	select the report from the ReportList tab and click **Execute**
delete a user-defined report	select the report from the ReportList tab and click **Delete** ***Note:*** 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.

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 183.

Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group emsadm to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.

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 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 SSPFS-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 SSPFS-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.

Restarting a device using the NPM

Application

Use this procedure to restart a device using the Network Patch Manager (NPM). You can restart a device using one of the following two NPM interfaces:

- Using the NPM CLUI on page 170
- Using the NPM GUI on page 173

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
- 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 (CSMON)
- 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 Succession Server Platform Foundation Software (SSPFS). Refer to the specific SSPFS 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.
- You must be assigned to user group emsadm to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SSPFS-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 steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

CAUTION

Stop or complete any maintenance activities associated with the patched device before you begin the restart.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM client applications on page 183.

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 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

4 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.
```

5 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...
```

6

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 155 if required.

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 183.

At the NPM GUI

2 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.

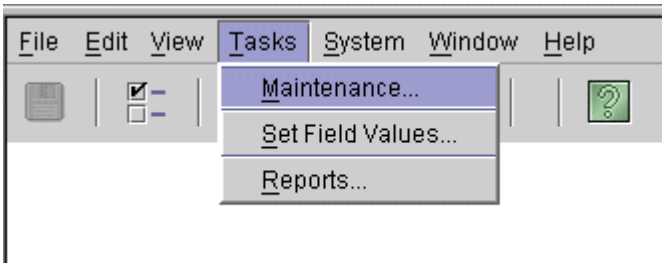
b Click **ENABLEDREMOVED** and then click **Execute**.

Once the report displays, a restart is required to disable the patches for the listed devices.

c Click **DISABLEDAPPLIED** and then click **Execute**.

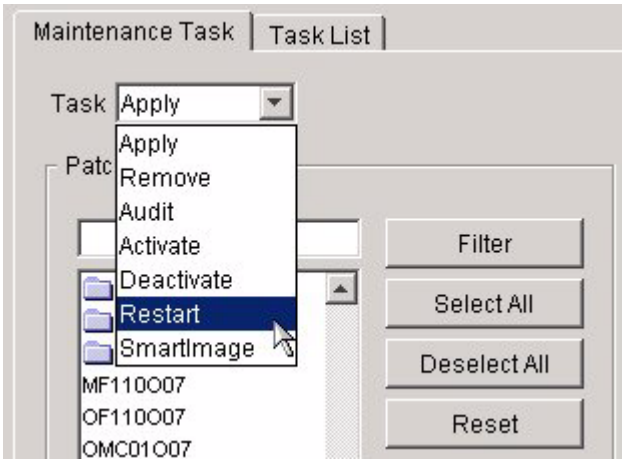
Once the report displays, a restart is required to enable the patches for the listed devices.

3 On the Tasks menu, click **Maintenance**.

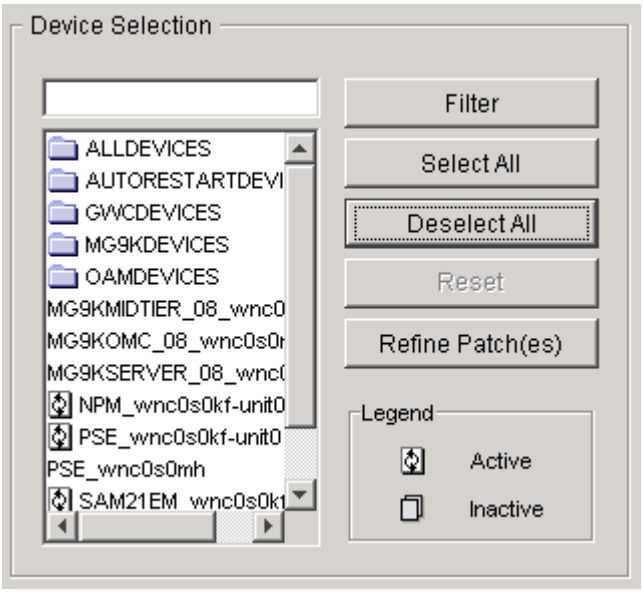


The Maintenance window is displayed.

4 In the Task list, click **Restart**.



5 In the Device Selection list, select the device, device list, or device set that you want to restart.



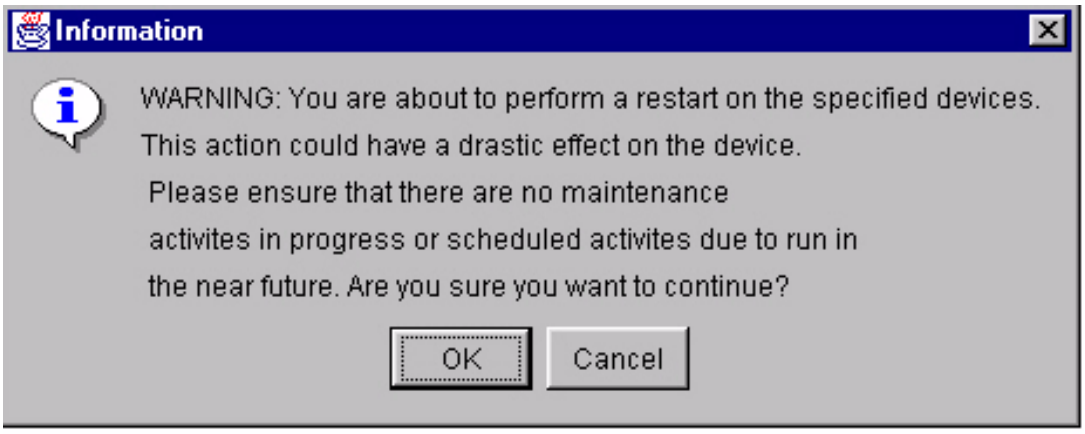
6

ATTENTION

Restarting the NPM makes it unavailable until it has successfully restarted. You will need to log in once it has restarted.

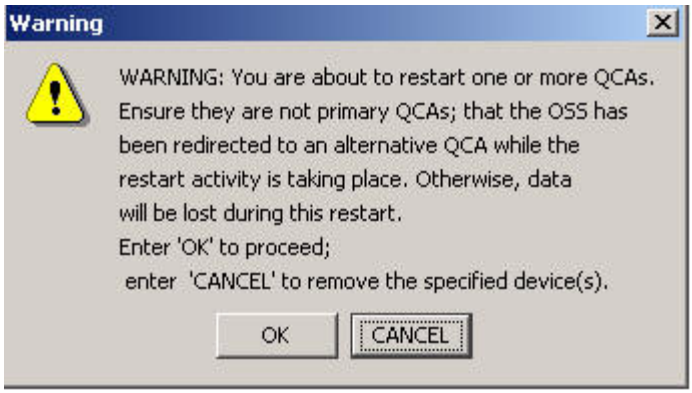
Click **Execute** to begin the restart.

The system returns the following warning.



7 Click **OK** to begin the restart.

If you are restarting a QCA device, the system returns the following warning:

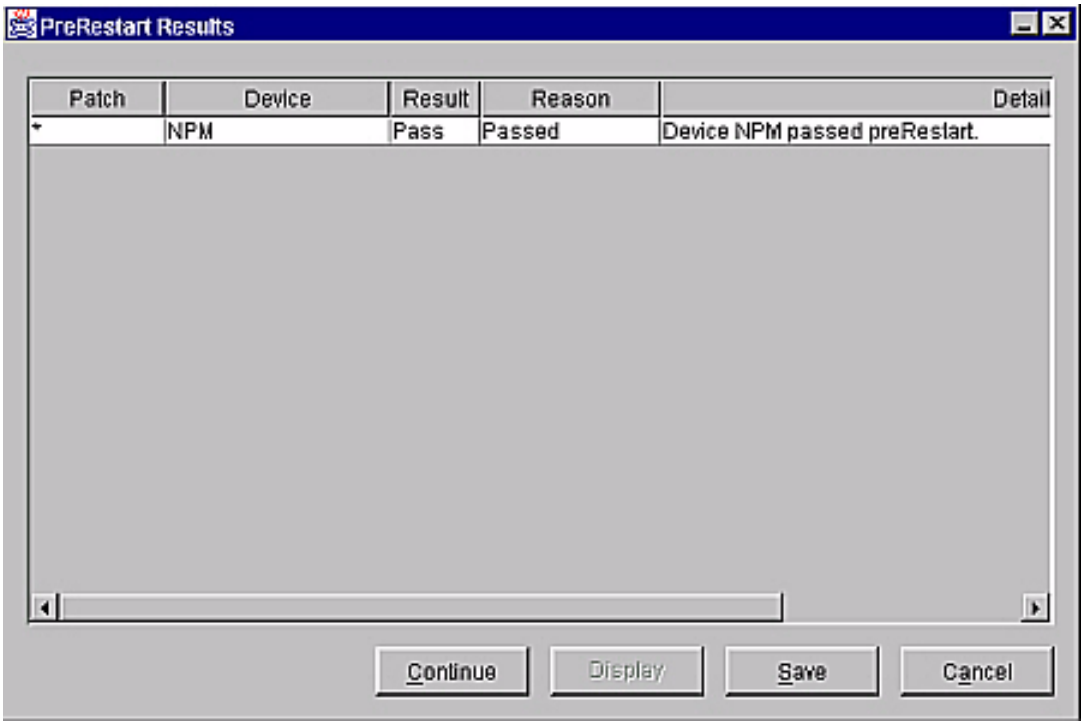


8

CAUTION
Loss of data
Carefully read the warning about QCAs before you proceed with a QCA restart.

If restarting a QCA is acceptable, click **OK** to proceed with the restart, otherwise click Cancel.

The results of the PreRestart phase are displayed.



9 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 155 if required.

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 through ESD to the NPM database

Application

Use this procedure to obtain NPM patch files if you are using ESD. This procedure should be performed on the machine where the NPM application is resident. In an HA cluster configuration, this procedure should be run on the Active unit.

Prerequisites

None

Action

Perform the steps that follow complete this procedure.

> **ATTENTION**
> In a two-server configuration, perform the steps that follow on the active server.

Obtaining the NPM patch files from ESD

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 SSPFS-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 SSPFS-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.

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 Make a directory for the patch files you want to install by typing

```
# mkdir /<directory>
```

and pressing the Enter key.

where

directory
is a valid directory name

Example

```
# mkdir /esd_patches
```

5 Change the permissions on the newly created directory by typing

 # chmod 777 /<directory>

and pressing the Enter key.

where

directory
is the directory name from step 4

Example

```
# chmod 777 /esd_patches
```

6 Access the newly created directory by typing

 # cd /<directory>

and pressing the Enter key.

where

directory
is the directory name from step 4

Example

```
# cd /esd_patches
```

7 Log in to the ESD server through FTP by typing

 # ftp <esd_server>

and pressing the Enter key.

where

esd_server
is the IP address of the ESD server

8 When prompted, enter your user ID and password for the ESD server.

9 Obtain a list of files and directories on the ESD server by typing

ftp> dir

and pressing the Enter key. Note the name and timestamp of the .tar.gz file.

10 Set the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

11 Transfer all the patches from the ESD server to the NPM by typing

```
ftp> mget *.patch
```

and pressing the Enter key.

To transfer individual patch files, type

```
ftp> get <patchfilename>
```

where

patchfilename
is the name of the patch you are transferring

12 Exit FTP by typing

```
ftp> quit
```

and pressing the Enter key.

13 Verify the patches are in the temporary directory on the Sun server that you created in step 4 by typing

```
# ls
```

and pressing the Enter key.

14 Change permissions for the patch files in the directory by typing

```
# chmod 777 *
```

and pressing the Enter key.

15

If	Do
you have access to http://www.nortel.com	step 16
you do not have access to http://www.nortel.com	step 17

16 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 first eight characters of the .tar.gzip file associated with the software component being upgraded and the date is the date of the file shown in step 9 above.

17 Create a patchlist file by typing

```
# ls *.patch > current.patchlist
```

18 Verify the NPM server application is running by typing

```
# servquery -status -group NPM
```

and pressing the Enter key.

19

If the NPM server is	Do
running	step 21
not running	step 20

20 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

21 Access the NPM command line interface (CLUI) by typing

```
# npm
```

and pressing the Enter key.

22 When prompted, enter your user ID and password.

Note: Do not change directories.

23 Retrieve the patch files for the NPM to process by typing

```
# getpatch current.patchlist
```

24 Quit from the NPM CLUI. Then, erase the downloaded patch files int the directory you created in step 4 by typing

```
# cd <directory>
```

(if not still in the directory), followed by typing

```
# rm *.patch
```

and pressing the Enter key.

where

directory
is the directory you created in step 4

25

If the network element to be patched is	Do
a GWC or MG 9000	Applying patches using the NPM on page 125
located on any simplex machine or an HA cluster that the NPM does NOT reside on	Applying patches using the NPM on page 125
located on an HA cluster that the NPM resides on	Patching the inactive node of a cluster during an upgrade on page 102

26 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 SSPFS-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 167.

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

- Launching applications from a web browser on page 185. You must use this method when launching an application for the first time.
- Launching applications from the JWS Application Manager on page 188.

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

- Launching applications from a desktop icon or Start menu (Windows only) on page 190.

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

- Launching specific applications using a URL on page 193.

  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 SSPFS-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 SSPFS-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

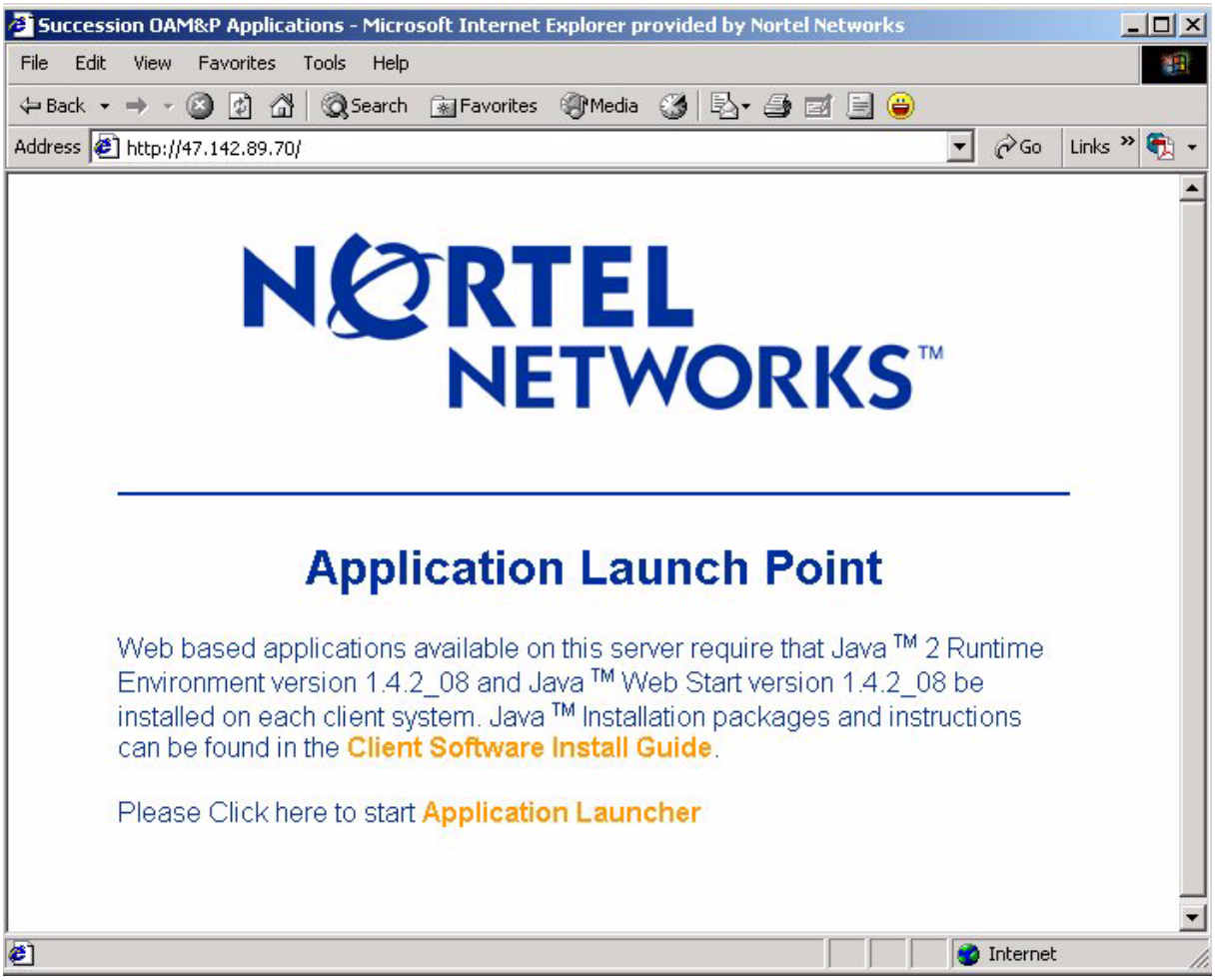
Launching applications from a web browser

At your workstation

1 Launch your web browser.

2 In the Address field, enter the name or IP address of the SSPFS-based server where the CS 2000 Management Tools are installed.

The Application Launch Point page appears.



3 Use the following table to determine your next step.

If	Do
you have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 9
you do not have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 4
you do not know which version of JRE and JWS you have	step 4

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

If	Do
you have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 8
you do not have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 5

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

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

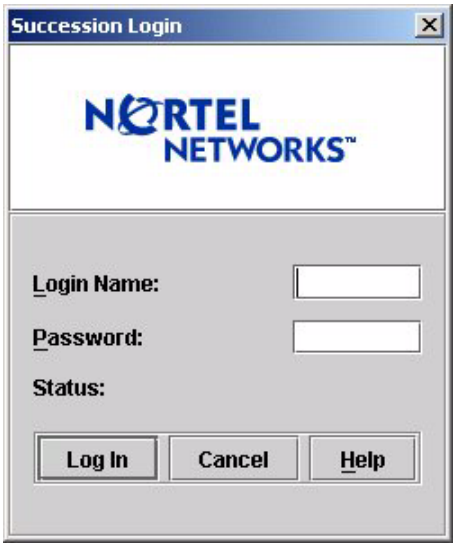
7 Click **Java 2 Runtime Environment Software Download** under Microsoft Windows or Sun Solaris to download and install the software.

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

8 Click **Back** to return to the Application Launch Point.

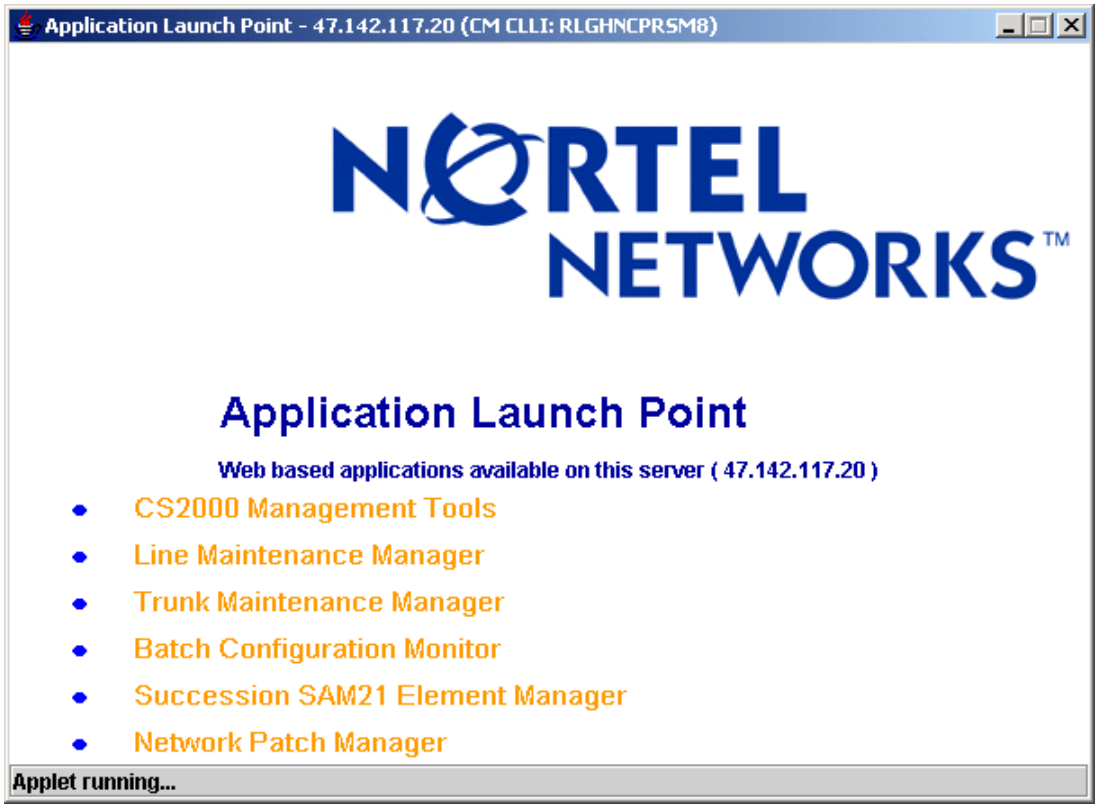
9 Click **Application Launcher**.

The Login window appears.



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

The Application Launch Point, similar to following, appears.



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

If you delay clicking an application link by 5 minutes or more after you log in, the login window will appear requiring you to log in again.

The interface for the application you launched, is displayed.

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

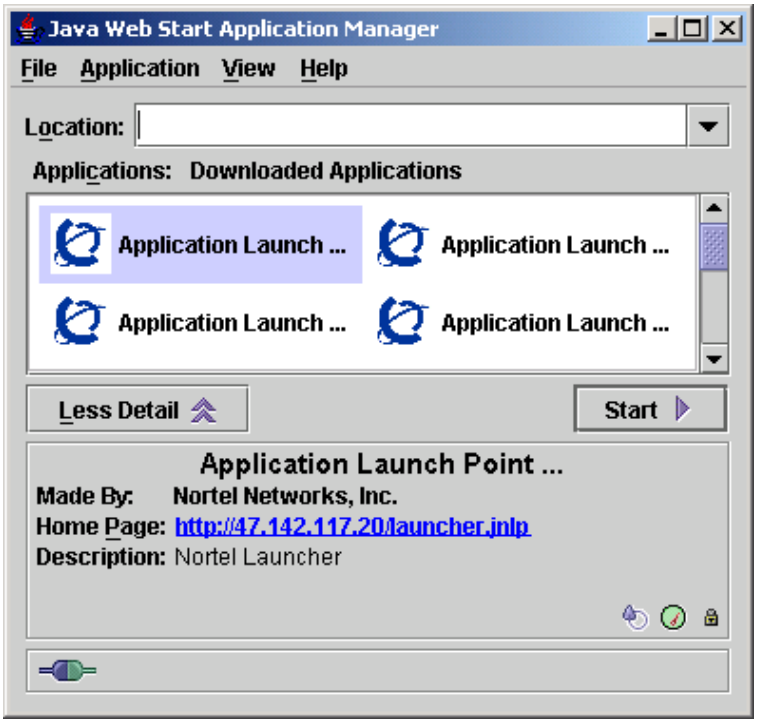
Launching applications from the JWS Application Manager

ATTENTION

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

At your workstation

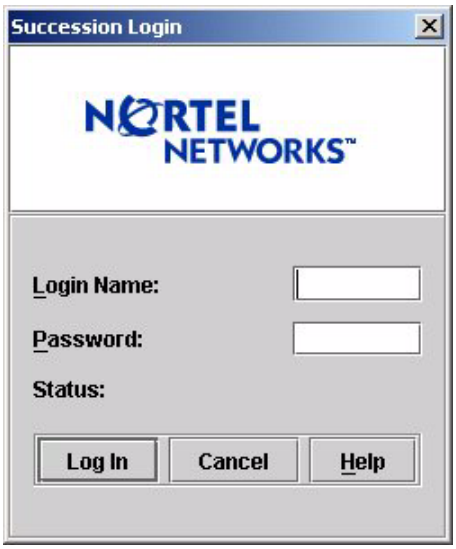
1 Launch the Java Web Start Application Manager.



2 If you do not see the downloaded applications as shown in the previous figure, then on the View menu click **Downloaded Applications**. Otherwise, skip to the next step.

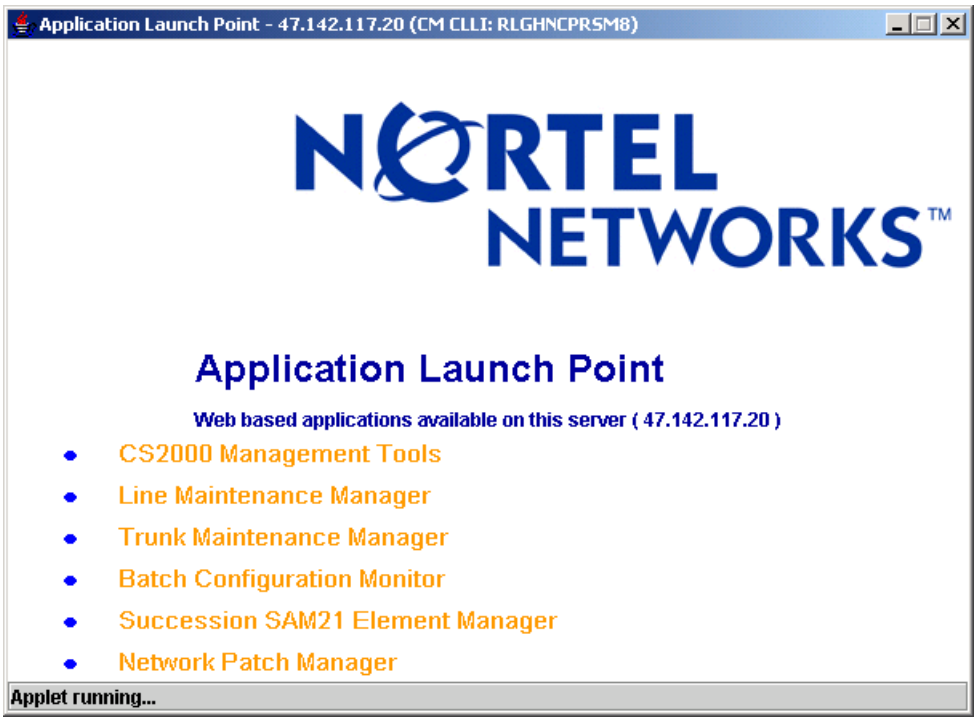
3 Double-click the Application Launch Point you want to access, or select the Application Launch Point and click Start.

The Login window appears.



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

The Application Launch Point, similar to following, appears.



5 Click the link for the application you want to launch.

The interface for the application you launched, is displayed.

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

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

ATTENTION

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

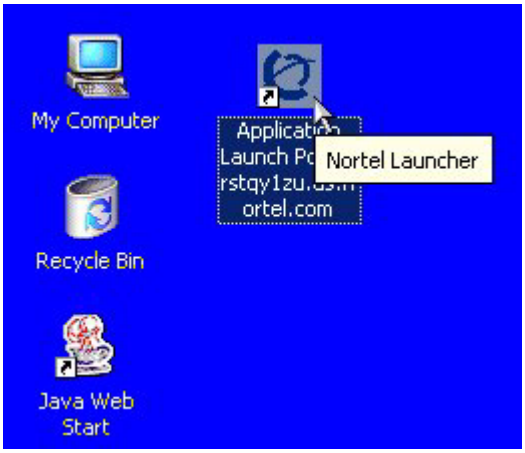
At your workstation

1 Use the following table to determine your next step.

If you want to launch an application from	Do
a desktop icon	step 2
the Start menu	step 4

2 To launch a CS 2000 Management Tools client application from a desktop icon, locate the short-cut icon on your desktop, and double-click it to start the application.

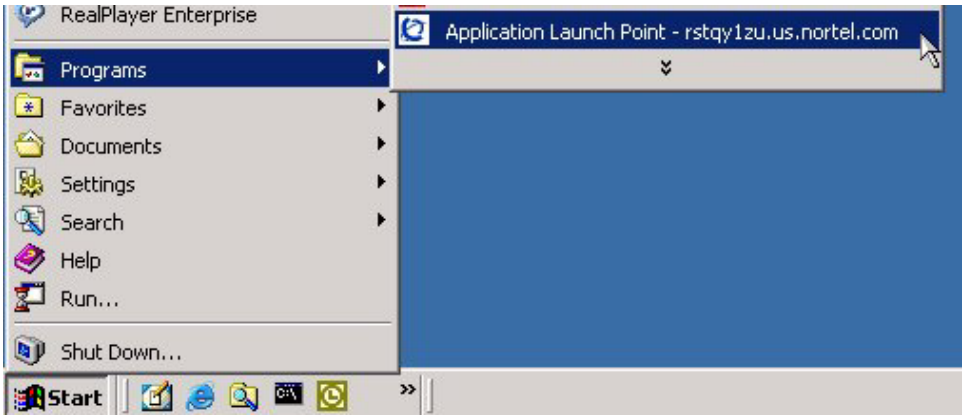
Note: For short-cut icons to be present on your desktop, you must have the correct settings under the Shortcut Options tab. Access the Shortcut Options tab through File->Preferences in the JWS Application Manager.



The Login window appears.

3 Proceed to step 5.

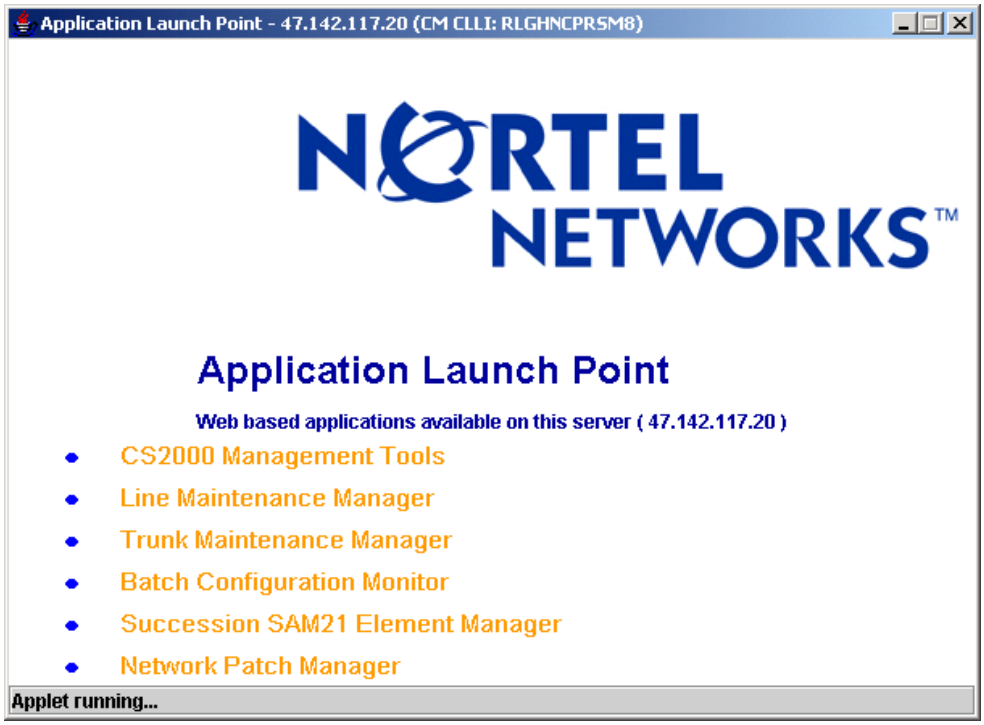
4 To launch a CS 2000 Management Tools client application from the Start menu, click Start->Programs, then click the CS 2000 Management Tools client application you want to launch.



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 185.

At your workstation

1 Launch your web browser.

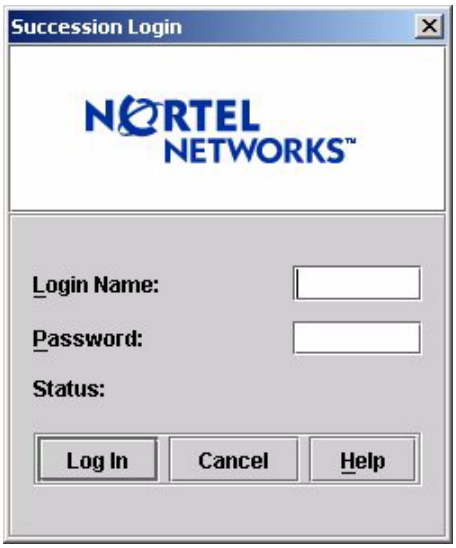
2 In the Address field, enter one of the following URLs for the application you want to launch:

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 SSPFS-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.

Confirming the upgrade on an SSPFS-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 SSPFS-based server upgrade” in document *ATM/IP Fault Management*, NN10408-900.

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.

ATTENTION
In a two-server configuration, perform the steps that follow on the newly active server, which now has the upgraded software.

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. In a two-server configuration log into the newly active server with the upgraded software on it.

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 SSPFS-based server upgrade” in document *ATM/IP Fault Management*, NN10408-900

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.

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.

ATTENTION
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 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 -
```

and pressing the Enter key.

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>
```

and pressing the Enter key.

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.

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.

On the active server

4 Access the command line interface to determine the server profile by typing

```
# cli
```

and pressing the Enter key.

5 Enter the number next to the View option in the menu.

6 Enter the number next to the sspfs_soft option in the menu.

Example response

```
=== Executing "sspfs_soft"

SSPFS version: 09.0 Build: 200508421 Server
Profile: cbm850

==="sspfs_soft" completed successfully
```

7 In the system response, note the server profile.

8 Exit the CLI by typing `x` until you return to the command prompt.

9 Use the following table to determine your next step.

If	Do
the Server Profile is cbm850	step 16
otherwise	step 10

10 Verify that all applications on the server are running by typing

```
# servquery -status all
```

and pressing the Enter key.

11 Use the following table to determine your next step.

If	Do
all applications are running	step 14
otherwise	step 12

12 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

13 Use the following table to determine your next step.

If	Do
all applications started	step 14
otherwise	contact your next level of support

14 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 16
otherwise	step 15

15 Start the PSE server application by typing

```
# pse start
```

and pressing the Enter key.

If	Do
PSE starts	step 16
otherwise	contact your next level of support

16 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) 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.	step 17
otherwise	step 21

17 Use the following table to determine your next step.

If	Do
you do not know the Ethernet address of the inactive server	step 18
otherwise	step 19

At the console connected to the inactive server

18 Determine the Ethernet address of the inactive server as follows:

a Log in to the inactive server through the console (port A) using the root user ID and password.

Ensure you are on the inactive server by typing ubmstat. If ClusterIndicatorACT is displayed in the response, which indicates you are on the active server, log out of that server and log in to the other server. The response must display ClusterIndicatorSTBY, which indicates you are on the inactive server.

b Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

c At the OK prompt, display the Ethernet address of the inactive server by typing

```
OK banner
```

and pressing the Enter key.

Example response:

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc.
All rights reserved. OpenBoot 4.8.0.build_04,
2048 MB memory installed, Serial #52964131.
Ethernet address 0:3:ba:28:2b:23, Host ID:
83282b23.
```

d Record the Ethernet address that is displayed.

On the active server

19 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

20 Proceed to step 22

On the active server

21 Start the cloning process on the active server by typing

```
# startb
```

and press the Enter key.

22 Use the following table to determine your next step.

If	Do
the system prompts you to enter the command “boot net - image”	step 23
otherwise	step 27

23 Connect to the console port of the inactive server.

If the console displays the	Do
login prompt	step 24
OK prompt	step 26

At the console connected to the inactive server

24 Log in to the inactive server using the root user ID and password.

25 Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

26 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

27 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):/>
```

28 Once cloning is complete, wait approximately 5 minutes before you proceed to the next step.

On the active server

29 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 30
otherwise	contact your next level of support

At your workstation

30 Establish a login session to the inactive server using one of the following methods:

If using	Do
telnet (unsecure)	step 31
ssh (secure)	step 36

31 Log in to the inactive server using telnet (unsecure) by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the physical IP address of the inactive server in the cluster

32 When prompted, enter your user ID and password.

33 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

34 When prompted, enter the root password.

35 Proceed to step 38.

36 Log in to the inactive server by typing

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

and pressing the Enter key.

where

server
is the physical IP address of the inactive server in the cluster

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.

37 When prompted, enter the root password.

On the inactive server

38 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 39
otherwise	contact your next level of support

39 You have completed this procedure. If applicable, return to the highlevel task or procedure that directed you to this procedure.

Installing optional software on a CBM 850

Purpose

This is a generic procedure that is used for installing optional software packages on the CBM 850. Consult Filesets available for the CBM 850 on page 208 to determine the optional software packages (filesets) that you can install through this procedure.

This procedure must be performed on a pre-cloned system. If the procedure is not performed on a pre-cloned system, clone the image of the active node to the inactive node of the cluster after the software package has been installed and configured, and after the active node has been made patch-current.

Filesets available for the CBM 850

The following table lists filesets (applications) included in the CBM0090 load. The table also shows which filesets are included with the CBM 850 at the time of installation (Base) and which filesets are optional and that you can install later.

Filesets available for the CBM 850 (Sheet 1 of 2)

Fileset	Description	Type
SDM_BASE.version_ 20.81.0.0	Load Lineup Information	Base
CBM_SETUP	CBM installation and upgrade tool; available only on CD	Base
NT_SIM.tools	Patching Tools	Base
SDM_ACE	SDM ACE distribution	optional
SDM_AFT.DMS500	SBA Automatic File Transfer	optional
SDM_BASE.base	Platform Base	Base
SDM_BASE.comm	Platform Maintenance Common	Base
SDM_BASE.gdd	Generic Data Delivery	Base
SDM_BASE.logs.client	Log Delivery Service Client	optional
SDM_BASE.logs	Log Delivery Service	Base
Note: Base = included with the CBM 850		

Filesets available for the CBM 850 (Sheet 2 of 2)

Fileset	Description	Type
SDM_BASE.mtce	Platform Maintenance	Base
SDM_BASE.omsl	OM Access Service	Base
SDM_BASE.tasl	Table Access Service	Base
SDM_BMI.bmi	Base Maintenance Interface	optional
SDM_DDMS_ossaps	OSS and Application Svcs	optional
SDM_DDMS_osscomms	OSS Comms Svcs	optional
SDM_BASE.util	Platform Utilities	Base
SDM_DEBUG.tools	SDM/CBM Debug Helper Tools	Base
SDM_DMA.dma	DMS Maintenance Application	optional
SDM_FTP.proxy	FTP Proxy	optional
SDM_GR740PT.gr740pt	GR740 Pass Through	optional
SDM_LOGS.mdm	Passport Log Streamer	optional
SDM_OMDD.omdd	OM Delivery	optional
SDM_REACHTHRU.rttl1	Reach Through SPM	optional
SDM_SBA.DMS500	SDM Billing Application	optional
SDM_SCFT.scft	Core File Transfer	optional
SDM_SWLD.swld	Bootpd and tftpd	optional
NTbkupmgr	Succession Provisioning Data Synch Manager	optional
NTdtsv	CEM DMS Data Server	optional
NTprxy	CEM Telnet Ftp Handler	optional
NTsaf	CEM Store and Forward	optional

Note: Base = included with the CBM 850

Procedure for installing optional software on a CBM 850

Use the following procedure to install optional software on a Core and Billing Manager (CBM) 850.

Prerequisites

There are no prerequisites for this procedure.

Action

ATTENTION
Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Installing optional software on a CBM 850

At your workstation

1 Open a connection to the active node of the CBM 850 using SSH and log in as the root user:

```
ssh -l root <ip_address>
```

where

<ip_address>
is the IP address of the active node of the CBM 850 cluster

2 Enter the password for the root user.

3 Use the following table to determine your next step.

If	Action
you are installing the DDMS application	Perform steps 1 and 5 only, of Procedure for installing DDMS on page 213, then go to step 5 of this procedure.
you are installing the OMDD application	Perform step 1 only, of Procedure for installing the OM Data Delivery software package on page 220, then go to step 5 of this procedure.

If	Action
you are installing the log delivery service application	Perform Procedure for installing the Passport Log Streamer application on page 229, then go to step 9 of this procedure.
you are installing the SBA or AFT applications	Perform Procedure to install the SBA and AFT software packages on page 231, then go to step 9 of this procedure.
you are installing GR740PT application server	Perform Procedure for installing GR740PT application server on page 231, then go to step 9 of this procedure.
you are installing the FTP Proxy application	Create logical volume: /cbmdata/00/esa, with size 25 Mbyte, using the logical volume creation procedure found in CBM 850 Security and Administration, NN10358-611, then go to step 4 of this procedure.
you are installing the Backup Restore Manager software	Perform procedure Installing the Backup Restore Manager software on page 243, then go to step 9 of this procedure.
you are installing any other optional software application	Go to step 4

4 Apply the software application package by performing the procedure Applying software packages on a CBM 850 using the CBMMTC interface on page 234.

5 Use the following table to determine your next step.

If	Action
you are installing any other applications that require you to create logical volumes	Return to step 3 in this procedure and follow the required action for the next application you are installing.
you are not installing any other applications that require you to create logical volumes	Go to step 6

6 Ensure that you have created any required logical volumes for all of the applications you are installing before continuing.

7 If you created any logical volumes in step 3, reboot the CBM 850:

```
init 6
```

8 After the node reboot is complete, use the following table to determine your next step.

If	Action
you are installing the DDMS application	Perform the remaining steps of Procedure for installing DDMS on page 213, starting with step 14, then go to step 9 of this procedure.
you are installing the OMDD application	Perform the remaining steps of Procedure for installing the OM Data Delivery software package on page 220, starting with step 2, then go to step 9 of this procedure.
you are installing the FTP Proxy application	Go to step 9.
you are installing any other optional software application	Go to step 9

9 Ensure that your CBMs are patch-current. For patching procedures, refer to ATM/IP Solution-level Security and Administration, NN10402-600.

10 Clone the image of the active node to the inactive node by performing the procedure, Cloning the image of the active node to the inactive node of a CBM 850 cluster on page 240.

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

Procedure for installing DDMS

This procedure enables you to install the DDMS application.

Prerequisites

The following prerequisites apply to using this procedure.

- For a successful installation of DDMS, verify that the Log Delivery Service application is in service.
- When Enhanced Password Control is in effect on the CM or core, the DDMS software has the ability to manage automatic password changing on the CBM and the CM, before passwords expire. It is not necessary to manually change any of the passwords for the SDM01-SDM04 userids on the CBM or CM. When the DDMS software is returned to service, it reads the tables, ofcopt and ofceng, on the CM to determine whether Enhanced Password Control is in effect. If Enhanced Password Control is in effect, the DDMS software reads the password lifetime value and automatically changes the passwords one day before they expire.

  If you make manual changes to the password lifetime value, or if you turn the Enhanced Password Control off or on, these changes must be synchronized with DDMS software by performing a bsy or rts of the DDMS application. If you change any of the SDM01-SDM04 passwords manually, you must apply the same password changes in the DDMS configuration file.

Action

ATTENTION
Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Installing DDMS on a CBM 850

At your workstation

1 Set Enhanced Password Control for the SDM01 userid.

```
permit sdm01 <sdm01_pswd> 4 10000 english all
```

where

<sdm0n_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 Set Enhanced Password Control for the SDM02 userid.

```
permit sdm02 <sdm02_pswd> 4 10000 english all
```

where

<sdm0n_pswd>
is the CM password for user SDM02

3 Set Enhanced Password Control for the SDM03 userid.

```
permit sdm03 <sdm03_pswd> 4 10000 english all
```

where

<sdm0n_pswd>
is the CM password for user SDM03

4 Set Enhanced Password Control for the SDM04 userid.

```
permit sdm04 <sdm04_pswd> 4 10000 english all
```

where

<sdm0n_pswd>
is the CM password for user SDM04

5 Create the first required logical volume for the DDMS application.

```
makelv /cbmdata/00/osscomms 16
```

6 Set the access privileges of the first logical volume for the DDMS application.

```
chmod 755 /cbmdata/00/osscomms
```

7 Set the ownership privileges of the first logical volume for the DDMS application.

```
chown maint:maint /cbmdata/00/osscomms
```

8 Create the second required logical volume for the DDMS application.

```
makelv /cbmdata/00/ossaps 112
```

9 Set the access privileges of the second logical volume for the DDMS application.

```
chmod 755 /cbmdata/00/ossaps
```

10 Set the ownership privileges of the second logical volume for the DDMS application.

```
chown maint:maint /cbmdata/00/ossaps
```

11 Create the third required logical volume for the DDMS application.

```
makelv /cbmdata/00/ossapslog 112
```

12 Set the access privileges of the third logical volume for the DDMS application.

```
chmod 755 /cbmdata/00/ossapslog
```

13 Set the ownership privileges of the third logical volume for the DDMS application.

```
chown maint:maint /cbmdata/00/ossapslog
```

14 Apply the two software application packages, OSS and Application Svcs and OSS Comms Svcs by performing the procedure Applying software packages on a CBM 850 using the CBMMTC interface on page 234. Specify /cdrom/cdrom/applications/cbm/packages as the source directory when you perform that procedure.

15 You are prompted automatically to configure the OSS Comms Svcs package. Use the following table to determine your next step.

Note: The OSS and Application Svcs package does not require configuration.

If	Do
you are prompted automatically to configure the OSS Comms Svcs package	step 19
you are not prompted automatically to configure the OSS Comms Svcs package	step 16

16 Access the config level of the maintenance interface:

```
cbmmtc config
```

17 In the list of applications, locate the OSS Comms Svcs application and record its application number (located next to the names of the applications). Select the application:

```
select <application number>
```

where

<application number>
is the number associated with the OSS Comms Svcs application, that you noted.

In response to the command, the OSS Comms Svcs application is highlighted on the cbmmtc config screen.

18 Invoke the configuration of the OSS Comms Svcs application.

```
config
```

19 When prompted to enter the logroute tool, as shown in the following figure, press Enter.

DDMS logroute tool banner

```
##########################################################
# Adding DDMS logroute configuration
```

DDMS logroute tool banner

```
##############################################################
##############################################################
Please add DDMS log routing:
        Device type     = file
        File            = /cbmdata/00/logs/ossaps/ossapslog
        Routing         = addrep
        log_type        = DDMS
Press <RETURN> when ready
```

The Logroute Main Menu appears, as shown in the following figure.

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    ==>
```

20 Set up a path and file to store DDMS customer logs. Select the Device List menu

1

The Device List Menu screen is displayed.

21 Select 1 to display the Device List screen.

If the list	Do
includes device /cbmdata/00/logs/ossaps/ossapslog	step 22
does not include device /cbmdata/00/logs/ossaps/ossapslog	step 23

22 Press the Enter key.

23 Begin to add a new device:

2

24 Select a file device:

3

Response:

```
Enter file name ==> /data/logs/
```

25 Complete the path name by typing

ossaps/ossapslog

You have now set up the log routing for the DDMS.

26 When prompted, enter STD log format (from the range displayed).

27 When prompted, set the ECORE option to ON.

28 Select addrep:

a

29 Enter the log identifier by typing, in uppercase

DDMS

30 When prompted to enter more log routing details, enter

N

31 Save the new device:

Y

Response:

```
Save completed -- press return to continue
```

32 Press the Enter key to return to the Add Device screen.

33 Return to the Device List Menu screen:

5

34 Return to the main menu screen:

6

35 Exit logroute:

6

The CM User Setup screen is displayed as shown in the following figure, and the required CM users, SDM01-SDM04, for

DDMS are added to the DDMS configuration file. The passwords for these users are the same as those entered in step 1

Note: *The userIDs and passwords are not case sensitive. You can change them after this installation is complete.*

Example of 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:
```

36 Add a new user for each of the required userIDs:

1

37 When prompted, enter the user name (for example, sdm01).

38 When prompted enter the user password.

Note: The first entry of a user name and password generates the following message: Error: file not valid. You can ignore this message.

39 If applicable, continue to add other user names and passwords at the prompt, otherwise continue with the next step.

40 Exit the CM User Setup screen:

0

The DDMS Clients Configuration screen is displayed as shown in the following example.

Example of DDMS Clients Configuration screen

```
              DDMS Clients Configuration

0. Quit
1. Add new clients
2. Remove existing clients
3. List existing clients
Enter choice:
```

41 Add a new DDMS client.

1

Note: The DDMS clients are the CS 2000 Management Tools servers with the SESM load.

42 When prompted, enter the IP address for each of the CS 2000 Management Tools servers, pressing the Enter key after each entry. If the CS 2000 Management Tools server is a cluster configuration, add the IP address of both the active and inactive units.

43 After you have entered all the IP addresses, type

done

44 Exit the DDMS clients configuration screen:

0

45 You have completed this procedure. Return to step 9 of the higher level task flow or procedure Installing optional software on a CBM 850.

Procedure for installing the OM Data Delivery software package

This procedure contains the steps for installing and configuring the OM Data Delivery application on the CBM 850 cluster.

Functional overview

The Operational Measurement Delivery (OMD) application collects customer-defined operational measurement (OM) data from the DMS switch, and stores the data in OM report files on the core manager in comma-separated value (CSV) format. The OMD application is configured using the OM user interface (OMUI).

An OM report file is a collection of OM groups that are monitored at selected reporting intervals. Secure File Transfer (SFT) or File Transfer Protocol (FTP) sends OM report files from the core manager to an operations support system (OSS). A data browser such as a spreadsheet program provides access to the contents of the files.

Report elements Report elements define the content of OM report files, and combine content of related OM groups for monitoring and analysis. A report element contains a user-defined report element name, a reporting interval for a report element (five minutes, or the office transfer period of 15 or 30 minutes), and names of the OM groups and registers.

Subtraction profiles The subtraction profile determines the change in the value of an OM group register between five-minute OM reports,

as defined in a report element. The subtraction profile applies only when the reporting interval is set to five minutes. The following table lists the types of subtraction profiles.

Subtraction profiles

Type	Description
Single	A single register represents a running total
Double	Two registers (base and extension) represent a running total
Non-subtraction	Subtraction is not performed on selected registers

Data collection schedules A data collection schedule defines start and stop times for OM report collection. The collecting interval determines how often in the time period an OM report collection occurs. The data is collected to the same report file for schedules with collecting intervals after midnight. The following table lists the data collection schedule types.

Data collection schedule repetition types

Repetition	Schedule information
Daily	Daily start and stop time. Format: `hhmm`, *where* `hh` = hour (00 to 24), and `mm` = minute (00 or 30). Specifies only a single time period; for multiple time periods in the same day, you must define multiple schedules.
Weekly	Weekly start and stop time. Values: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. Format: `hhmm`; multiple days can be specified in same schedule.
Monthly	Monthly start and stop time. Values:1 to 31. Format: `hhmm`; multiple days can be specified in the same schedule.

File rotation schedules File rotation schedules specify when to rotate report files. File rotation closes an open report file and moves it

to the */omdata/closedNotSent* directory on the core manager. Each file rotation schedule contains

- a user-defined file rotation schedule name
- a repetition rate for the rotation schedule based on either the number of report records collected or the number of hours to collect records
- a schedule that defines the time to rotate the report file

The data collection and file rotation schedules operate independently of each other. If a file rotation schedule event occurs during a scheduled data collection period, the file rotation schedule closes and rotates the OM report file, and a new OM report file with the same name is opened. The new file starts collecting immediately and continues until the end of the collection period. The open OM report file remains in the */omdata/open* directory until the file rotation schedule closes it and rotates it to the */omdata/closedNotSent* directory.

File transfer destinations File transfer destinations define remote downstream destinations of OM report files. Each destination entry contains

- a user-defined file transfer destination name
- the valid IP address of a remote destination host (xxx.xxx.xxx.xxx)
- the FTP port address of the remote host (default: 21)
- the remote host login ID and password

> ***Note:*** The core manager does not authenticate the IP and port addresses or the login ID and password.

An invalid destination causes the file transfer to fail. When a file fails to transfer, log entries are written to the customer log file at */var/adm/custlog*. The file is not re-sent, and the report file must be transferred manually using either the OMFTP command, SFT or standard FTP.

File transfer schedules File transfer schedules specify when to transfer OM report files downstream. Each file transfer schedule contains a

- user-defined file transfer schedule name
- repetition rate for the transfer schedule
- schedule defining when to transfer the report file (if using a repetition rate)

- remote file transfer destination host system (<16 destinations/schedule)
- destination storage directory for each defined transfer destination

The files are transferred downstream using FTP, and move from the /omdata/closedNotSent directory to the /omdata/closedSent directory. If a scheduled file transfer fails, a log is raised and the report file that could not be transferred moves to the /omdata/closedSent directory. The OMDD keeps track of the destination to which the report file could not be transferred. Then, at the next scheduled file transfer, the OMDD attempts to send the report file to the destination again. The OMDD will repeat this activity until one of the following situations occurs:

- the file is transferred successfully
- the file exceeds the retention period for the closedNotSent directory
- the file gets deleted during an audit because the omdata filesystem usage has exceeded the allowable limit
- the file is deleted by the omdelete utility

Report registrations A report registration links information from the report element and schedules for data collection, file rotation and file transfer to collect OM data. The user can create up to 32 report registrations. Once a report registration has been created, it can be deleted but not modified. Each report registration contains user-defined names for the report registration, report elements and each schedule type. The schedules become active immediately after the creation of the report registration.

An OM report file opened by the data collection schedule in the */omdata/open* directory uses the name of the report registration as part of the OM report file name. Linking a file transfer schedule into a report registration provides regular and automatic transfers of OM report files to remote downstream destinations. Unless you link a file transfer schedule to a report registration, you must manually transfer your OM report files downstream.

Report registration limit The report registration limit is the maximum number of report registrations that can be configured on a core manager without affecting processing performance. The number of report registrations range from 1 to 32 (default value: 32). To set the limit, use the Set Report Registration Limit option from the OMUI main menu.

File retention periods A cleanup of OM report files that have been sent downstream automatically occurs every night at midnight (00:00 or

24:00). Files in the */omdata/closedSent* directory are deleted at an interval based on the file retention period defined in the OMUI (range: 1 to 14 days). The default interval is set to 7 days at OMD installation. Unsent OM report files older than 32 days in the */omdata/closedNotSent* directory are deleted. This 32-day default value is read from a configuration file set up when the core manager is commissioned.

OMD data collection capacity Collection of more than 10,000 tuples reduces core manager performance and the retention period for OM report files.To determine the number of tuples in an OM group, either monitor the OM group and count the tuples in the report file or use the OMSHOW command from the MAP (maintenance and administration position) on the DMS switch. Use the formulas in the following table to calculate the limit for OMD data collection.

Formulas for calculating the limit for OMD data collection

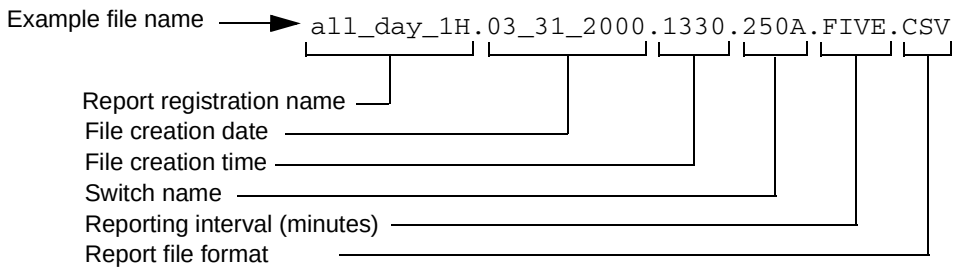
OMD data capacity transfer type	Formula
5- and 15-minute	**x+ y/3 = n <= 10,000 tuples** *(without loss of data)*
5- and 30-minute	**x+ z/6 = n <= 10,000 tuples** *(without loss of data)*
where: **x** = the number of OM tuples collected every 5 minutes **y** = the number of OM tuples collected every 15 minutes **z** = the number of OM tuples collected every 30 minutes **n** < 10,000 tuples	

The following table lists the current OMD data collection capacity.

OMD maximum data collection capacity

Transfer type	Capacity (number of tuples)
5-minute	6000
15-minute	12,000
30-minute	24,000

OM report file naming Report files are named according to the report registration name, file creation date and time, name of the switch generating the OMs, and reporting interval. Refer to the following example file name and explanation.



OM report file contents Tuple information for an OM group can be viewed in CSV format from the OM report file on the core manager, and by entering the OMSHOW command on the MAP. The following table shows an OM report file.

Contents of an OM report file

Date	Time	Switch Names	Group Name	Key/Info Field	Reg1 Name	Reg1 Value	Reg2 Name	Reg2 Value	Reg31 Name	Reg31 Value
2/23/00	3:35 :00	250U	TRK	ISU_GWC.2W.0.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	ESADGTR.OG.0.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	HSET.OG.3.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	JACK.OG.2.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	LTU.OG.2.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	MONTALK.OG.0.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	OCKT.OG.0.0	AOF	0	ANF	0		

Audits The OM report files are stored in the omdata filesystem. This filesystem is audited every 30 minutes for the amount of usage. To

ensure that the omdata filesystem usage does not reach 100% at any time, the system performs the following actions:

- When the filesystem usage reaches 60%, Major trouble log SDM338 is raised indicating that OM report files will be deleted at the time of the next audit, if usage exceeds 90%. Then, if usage exceeds 90% at the time of the next audit log SDM639 is raised indicating all report files in the closedSent directory will be deleted, and the report files are deleted.
- If omdata filesystem usage does not fall below 80% after deletion of all report files in the closedSent directory, report files from the closedNotSent directory will be deleted, starting from the oldest file, until the usage is at 80% or less. As each report file is deleted from the closedNotSent directory, log SDM631, which describes the action, is raised.

Prerequisites

Ensure that the OM Access Service and Table Access Service application filesets are installed and in service on your 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 to accommodate the amount of data transferred by the front end for a transfer period of every 30 minutes.

Action

ATTENTION

Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Installing and configuring the OM Data Delivery application on a Core and Billing Manager 850

At your workstation

1 Create the following logical volume (directory for a file system) required for the OMDD software package you are installing:

```
makelv /cbmdata/00/omdata 1008
```

2 Using the procedure, Applying software packages on a CBM 850 using the CBMMTC interface on page 234 apply the SDM_OMDD.omdd software package located in the /cdrom/cdrom/applications/cbm/packages directory. Since

CD-ROM is being used to install the application, specify /cdrom/cdrom/applications/cbm/packages as the directory path of the source directory when you perform that procedure.

3 Access the Config level of the CBM maintenance interface:

```
cbmmtc config
```

4 Configure OM Data Delivery:

```
config <n>
```

where

<n>
is the number next to OM Data Delivery under fileset description

5 The system indicates that the Tuple Number option is inactive and prompts you to determine whether you want to activate it.

Note: The Tuple Number option allows you to activate or disable a tuple number so that it can be included in a CSV file with other OM information.

If you	Do
want to activate the Tuple Number option	Type **y**
do not want to activate the Tuple Number option	Type **n**

6 The system prompts you to confirm whether the Multiservice Data Manager (MDM) and core manager are integrated. To indicate that the MDM is connected to the core manager for collecting Passport 15000 performance measurement data, type

```
y
```

7 Configure the core manager to communicate with the MDM as follows. When prompted, enter the IP address of the first MDM you want to connect to.

8 When prompted, enter the hostname of the first MDM.

9 When prompted, enter the IP address of the second (alternate) MDM you want to connect to.

10 When prompted, enter the hostname of the second MDM.

11 When prompted, enter the port for 5-minute performance PM (performance measurement) data. The default port is 1646.

12 When prompted, enter the port for 30-minute PM data. The default port is 1647.

13 You are prompted as to whether you want to use custom connection retry settings. In case of connection failure, OMDD will try connecting to the MDMs, alternatively. When prompted, indicate whether you want to use custom connection retry settings.

If you	Do
want to use custom retry settings	Type **y** then go to step 14
do not want to use custom retry settings but want, instead, to use default settings	Type **n** then go to step 19

14 Configure the custom retry settings. Enter a numeric value (in seconds) for the first connection retry interval.

Note: Values higher than 300 seconds are not recommended as they can adversely affect recovery time.

15 Enter the number of retry attempts for the first retry interval.

16 Enter a numeric value (in seconds) for the second connection retry interval.

17 Enter the number of retry attempts for the second connection retry interval.

18 Enter a numeric value (in seconds) for the third connection retry interval.

19 When prompted, confirm the configuration data you have entered by typing y, otherwise type n to re-enter all of the configuration data.

20 The system indicates that the configuration is complete.

Press the Enter key.

21 The system indicates that the changes will take place after the OM Data Delivery application is restarted.

Press the Enter key to restart the OM Data Delivery application.

22 Exit the maintenance interface by typing

```
quit all
```

23 You have completed this procedure. Return to step 9 of the higher level task flow or procedure Installing optional software on a CBM 850.

Procedure for installing the Passport Log Streamer application

The following procedure contains the steps for installing and configuring the Passport Log Streamer application on the CBM 850 cluster.

For full operation, the log delivery application requires installation of the following application filesets:

- log delivery service (base software)
- log delivery service client (optional software)
- Generic Data Delivery (base software)
- Passport Log Streamer, if the core manager needs to communicate with the Multiservice Data Manager (MDM) for fault data. (optional software)

Prerequisites

Before performing this procedure, ensure that there are no disk faults on the core manager.

In order to ensure that the Passport Log Streamer is able to communicate with the configured MDMs and to collect logs, any restrictions for the configured MDM ports must be removed from all of the firewalls that exist between the MDM and the CBM 850.

Action

ATTENTION

Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Installing and configuring the Passport Log Streamer application on the Core and Billing Manager 850

At your workstation

1 Perform the procedure Applying software packages on a CBM 850 using the CBMMTC interface on page 234 to apply the SDM_LOGS.mdm_21.39.9.0.pkg software package located in the /cdrom/cdrom/applications/cbm/packages directory. Since CD-ROM is being used to install the application, specify /cdrom/cdrom/applications/cbm/packages as the directory path of the source directory when you perform that procedure.

2 Configure the Passport Log Streamer application. When prompted, enter the IP address for the first MDM node.

3 When prompted, enter the IP address for the second MDM node.

4 When prompted, enter the port number configured for the pserver application on the first MDM node.

5 When prompted, enter the port number configured for the pserver application on the second MDM node.

6 When prompted, indicate that you do not want to receive MDM logs by entering n.

7 When prompted, indicate that you do not want to specify Passport 15000 log filters by entering n.

8 When prompted, indicate that you do not want to specify Passport 8600 log filters by entering n.

9 When prompted, confirm the configuration data you entered by entering y.

10 Place the log delivery service application and the Passport Log Streamer application into service by accessing the Application (Appl) level of the CBM maintenance interface:

appl

11 Busy the application filesets:

bsy <*fileset_number*> <fileset_number>

where

fileset_number is the number next to each of the following application filesets:

- Log delivery service
- Passport Log Streamer

12 Return the application filesets to service:

rts <*fileset_number*> <fileset_number>

where

fileset_number is the number next to each of the application filesets you busied in the previous step

Once the application filesets are in service, the system retrieves any current log records. To view or store the log records, refer to procedure “Displaying or storing log records using log receiver” in Core and Billing Manager Fault Management, NN10351-911.

13 Exit the CBM maintenance interface:

quit all

14 You have completed this procedure. Return to step 9 of the higher level task flow or procedure Installing optional software on a CBM 850.

Procedure to install the SBA and AFT software packages

This procedure enables you to install the SuperNode Billing Application (SBA) and Automatic File Transfer (AFT) software packages on the CBM 850 cluster.

Prerequisites

There are no prerequisites for this procedure.

Action

Installing the SBA and AFT software packages on a CBM 850

At your workstation

1 Using the procedure Applying software packages on a CBM 850 using the CBMMTC interface on page 234, apply the SBA and AFT software packages located in the /cdrom/cdrom/applications/cbm/packages directory.

2 Create the necessary logical volumes (directories for file systems) required for the SBA using procedure “Adding a logical volume through the command line” in Core and Billing Manager 850 Accounting, NN10363-811.

3 To configure the SBA for operation, refer to Core and Billing Manager 850 Accounting, NN10363-811, for the procedures to use.

4 To configure AFT for operation, refer to Core and Billing Manager 850 Accounting, NN10363-811, for the procedures to use.

5 You have completed this procedure. Return to step 9 of the higher level task flow or procedure Installing optional software on a CBM 850

Procedure for installing GR740PT application server

This procedure enables you to install the GR740PT application server.

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 the

EADAS SOCs (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 eadas_dc_interface	Setting for eadas_nm_interface	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

EADAS channel assignments

Description	Service name	TCP port	MTS offset
NM EADAS lc 2	NM_EADAS_LOG_CHAN2	9554	238
NM EADAS lc 3	NM_EADAS_LOG_CHAN3	9555	239

Action

Installing GR740PT application server

At your workstation

1 Using procedure Applying software packages on a CBM 850 using the CBMMTC interface on page 234, apply the GR740PT software package located in the /cdrom/cdrom/applications/cbm/packages directory.

2 When prompted to: Enter mode of security, use the following table to determine your response.

If	Do
you are not configuring GR740PT in non-secure mode	select 1. Non-secure
you are configuring GR740PT in local secure mode	select 2. Local (SSH) security

3 You have completed this procedure. Return to step 9 of the higher level task flow or procedure Installing optional software on a CBM 850

Procedure for Applying software packages on a CBM 850 using the CBMMTC interface

This procedure enables you to install optional software packages on the nodes of a CBM 850 cluster.

Prerequisites

There are no prerequisites for this procedure.

Action

ATTENTION
Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Applying software packages on a CBM 850 using the CBMMTC interface

At your workstation

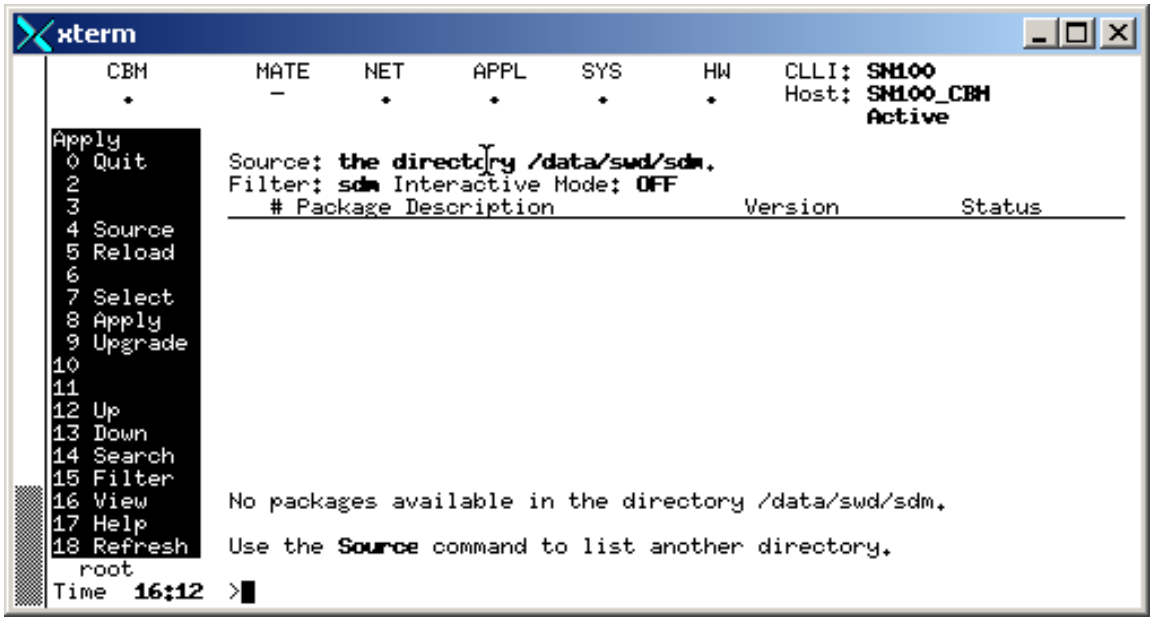
1 From the command line prompt, access the apply level of the cbm maintenance interface:

```
cbmmtc apply
```

The system displays the apply level screen of the cbm maintenance interface, which shows a list of the packages, if any exist, in the default source directory.

Note: Up to 12 software packages can be displayed at a time. Use the Down command (command 13 as shown in the following example) to view other packages.

Example of cbm maintenance interface apply level



2 Use the following table to determine your next step.

If	Do
CD-ROM is being used to deliver the CBM software	step 3, and specify: /cdrom/cdrom/applications/cbm/packages as the <source_directory_name>
you want to exit from the cbm maintenance interface	step 13

3 Insert the CD-ROM into the CD drive if it is not already present in the drive.

4 At the command line located at the bottom of the cbmmtc user interface screen, type:

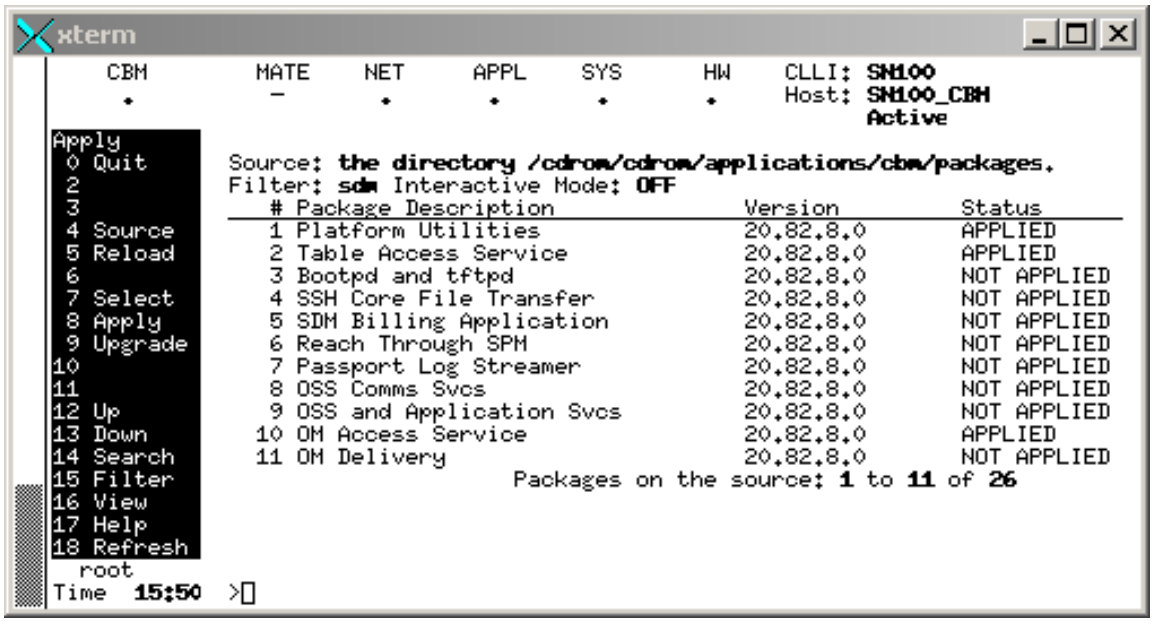
`source <source_directory_name>`

where

<source_directory_name>
is the full pathname of the directory containing the package that you want to apply. Since CD-ROM is being used for the installation, specify /cdrom/cdrom/applications/cbm/packages as the source_directory_name

As shown in the following example, the system displays the apply level screen of the cbm maintenance interface, which shows a list of all packages in the source directory that you specified.

Example of apply level showing the CD-ROM source directory



5 In the list of packages, locate the packages to be applied and take note of their numbers (located next to the names of the packages). Select the packages that you have decided to apply:

`select <package number> ... <package number>`

where

<package number>
is the number associated with a package, that you noted. Each package number is separated by preceding and succeeding spaces.

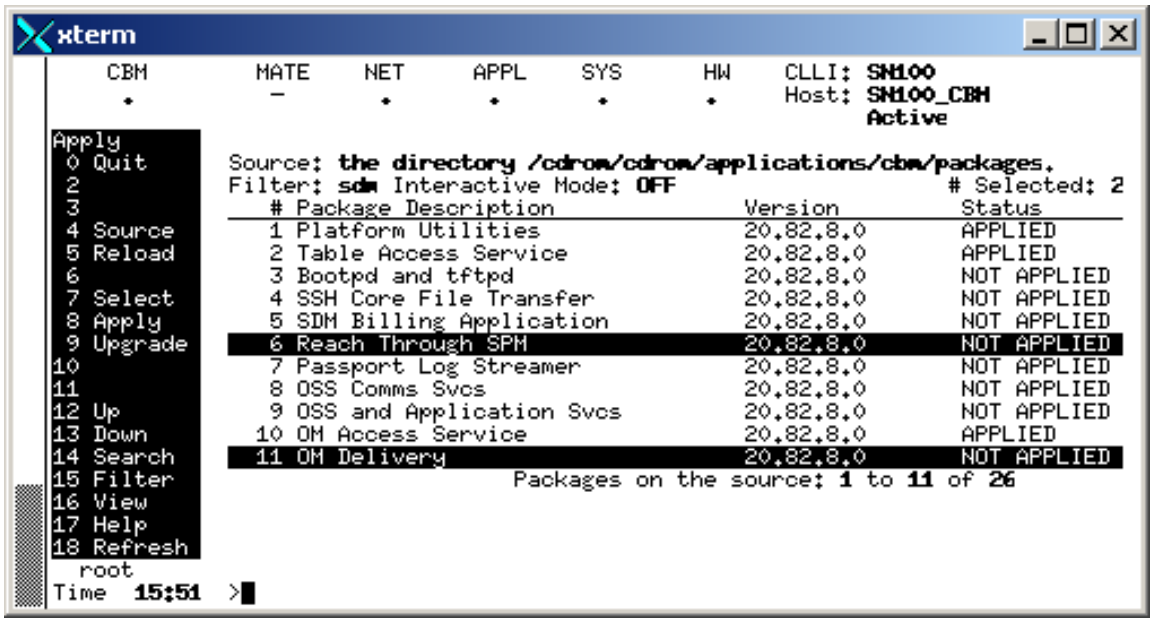
Example
To select the Reach Through SPM application, which is number 6, and OM Delivery, which is number 11 in the sample screen display shown in the previous figure, enter

select 6 11

To de-select any packages that you selected, re-enter the select command for the packages you want to de-select. The highlighting on the packages that you de-select will be removed.

The packages you selected are highlighted on the cbmmtc apply screen, as shown in the following figure.

Example of selecting packages to apply

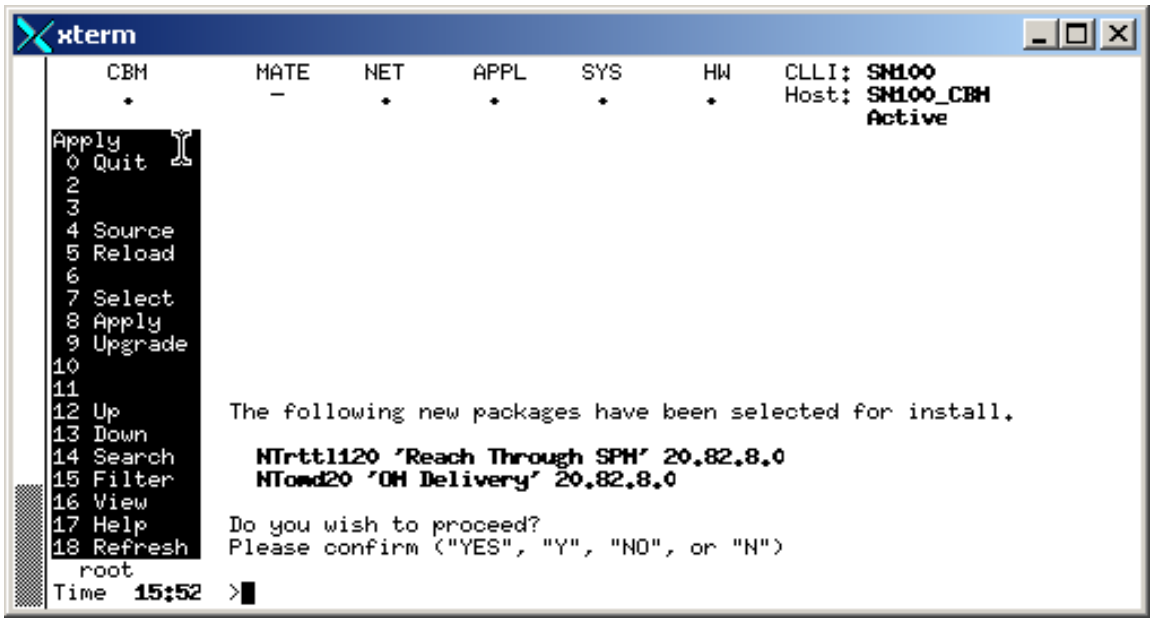


6 Apply the selected packages:

```
apply
```

7 If a prerequisite package for the package(s) you have selected to apply is not already been applied on the system, the system SWIM tool will automatically select and apply the pre-requisite package unless the package is currently selected to be applied.

Example of results screen after applying packages



The system prompts if you want to continue with applying the selected packages.

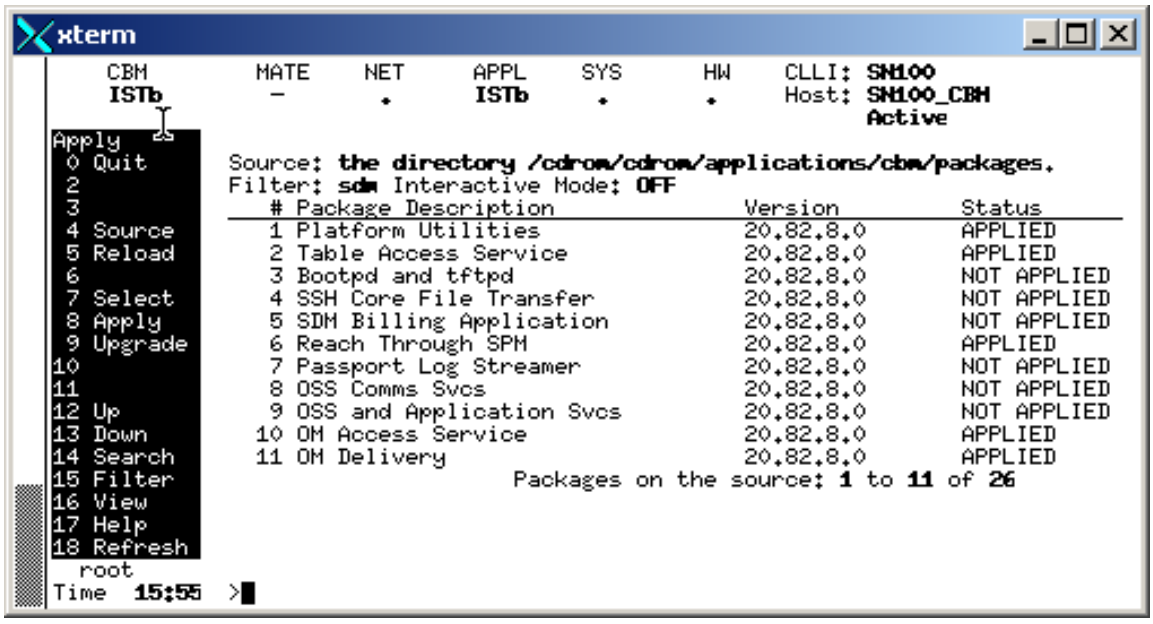
8 Use the following table to determine your next step

If	Do
you want to continue the package application	step 9
you do not want to continue the package application	step 12

9 Type yes in response to the prompt.

The status of each package application displays on the cbmmtc apply screen, as shown in the following figure.

Example apply level showing the status of applied packages



10 When the application is completed, the installed packages will appear in the list that displays when you enter the cbmmtc packages level. Verify that the status of the new packages indicates Applied under the Status column.

ATTENTION

It is important that packages installed on the system not be left with a Partial status. If any package installed application fails or otherwise shows a Partial status, contact your next level of support for assistance.

11 If applicable, review details about the CBM package application by performing procedure Viewing software transaction history and logs on the CBM 850 on page 251, otherwise continue with step 13.

12 Type no in response to the prompt.

13 Exit from the cbm maintenance interface:

```
quit all
```

14 You have completed this procedure. Return to step 9 of the higher level task flow or procedure Installing optional software on a CBM 850.

Procedure for cloning the image of the active node to the inactive node

This procedure enables you to clone the image of the active node onto the inactive node of a CBM 850 cluster.

Prerequisites

There are no prerequisites for this procedure.

Action

ATTENTION

Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Cloning the image of the active node to the inactive node of a CBM 850 cluster

At your workstation

1 Start the cloning process by typing

```
startb
```

and press the Enter key.

2 Use the following table to determine your next step.

If the system	Do
prompts you for the Ethernet address	step 3
indicates it is using Ethernet address <EthernetAddress>	record the IP address, then go to step 8

At the console connected to the inactive node

3 Log in to the inactive node through the console using the root user ID and password.

4 If the system is not already at the OK prompt, bring the system to the OK prompt:

```
init 0
```

5 At the OK prompt, display the Ethernet address of the inactive node:

```
OK banner
```

Example response:

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.
```

6 Record the Ethernet address that is displayed.

At your workstation (session connected to Active node)

7 Enter the Ethernet address of the inactive node you recorded in step 6.

8 Use the following table to determine your next step.

If the system	Do
prompts you to enter the command: boot net - image	step 9
does not prompt you to enter the command: boot net - image	step 10

At the console connected to the inactive node

9 When prompted, boot the inactive node from the image of the active node by typing

`OK boot net - image`

and press the Enter key.

Note: There must be a space after the dash.

Example response:

```
SC Alert: Host System has Reset

Sun Fire V240, No Keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.

Rebooting with command: boot net - image
.
.
.
SC Alert: Host System has Reset
```

At your workstation (session connected to the Active node)

10 Monitor the progress of the cloning from the active node. Cloning the inactive node takes approximately one hour to complete.

Example response:

```
Waiting for network response from
unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning: /export/d2
.
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become
normal.
Deleted snapshot 0.
Deleted snapshot 1.
Deleted snapshot 2.
Deleted snapshot 3.
d99: Soft Partition is cleared
```

11 You have completed this procedure. Return to step 11 of the higher level task flow or procedure Installing optional software on a CBM 850.

Procedure for installing the Backup Restore Manager software

This procedure enables you to install the Backup Restore Manager software. The Backup Restore Manager application functionality requires the appropriate software resident and configured on platforms that require synchronized imaging. Although no Core and Billing Manager 850 data is backed up through the Backup Restore Manager, the Backup Restore Manager software must be installed on the CBM 850 to allow control of the XA-core and 3PC (Compact) backup.

Prerequisites

There are no prerequisites for this procedure.

Action

ATTENTION
Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Installing the Backup Restore Manager software

At the CI prompt on the core

1 Enter the following command:

```
permit <backupuser> <backupuser_pswd> 4 10000
english all
```

where

<backupuser>
is the user name for the core, that is up to 16 characters in length, that will be used by SBRM for login

<backupuser_pswd>
is the password for the <backupuser> user you are creating, which can be up to 16 characters in length

4
is the priority

10000
is the stack size

english
the language setting

all
is the privilege setting

Note 1: If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

Note 2: If Enhanced Password Control is in effect on the CM and after the user is permitted on the switch, log in to the core manually with this user first. The core will prompt you to change the password at the first login after the login is permitted. Change the password and then perform step 1 again.

The SBRM does not have the ability to manage passwords. Therefore, you must re-run the configuration script in step 4.

At your workstation

2 Apply the software application package, NTbkupmgr by performing the procedure Applying software packages on a CBM 850 using the CBMMTC interface on page 234. Specify /cdrom/cdrom/applications/cbm/packages as the source directory when you perform that procedure.

3 When the installation is complete, exit from the cbmmtc.

4 At the command line prompt, change directory to the directory containing configuration script:

```
cd /opt/nortel/bkresmgr/cbm/scripts
```

5 Run the configuration script:

```
./bkmgr_config.sh
```

6 You are first prompted for the user name. The user name is that used to log in to the core to initiate an image dump. The script restricts the user name to a maximum of 16 characters. The user name entered must first be enabled on the core in step 1

7 You are prompted for the user name you entered in step 6).

8 You are first prompted for the password. The configuration script restricts the password to a maximum of 16 characters. Use the password set up in step 1

9 You are prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored.

Note: Verify that this device has enough space to store the backup.

10 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.

11 You have completed this procedure. Return to step 9 of procedure Installing optional software on a CBM 850.

Removing software packages from a CBM 850

Purpose

This procedure enables you to remove software packages from both nodes of a CBM 850 cluster.

When a software package is removed, the data within those file systems is removed. However, the file systems associated with that package are not removed and cannot be removed automatically.

ATTENTION

This procedure should be performed only if an error condition requires that you remove the Supernode Billing Application (SBA) or Automatic File Transfer (AFT) immediately after they have been installed and before the billing stream has been activated for the FIRST time. If you must remove either SBA or AFT after the billing stream has been activated for the first time, contact your Nortel Service Representative for assistance.

Prerequisites

There are no prerequisites for this procedure.

Limitations and Restrictions

When removing a package that is a requisite package for other installed packages, the software manager (SWIM) notifies you about this and the remove operation is aborted. To removed packages with dependencies, you must first remove the dependant packages listed in the SWIM screen before trying to remove the supported package.

Action

ATTENTION
Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Removing software packages from a CBM 850

At your workstation

1 Open a connection to the active node of the CBM 850 cluster using SSH and log in as the root user:

```
ssh -l root <ip_address>
```

where

<ip_address>
is the IP address of the active node of the CBM 850 cluster

2 Enter the password for the root user.

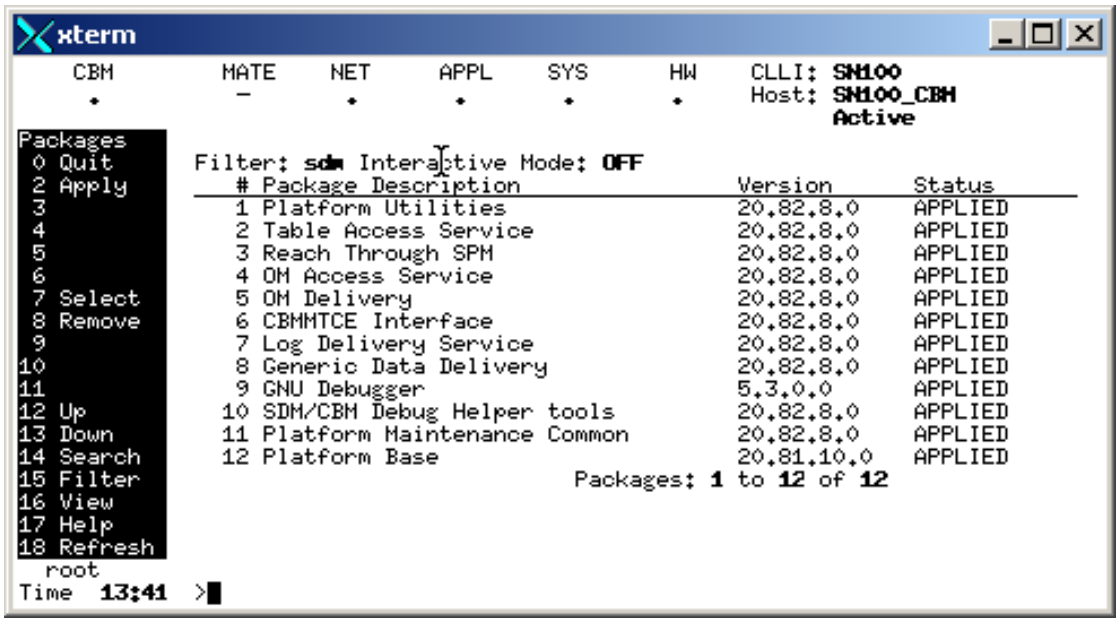
3 From the command line prompt, access the packages level of the cbm maintenance interface:

```
cbmmtc packages
```

The system displays the packages level screen of the cbm maintenance interface, as shown in the following figure. This view shows a list of all packages installed on the system.

Note: *Only 12 packages can be displayed at a time, you may need to scroll to the next screen by entering the Down command (command 13 on the left side of the window).*

Example of the cbm maintenance interface packages level



4 In the list of packages displayed on the active node, locate the packages to be removed and take note of their numbers (located next to the names of the packages). Select the packages that you have decided to remove:

`select <package number> <package number>`

where

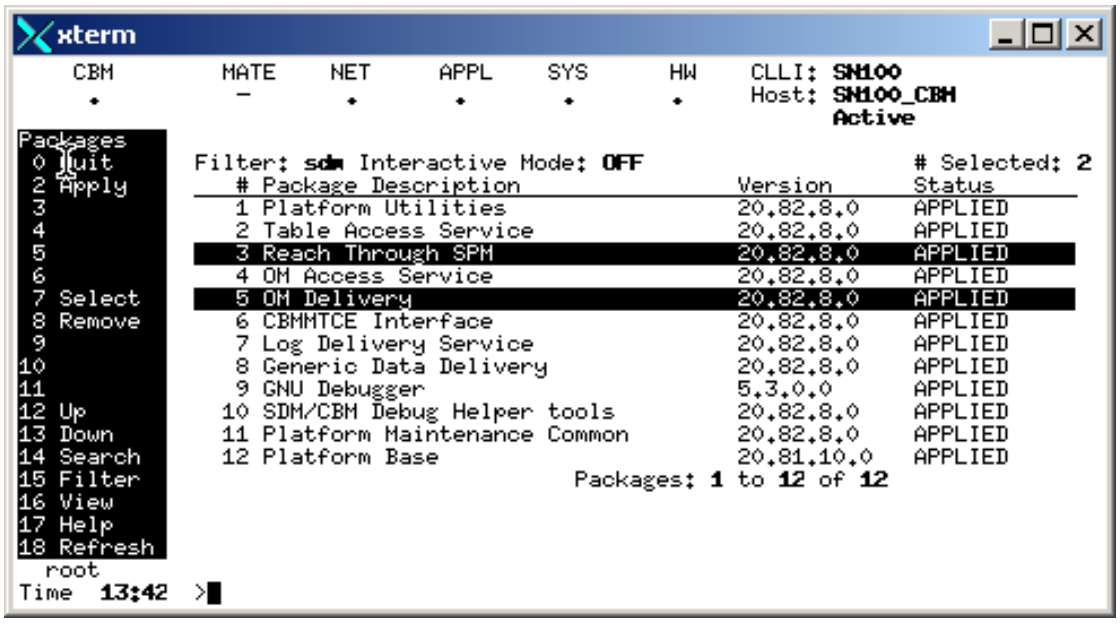
<package number>
is the number associated with a package, that you noted. Each package number is separated by preceding and succeeding spaces.

Example
To select Reach Through SPM, number 3 in the previous figure, and OM Delivery, number 5 in the previous figure, enter

select 3 5

The selected package is highlighted on the packages screen as shown in the following figure.

Example screen of packages selected for removal



5 To deselect a selected package, re-enter the select command for the specific package you want to deselect. The highlighting on the packages that you de-select will be removed.

6 Remove the package from the system:

`remove`

ATTENTION

If you try to remove a package that is a requisite package for some other package(s), SWIM will notify you about this, the remove command will fail, and the program will exit. In this event, you must first remove the dependant packages listed in the SWIM output before trying to remove the requisite package.

The system prompts you once to ensure that you want to continue with the package removal.

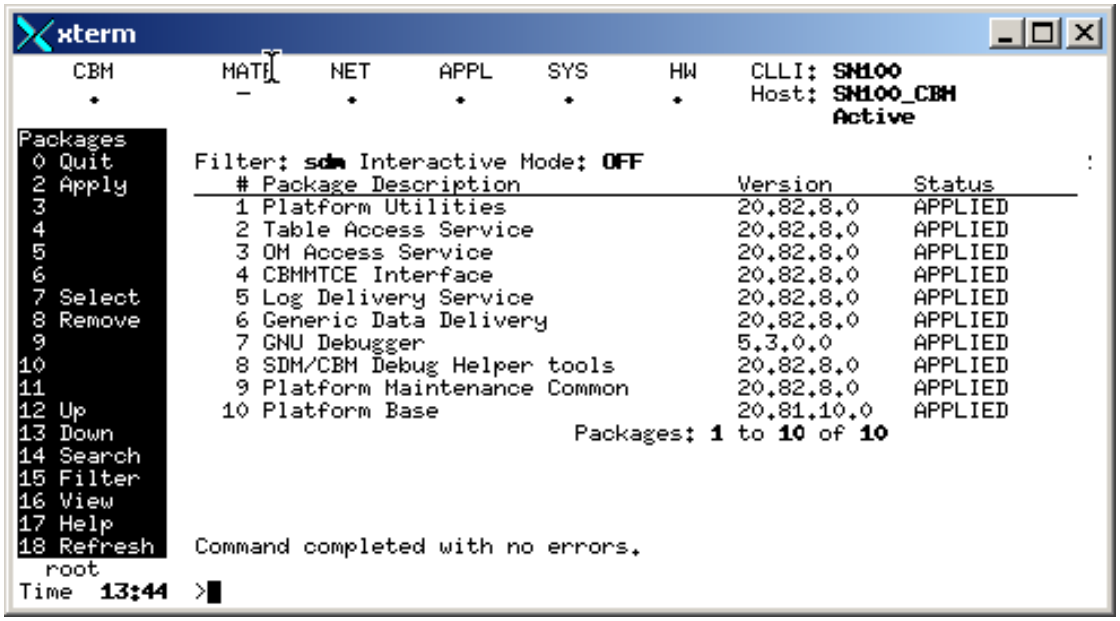
7 Use the following table to determine your next step.

If	Do
you want to continue the package removal	step 8
you do not want to continue the package removal	step 10

8 Type yes in response to the prompt.

The status of the package application displays on the cbmmtc packages screen. The removal will be automatically attempted on the mate node after the removal is completed on the active node.

Example of screen display after package removal



If the removal was successful, the package will no longer appear in the packages list that displays on either the active or inactive nodes. If the removal was not successful, then an error occurred during removal. The package will continue to appear in the packages list with an Applied or Partial status.

Note: *It is important that packages not be left on the system with a "Partial" status. In this event, or if the package removal failed, contact your next level of support for assistance.*

9 If applicable, view details about the CBM package removal, using procedure Viewing software transaction history and logs on the CBM 850 on page 251, otherwise continue with step 11.

10 Type no in response to the prompt.

11 To remove other packages from the system, return to step 4 otherwise continue with the next step.

12 Exit from the cbm maintenance interface:

```
quit all
```

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

Viewing software transaction history and logs on the CBM 850

Purpose

This procedure enables you to view additional details about the package transactions, either package configuration or package removal, that you have performed on a CBM 850.

Prerequisites

There are no prerequisites for this procedure.

Action

ATTENTION
Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Viewing software transaction history and logs on the CBM 850

At your workstation

1 This procedure enables you to view logs that are local to each of the nodes in the CBM 850 cluster. Therefore, you must first choose the node in the cluster for which you want to view logs and then create a connection to that node.

If	Do
you are already connected to the CBM 850 for which you want to view logs	step 4
you are not already connected to a CBM 850 for which you want to view logs	step 2

2 Using SSH, open a connection to the node in the CBM 850 cluster for which you want to view logs and log in as the root user:

```
ssh -l root <ip_address>
```

where

<ip_address>
is the IP address of the CBM 850 node for which you want to view logs

3 Enter the password for the root user.

4 Determine the next step to perform.

If	Do
you have already accessed the cbmmtc user interface	step 6
you have not accessed the cbmmtc user interface	step 5

5 Type the following on the command line:

```
cbmmtc
```

6 Type the following on the command line located at the bottom of the cbmmtc user interface screen:

```
history
```

The system displays the information about the package transactions you have performed, including a log file and the results of the individual operations. Included also in this information is an indication as to the node on which the operations were performed. If the operations were performed on the active node, no special identifier, is provided. However, if the operations were performed on the inactive node, the inactive node identifier appears in the information displayed.

7 If applicable, you can view more details about a specific log displayed in the history command output by typing:

```
ViewLog  <#>
```

where

<#>
is the number of the log in the log file.

8 Exit from the cbmmtc user interface:

```
quit all
```

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

Using the Queryloads tool to display patches and packages applied on the CBM 850

Purpose

This procedure shows how to use the Queryloads tool to display information about patches that have been applied to a CBM 850 node. For several of the queries, the tool allows you to select either a formatted report display or a raw XML data display.

Prerequisites

Verify that an emsadm userid has been configured.

Action

ATTENTION
Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

Using the Queryloads tool to display patches and packages applied on the CBM 850

At your workstation

1 Open a connection to the active node of the CBM 850 cluster using SSH and log in as the emsadm user:

```
ssh -l <emsadm_user> <ip_address>
```

where

<emsadm_user>
is the emsadm user login name

<ip_address>
is the IP address of the active node of the CBM 850 cluster

2 Enter the password for the emsadm user.

3 Determine the type of query you want to launch.

Query	Do
List the products that can be specified in the Queryloads queries	step 4
List in text format all installed packages or only installed packages that you specify	step 6

Query	Do
List in XML format all installed packages or only installed packages that you specify	step 19
Store package information in a file that you designate	step 29
List in text format all installed patches (including Sun patches) or only installed patches that you specify	step 31
List in XML format all installed patches (including Sun patches) or only installed patches that you specify	step 45
Store patch information in a file that you designate	step 58
List packages or patches missing from the baseline	step 60
You want to obtain usage help for the Queryloads tool	step 62

4 At the prompt, invoke the queryloads tool:

`queryloads -m products`

The system displays each of the products that are available for your queries using the Queryloads tool as shown in the following figure.

```
CBM00070    Core and Billing Manager    7.0.0
```

5 Go to step 63.

6 Use the following table to determine the step to perform to list packages in text format.

If	Do
you want to list all packages installed on both nodes	step 7
you want to list all packages installed on the inactive node	step 9
you want to list all packages installed on the active node	step 11
you want to list only packages that you specify, that are installed on both nodes	step 13

If	Do
you want to list only packages that you specify, that are installed on the inactive node	step 15
you want to list only packages that you specify, that are installed on the active node	step 17

7 List all packages installed on both nodes:

```
queryloads -m packages
```

8 Go to step 63

9 List all packages installed on the inactive node:

```
queryloads -m packages -n inactive
```

If you receive a password prompt while querying the inactive node, make sure that the inactive node is in service. If the inactive node is in service and you are still prompted for a password, contact your next level of support.

10 Go to step 63

11 List all packages installed on the active node:

```
queryloads -m packages -n active
```

12 Go to step 63

13 List only packages that you specify, that are installed on both nodes:

```
queryloads -m packages | grep
<unique_package_identifier>
```

where

<unique_package_identifier>
is the identifier of the package you want to list. Use the following table to determine the correct identifier.

The following table shows sample unique package identifiers.

Type of package	Package name	Examples of possible <unique_package_identifiers>[a]
Nortel packages	NTbmi20 NTsba20	NT
Sun packages	SUNWaudh SUNWIpmsg	SUN

a.The entry for <unique_package_identifier> is case-sensitive.

14 Go to step 63

15 List only packages that you specify, that are installed on the inactive node. Refer to the table in step 13 for an example of unique package identifiers:

```
queryloads -m packages -n inactive | grep
<unique_package_identifier>
```

where

<unique_package_identifier>
is the identifier of the package you want to list.

If you receive a password prompt while querying the inactive node, make sure that the inactive node is in service. If the inactive node is in service and you are still prompted for a password, contact your next level of support.

16 Go to step 63

17 List only packages that you specify, that are installed on the active node. Refer to the table in step 13 for an example of unique package identifiers:

```
queryloads -m packages -n active | grep
<unique_package_identifier>
```

where

<unique_package_identifier>
is the identifier of the package you want to list.

18 Go to step 63

19 Use the following table to determine the step to perform to list packages in XML format.

If	Do
you want to list all packages installed on both nodes	step 20
you want to list all packages installed on the inactive node	step 21
you want to list all packages installed on the active node	step 22
you want to list only packages that you specify, that are installed on both nodes	step 23
you want to list only packages that you specify, that are installed on the inactive node	step 25
you want to list only packages that you specify, that are installed on the active node	step 27

20 List all packages installed on both nodes:

```
queryloads -m packages -x
```

Go to step 63.

21 List all packages installed on the inactive node:

```
queryloads -m packages -x -n inactive
```

If you receive a password prompt while querying the inactive node, make sure that the inactive node is in service. If the inactive node is in service and you are still prompted for a password, contact your next level of support.

Go to step 63.

22 List all packages installed on the active node:

```
queryloads -m packages -x -n active
```

Go to step 63.

23 List only packages that you specify, that are installed on both nodes:

```
queryloads -m packages -x | grep
<unique_package_identifier>
```

where

<unique_package_identifier>
is the identifier of the package you want to list.

The following table shows sample unique_package_identifiers.

Type of package	Package name	Examples of possible <unique_package_identifiers>[a]
Nortel packages	NTbmi20 NTsba20	NT
Sun packages	SUNWaudh SUNWIpmsg	SUN

a.The entry for <unique_package_identifier> is case-sensitive.

24 Go to step 63

25 List only packages that you specify, that are installed on the inactive node. Refer to the table in step 23 for an example of unique package identifiers:

```
queryloads -m packages -x -n inactive | grep
<unique_package_identifier>
```

where

<unique_package_identifier>
is the identifier of the package you want to list.

If you receive a password prompt while querying the inactive node, make sure that the inactive node is in service. If the inactive node is in service and you are still prompted for a password, contact your next level of support.

26 Go to step 63

27 List only packages that you specify, that are installed on the active node. Refer to the table in step 23 for an example of unique package identifiers:

```
queryloads -m packages -x -n active | grep
<unique_package_identifier>
```

where

<unique_package_identifier>
is the identifier of the package you want to list.

28 Go to step 63

29 At the prompt, invoke the queryloads tool:

```
queryloads -pkg <-d> <source> -o
<output_file_name>
```

where

<-d>
is an option that must be entered if you are specifying a source directory.

<source>
is the directory containing the packages for which you want to extract information (for example, /cdrom/cdrom/applications/cbm/packages).

<output_file_name>
is a file name you designate for the file to hold the packages information. The system attaches the extension .packages to this file name.

Note: If queryloads is invoked from within the directory containing the package(s), you do not need to enter either the -d option or a source directory name.

The package information is stored in the output_file.packages file. If you have not specified a full pathname for the output_file_name, then it will be located in the current directory.

30 Go to step 63

31 When you ask for a display of patches in text format, the system displays each patch and the packages to which the patch is applied, as shown in the following example.

Example

```
11700-01:108528-29:SUNWcarx, SUNWcar, SUNWcsr, SUNWhea
109025:108528-13, 108989-01, 108991-09, 108995-02:SUNWcsr, SUNWtoo, SUNWtoox
113684-04::SUNWkvm
111881-03:108528-18:SUNWcsu, SUNWcsxu
109039-10::SUNWatm, SUNWatmu
```

32 Use the following table to determine the step to perform to list patches in text format.

If	Do
you want to list all patches (including Sun patches) installed on both nodes	step 33
you want to list all patches (including Sun patches) installed on the inactive node	step 35
you want to list all patches (including Sun patches) installed on the active node	step 37
you want to list only patches that you specify, that are installed on both nodes	step 39
you want to list only patches that you specify, that are installed on the inactive node	step 41
you want to list only patches that you specify, that are installed on the active node	step 43

33 List all patches installed on both nodes:

```
queryloads -m patches
```

34 Go to step 63

35 List all patches installed on the inactive node:

```
queryloads -m patches -n inactive
```

If you receive a password prompt while querying the inactive node, make sure that the inactive node is in service. If the inactive node is in service and you are still prompted for a password, contact your next level of support.

36 Go to step 63

37 List all patches installed on the active node:

```
queryloads -m patches -n active
```

38 Go to step 63

39 List only patches that you specify, that are installed on both nodes:

```
queryloads -m patches | grep
<unique_patch_identifier>
```

where

<unique_patch_identifier>
is the identifier of the patch you want to list. The following table shows sample unique_patch_identifiers.

Type of patch	Patch name	Examples of possible <unique_patch_identifiers>[a]
Patches that update a specific software package	NTBMI077505-01 (patch applying to package NTbmi7)	NTBMI, NTBMI07, BMI
A specific patch	NTSIM077505-07	NTSIM077505-07
Nortel patches	Not applicable	NT
SUN patches	112162-03::SUNWcarx, SUNWcsr	SUN

a.The entry for <unique_patch_identifier> is case-sensitive.

40 Go to step 63

41 List only patches that you specify, that are installed on the inactive node. Refer to the table in step 39 for an example of unique package identifiers:

```
queryloads -m patches -n inactive | grep
<unique_patch_identifier>
```

where

<unique_patch_identifier>
is the identifier of the patch you want to list.

If you receive a password prompt while querying the inactive node, make sure that the inactive node is in service. If the inactive node is in service and you are still prompted for a password, contact your next level of support.

42 Go to step 63

43 List only patches that you specify, that are installed on the active node. Refer to the table in step 39 for an example of unique package identifiers:

queryloads -m patches -n active | grep <unique_patch_identifier>

where

<unique_patch_identifier>
is the identifier of the patch you want to list.

When you ask for a display of patches in XML format, the system displays each patch and the packages to which the patch is applied, as shown in the following example.

Example

```
<patch>
   <patchid>112097-02</patchid>
    <obsolete></obsolete>
    <requires></requires>
    <imcompat></imcompat>
   <packages>SUNWcsu</packages>
</patch>
<patch>
   <patchid>109667-04</patchid>
    <obsolete></obsolete>
    <requires></requires>
    <imcompat></imcompat>
   <packages>SUNWntpu</packages>
</patch>
```

44 Go to step 63

45 Use the following table to determine the step to perform to display patches in XML format.

If	Do
you want to list all patches (including Sun patches) installed on both nodes	step 46
you want to list all patches (including Sun patches) installed on the inactive node	step 48
you want to list all patches (including Sun patches) installed on the active node	step 50
you want to list only patches that you specify, that are installed on both nodes	step 52

If	Do
you want to list only patches that you specify, that are installed on the inactive node	step 54
you want to list only patches that you specify, that are installed on the active node	step 56

46 List all patches installed on both nodes:

```
queryloads -m patches -x
```

47 Go to step 63

48 List all patches installed on the inactive node:

```
queryloads -m patches -x -n inactive
```

If you receive a password prompt while querying the inactive node, make sure that the inactive node is in service. If the inactive node is in service and you are still prompted for a password, contact your next level of support.

49 Go to step 63

50 List all patches installed on the active node

```
queryloads -m patches -x -n active
```

51 Go to step 63

52 List only patches that you specify, that are installed on both nodes:

```
queryloads -m patches -x | grep <unique_patch_identifier>
```

where

<unique_patch_identifier>
is the identifier of the patch you want to list. The following table shows sample unique_patch_identifiers.

Type of patch	Patch name	Examples of possible <unique_patch_identifiers>[a]
Patches that update a specific software package	NTBMI077505-01 (patch applying to package NTbmi7)	NTBMI, NTBMI07, BMI
A specific patch	NTSIM077505-07	NTSIM077505-07

Type of patch	Patch name	Examples of possible <unique_patch_identifiers>[a]
Nortel patches	Not applicable	NT
SUN patches	112162-03::SUNWcarx, SUNWcsr	SUN

a.The entry for <unique_patch_identifier> is case-sensitive.

53 Go to step 63

54 List only patches that you specify, that are installed on the inactive node. Refer to the table in step 52 for an example of unique package identifiers:

```
queryloads -m patches -x -n inactive | grep
<unique_patch_identifier>
```

where

<unique_patch_identifier>
is the identifier of the patch you want to list.

If you receive a password prompt while querying the inactive node, make sure that the inactive node is in service. If the inactive node is in service and you are still prompted for a password, contact your next level of support.

55 Go to step 63

56 List only patches that you specify, that are installed on the active node. Refer to the table in step 52 for an example of unique package identifiers:

```
queryloads -m patches -x -n active | grep
<unique_patch_identifier>
```

where

<unique_patch_identifier>
is the identifier of the patch you want to list.

57 Go to step 63

58 At the prompt, invoke the queryloads tool:

```
queryloads -patch <-d> <source> -o
<output_file_name>
```

where

<-d>
is an option that must be entered if you are specifying a source directory.

<source>
is the directory containing the patches for which you want to extract information (for example, /cdrom/cdrom/applications/cbm/patches).

<output_file_name>
is a file name you designate for the file to hold the patches information. The system attaches the extension .patches to this file name.

Note: If queryloads is invoked from within the directory containing the patch(es), you do not need to enter either the -d option or a source directory name.

The patch information is stored in the output_file.patches file.

59 Go to step 63

60 At the prompt, invoke the queryloads tool:

```
queryloads -m audit -p <product>
```

where

-p
is an option that must be entered if you are specifying a product.

<product>
is a product that you listed using the Queryloads -m products command, as described in step 4.

Example
The following example shows how to enter a product name, based on the sample product listing shown in step 4:

queryloads -m audit -p CBM00070

61 Go to step 63

62 At the prompt, invoke the queryloads tool:

```
queryloads -h
```

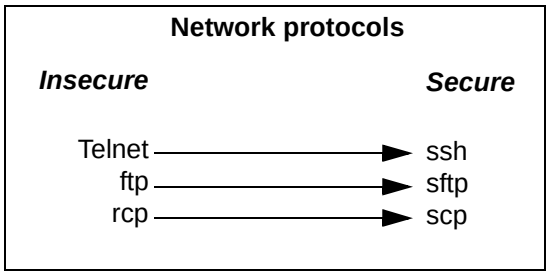
63 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

OpenSSH overview

Functional description

ATTENTION
This document is an overview only of the OpenSSH functionality. Nortel does not provide any detailed usage information or client installation procedures. For this information, refer to the official OpenSSH website located at http://www.openssh.com/.

OpenSSH is an open source version of the Secure Shell (SSH) protocol suite of network connectivity tools. Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. OpenSSH is a suite of tools that provides strong authentication and secure communications over unsecure channels.



The suite of OpenSSH tools is as follows:

- SSH (secure shell) - a replacement for telnet

  Using SSH, you can log in to the core manager from a remote system or log in to a remote system from the core manager. You can also execute commands on a remote system. SSH connects and logs into the specified hostname. You must provide your identity to the remote machine. You can also establish a secure CM session from a remote system through the core manager using SSH.

  Access to some functions requires the use of SSH-compatible client software for access to secure telnet and ftp services (using the SSH standard). SSH clients are bundled with some operating systems, but can to be obtained separately. The following table lists some

sources for SSH clients (sources are not limited to those listed in this table).

Sources for SSH clients

Source	Type
PUTTY	freeware
OpenSSH	freeware
SSH Inc.	commercial
Secure CRT	commercial
WinSCP	freeware

- scp (secure copy) - improved (secure) functionality of rcp (remote copy)

  Using scp, you can securily copy files to and from the core manager or a remote system. Scp uses ssh for data transfer, and uses the same authentication and provides the same security as SSH.

- sftp (secure file transfer program) - a replacement for ftp

  Using sftp, you can perform secure file transfers. Sftp is an interactive program that connects and logs into the specified host, then enters an interactive command mode.

- sshd (OpenSSH SSH daemon) - the server-side daemon

  sshd is the daemon program for SSH. Together these programs provide secure encrypted communications between two hosts over an insecure network.

Note: The functionality of OpenSSH does not interfere with existing networking services, such as telnet, FTP, DCE, NTP, or SFT.

The implementation of OpenSSH on the CS 2000 Core Manager provides three authentication methods:

1 password

2 keys (when you are creating the key, you are asked to add an encrypted password associated with this key)

3 combination of keys and password

The SDM/CBM/CS 2000 Core Manager and the client system administrator must be familiar with the key authentication method, before using it. For detailed instructions on the use of key

authentication, refer to the official OpenSSH website http://www.openssh.com/.

The basic utilities of OpenSSH are:

- ssh-add - adds RSA or DSA identities to the authentication agent
- ssh-agent - authentication agent
- ssh-keygen - authentication key generation, management and conversion
- sftp-server - an sftp server subsystem

For detailed instructions on the use of key authentication, refer to the official OpenSSH website http://www.openssh.com/.

Note: Because the man command is not supported on the SDM, it is not available from SSH shell level.

Related procedures

Refer to the procedure “Installing OpenSSH” in the applicable component Upgrades document to install the OpenSSH fileset.

For additional information, refer to the following web sites:

- http://www.openssh.com/ - for Sun, HP, Linux and AIX
- http://www.chiark.greenend.org.uk/%7Esgtatham/putty/ - a free Win32 Telnet/SSH client for Windows