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 on CD-ROM. The software patches are delivered by way of the electronic software delivery (ESD) method through a high-speed internet connection.

This NTP contains the procedures for applying or removing software packages to or from the CBM 850 cluster using the cbmmtc user interface, and for patching the CBM 850 cluster using functionality provided by the Software Inventory Manager (SIM).

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 9

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.

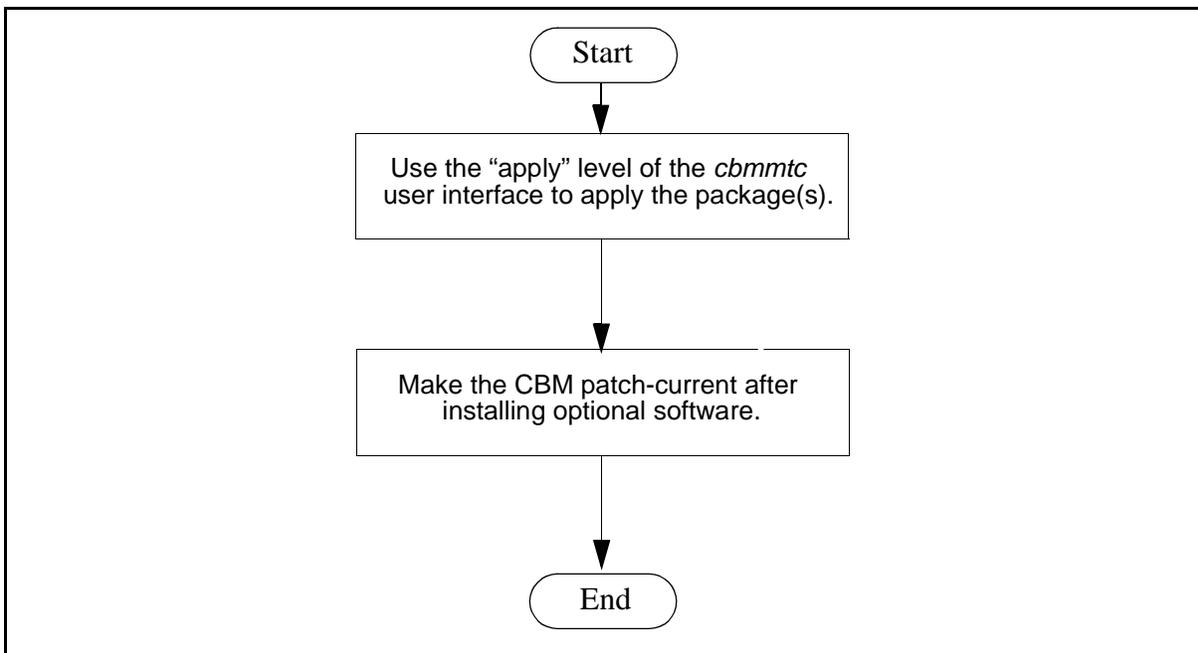### Guide to the software package application procedures

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 73
Removing software packages from a CBM 850 on page 106
Viewing software transaction history and logs on the CBM 850 on page 112
Using the Queryloads tool to display patches and packages applied on the CBM 850 on page 133

The following flowchart shows the basic task flow for package application or removal using the cbmmtc user interface. To perform the

tasks shown in the flowchart below, use the procedures listed in the table above.

Basic task flow for installing software packages on the CBM 850

```
                          ( Start )
                              |
                              v
              +-------------------------------+
              | Use the "apply" level of the  |
              |    cbmmtc user interface to   |
              |      apply the package(s).    |
              +-------------------------------+
                              |
                              v
              +-------------------------------+
              | Make the CBM patch-current    |
              |  after installing optional    |
              |          software.            |
              +-------------------------------+
                              |
                              v
                          (  End  )
```

Software patch application

Patches are applied safely to applications that are running on a CBM 850 cluster and that are not in OFFL state: applications are automatically busied before patch application and are then automatically returned to service after patches have been applied. Patching affects service only for the applications that are modified or updated by the patch

Setting up patching rules using patch filters

There are four types of patches that can be applied on the CBM 850: active apply, inactive apply, manual apply, and interactive. The patch type is used to trigger the appropriate handling of the patch while the patch is being applied using the SIM patching tool:

* "Active apply" patches can be applied automatically by setting a patching schedule for the active node of the CBM 850 cluster through the SIM patching tool, "patchconfig". Patches are applied first on the active node of the cluster and are then automatically applied on the other (inactive) node of the cluster.

* "Inactive apply" patches can be applied automatically by setting a patching schedule for the inactive node of the CBM 850 cluster through the SIM patching tool, "patchconfig". Patches are applied

first on the inactive node of the cluster and are then automatically applied on the other node of the cluster after a SwAct, which prevents impact on any running applications.

- "Manual" patches cannot be applied automatically and, thus, cannot be scheduled. Any special instructions for manual-apply patches will be displayed prior to the patch being applied.

- "Interactive" patches require special handling. These patches are not applied on the system by the SIM tool, but are instead moved by the SIM tool to a special directory for application at a later time. At the same time the SIM tool will display any special instructions for applying the interactive patches.

   Note: Both "Inactive" and "Manual" patches may also require a reboot of the node. If a patch that requires a reboot is applied, the system will prompt you to reboot the node.

The SIM patching tools can be used to override the embedded patch handling requirements for a patch with a more conservative handling procedure. This feature is enabled by setting patch filters. The filters are configured, updated, or removed through the "patchfilter" tool. The filtering mechanism is based on the filter pattern matching either the patch name, the name of the package of patch updates, or the category of the patch.

On the CBM 850, two types of filters can be set: manual filters and inactive filters. When a manual filter is set, active-apply patches and inactive-apply patches matching specified criteria will always be treated as manual-apply patches. When an inactive filter is set, active-apply patches matching specified criteria will be treated as inactive-apply patches.

Manual-apply and interactive patches cannot be filtered to become inactive-apply patches, nor can any patches be filtered to become active-apply patches. In all such cases, the more conservative application handling embedded within the patch takes precedence.

Checking the integrity and authenticity of patches

Patches must pass an integrity check provided by the patching tool before they can be applied. Patches that fail the integrity check are moved to the "/swd/fixes/rejected" directory and are not applied on the CBM 850.

Setting up automatic patching schedules and applying patches on the CBM 850

Automatic patching is the recommended method of applying patches on the CBM 850 cluster. The configurable patch application schedule for automatic patching is set through the SIM "patchconfig" tool. Configurable patch application schedules allow patches to be applied automatically during less busy time periods. The SIM tool detects any patches that require a reboot after application and automatically conducts the reboot. The SIM tool also automatically initiates a SwAct for inactive-apply patches, since inactive-apply patches are applied first on the inactive node of a cluster.

During the execution of the automatic patching schedule, the following actions occur in the order shown:

- The integrity of all of the patches is checked.

- The manual and inactive filter files are consulted. Any active-apply patches that match the criteria of an inactive filter are moved to the "/swd/fixes/inactive" directory. Any active-apply or inactive-apply patches matching the criteria of the manual filter are moved to the "/swd/fixes/manual" directory and are not applied through automatic patching.

- A check of the patches is performed to ensure that any requirements of the patches are met. Only patches that successfully pass this check can be applied through automatic patching.

- A reboot check is performed and any patches that require a reboot are identified to the system.

- All "sane" patches are then applied on the CBM 850. The active-apply schedule will cause the patches to be applied first on the active node and then automatically on the inactive node. The inactive-apply schedule will cause the patches to be applied first on the inactive node and then, after a SwAct, automatically on the other (newly-inactive) node.

- The system is automatically rebooted if at least one of the patches that was applied required a reboot. The reboot occurs only after all of the patches on a node have been applied.

  Note: If a *reboot filter is set, patches requiring reboots must be applied manually during a maintenance window from the /swd/fixes/manual directory.

- Any patches filtered through the *reboot filter, or through any other filtering, causing patches to be moved to the /swd/fixes/manual directory, must be applied manually at a different time.

Manually applying patches on the CBM

Although the recommended method of applying patches on the CBM is through an automatic patching schedule, it is possible to also apply patches manually. Patches are applied manually in an interactive mode. After specifying a single patch or the directory containing the patches, the SIM tool performs the patch application and prompts you before conducting any required reboots or SwActs.

Clearing patching alarms

SDM610 patching alarms are raised in response to problems if they occur during the patching process. An SDM610 alarm is raised on the node of the CBM 850 cluster on which the alarm is generated. After a SwAct, the alarm still applies to the node on which it was originally generated. Thus, care must be taken to correctly identify the node on which the alarm was generated before performing alarm clearing activities.

SDM610 alarms are raised in response to the following problems if they occur during patching:

- A minor alarm is raised in response to a patch application that fails. Up to five failed minor patch alarms can be raised. At the occurrence of the sixth alarm, a critical alarm is raised and the patching tool exits. Critical alarms raised in response to failed patches appear in the banner of the cbmmtc user interface, under CBM.

- A reboot that fails during a patch transaction causes a minor alarm to be raised.

- A SwAct that fails during a patch transaction causes a minor alarm to be raised.

A minor alarm is cleared automatically when the patch that caused the alarm to be raised is successfully applied. A critical alarm will be cleared automatically when one or more of the failed patching minor alarms is cleared. Therefore, it is recommended that you always attempt to clear alarms by re-applying failed patches. If this does not clear an alarm, you should then contact your next level of support for assistance. When necessary, minor alarms can be cleared through the SIM "simAlarmClear" tool.

Removing patches from the CBM 850

The SIM tool can be used to remove applied patches from the CBM 850. The removal of a patch restores the software package to its state prior to the patch application. Upon removal of a patch, all data associated with the patch are removed from the system, but the file systems and data associated with the package that was being patched still remain.

Patches are removed first from the active node of a CBM 850 cluster and are then removed automatically from the inactive node of the cluster. It is also possible to remove patches only from the inactive node.

> *Note:* Patches to be removed may also require a reboot of the node. If a patch that requires a reboot is removed, the system will prompt you to reboot the node.

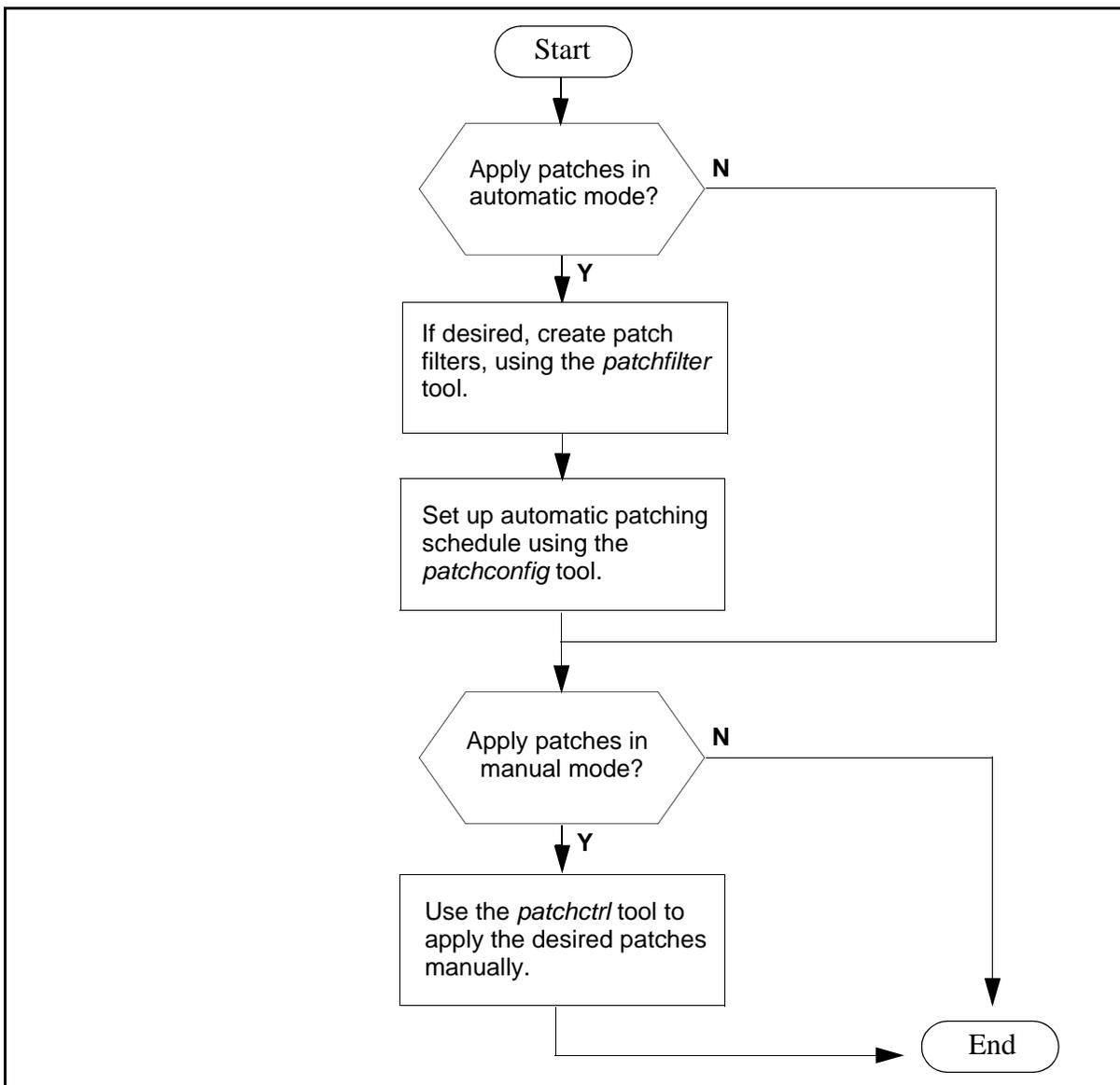### Querying the system for patch information using Queryloads

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

Guide to the SIM patching tool procedures

The following table provides a list of the procedures you can perform to apply patches on the CBM 850.

Procedure
Delivering patches to a CBM 850 on page 114
Setting up patch filters for a CBM 850 cluster on page 116
Setting up automatic patching on a CBM 850 cluster and removing previously-configured schedules on page 122
Manually applying patches to a CBM 850 on page 125
Removing a patch from a CBM 850 on page 130
Using the Queryloads tool to display patches and packages applied on the CBM 850 on page 133
Clearing an SDM610 alarm on page 146
Creating a user allowed to perform patching on a CBM on page 148

The following flowchart shows the basic task flow for patching using the SIM patching tool. To perform the tasks shown in the flowchart below, use the procedures listed in the table above.

Basic task flow for applying patches on the CBM 850

```
                    ┌─────────┐
                    │  Start  │
                    └────┬────┘
                         │
                         ▼
                    ╱─────────╲
                   ╱ Apply     ╲        N
                  ╱  patches in  ╲──────────────────────┐
                  ╲  automatic    ╱                      │
                   ╲ mode?       ╱                       │
                    ╲───────────╱                        │
                         │ Y                             │
                         ▼                               │
              ┌──────────────────────┐                  │
              │ If desired, create    │                 │
              │ patch filters, using  │                 │
              │ the patchfilter tool. │                 │
              └──────────┬───────────┘                  │
                         ▼                               │
              ┌──────────────────────┐                  │
              │ Set up automatic      │                 │
              │ patching schedule     │                 │
              │ using the patchconfig │                 │
              │ tool.                 │                 │
              └──────────┬───────────┘                  │
                         │◄──────────────────────────────┘
                         ▼
                    ╱─────────╲
                   ╱ Apply     ╲        N
                  ╱  patches in  ╲──────────────────────┐
                  ╲  manual mode? ╱                      │
                   ╲            ╱                        │
                    ╲──────────╱                         │
                         │ Y                             │
                         ▼                               │
              ┌──────────────────────┐                  │
              │ Use the patchctrl     │                 │
              │ tool to apply the     │                 │
              │ desired patches       │                 │
              │ manually.             │                 │
              └──────────┬───────────┘                  │
                         │                               ▼
                         └──────────────────────►  ┌─────────┐
                                                   │   End   │
                                                   └─────────┘
```

Upgrading the CBM 850

Upgrade strategy

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
- upgrading the SSPFS 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 SSPFS upgrade.

ATTENTION
For a successful CBM 850 upgrade, all CBM software applications must be either in-service or offline.

ATTENTION
In order to perform the CBM 850 upgrade, the two nodes of the CBM 850 cluster must be in service.

ATTENTION
Before starting the upgrade, ensure that the currently-running CBM node is patch-current.

Procedures

Upgrading the CBM 850 consists of the following tasks:

-
-
-

Preparing to upgrade the CBM 850

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

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

(I)SN07 to (I)SN08 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
1	Ensure that no SBA alarms are currently raised.		Use procedure "SBA alarm troubleshooting" in NN10351-911, *Core and Billing Manager 850 Fault Management* to check for alarms.
2	Ensure that adequate backup space is available on the core. During the CBM 850 upgrade, the billing application will go into backup.		To determine the amount of backup disk space required, see "Disk Space Requirements" in "Preparing for SBA installation and configuration" in NN10363-811, *Core and Billing Manager 850 Accounting*. To reconfigure backup volumes, refer to the procedure "Configuring SBA backup volumes on the core" in NN10363-811, *Core and Billing Manager 850 Accounting*.

(I)SN07 to (I)SN08 CBM 850 upgrade preparation checklist

	Activities	√	Procedures

3	Ensure that the SN07 CBM 850 system is patch-current.		1. Launch your web browser.
			
			2. Search for www.nortelnetworks.com
			
			3. Under the pulldown menu labeled "Support and Training", select "software downloads".
			
			4. In the "Find Products" box at the right side of the screen, click "Families"
			
			5. In the "Product Families" list that displays, click "DMS"
			
			6. In the "DMS: General Availability" list that displays, click "Software" under the "Core and Billing Manager" entry.
			
			7. At the top of the list of software entries that displays, click "Filter and Sort"
			
			8. Make the appropriate selections (such as CBM00070) in the sort boxes and then click "GO"
			
			9. Create a directory in the "root" directory (/) on the CBM 850 to hold the patches that you have selected:
			
			`mkdir /<directory name>`
			
			10. Download the patches from the RPS ftp site to an intermediary location. Then, ftp the patches from this location to the directory on your CBM 850 that you created in step 9.
			
			11. Apply the patches on the CBM 850 by first logging in to the CBM 850 as the root user and then entering the following command:
			
			`patchctrl -d <directory name>`
			
			where <directory name> is the full pathname of the directory containing the patches.

(I)SN07 to (I)SN08 CBM 850 upgrade preparation checklist

	Activities	√	Procedures
4	Prior to the upgrade, verify that your system has a minimum of 1.074 Gbytes of available disk space on the "/opt" file system, and a minimum of 1.077 Gbytes of available disk space on the "/var" file system.		If required, refer to procedure "Verifying disk utilization on an SSPFS-based server" in the *ATM/IP Security and Administration document*, NN10402-600.

Upgrading the CBM 850

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

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

(I)SN07 to (I)SN08 CBM 850 upgrade checklist

	Activities	√	Procedures
1	Start the SSPFS platform and software upgrade.		Perform the steps in the procedure Upgrading SSPFS software on page 39 to the point at which you are prompted by the system to select the media used for the CBM upgrade.
2	Upgrade the CBM 850 software and applications.		The CBM 850 software and application upgrade occurs automatically as part of the SSPFS upgrade. When, during that upgrade, you are prompted to select the media used for the CBM upgrade, perform Procedure for upgrading a CBM 850 on page 14

Procedure for upgrading a CBM 850

ATTENTION
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 a return to the previous SSPFS and CBM 850 release.

At your workstation

1   The CBM 850 upgrade process is automatically initiated during the SSPFS upgrade process. When the program that runs the CBM 850 upgrade starts, the following banner 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):
```

In response to the prompt you may:

- enter "cdrom" to start the upgrade

- enter "shell" to suspend the upgrade and enter a Maintenance shell before continuing the upgrade

- enter "fallback" to cancel the entire upgrade procedure

  Note: In release (I)SN08, 'esd' is only supported for emergency use when the cdrom media is defective. Therefore, 'esd' cannot be entered as the initial media for the

upgrade; only 'cdrom' can be entered as the initial media for the upgrade.

Use the following table to determine your next step.

If	Action
you entered "shell"	Go to step 2
you entered "fallback"	Go to step 3
you entered "cdrom"	Go to step 4

2   The system displays the following:

You have selected to enter a Maintenance Shell. Please contact next level of support to determine the proper course of action.

During the first part of the CBM 850 upgrade, that is, preparing the CBM upgrade media, the system informs you about what you will be prompted for when you exit the shell.

Proceed with shell? (yes | no):

Once the action has been completed, enter 'exit' at the command line prompt to return to the upgrade.

If	System response
you entered "yes"	A maintenance shell prompt appears. You may then either: - enter commands to perform some action or - enter "exit". When you enter "exit", the system will re-perform the last action it performed before you entered the maintenance shell. Go back to the step that you were performing when you selected to enter a maintenance shell.When you enter "exit", you are re-prompted to enter either "cdrom", "shell", or "fallback".
you entered "no"	When you enter "no", the system will re-perform the last action it performed before you entered the maintenance shell. Go back to the step that you were performing when you selected to enter a maintenance shell.

3   The system displays the following:

You have selected to perform a fallback. This choice will cancel the entire UPGRADE.

Proceed with fallback? (yes|no):

If	System response
you entered "yes"	The CBM 850 upgrade is cancelled and the node is brought to the ok prompt. Perform the procedure <u>Executing a fallback during an SSPFS-based server upgrade on page 57</u> starting with step 3. (See "Executing a fallback during an SSPFS-based server upgrade" in NN10408-900, *ATM/IP Fault Management* for more information.)
you entered "no"	When you enter "no", the system will re-perform the last action it performed before you selected to fallback. Go back to the step that you were performing when you selected to fallback.

4   The system displays the following:

Please insert the CBM CD disk into the CDROM drive.

Once the CD has been inserted, please select one of the following:

  - enter 'continue' to start the CBM portion of the upgrade.

  - enter 'shell' to suspend the upgrade and enter a Maintenance Shell.

  - enter 'media' to select a different CBM software delivery method.

  - enter 'fallback' to cancel the entire UPGRADE procedure.

Choice (continue | shell | media | fallback):

Insert the CBM CD disk into the CDROM drive and then respond to the system prompt.

If	Action
you entered "shell"	See step <u>2</u> for the system response.
you entered "fallback"	See step <u>3</u> for the system response.
you entered "continue"	See step <u>5</u> for the system response.

5   Use the following table to determine your next step:

If	Action
problems were encountered after you inserted the CD	Go to step 7.
no problems were encountered after you inserted the CD	Go to step 6

6   The system displays the following:

```
====== Allowing time for CD media to automount (est. 10 sec) ... Completed.
====== Checking CD media (est. 2 sec) ... Completed.
====== Preparing CBM CD Media for use (est. 5 min.) ... Completed
NOTIFICATION: ejecting cdrom (est. 1 sec) ... Completed.
=========================================================
=== Invoking cbm_setup script to invoke the CBM portion of the Upgrade.
=========================================================
```

Go to step 10.

7   The system displays the following:

```
====== Allowing time for CD media to automount (est. 10 sec) ... Completed.
====== Checking CD media (est. 2 sec) ... ERROR:
```
The system displays the text for the particular error that was encountered.

Please insert the CBM CD disk into the CDROM drive.

Once the CD has been inserted, please select one of the following:

 - enter 'continue' to start the CBM portion of the upgrade.

 - enter 'shell' to suspend the upgrade and enter a Maintenance Shell.

 - enter 'media' to select a different CBM software delivery method.

 - enter 'fallback' to cancel the entire UPGRADE procedure.

Choice (continue | shell | media | fallback):

If	Action
you entered "shell"	See step 2 for the system response.
you entered "fallback"	See step 3 for the system response.

If	Action
you entered "media"	See step 8 for the system response.
you entered "continue"	See step 5 for the system response.

8   The system displays the following:

> 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):

In response to the prompt you may:

- enter "esd" to select an ESD image to be used for the upgrade

    Note: The "esd" selection is only available when the cdrom media is defective and when an esd media has been prepared by Nortel for recovery purposes. Therefore, you should contact your next level of support before proceeding with the upgrade.

- enter "shell" to suspend the upgrade and enter a Maintenance shell before continuing the upgrade

- enter "fallback" to cancel the entire upgrade procedure

Use the following table to determine your next step.

If	Action
you entered "shell"	Go to step 2
you entered "fallback"	Go to step 3
you entered "esd"	Go to step 9
you entered "cdrom"	Go to step 4

9   If only one ESD image is found in the /swd/sdm directory, that image is selected by the system, by default, and you will not receive any additional prompts. If more than one ESD image is

found in the /swd/sdm directory, the system will display the list of images and a series of prompts for selecting the image to use as shown in the following example:

There appears to be more than one ESD image located within the /swd/sdm directory.

Please choose which ESD file you would like to use:

The system displays a list of ESD files from which to choose, for example:
1: CBM08_21.57.2.99.iso.gz.tape
2: CBM08_21.99.99.99.iso.gz.tape
3: CBM08_22.57.6.0.iso.gz.tape

  - enter 'shell' to suspend the upgrade and enter a Maintenance Shell to retrieve the ESD image if it is not available.

  - enter 'media' to re-select the CBM software delivery method.

  - enter 'fallback' to cancel the entire UPGRADE procedure

choice (1-4 | esd | shell | media | fallback):

Once you have chosen a valid ESD image from the list, the system displays the following:

======== Verifying that this is a CBM ISO image (est. 2 sec) ... Completed.

======== Verifying disk space (est. 2 sec) ... Completed.

======== Preparing the CBM ESD Media for use (est. 3 min) ... Working

10   When the CBM upgrade begins, the upgrade program checks for any Major or Critical alarms on either node of the CBM 850 cluster and notifies you with information about any alarms that have been found. If alarms are found by the program, you may:

- enter 'shell' to suspend the upgrade and enter a Maintenance shell in order to address the problems indicated by the alarms

- enter 'fallback' to cancel the entire upgrade and fall back to the previous release

- enter 'continue' to continue the upgrade if the level or severity of the alarm does not warrant correction at this time

The following examples show samples of system displays when errors are discovered.

Example 1

The following example shows a sample upgrade display when alarms have been discovered and you choose to suspend the upgrade by entering 'shell' and address the alarms. This sample

does not show any commands entered to perform an alarm correction activity, but it does show exiting from the shell:

```
==================================================
===      CBM Setup Program - UPGRADE procedure
==================================================
======== Examine CBM Alarms (est. 1 min)...Warning:
==================================================
        Detected MAJOR and/or CRITICAL alarms
```

Local Node:

Major:1

  ** SPFS340 MSH: Cluster nodes out of sync.

Please investigate the alarms and/or contact your next level of support to determine the next course of action.

  - enter 'shell' to suspend the upgrade and enter a Maintenance Shell

  - enter 'fallback' to cancel the entire UPGRADE procedure

  - enter 'continue' to proceed with the UPGRADE

NOTE:

During the upgrade, it is expected that the Cluster Nodes be out of Sync (i.e. SPFS340 MSH: Cluster nodes out of Sync). This is the only alarm that may be ignored - ALL OTHER ALARMS should be investigated before continuing.

Choice (shell/fallback/continue):shell

You have selected to enter a Maintenance Shell. Please contact next level of support to determine the proper course of action.

Proceed with shell? (yes|no):yes

Once the action has been completed, enter 'exit' at the command line prompt to return to the upgrade.

cbm_upgrade_shell:>

In response to the Maintenance Shell prompt, you may examine the alarms and perform any required actions. When you have completed any alarm examination and correction, you may enter "exit" to exit from the Maintenance Shell and resume the upgrade.

cbm_upgrade_shell:>exit

If you have resolved all of the alarms that have been discovered, the upgrade resumes. If you have not resolved all of the alarms that have been discovered, you will be prompted as to whether to continue the upgrade.

Example 2

The following example shows a sample upgrade display when alarms have been discovered and you choose to continue the upgrade without first correcting any alarms:

```
==================================================
===      CBM Setup Program - UPGRADE procedure
==================================================
======= Examine CBM Alarms (est. 1 min)...Warning:
==================================================
        Detected MAJOR and/or CRITICAL alarms
```

Local Node:

Major:1

  ** SPFS340 MSH: Cluster nodes out of sync.

Please investigate the alarms and/or contact your next level of support to determine the next course of action.

  - enter 'shell' to suspend the upgrade and enter a Maintenance Shell

  - enter 'fallback' to cancel the entire UPGRADE procedure

  - enter 'continue' to proceed with the UPGRADE

NOTE:

During the upgrade, it is expected that the Cluster Nodes be out of Sync (i.e. SPFS340 MSH: Cluster nodes out of Sync). This is the only alarm that may be ignored - ALL OTHER ALARMS should be investigated before continuing.

Choice (shell/fallback/continue):continue

You have selected to proceed with the upgrade. Please confirm that you wish to proceed with the upgrade.

Proceed with upgrade? (yes|no):yes

11   The CBM upgrade program examines the upgrade environment and prepares the system for the CBM upgrade.

Example

The following example shows a sample of the display that occurs as the upgrade environment is being examined:

```
======= Verify the CBM base directory (est. 5 sec) ... Completed
======= Verify disk space (est. 10 sec) ... Completed.
==== Preinstall CBM software management tools (est. 10 sec) ... Completed.
======= Prepare upgrade filesystem (est. 10 sec) ... Completed.
```

If problems are encountered during this portion of the upgrade, you will be prompted to enter either "shell" to suspend the upgrade and enter a Maintenance Shell or "fallback" to cancel the entire upgrade procedure. For a sample of the system response when you enter "shell", see step 2. For a sample of the system response when you enter "fallback", see step 3.

12   After the upgrade environment is prepared, any required CBM packages are applied.

Example 1

The following example shows a sample of the kind of display that occurs when any required CBM packages are applied:

```
======= Examine installed software (est. 15 sec) ... Completed.
======= UPGRADE required packages (est. 5 min) ...
   NT Software Inventory Manager   COMPLETELY INSTALLED
   SDM/CBM Debug Helper tools       REQUIRED - Applying - Completed.
   CBM version Info Files           REQUIRED - Applying - Completed.
   Platform Maintenance Common      REQUIRED - Applying - Completed.
   CBMMTCE Interface                REQUIRED - Applying - Completed.
   Platform Utilities               REQUIRED - Applying - Completed.
   Generic Data Delivery            REQUIRED - Applying - Completed.
   Log Delivery Service             REQUIRED - Applying - Completed.
   Table Access Service             REQUIRED - Applying - Completed.
   OM Access Service                REQUIRED - Applying - Completed.
   GNU Debugger                     COMPLETELY INSTALLED
```

Example 2

The following example shows a sample of the kind of display that occurs when a problem prevents a required CBM package from being applied. The display shows the dialog that would normally occur when a recovery procedure is performed.

```
======= Examine installed software (est. 15 sec) ... Completed.
======= UPGRADE required packages (est. 5 min) ...
   NT Software Inventory Manager   COMPLETELY INSTALLED
   SDM/CBM Debug Helper tools       REQUIRED - Applying - Completed.
   CBM version Info Files           REQUIRED - Applying - Completed.
   Platform Maintenance Common      REQUIRED - Applying - Failed
```

Please see the log file [log file path specified by the system] for more information on the failure.

Please contact your next level of support to determine the next course of action.

  - enter 'shell' to suspend the upgrade and enter a Maintenance Shell.

- enter 'fallback' to cancel the entire UPGRADE procedure

choice (shell | fallback): shell

You have selected to enter a Maintenance Shell. Please contact next level of support to determine the proper course of action.

Proceed with shell? (yes | no): yes

Once the action has been completed, enter 'exit' at the command line prompt to return to the upgrade.

At this point, your next level of support is helping you to replace the faulty package.

cbm_upgrade_shell: exit

======Removing package Platform Maintenance Common (est. 10 sec) ... Completed.

Platform Maintenance Common	REQUIRED - Applying - Completed.
CBMMTCE Interface	REQUIRED - Applying - Completed.
Platform Utilities	REQUIRED - Applying - Completed.
Generic Data Delivery	REQUIRED - Applying - Completed.
Log Delivery Service	REQUIRED - Applying - Completed.
Table Access Service	REQUIRED - Applying - Completed.
OM Access Service	REQUIRED - Applying - Completed.
GNU Debugger	COMPLETELY INSTALLED

13 After the required CBM packages have been applied, the SWIM tool applies any upgrade software packages for applications installed on the system. If any of the software upgrade packages require configuration, the configuration is initiated by the system. You are prompted to press the Return key to start each of the individual configuration programs that run.

Note: If any of the packages have a SWIM UPGRADE configuration script, you are notified by the system and prompted to start their execution.

Example

The following example shows a sample of the kind of display that occurs when upgrade packages for applications installed on the system are applied:

==== UPGRADE value added software using the CBM SWIM tool (est. NA) ...

The following new packages have been selected.

NTswd21 'Bootpd and tftpd' 21.44.4.0

NTscrt21 'SSH Core File Transfer' 21.44.4.0

.

.

.

NTaft21 'SBA Automatic File Transfer' 21.4..4.0

APPLYING Package NTpls21 Version 21.44.4.0
APPLIED Package NTpls21 Version 21.44.4.0
APPLYING Package NTace21 Version 21.44.4.0
APPLIED Package NTace21 Version 21.44.4.0

.

.

.

APPLIED Package NTaft21 Version 21.44.4.0

14   After any upgrade packages for applications installed on the system have been applied and after any required configurations have been performed, the upgrade program applies any patches that are present in the ISO image on the CBM CD.

Example

The following example shows a sample of the kind of display that would occur when patches are applied by the SIM patching tool:

====== Verify and Apply Patches using the SIM patching tool ...
############### Starting: COPYING FILES #############
This may take a moment depending on how many files there are.
############### Completed: COPYING FILES #############
############### Starting: INTEGRITY CHECK #############
Notification: Checking integrity of: NTBMI214404-01.
Success: Integrity confirmed for NTBMI214404.01.
############## Completed: INTEGRITY CHECK #############
############### Starting: PREREQUISITE CHECK #############
Determining if all requisites are installed or available.
Please note: This stage may take a few moments to complete.
############### Completed: PREREQUISITE CHECK #############
########### Starting: APPLICATION PHASE (for active) ###########
Applying NTBMI214404-01 ...
Success: NTBMI214404-01 applied successfully.
Please see the log file: /opt/nortel/sim/logs/PatchLog for additional details.
====== UPGRADE - CBM SIM patching tool end.

15 After the new patches have been applied, the upgrade program performs some additional tasks to complete the upgrade, including preserving logs, preparing data formatting, removing the old release from the upgrade environment, creating load baseline information, and checking the system for alarms. After the CBM upgrade is complete, control of the upgrade process is returned to the SSPFS upgrade.

Example

The following example shows a sample display that occurs at this point in the upgrade:

===== Preserve Logs (est. 5 sec) ... Completed.

===== Prepare Dataformatting (est. 5 sec) ... Completed.

===== Removing Old Release [20] From Upgrade Environment (est. NA) ...
The system displays the names of software packages as they are removed from the system.

===== Creating Load Baseline Information (est. 10 sec) ... Completed.
The upgrade procedure will now return control to the SSPFS portion of the upgrade. CBM Alarms will once again be examined for Major or Critical alarms.

====== Examine CBM Alarms (est. 1 min) ...

If any alarms exist, an alarm summary will be displayed and you will be prompted to enter 'shell' , 'fallback', or 'continue'. For information about how to respond to any alarms that are discovered, see step 10.

16 When the CBM upgrade is complete, control will be returned to the SSPFS upgrade program.

Note: At this time you should make sure that you have inserted the correct SSPFS upgrade CDROM disk into the CDROM drive. When you have entered "OK" in response to the system prompt, you will not have control over the system for approximately five minutes.

The SSPFS upgrade program resumes and activates the SOLARIS_9 upgraded environment. The inactive node of the cluster then reboots.

Note: This reboot will take considerably longer than a regular system reboot.

At this point, the automatic portion of the upgrade is complete and manual steps must be performed to complete the upgrade process. Perform the following steps to ensure that the inactive node has been successfully rebooted:

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

ubmstat

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

b   Enter the following command to determine whether all filesystems are in "STANDBY normal UP clean" (standby) state:

udstat

Re-run this command until all filesystems are shown to be in the standby state.

c   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.

Use the following table to determine your next step.

If	Do
you wish to fall back at this point to cancel the upgrade procedure because something is unsatisfactory	Perform the procedure Executing a fallback during an SSPFS-based server upgrade on page 57 (See "Executing a fallback during an SSPFS-based server upgrade" in NN10408-900, *ATM/IP Fault Management* for more information.)
you wish to complete the upgrade	Go on to section Completing the CBM 850 upgrade on page 28

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

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
1	Ensure that no SBA alarms are currently raised.		Use procedure "SBA alarm troubleshooting" in NN10351-911, *Core and Billing Manager 850 Fault Management* to check for alarms.
2	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 will be sent downstream by performing "Closing billing files" in NN10363-811, *Core and Billing Manager 850 Accounting*. Send the billing files downstream by performing procedure "Sending billing files from disk" in NN10363-811, *Core and Billing Manager 850 Accounting*. If you are unable to send billing files to a downstream destination, Nortel recommends that you back up the billing files to DVD, using the procedure "Copying billing files to DVD using SBADVDWRITE" in NN10363-811, *Core and Billing Manager 850 Accounting*.
3	If your system contains billing streams that meet all of the following qualifications, you must take the AFT and SBA applications offline: - use file format type DIRP - use stream record format BC - validate the SENSOR_TYPE, SENSOR_ID, RECORD_OFFICE_TYPE, RECORD_OFFICE_ID fields in the header and trailer records.		On the active node of the CBM 850 cluster, perform <u>Procedure for taking the AFT and SBA applications offline on page 34</u>

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
4	Complete the SSPFS platform and software upgrade procedure.		Complete the procedure <u>Upgrading SSPFS software on page 39</u> starting with step 12.
5	Bring up the upgraded services on the newly-upgraded unit, making it the newly-active unit.		On the active node of the cluster, perform a swact by entering the following command: **init 6** When the swact completes, continue with step 6.
6	If you took the SBA and AFT offline in step 3 of this table, you must now return these applications to service.		To return the SBA and AFT to service, perform <u>Procedure for returning SBA and AFT to service on page 36</u>
7	Verify that the billing system is collecting billing records and verify the billing streams.		To verify that the billing system is collecting billing records and to verify the billing stream, perform <u>Procedure for determining whether the billing system is collecting billing records and to verify a billing stream on page 38</u>

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures

8	Ensure that any SN08 CBM 850 patches have been applied.		1. Launch your web browser.
			
			2. Search for www.nortelnetworks.com
			
			3. Under the pulldown menu labeled "Support and Training", select "software downloads".
			
			4. In the "Find Products" box at the right side of the screen, click "Families"
			
			5. In the "Product Families" list that displays, click "DMS"
			
			6. In the "DMS: General Availability" list that displays, click "Software" under the "Core and Billing Manager" entry.
			
			7. At the top of the list of software entries that displays, click "Filter and Sort"
			
			8. Make the appropriate selections (such as CBM00080) in the sort boxes and then click "GO"
			
			9. Create a directory in the "root" directory (/) on the CBM 850 to hold the patches that you have selected:
			
			`mkdir /<directory name>`
			
			10. Download the patches from the RPS ftp site to an intermediary location. Then, ftp the patches from this location to the directory on your CBM 850 that you created in step 9.
			
			11. Apply the patches on the CBM 850 by first logging in to the CBM 850 as the root user and then entering the following command:
			
			`patchctrl -d <directory name>`
			
			where \<directory name\> is the full pathname of the directory containing the patches.

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
9	At this point, you must decide whether things look well with both the SSPFS and CBM upgrades. You can choose either to accept the new environment permanently, or you can choose to roll back to the state prior to the upgrade and lose all upgrade work.		If you have decided to fall back to the state prior to the upgrade, go to step 10 in this table. If you have decided to accept the new environment, go to step 11 in this table.

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
10	If you have decided to fall back to the state prior to the update, perform this step.		1. Log in to the inactive unit (the unit on which the "init 6" command was performed) and enter the following command: **GetRunningClusterNodeNames** Ensure that the system returns TWO nodes. If it doesn't, wait for one minute and retry the command. If the system still doesn't return TWO nodes, contact your next level of support before proceeding with this upgrade. 2. If your system contains billing streams that meet all of the following qualifications, you must take the AFT and SBA applications offline: - use file format type DIRP - use stream record format BC - validate the SENSOR_TYPE, SENSOR_ID, RECORD_OFFICE_TYPE, RECORD_OFFICE_ID fields in the header and trailer records. To take the SBA and AFT offline, perform the procedure, Procedure for taking the AFT and SBA applications offline on page 34.
	Note: Step 3 allows you to fall back to the state prior to the update. After a fallback, file systems gradually become fully-active on the newly-active unit. While file systems are becoming fully-active, you may see applications going into system-busy state. After the file systems have become fully-active, however, the applications will come into service automatically.		3. Perform the procedure Confirming the upgrade on an SSPFS-based server on page 59 and follow the steps to rollback to the state prior to the upgrade. Perform steps 1, 4, 6, and 8-9. Then return to this step in this table. 4. Return the SBA and AFT to service by performing the procedure, Procedure for returning SBA and AFT to service on page 36. After performing this step, you have completed the upgrade procedure.

(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist

	Activities	√	Procedures
11	If you have decided to accept permanently the new environment, perform this step.		Perform the procedure <u>Confirming the upgrade on an SSPFS-based server on page 59</u> and follow the steps to accept the upgraded environment.
12	Edit the object properties in the IEMS for the CBM SSPFS platform you just upgraded to reflect the new software version.		Refer to either of the procedures that follow to update the software version in the Device Version field. - <u>Editing and viewing object properties using Java Web Client on page 153</u> -<u>Editing and viewing object properties using Web Client on page 158</u>

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

Procedure for taking the AFT and SBA applications offline

At your workstation

1   From the command line, access the APPL level of the maintenance interface:

cbmmtc appl

If AFT application	Do
is installed on your system	step 2
is not installed on your system	step 5

2   Busy the AFT application:

bsy <application_number>

where

   <application_number>
      is the number next to the Automatic File Transfer application

3   Confirm the command:

y

4   Offline the AFT application:

offl <application_number>

where

   <application_number>
      is the number next to the Automatic File Transfer application

5   Busy the SuperNode Billing Application (SBA):

bsy <application_number>

where

   <application_number>
      is the number next to the SuperNode Billing Application

6   Confirm the command:

y

7   Take the SBA offline:

`offl <application_number>`

where

    <application_number>
        is the number next to the SuperNode Billing Application

8   You have completed this procedure. Return to the table <u>(I)SN07 to (I)SN08 CBM 850 upgrade completion checklist on page 28</u>

Procedure for returning SBA and AFT to service

At your workstation

1   Access the APPL level of the maintenance interface:

`cbmmtc appl`

2   Wait until the Table Access Service application is in service (InSv), then continue with the procedure. If the application does not return to service after 15 minutes, contact your next level of support.

3   Busy the SBA:

`bsy <application_number>`

where

    <application_number>
      is the number next to the SuperNode Billing Application

4   Confirm the command:

`y`

5   Return the SBA to service:

`rts <application_number>`

where

    <application_number>
      is the number next to the SuperNode Billing Application

Note: Check to ensure that all billing streams are either in-service or in recovery on the core side before continuing.

If AFT application	Do
is installed on your system	step 6
is not installed on your system	step 8

6   Busy the AFT application:

`bsy <application_number>`

where

    <application_number>
      is the number next to the Automatic File Transfer application

7   Confirm the command:

`y`

8   Return the AFT application to service:

`rts <application_number>`

where

> **`<application_number>`**
>   is the number next to the Automatic File Transfer
>   application

9   Exit from SDMMTC:

`quit all`

10   Access the BILLMTC level:

`billmtc`

11   Access the APPL level:

`appl`

12   Access the AFT level:

`aft`

13   Restart the AFT session:

`start <session_name>`

Example response:

*** WARNING: Started AFT session: <session_name>

14   You have complete this procedure. Return to the table

Procedure for determining whether the billing system is collecting billing records and to verify a billing stream

At your workstation

1   Verify that billing is collecting records:

query <stream_name>

where

<stream_name>
   is the name of the billing stream, for example, ama.

Note the number of records, wait approximately 10 seconds, and repeat the query command.

If the number of records	Do
increased from the first query command (meaning billing is working)	step 2
did not increase from the first query command (meaning billing is not working)	contact your next level of support

2   You have completed this procedure. Return to the table (I)SN07 to (I)SN08 CBM 850 upgrade completion checklist on page 28

Upgrading SSPFS software

Application

Use this procedure to upgrade the SSPFS software on a Sun Netra t1400 or Sun Netra 240 from (I)SN06.2 or (I)SN07 to the (I)SN08 release.

Prerequisites

This procedure has the following prerequisites:

- Ensure you have SSPFS Disk 1, SSPFS Disk 2, and SSPFS Disk 3 for the (I)SN08 release.

- Ensure you have backed up your Oracle data and file systems before proceeding with this procedure. If required, refer to the following procedures:

  — Performing a backup of oracle data on an SSPFS-based server on page 44

  — Performing a backup of file systems on an SSPFS-based server on page 50

  Note: Backing up the Oracle data is not applicable on an SSPFS-based server that is hosting the Core Billing Manager (CBM).

- Ensure that none of the user-defined group identifications (GIDs) and user identifications (UIDs) conflict with the GIDs and UIDs that the SSPFS requires during the upgrade. If required, refer to procedure Verifying group IDs and user IDs on an SSPFS-based server on page 1.

  Note: It is not necessary to verify the group IDs or user IDs on an SSPFS-based server that is hosting the Core and Billing Manager (CBM).

- Ensure the site spec book is available with IP addresses, hostnames, and non-system logins.

Action

Perform the following steps to complete this procedure.

At the server console

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

> ***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.

At the server console

3   Ensure you are at the root directory level by typing

`# cd /`

and pressing the Enter key.

4   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.

> ***Note:*** The execution of this step takes approximately 5 minutes to complete on a Netra t1400, and 3 minutes on a Netra 240. These completion times for the execution of the pre-upgrade script are averages and can vary based on such factors as machine load.

5   Start the upgrade process by typing

`# /liveupgrade.ksh`

and pressing the Enter key.

If prompted, accept the specified device as the boot device by typing

`yes`

and pressing the Enter key.

> *Note:* The execution of this step takes approximately 75 minutes to complete on a Netra t1400, and 40 minutes on a Netra 240 depending on the system configuration. However, during this time, the server is fully functional and applications can be used.

Once this step completes, the system will eject SSPFS Disk 1 and prompt you to insert SSPFS Disk 2.

At the server

6   Remove "SSPFS Disk 1" from the CD ROM drive, and insert "SSPFS Disk 2".

At the server console

7   When ready, indicate you want to proceed by typing

  # **ok**

and pressing the Enter key

> *Note:* The execution of this step takes approximately 35 minutes to complete on a Netra t1400, and 25 minutes on a Netra 240 depending on the system configuration.

Once this step completes, the system will eject SSPFS Disk 2 and prompt you to insert SSPFS Disk 3.

At the server

8   Remove "SSPFS Disk 2" from the CD ROM drive, and insert "SSPFS Disk 3".

At the server console

9   When ready, indicate you want to proceed by typing

  # **ok**

and pressing the Enter key

> *Note:* The execution of this step takes approximately 95 minutes to complete on a Netra t1400, and 40 minutes on a Netra 240 depending on the system configuration.

10 Use the following table to determine your next step.

If you	Do
are prompted with "Please select the software delivery method that is being used for the CBM load?	continue with Procedure for upgrading a CBM 850 on page 14 to upgrade the Core Billing Manager (CBM)
are not prompted with "Please select the software delivery method that is being used for the CBM load?	step 11

11 Wait until the upgraded server fully comes up from the boot before you proceed.

12 Log back in to the server using the root user ID and password.

13 Verify that your system is running the SN08 version of the SSPFS as follows:

> *Note:* You must be the root user to execute the steps that follow.

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

 X - exist

select -
```

b Enter the number next to the "View" option in the menu.

Example response

```
View
 1 - sspfs_soft (Display Software
     Installation Level Of SSPFS)
 2 - chk_sspfs (Check SSPFS Processes)
 3 - sw_conf (The software configuration of
     the wrtypyxp)
 4 - cpu_util (Overall CPU utilization)
 5 - cpu_util_proc (CPU utilization by
     process)
 6 - port_util (I/O port utilization)
 7 - disk_util (Filesystem utilization)

 X - exist

select -
```

c Enter the number next to the "sspfs_soft" option in the menu.

Example response

```
=== Executing "sspfs_soft"

SSPFS version: 08.0 Build: 200508421 Server
Profile: cbm850

==="sspfs_soft" completed successfully
```

d Note the SSPFS version.

If the SSPFS version is	Do
08.0	step 14
anything else	contact your next level of support

At the server

14   Remove "SSPFS Disk 3" from the CD ROM drive.

You have completed this procedure.

Performing a backup of oracle data on an SSPFS-based server

Application

Use this procedure to perform a backup of oracle data on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240) running the (I)SN06.2 or greater release of the SSPFS.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)

   Note: If the server is hosting the Integrated EMS, it is highly recommended to purge the Integrated EMS event and performance data prior to executing the data backup. This reduces the size of the oracle space used by the Integrated EMS, and therefore, reduces the backup time, and can avoid a backup failure. The purge capability is only available in (I)SN07 onward.

- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core and Billing Manager (CBM)

   Note: If the server is hosting the Core and Billing Manager (CBM), an oracle data backup is not required.

ATTENTION

It is recommended that provisioning activities be put on hold during the time of the data backup.

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS (I)SN06.2 or greater

- for a Sun Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data

- for a Sun Netra 240, you need one or more blank CD-R, DVD-R, CD-RW or DVD-RW to store the data

   Note 1: The backup utility limits the storage to 2 GB on a DVD-R and DVD-RW.

   Note 2: If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure "Preparing a CD-RW or DVD-RW for use" in the ATM/IP Security and Administration document, NN10402-600, if required.

ATTENTION

The database must be in sync with the Communication Server 2000 and the MG 9000 Manager (if present). Therefore, ensure you have an image of both before you proceed. Performing a restore from the Oracle database alone can cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

Action

ATTENTION

In a two-sever configuration, execute this procedure on the Active server.

At the server

1   Insert the blank tape, CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the Active server.

At your workstation

2   Log in to the server by typing

> `telnet <server>`

and pressing the Enter key.

where

    server
        is the IP address or hostname of the SSPFS-based server on which you want to perform the backup

        Enter 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 - root`

and pressing the Enter key.

5   When prompted, enter the root password.

6   If the server is hosting the Integrated EMS, and you want to purge the event and performance data, do step 7, otherwise proceed to step 8.

7   Purge the Integrated EMS event and performance data as follows:

    Note: Purging the Integrated EMS event and performance data prior to executing the data backup, reduces the size of the oracle space used by the Integrated EMS, and therefore, reduces the backup time, and can avoid backup failure. The purge capability is only available in (I)SN07 onward.

    a

ATTENTION

This step stops the Integrated EMS server, therefore, ensure it is acceptable at this time to stop the Integrated EMS server.

    Stop the Integrated EMS server by typing

`# servstop IEMS`

and pressing the Enter key.

    b Run the script to purge the data by typing

        # **`/opt/nortel/iems/current/bin/purgeTempData.sh`**

        and pressing the Enter key.

    c Start the Integrated EMS server by typing

        # **`servstart IEMS`**

        and pressing the Enter key.

8   Use the following table to determine your next step.

If you are using	Do
a tape	step 9
a CD or DVD	step 10

9   Rewind the tape by typing

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

and pressing the Enter key.

10   Backup the data by typing

$ **`/opt/nortel/sspfs/bks/bkdata`**

and pressing the Enter key.

Example response:

`Backup Completes Successfully`

If you are using	Do
a tape	step 11
a CD or DVD	step 12

11 Verify the backup to tape was successful as follows:

a List the content of the tape by typing

`tar tvf /dev/rmt/0`

and pressing the Enter key.

Example response:

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:16 2005
opt/oracle.dmp.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:16 2005
opt/critdata.cpio
```

b Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

You have completed this procedure.

> *Note:* To restore the data from this tape, refer to procedure "Restoring the oracle data on an SSPFS-based server" in the ATM/IP Security and Administration document, NN10402-600.

12 Verify the backup to CD or DVD was successful as follows:

a Reinsert the backup CD or DVD into the drive.

b List the content of the CD or DVD by typing

`tar tvf /cdrom/*bkdata*/*.tar`

and pressing the Enter key.

Example response:

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:17 2005
opt/oracle.dmp.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:17 2005
opt/critdata.cpio
```

> *Note:* When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.

13   Eject the CD from the drive as follows:

    a   Ensure you are at the root directory level by typing

       `# cd /`

       and pressing the Enter key.

    b   Eject the CD by typing

       `# eject cdrom`

       and pressing the Enter key.

       Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

       # /etc/init.d/volmgt stop

       # /etc/init.d/volmgt start

       Then press the eject button located on the front of the DVD drive.

    c   Remove the CD or DVD from the drive, label it, and store it in a safe place.

       You have completed this procedure.

       Note: To restore the data from this CD or DVD, refer to procedure "Restoring the oracle data on an SSPFS-based server" in the ATM/IP Security and Administration document, NN10402-600.

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) running the (I)SN06.2 or greater release of the SSPFS.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (EMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

Prerequisites

This procedure has the following prerequisites:

- you must be running SSPFS (I)SN06.2 or greater
- you must perform a data backup prior to performing this procedure (refer to procedure <u>Performing a backup of oracle data on an SSPFS-based server on page 44</u>, if required)

  Note: The data backup is not required prior to this procedure for the Core and Billing Manager (CBM) product family.

- for a Sun Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data
- for Sun Netra 240, you need one or more blank CD-R, CD-RW, DVD-R or DVD-RW to store the data

  Note 1: The backup utility limits the storage to 2 GB on a DVD-R and DVD-RW.

  Note 2: If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure "Preparing a CD-RW or DVD-RW for use" in the ATM/IP Security and Administration document, NN10402-600, if required.

Action

> **ATTENTION**
> In a two-sever configuration, execute this procedure on the Active server.

At the server

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

Enter 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 - root`

and pressing the Enter key.

5 When prompted, enter the root password.

If you are using	Do
a tape	step 6
a CD or DVD	step 7

6 Rewind the tape by typing

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

and pressing the Enter key.

7   Backup 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 CD or DVD, the system will prompt you to insert another blank CD or DVD if more than one is needed.

If you are using	Do
a tape	step 8
a CD or DVD	step 9

8   Verify the backup to tape was successful as follows:

a   List the content of the tape by typing

gtar -tvMf /dev/rmt/0

and pressing the Enter key.

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

You have completed this procedure.

9   Verify the backup to CD or DVD was successful as follows:

a   Reinsert the backup CD or DVD into the drive.

b   List the content of the CD or DVD by typing

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

and pressing the Enter key.

> *Note:* When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.

10   Eject the CD from the drive as follows:

    a   Ensure you are at the root directory level by typing

        `# `**`cd /`**

        and pressing the Enter key.

    b   Eject the CD by typing

        `# `**`eject cdrom`**

        and pressing the Enter key.

        Note: If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

        # **/etc/init.d/volmgt stop**

        # **/etc/init.d/volmgt start**

        Then, press the eject button located on the front of the DVD drive.

    c   Remove the CD or DVD from the drive, label it, and store it in a safe place.

        You have completed this procedure.

Verifying group IDs and user IDs on an SSPFS-based server

Application

Use this procedure to verify the group identifiers (GID) and user identifiers (UID) defined on a Succession Server Platform Foundation Software (SSPFS)-based server, to ensure that none of the user-defined GIDs or UIDs conflict with GIDs and UIDs that the SSPFS requires during an upgrade.

ATTENTION

It is necessary to perform this procedure prior to upgrading the SSPFS, as the SSPFS upgrade expects certain GIDs and UIDs to be free. If those GIDs and UIDs are not free, the SSPFS upgrade will fail.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform this procedure on the Active server.

At your workstation

1   Log in to the server by typing

> `telnet <IP address>`

and pressing the Enter key.

where

IP address
is the IP address or host name of the SSPFS-based server

2   When prompted, enter your user ID and password.

3   Display the GIDs that exist on the system by typing

     # **cut -f1,3 -d':' /etc/group**

     and pressing the Enter key.

4   Compare the groups you obtained in the system response with the following groups:

     root, other, bin, sys, adm, uucp, mail, tty, lp, nuucp, staff, daemon, sysadmin, oinstall, dba, data, maint, succssn, sshd, maint2, trkadm, trkrw, trksprov, trkmtc, trkro, lnadm, lnrw, lnsprov, lnmtc, lnro, mgcadm, mgcrw, mgcsprov, mgcmtc, mgcro, mgadm, mgrw, mgsprov, mgmtc, mgro, emsadm, emsrw, emssprov, emsmtc, emsro, nobody, noaccess, nogroup, and passthru

     Note: The passthru group is only applicable to SN07.

5   Note any groups displayed in the system response that are not in the above list. These are user-defined groups.

6   Note any user-defined groups that have a GID number in the 10, 100, or 1000 range.

     User-defined groups that have a GID number in the 10, 100, or 1000 range need to be moved to a different GID value before starting the SSPFS upgrade.

7   Report any user-defined groups that have a GID number in the 10, 100, or 1000 range to your next level of support, who will assist in moving each group to a different GID, and updating the impacted file systems to reflect the new GID.

8   Display the users that exist on the system by typing

     # **cut -f1,3 -d':' /etc/passwd**

     and pressing the Enter key.

9   Compare the users you obtained in the system response with the following users:

     root, daemon, bin, sys, adm, lp, uucp, nuucp, listen, nobody, noaccess, nobody4, sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, nortel, oracle, Administrator, and nt120 through to nt220.

10   Note any users displayed in the system response that are not in the above list. These are user-defined users.

11   Note any user-defined users that have a UID number below 50000.

    User-defined users that have a UID number below 50000 need to be moved to a different UID value before starting the SSPFS upgrade.

12   Report any user-defined users that have a UID number below 50000 to your next level of support, who will assist in moving each user to a different UID, and updating the impacted file systems to reflect the new UID.

    You have completed this procedure.

Executing a fallback during an SSPFS-based server upgrade

Application

Use this procedure to rollback to the state prior to the upgrade.

ATTENTION
Only use this procedure when directed to do so.

Prerequisites

You must perform this procedure on the newly upgraded node.

Action

Perform the following steps to complete this procedure.

At the node console

1   Rollback to the state prior to the upgrade by typing

    # **/SSPFS_Upgrade.fallback**

    and pressing the Enter key.

    The upgraded server is taken down to the OK prompt.

If your server configuration is a	Do
one-server configuration	step 2
two-server configuration	step 3

2   Restore the oracle data on the server using procedure "Restoring the oracle data on an SSPFS-based server" in the ATM/IP Security and Administration document, NN10402-600

    You have completed this procedure.

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

4   Verify the status of replicated disk volumes by typing

`# udstat`

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 5
not ACTIVE	contact your next level of support

5   Clone the image of the active server onto the other server. If required, refer to procedure

Once the clone is complete, the cluster is restored as it was before the upgrade.

You have completed this procedure.

Confirming the upgrade on an SSPFS-based server

Application

Use this procedure to either accept the upgraded environment permanently, or rollback to the state prior to the upgrade.

ATTENTION
Only use this procedure when directed to do so.

Prerequisites

In a two-server configuration, you must perform this procedure on the newly upgraded node in the cluster, which is now the active node.

Action

Perform the following steps to complete this procedure.

At the sever 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 in to the active node.

2   Use the following table to determine your next step:

If	Do
you choose to accept the upgraded environment	step 3 only
you choose to rollback to the state prior to the upgrade	step 4

3   Accept the upgraded environment by typing

/SSPFS_Upgrade.accept

and pressing the Enter key.

You are now ready to clone the image of this upgraded node onto the other node. Refer to procedure Cloning the image of one node in a cluster to the other node on page 61.

You have completed this procedure.

4   Rollback to the state prior to the upgrade by typing

      # **/SSPFS_Upgrade.fallback**

      and pressing the Enter key.

      The upgraded server is taken down to the OK prompt.

If your server configuration is a	Do
one-server configuration	step 5
two-server configuration	step 6

5   Restore the oracle data on the server using procedure "Restoring the oracle data on an SSPFS-based server" in the ATM/IP Security and Administration document, NN10402-600

      You have completed this procedure.

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

7   Boot the server by typing

      OK **boot**

      and pressing the Enter key.

8   Verify the status of replicated disk volumes by typing

      # **udstat**

      and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 9
not ACTIVE	contact your next level of support

9   Clone the image of the active server onto the other server. <u>Cloning the image of one node in a cluster to the other node on page 61</u>

      Once the clone is complete, the cluster is restored as it was before the upgrade.

      You have completed this procedure.

Cloning the image of one node in a cluster to the other node

Application

Use this procedure to clone the image of the active node in a cluster to the inactive node.

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password

- you need console access to the Inactive node if this is the first time you clone, or if you replaced the Inactive unit or executed a reverse restore (switched unit 0 and 1)

ATTENTION
Ensure no provisioning activities are in progress, or are scheduled to take place during this procedure.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Establish a login session to the Active node using one of the following methods:

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

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

   a Log in to the Active node by typing

   > telnet <server>

   and pressing the Enter key.

   where

   server
   is the cluster IP address, which automatically defaults to the Active node in the cluster

   b When prompted, enter your user ID and password.

   c Change to the root user by typing

      `$ `**`su - root`**

    and pressing the Enter key.

   d When prompted, enter the root password.

    Proceed to step 4.

3 Log in using ssh (secure) as follows:

   a Log in to the Active node by typing

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

    and pressing the Enter key.

    where

    server
      is the cluster IP address, which automatically defaults to
      the Active node 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.

   b When prompted, enter the root password.

4 Verify the status of replicated disk volumes by typing

    `# `**`udstat`**

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 5
not ACTIVE	contact your next level of support

5   Determine the server profile as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

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

 X - exit

select -
```

b Enter the number next to the "View" option in the menu.

Example response

```
View
 1 - sspfs_soft (Display Software
     Installation Level Of SSPFS)
 2 - chk_sspfs (Check SSPFS Processes)
 3 - sw_conf (The software configuration of
     the wrtypyxp)
 4 - cpu_util (Overall CPU utilization)
 5 - cpu_util_proc (CPU utilization by
     process)
 6 - port_util (I/O port utilization)
 7 - disk_util (Filesystem utilization)

 X - exit

select -
```

c Enter the number next to the "sspfs_soft" option in the menu.

Example response

```
=== Executing "sspfs_soft"

SSPFS version: 08.0 Build: 200508421 Server
Profile: cbm850

==="sspfs_soft" completed successfully
```

d Note the Server Profile.

If the Server Profile is	Do
cbm850	step 17
anything else	step 6

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

`servquery -status all`

and pressing the Enter key.

Example response:

```
APP NAME                        STATUS
========                        ======
SNMP_POLLER                     RUNNING
DELEGATE                        RUNNING
PROP_SRV                        RUNNING
WEBSERVER                       RUNNING
DATABASE                        RUNNING
SAM21EM                         RUNNING
SESMService                     RUNNING
CORBA                           RUNNING
ORA_ARCHIVE_ROTATOR             RUNNING
OMPUSH                          RUNNING
BOOTP                           RUNNING
WEBSERVICES                     RUNNING
ORA_AUTO_BACKUP                 RUNNING
APS                             RUNNING
NPM                             RUNNING
```

7 Use the following table to determine your next step.

If	Do
all applications are running	step 10
one or more applications are not running	step 8

8 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

9 Use the following table to determine your next step.

If	Do
one or more applications do not start	contact your next level of support
all applications are running	step 10

10 Use the following table to determine your next step.

If this server is	Do
running the NPM software	step 11
not running the NPM software	step 13

Note: The Network Patch Manager (NPM) software is running on this server if NPM appeared in the response from step 6.

11 Verify the Patching Server Element (PSE) server application is running by typing

pse status

and pressing the Enter key.

If PSE is	Do
running	step 13
not running	step 12

12 Start the PSE server application by typing

pse start

and pressing the Enter key.

If PSE	Do
does not start	contact your next level of support
starts	step 13

13   Use the following table to determine your next step.

If this server is	Do
running the CS 2000 Management Tools software	step 14
not running the CS 2000 Management Tools software	step 17

14   Verify that the SESMservice application is fully functional by typing

ptmctl status

and pressing the Enter key.

Example response:

```
SESM STATUS
--------------------------
COMPONENT                STATUS
---------                ------
Proxy Agent              RUNNING
RMI Registry             RUNNING
Snmpfactory              RUNNING
MI2 Server               RUNNING

  Current number of SESM processes running: 4 (of 4)

  SESM APPLICATION STATUS: All Applications ready
```

15   Use the following table to determine your next step.

If the SESMService is	Do
not fully functional	contact your next level of support
fully functional	step 16

16   Deconfigure NDS replication before cloning the node by typing

#cp /etc/nsswitch.files /etc/nsswitch.conf

#cp /etc/pam.conf.orig /etc/pam.conf

#cd /opt/nortel/applications/security/current_s1is ext/swmgmt/bin

#./configure_s1isext.sh -replica disable

and pressing the Enter key.

17   Use the following table to determine your next step.

If	Do
this is the first time you are cloning the unit, or you replaced the unit or executed a reverse restore (i.e. switched unit 0 and unit 1)	step 18
this is not the first time you are cloning the unit, and you did not replace the unit or execute a reverse restore (i.e. switched unit 0 and unit 1)	step 21

18   Use the following table to determine your next step.

If you	Do
know the Ethernet address of the Inactive unit	step 20
do not know the Ethernet address of the Inactive unit	step 19

At the console connected to the inactive node

19   Determine the Ethernet address of the Inactive node as follows:

    a   Log in to the inactive node through the console (port A) using the root user ID and 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. 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 node 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   Take note of the Ethernet address that is displayed.

At your workstation (login session to the Active node)

20   Start the cloning process by typing

     # **startb <Ethernet address>**

     and press the Enter key.

     where

        Ethernet address
          is the Ethernet address of the Inactive unit

     Proceed to step 22

21   Start the cloning process by typing

     # **startb**

     and press the Enter key.

22   Use the following table to determine your next step.

If the system	Do
prompts you to enter the command "boot net - image"	step 23
does not prompt you to enter the command "boot net - image"	step 27

23   Connect to the console port of the Inactive node.

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

At the console connected to the inactive node

24   Log in 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 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 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
```

At your workstation (login session to the Active node)

27 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
```

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

At your workstation (login session to the Active node)

29 Verify the status of replicated disk volumes by typing

udstat

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 30
not ACTIVE	contact your next level of support

At your workstation

30 Establish a login session to the Inactive node using one of the following methods:

If using	Do
telnet (unsecure)	step 31
ssh (secure)	step 32

31 Log in to the Inactive node using telnet (unsecure) as follows:

a Log in to the Inactive node by typing

> **> telnet <server>**

and pressing the Enter key.

where

server
is the physical IP address of the Inactive node in the cluster

b When prompted, enter your user ID and password.

c Change to the root user by typing

> **$ su - root**

and pressing the Enter key.

d When prompted, enter the root password.

Proceed to step 33.

32 Log in using ssh (secure) as follows:

a Log in to the Inactive node by typing

> **> ssh -l root <server>**

and pressing the Enter key.

where

server
is the physical IP address of the Inactive node 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.

b When prompted, enter the root password.

33   Verify the status of replicated disk volumes by typing

udstat

and pressing the Enter key.

If all file systems are	Do
ACTIVE	step 34
not ACTIVE	contact your next level of support

At your workstation (login session to the Active node)

34   Complete the cloning process by typing

finishb

and pressing the Enter key.

Sessions on both the Active and Inactive nodes

35   Reconfigure NDS replication on both the active and inactive nodes after the cloning process is completed by typing

#cp /etc/nsswitch.saml /etc/nsswitch.conf

#cp /etc/pam.conf.is /etc/pam.conf

and pressing the Enter key.

You have completed 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 73 to determine the optional software packages (filesets) that you can install through this procedure.

Note: This procedure should be performed on a pre-cloned system. If the procedure is not performed on a pre-cloned system, you must 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 CBM0080 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 may install later.

Filesets available for the CBM 850 (Sheet 1 of 3)

Fileset	Description	Type
SDM_BASE.version_20.81.0.0	Load Lineup Information	Base
CBM_SETUP	CBM installation and upgrade tool; 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 3)

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_NTiwb.iaa	Integrated Accounting Application	optional
SDM_NTiaa.iaa	Integrated Accounting Application	optional
SDM_EM.lep	Integrated Accounting Application	optional
SDM_EM.aev	IAA Accounting Event Message Viewing	optional
SDM_EM.aep	IAA Accounting Event Message Processing	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
Note: Base = included with the CBM 850		

Filesets available for the CBM 850 (Sheet 3 of 3)

Fileset	Description	Type
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

> *Note:* 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.

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	1. Perform steps 1 and 2 only, of Procedure for installing DDMS on page 80 2. Go to step 5
you are installing the OMDD application	1. Perform step 1 only, of Procedure for installing the OM Data Delivery software package on page 86 2. Go to step 5
you are installing the log delivery service application	1. Perform Procedure for installing the Passport Log Streamer application on page 89 2. Go to step 8

If	Action
you are installing the SBA or AFT applications	1**.** Perform [Procedure to install the SBA and AFT software packages on page 91](#) 2. Go to step [8](#)
you are installing GR740PT application server	1. Perform [Procedure for installing GR740PT application server on page 92](#) 2. Go to step [8](#)
you are installing the FTP Proxy application	1. Create the logical volume, /cbmdata/00/esa, with size 25 Mbyte, using the logical volume creation procedure in the *CBM 850 Security and Administration* NTP, NN10358-611. 2. Go to step [4](#).
you are installing the Backup Restore Manager software	1. Perform [Installing the Backup Restore Manager software on page 104](#) 2. Go to step [8](#)
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 94](#). 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.

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 and follow the required action for the application you are installing.
you are not installing any other applications that require you to create logical volumes	Go to step 6

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

`init 6`

> *Note:* Be sure that you have created any required logical volumes for all of the applications you are installing before performing this step.

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

If	Action
you are installing the DDMS application	1. Perform the remaining steps of Procedure for installing DDMS on page 80, starting with step 3 2. Go to step 8
you are installing the OMDD application	1. Perform the remaining steps of Procedure for installing the OM Data Delivery software package on page 86, starting with step 2 2. Go to step 8
you are installing the FTP Proxy application	Go to step 8.
you are installing any other optional software application	Go to step 8

8   Ensure that your CBMs are patch-current by performing the procedure, Making the CBM 850 patch-current after optional software package installation on page 100.

9   Clone the image of the active node to the inactive node by performing the procedure, .

10   You have completed this procedure.

Procedure for installing DDMS

This procedure enables you to install the DDMS application.

Note 1: For a successful installation of DDMS, the Log Delivery Service application must be in service.

Note 2: 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.

Installing DDMS on a CBM 850

At your workstation

1   Enter each of the following commands:

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

permit sdm02 <sdm02_pswd> 4 10000 english all

permit sdm03 <sdm03_pswd> 4 10000 english all

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

where

     <sdm0n_pswd>
        is the CM password for user SDM0n

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, DDMS software has the ability to manage automatic password changing on the CBM and the CM, before the passwords expire. You do not, therefore, have to manually change any of the SDM01-SDM04 passwords 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 on or off Enhanced Password Control, these changes should be synchronized with DDMS software by performing a bsy or rts of DDMS. If, however, you change any of the SDM01-SDM04 passwords manually, you need to apply the same password changes in the DDMS configuration file.

2   Create the required logical volumes for the DDMS application.

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

```
chmod 755 /cbmdata/00/osscomms

chown maint:maint /cbmdata/00/osscomms

makelv /cbmdata/00/ossaps 112

chmod 755 /cbmdata/00/ossaps

chown maint:maint /cbmdata/00/ossaps

makelv /cbmdata/00/ossapslog 112

chmod 755 /cbmdata/00/ossapslog

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

3   Apply the two software application packages, OSS and Application Svcs and OSS Comms Svcs by performing the procedure <u>Applying software packages on a CBM 850 using the CBMMTC interface on page 94</u>. Specify /cdrom/cdrom/applications/cbm/packages as the source directory when you perform that procedure.

4   You should be prompted automatically to configure the OSS Comms Svcs package; the OSS and Application Svcs package does not require configuration. Use the following table to determine your next step.

If	Do
you are prompted automatically to configure the OSS Comms Svcs package	step <u>8</u>
you are not prompted automatically to configure the OSS Comms Svcs package	step <u>5</u>

5   Access the config level of the maintenance interface:

```
cbmmtc config
```

6   In the list of applications, locate the OSS Comms Svcs application and take note of its 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 will be highlighted on the cbmmtc config screen.

7   Invoke the configuration of the OSS Comms Svcs application.

        config

8   When prompted to enter the logroute tool, as shown in table
             <u>DDMS logroute tool banner</u>, press Enter. The Logroute Main
             Menu appears, as shown in figure <u>Logroute tool main menu</u>.

DDMS logroute tool banner

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

Logroute tool main menu

```
                        Logroute Main Menu


                1 –      Device List
                2 –      Global Parameters
                3 –      CM Configuration File
                4 –      GDD Configuration
                5 –      Help
                6 –      Quit Logroute






    Enter Option   ==>
```

9   Set up a path and file to store DDMS customer logs as follows:

a Select the Device List menu:

1

The Device List Menu screen is displayed.

b Select 1 to display the Device List screen.

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

c Press the Enter key.

d Begin to add a new device:

2

e Select a file device:

3

Response:

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

f Complete the path name by typing

ossaps/ossapslog

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

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

h When prompted, set the ECORE option to ON.

i Select addrep:

a

j Enter the log identifier by typing, in uppercase

DDMS

k When prompted to enter more log routing details, enter

N

l Save the new device:

y

Response:

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

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

m Return to the Device List Menu screen:

   5

n Return to the main menu screen:

   6

o Exit logroute:

   6

p The CM User Setup screen is displayed as shown in the following example.

   The required CM users, SDM01-SDM04, for DDMS will be added to the DDMS configuration file. The passwords for these users should be the same as those entered in step 1

   Note: The userIDs and passwords are not case sensitive and will be the same. 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:
```

10 Follow sub-steps a through c for each of the required userIDs:

a Add a new user:

   1

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

c When prompted enter the user password.

   Note: Your first entry of a user name and password will cause an error message: "Error: file not valid." Ignore this message and continue to add the other user names and passwords.

d 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:
```

11   Follow sub-steps a through c to configure the DDMS clients.

Note: The DDMS clients are the CS 2000 Management Tools servers with the SESM load. If the CS 2000 Management Tools server is a cluster configuration, add the IP address of both units (active and inactive unit).

a   Add a new client:

1

b   When prompted, enter the IP address for each of the CS 2000 Management Tools servers. Press the Enter key after each entry and type "done" once you have entered all the IP addresses.

c   Exit the DDMS clients configuration screen:

0

12   You have completed this procedure. Return to step 8 of procedure Installing optional software on a CBM 850.

Procedure for installing the OM Data Delivery software package

The OM Data Delivery application collects and stores operational measurement (OM) data from the switch. The application stores the data in comma separated value (CSV) files that are sent to the client operations support system (OSS). This procedure contains the steps for installing and configuring the OM Data Delivery application on the CBM 850 cluster.

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 needs to increase the buffer size within the OM Access Service to 2.5 MB. This is done to accommodate the amount of data being transferred by the front end for a transfer period of every 30 minutes.

> *Note:* 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.

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, <u>Applying software packages on a CBM 850 using the CBMMTC interface on page 94</u> 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**
	Go to step 6
do not want to activate the Tuple Number option	Type **n**
	Go to step 6

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:

a   When prompted, enter the IP address of the first MDM you want to connect to.

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

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

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

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

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

8   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**
	Go to step 9
do not want to use custom retry settings but want, instead, to use default settings	Type **n**
	Go to step 10

9   Respond to the prompts with your custom retry settings:

> *Note:* The retry setting values shown here are examples. Retry setting values are in seconds (values higher than 300 seconds are not recommended as they may adversely affect recovery time).

```
Enter the first connection retry interval: 2
```

```
Enter the number of retry attempts at that
interval: 10
```

```
Enter the second connection retry interval: 10
```

```
Enter the number of retry attempts at that
interval: 40
```

```
Enter the third connection retry interval: 60
```

10   When prompted, confirm the configuration data you have entered by typing **y**

> *Note:* If you type **n**, you will be prompted to re-enter all of the configuration data.

11   The system indicates that the configuration is complete.

Press the Enter key.

12   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.

13   Exit the maintenance interface:

```
quit all
```

14   You have completed this procedure. Return to step 8 of 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 should be removed from all of the firewalls that exist between the MDM and the CBM 850.

Note: 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.

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

At your workstation

1   Perform the procedure 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 as follows:

    a   When prompted, enter the IP address for the first MDM node.

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

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

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

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

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

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

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

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

```
appl
```

    a 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

    b 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, see the procedure "Displaying or storing log records using log receiver" in the Fault Management document.

    c Exit the CBM maintenance interface:

```
quit all
```

4 You have completed this procedure. Return to step <u>8</u> of procedure <u>Installing optional software on a CBM 850</u>.

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.

Note: 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.

Installing the SBA and AFT software packages on a CBM 850

At your workstation

1   Using the procedure , 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. For the procedure used to create logical volumes, see "Adding a logical volume through the command line" in the NTP NN10363-811, *CBM 850 Accounting*.

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.

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 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
NM EADAS lc 2	NM_EADAS_LOG_CHAN2	9554	238
NM EADAS lc 3	NM_EADAS_LOG_CHAN3	9555	239

Note: 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.

Installing GR740PT application server

At your workstation

1   Using the procedure Applying software packages on a CBM 850 using the CBMMTC interface on page 94, apply the GR740PT software package located in the /cdrom/cdrom/applications/cbm/packages directory.

   Note: During configuration of GR740PT, use the following table to determine your response to the prompt, "Enter mode of security".

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

2   You have completed this procedure. Return to step 8 of 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.

Note: 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.

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: 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 cbm maintenance interface apply level screen display showing any available packages

If	Do
CD-ROM is being used to deliver the CBM software	step 2, specifying: /cdrom/cdrom/applications/cbm/packages as the <source_directory_name>
you want to exit from the cbm maintenance interface	step 6

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

3   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

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 cbm maintenance interface apply level screen display showing packages available in the source directory (CD-ROM)

```
 xterm                                                            _ □ ×
    CBM          MATE    NET     APPL    SYS     HW     CLLI: SN100
     •            —       •       •       •       •     Host: SN100_CBM
                                                              Active
Apply
 0 Quit         Source: the directory /cdrom/cdrom/applications/cbm/packages.
 2              Filter: sdm Interactive Mode: OFF
 3                 # Package Description          Version        Status
 4 Source          1 Platform Utilities          20.82.8.0       APPLIED
 5 Reload          2 Table Access Service         20.82.8.0       APPLIED
 6                 3 Bootpd and tftpd             20.82.8.0       NOT APPLIED
 7 Select          4 SSH Core File Transfer       20.82.8.0       NOT APPLIED
 8 Apply           5 SDM Billing Application      20.82.8.0       NOT APPLIED
 9 Upgrade         6 Reach Through SPM            20.82.8.0       NOT APPLIED
10                 7 Passport Log Streamer        20.82.8.0       NOT APPLIED
11                 8 OSS Comms Svcs               20.82.8.0       NOT APPLIED
12 Up              9 OSS and Application Svcs     20.82.8.0       NOT APPLIED
13 Down           10 OM Access Service            20.82.8.0       APPLIED
14 Search         11 OM Delivery                  20.82.8.0       NOT APPLIED
15 Filter                     Packages on the source: 1 to 11 of 26
16 View
17 Help
18 Refresh
   root
Time  15:50  >
```

4 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 above, enter

> **`select  6  11`**

If the command is successful, the packages you selected will be highlighted on the cbmmtc apply screen, as shown below in the sample cbm maintenance screen.

Example of cbm maintenance interface apply level screen display showing packages you have selected for application

```
╳ xterm                                                        _ □ ✕
     CBM         MATE    NET     APPL    SYS     HW     CLLI: SN100
      •           —       •       •       •       •     Host: SN100_CBM
                                                              Active
 Apply
  0 Quit      Source: the directory /cdrom/cdrom/applications/cbm/packages.
  2           Filter: sdm Interactive Mode: OFF                    # Selected: 2
  3             # Package Description              Version      Status
  4 Source      1 Platform Utilities              20.82.8.0    APPLIED
  5 Reload      2 Table Access Service            20.82.8.0    APPLIED
  6             3 Bootpd and tftpd                20.82.8.0    NOT APPLIED
  7 Select      4 SSH Core File Transfer          20.82.8.0    NOT APPLIED
  8 Apply       5 SDM Billing Application         20.82.8.0    NOT APPLIED
  9 Upgrade     6 Reach Through SPM               20.82.8.0    NOT APPLIED
 10             7 Passport Log Streamer           20.82.8.0    NOT APPLIED
 11             8 OSS Comms Svcs                  20.82.8.0    NOT APPLIED
 12 Up          9 OSS and Application Svcs        20.82.8.0    NOT APPLIED
 13 Down       10 OM Access Service               20.82.8.0    APPLIED
 14 Search     11 OM Delivery                     20.82.8.0    NOT APPLIED
 15 Filter              Packages on the source: 1 to 11 of 26
 16 View
 17 Help
 18 Refresh
   root
 Time  15:51  >█
```

> *Note:* If you want 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.

5   Apply the selected packages:

apply

> *Note:* If a pre-requisite package for the package(s) you have selected has not already been applied on the system, SWIM will select (if you have not already selected the package in a previous step) and apply the pre-requisite package.

The system will prompt you once to ensure that you want to continue with the package application.

Example of cbm maintenance interface apply level screen display showing packages selected for application after the apply command has been issued

```
xterm                                                    _ □ ✕
     CBM        MATE    NET    APPL    SYS    HW    CLLI: SN100
      •          —       •      •       •      •    Host: SN100_CBM
Apply      I                                              Active
 0 Quit
 2
 3
 4 Source
 5 Reload
 6
 7 Select
 8 Apply
 9 Upgrade
10
11
12 Up        The following new packages have been selected for install.
13 Down
14 Search       NTrttl120 'Reach Through SPH' 20.82.8.0
15 Filter       NTowd20 'OM Delivery' 20.82.8.0
16 View
17 Help      Do you wish to proceed?
18 Refresh   Please confirm ("YES", "Y", "NO", or "N")
    root
Time  15:52  >█
```

If	Do
you want to continue the package application	step a
you do not want to continue the package application	step b

   a Type yes in response to the prompt.

       The status of each package application displays on the cbmmtc apply screen.

Example of cbm maintenance interface apply level screen display showing the status of the packages after they have been applied


```
xterm                                                                    _ □ ✕
        CBM        MATE    NET     APPL    SYS     HW      CLLI: SN100
        ISTb        -       .      ISTb     .       .      Host: SN100_CBM
                                                                 Active
Apply
 0 Quit          Source: the directory /cdrom/cdrom/applications/cbm/packages.
 2               Filter: sdm Interactive Mode: OFF
 3                # Package Description               Version         Status
 4 Source         1 Platform Utilities               20.82.8.0       APPLIED
 5 Reload          2 Table Access Service             20.82.8.0       APPLIED
 6                3 Bootpd and tftpd                 20.82.8.0       NOT APPLIED
 7 Select          4 SSH Core File Transfer          20.82.8.0       NOT APPLIED
 8 Apply           5 SDM Billing Application          20.82.8.0       NOT APPLIED
 9 Upgrade         6 Reach Through SPM               20.82.8.0       APPLIED
10                7 Passport Log Streamer            20.82.8.0       NOT APPLIED
11                8 OSS Comms Svcs                   20.82.8.0       NOT APPLIED
12 Up              9 OSS and Application Svcs        20.82.8.0       NOT APPLIED
13 Down           10 OM Access Service               20.82.8.0       APPLIED
14 Search         11 OM Delivery                     20.82.8.0       APPLIED
15 Filter                       Packages on the source: 1 to 11 of 26
16 View
17 Help
18 Refresh
   root
Time  15:55  >
```

When the application is completed:

- The status of the packages shown on the cbmmtc apply screen (under the Status column) will indicate "Applied".

   Note: It is important that packages not be left on the system with a "Partial" status. In this event, or if the package application failed, contact your next level of support for assistance.

- The packages will appear in the list that displays when you enter the cbmmtc packages level.

   If you want to view details about the CBM package application, perform the procedure Viewing software transaction history and logs on the CBM 850 on page 112

   Go to step 6.

   b Type no in response to the prompt.

6 Exit from the cbm maintenance interface:

   quit all

7 You have completed this procedure. Return to step 8 of procedure Installing optional software on a CBM 850.

Procedure for making the CBM 850 patch-current

This procedure enables you to make the CBM 850 cluster patch-current after the installation of optional software packages.

Note: 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.

Making the CBM 850 patch-current after optional software package installation

At your workstation

1   Apply any patches for the optional software packages that you have installed:

   ```
   patchctrl -d
   /cdrom/cdrom/applications/cbm/patches
   ```

   Note: During installation, you may receive a prompt from the system to continue or abort the procedure because the inactive node is not available. <u>You should enter Continue</u>.

2   If you are informed by the system that there are interactive patches that could not be applied, enter the following command to apply each of these interactive patches:

   ```
   patchctrl -f /swd/fixes/interactive/<patch_id>
   ```

   where

   <patch_id>
       is the ID of the interactive patch that you are applying

3   If any special instructions display for manual patches that could not be applied, enter the following command to apply each of these manual patches:

   ```
   patchctrl -f /swd/fixes/manual/<patch_id>
   ```

   where

   <patch_id>
       is the ID of the manual patch that you are applying

4   You have completed this procedure. Return to step <u>9</u> of procedure <u>Installing optional software on a CBM 850</u>.

   Note: After you have completed this procedure, contact your patching prime to ensure you have now applied all required patches.

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.

Note: 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.

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.

If the system	Do
prompts you for the Ethernet address	step 2
indicates it is using Ethernet address <EthernetAddress>	step 7

At the console connected to the inactive node

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

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

init 0

4   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.
```

5   Take note of the Ethernet address that is displayed.

At your workstation (session connected to Active node)

6   Enter the Ethernet address of the inactive node you noted in step 5.

7   Use the following table to determine your next step.

If the system	Do
prompts you to enter the command "boot net - image"	step 8
does not prompt you to enter the command "boot net - image"	step 9

At the console connected to the inactive node

8   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 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
```

At your workstation (session connected to the Active node)

9   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
```

10   You have completed this procedure. Return to step 10 of 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.

> *Note:* 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.

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 into 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 3.

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 94. Specify /cdrom/cdrom/applications/cbm/packages as the source directory when you perform that procedure.

3   **When the installation is complete, exit from CBMMTC. At the command line prompt, change directory to the directory containing appropriate configuration script:**

`cd /opt/nortel/bkresmgr/cbm/scripts`

4   **Run the configuration script:**

`./bkmgr_config.sh`

5   As the script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core in step 1

6   As the script continues to run, you are then prompted for the user you entered (in step 5). The script restricts the password to a maximum of 16 characters. This password is the one that was set up in step 1

7   As the script continues to run, you are then 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. You should ensure that this device has enough space to store the backup.

8   As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.

9   You have completed this procedure. Return to step 8 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

```
X xterm                                                        _ □ X
     CBM          MATE    NET    APPL    SYS    HW    CLLI: SN100
      •            —       •      •       •      •    Host: SN100_CBM
                                                            Active
Packages
 0 Quit        Filter: sdm Interactive Mode: OFF
 2 Apply          # Package Description              Version      Status
 3                1 Platform Utilities               20.82.8.0    APPLIED
 4                2 Table Access Service             20.82.8.0    APPLIED
 5                3 Reach Through SPM                20.82.8.0    APPLIED
 6                4 OM Access Service                20.82.8.0    APPLIED
 7 Select         5 OM Delivery                      20.82.8.0    APPLIED
 8 Remove         6 CBMMTCE Interface                20.82.8.0    APPLIED
 9                7 Log Delivery Service             20.82.8.0    APPLIED
10                8 Generic Data Delivery            20.82.8.0    APPLIED
11                9 GNU Debugger                     5.3.0.0      APPLIED
12 Up            10 SDM/CBM Debug Helper tools       20.82.8.0    APPLIED
13 Down          11 Platform Maintenance Common      20.82.8.0    APPLIED
14 Search        12 Platform Base                    20.81.10.0   APPLIED
15 Filter                             Packages: 1 to 12 of 12
16 View
17 Help
18 Refresh
  root
Time  13:41  > 
```

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

```
┌───────────────────────────────────────────────────────────────────┐
│ ✕ xterm                                                   _ □ ✕     │
├───────────────────────────────────────────────────────────────────┤
│   CBM          MATE    NET     APPL    SYS     HW    CLLI: SN100     │
│    •            —       •       •       •       •    Host: SN100_CBM │
│                                                            Active    │
│ Packages                                                            │
│  0 Quit      Filter: sdm Interactive Mode: OFF        # Selected: 2 │
│  2 Apply        # Package Description            Version    Status   │
│  3              1 Platform Utilities             20.82.8.0  APPLIED  │
│  4              2 Table Access Service           20.82.8.0  APPLIED  │
│  5              3 Reach Through SPM              20.82.8.0  APPLIED  │
│  6              4 OM Access Service              20.82.8.0  APPLIED  │
│  7 Select       5 OM Delivery                   20.82.8.0  APPLIED  │
│  8 Remove       6 CBMMTCE Interface              20.82.8.0  APPLIED  │
│  9              7 Log Delivery Service           20.82.8.0  APPLIED  │
│ 10              8 Generic Data Delivery          20.82.8.0  APPLIED  │
│ 11              9 GNU Debugger                   5.3.0.0    APPLIED  │
│ 12 Up          10 SDM/CBM Debug Helper tools     20.82.8.0  APPLIED  │
│ 13 Down        11 Platform Maintenance Common    20.82.8.0  APPLIED  │
│ 14 Search      12 Platform Base                  20.81.10.0 APPLIED  │
│ 15 Filter                          Packages: 1 to 12 of 12          │
│ 16 View                                                             │
│ 17 Help                                                             │
│ 18 Refresh                                                          │
│   root                                                              │
│ Time  13:42  >█                                                     │
└───────────────────────────────────────────────────────────────────┘
```

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 <u>Viewing software transaction history and logs on the CBM 850 on page 112</u>, otherwise continue with step <u>11</u>.

10   Type **no** in response to the prompt.

11   To remove other packages from the system, return to step <u>4</u> 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.

Note: 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.

Procedure

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, such as "active node", is provided. If the operations were performed on the inactive node, however, the identifier, "inactive node" appears in the information displayed. For more details about a specific log displayed in the history command output, enter:

```
ViewLog  <#>
```

where

```
<#>
```
        is the number of the log in the log file.

7   Exit from the cbmmtc user interface:

```
quit all
```

8   You have completed this procedure.

Delivering patches to a CBM 850

Purpose

This procedure describes how patches can be delivered to a CBM 850.

The recommended method of software delivery is electronic software delivery (ESD), through secure FTP file transfer. Patches that are to be applied should be transferred to the /swd/fixes/incoming directory on the active node of the CBM 850 cluster. Patches in the /swd/fixes/incoming directory that are to be manually applied will be moved automatically to the /swd/fixes/manual directory during scheduled patch applies.

> *Note 1:* The CBM 850 can be set up to receive automatic delivery of patches through RPS if the site is set up in Galaxy. The patches will be downloaded to the /swd/fixes/incoming directory.

> *Note 2:* 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.

Procedure

Delivering patches to 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"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

   > *Note:* If an "emsadm" user has not been configured, perform the procedure <u>Creating a user allowed to perform patching on a CBM on page 148</u>

2   Enter the password for the "emsadm" user.

3   Determine the next step to perform.

If	Do
you want to have the patches applied automatically	step 4
you want to apply the patches manually	step 6

4   At the prompt, electronically transfer (ftp) the patches to the /swd/fixes/incoming directory on the active node of the CBM 850 cluster.

Note: The /swd/fixes/incoming directory is duplicated on both CBM 850 nodes in the cluster. Therefore, you only need to ftp the patches to the directory located on the active node of the cluster.

5   Determine the next step to perform.

If	Do
you want to set up patch filters before applying patches	Setting up patch filters for a CBM 850 cluster on page 116 then go to step 8
you want to configure the automatic patching schedule without setting any patch filters	Setting up automatic patching on a CBM 850 cluster and removing previously-configured schedules on page 122 then go to step 8

6   At the prompt, electronically transfer (through secure FTP file transfer, using sftp commands) the patches to the CBM 850. Place the patches in a replicated directory other than in those under the /swd/fixes directory, that can be used for patching. For additional information about secure FTP transfer, see OpenSSH overview on page 150

7   Perform the procedure Manually applying patches to a CBM 850 on page 125.

8   You have completed this procedure.

Setting up patch filters for a CBM 850 cluster

Purpose

This procedure enables you to set up patch filters for a CBM 850 cluster. A patch filter enables you to define more conservative handling for patches by overriding the normal patch handling for a patch type. Thus, a patch may be treated as an "inactive apply" patch or a "manual apply" patch even though the patch was packaged as an "active apply" patch. In addition, a patch may be treated as a "manual apply" patch even though the patch was packaged as an "inactive apply" patch.

> *Note:* 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.

Procedure

Setting up patch filters for a CBM 850 cluster

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

   > *Note:* If an "emsadm" user has not been configured, perform the procedure <u>Creating a user allowed to perform patching on a CBM on page 148</u>

2 Enter the password for the "emsadm" user.

3 From the command line prompt, invoke the patchfilter tool:

patchfilter

4   The system prompts you for inactive filters. In response to the system display, determine the next step you want to perform.

If	Do
you want to add an inactive filter	step 5
you want to remove an existing inactive filter	step 8
you want to save the current inactive filter and proceed to the steps for setting manual filters	step 11
you want to abort the program	step 18

5   In response to the prompt, type:

add

6   In response to the prompt, type:

<filter name>

where

<filter name>
is either the entry "*reboot" or a unique text string that identifies the patch or patches that the filtering will apply to:

- *reboot is the name of a special filter that can be set to identify any patch that requires a reboot of the system when the patch is applied.

    Note: The *reboot filter set as an inactive filter causes all active and inactive patches requiring reboots to become inactive-apply patches.

- an alphanumeric text string can be created that represents the desired behavior of the filter.

---

10 Use the following table to determine your next step.

If	Do
you want to remove another inactive filter	step 8
you want to add an inactive filter	step 5
you want to save your changes to the current inactive filter and proceed to the steps for setting manual filters	step 11
you want to abort the program without first saving any changes	step 18

11 To save your inactive filter changes, type:

   save

12 The system prompts you for manual filters. In response to the system display, determine the next step you want to perform.

If	Do
you want to add a manual filter	step 13
you want to remove a manual filter	step 15
you want to save your changes and exit from the patchfilter program	step 17
you want to abort the program	step 18

13 In response to the prompt, type:

   add

14 In response to the prompt, type:

   <filter name>

   Note: For an explanation of <filter name>, see step 6. When you configure the *reboot filter (explained in step 6) for a

manual filter, all patches (either active apply or manual apply) requiring a system reboot will be made manual-apply patches.

If	Do
you want to add another manual filter	step 13
you want to remove a manual filter	step 15
you want to save your changes and exit from the patchfilter program	step 17
you want to abort the program without first saving any changes	step 18

15   In response to the prompt, type:

`remove`

16   In response to the prompt, type:

`<filter number>`

where

> **<filter number>**
> is the number located to the left of the filter in the patchfilter command display.

If	Do
you want to remove another manual filter	step 15
you want to add a manual filter	step 13
you want to save your changes and exit from the patchfilter program	step 17
you want to abort the program without first saving any changes	step 18

17   To save your changes, type:

`save`

Go to step 19.

18   In response to the prompt, type:

`abort`

Confirm that you want to abort by typing Yes.

19   You have completed this procedure. Proceed to

Setting up automatic patching on a CBM 850 cluster and removing previously-configured schedules

This procedure enables you to set up automatic patching schedules for a CBM 850 cluster.

Both "active apply" and "inactive apply" patch types can be scheduled for automatic application. "Active apply" patches are applied first on the active node of a CBM 850 cluster and then on the inactive node. "Inactive apply" patches are applied first on the inactive node of a CBM 850 cluster and then on the active node.

Only one active schedule and one inactive schedule can be set and can be operational at any given time. Whenever a new active or inactive schedule is configured, the existing active or inactive schedule is replaced by the new one.

The "patchconfig" tool is used to set the automatic patching schedules. The tool prompts you first to set up the schedule for the active node. The tool then prompts you to set up the schedule for the inactive node. Finally, the tool prompts you whether you want the patches to be deleted automatically from the patching source directory after the patches have been applied successfully.

Note 1: In order for patches to be applied using the schedules you set with the procedure, the patches must be located in the /swd/fixes/incoming directory.

Note 2: 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.

Setting up automatic patching on a CBM 850 cluster and removing previously-configured schedules

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

Note: If an "emsadm" user has not been configured, perform the procedure Creating a user allowed to perform patching on a CBM on page 148

2   Enter the password for the "emsadm" user.

3   From the command line prompt, invoke the patch configuration tool:

patchconfig

In response, the system starts displaying screens that provide you with all of the information you need to configure an automatic patching schedule first for the active node and then for the inactive node.

   Note 1: You are always prompted to set up the Active patching schedule first. Once the active patching schedule has been entered, you are then automatically prompted to enter the Inactive patching schedule. After the Inactive patching schedule prompts, you are then prompted, through the auto-delete value, whether you want the patches to be deleted automatically from the patching source directory after the patches have been applied successfully.

   Note 2: If you do not want to set up an Active patching schedule, you should enter "none" when you are prompted for that schedule. You are then prompted automatically for the Inactive patching schedule. If you do not want to set up an Inactive patching schedule, you should enter "none" when you are prompted for that schedule.

   Note 3: If you want to remove an existing Active patching schedule, or if you want to remove an existing Inactive patching schedule, you should enter "none" when you are prompted for that schedule. This will remove the currently-defined schedule.

   Note 4: If you enter "abort" in response to any of the patchconfig program prompts, all information that you have entered during that configuration session will be deleted from the system and will not be saved. Any existing Active and Inactive schedules, and any existing auto-delete value, will remain as they were before you started the patchconfig session.

4   Determine whether any patches to be applied are located in the /swd/fixes/manual directory. If patches do exist in this directory, apply the patches with the procedure, Manually applying

<u>patches to a CBM 850</u>. This step should be performed after each schedule, that is, the schedule for the active unit and the schedule for the inactive unit, is executed.

5   Ensure that all patches have been applied successfully to both units in the cluster, by performing the procedure <u>Using the Queryloads tool to display patches and packages applied on the CBM 850</u>

6   You have completed this procedure.

Manually applying patches to a CBM 850

Purpose

This procedure enables you to manually apply patches to a CBM 850 cluster. You apply the patches using the "patchctrl" tool. The patchctrl tool applies a single patch or multiple patches located in the source directory that you specify. The patchctrl tool automatically ensures that patches are applied in the correct order when the patches require additional patches from the source directory or patches that are already applied on the node.

> *Note:* Although the patchctrl tool can be invoked from any directory, it should not be invoked from within a replicated file system.

With this procedure, you may apply three types of patches: "active apply" patches, "inactive apply" patches, or "manual apply" patches. "Active apply" patches are applied on the active node of a CBM 850 cluster first and then on the inactive node of the cluster. "Inactive apply" patches are normally applied on the inactive node of a CBM 850 cluster first and then on the active node of the cluster. "Manual apply" patches can be applied on either node of a CBM 850 cluster first and are then applied on the other node of the cluster.

> *Note:* "Interactive" patches are not applied on the system but are, instead, moved by the patchctrl tool to a special directory for possible manual application at a later time. When the patches have been moved to this directory, the release notes that accompany the patches can, however, be displayed using the patchctrl tool.

If the patch requires a reboot of a CBM node, the tool will detect this and will prompt you to authorize the reboot before it continues with the application of the patches. The system also prompts you to authorize the SwAct of the nodes if the patches are applied on the inactive node first.

> *Note 1:* If any patches have been applied on only one node of the cluster and a SwAct to the other node in the cluster is aborted by the customer, it is the responsibility of the customer to remove any patches that have been applied on the one node in the cluster.

> *Note 2:* 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.

Procedure

Manually applying patches to 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 "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

Note 1: If an "emsadm" user has not been configured, perform the procedure Using the Queryloads tool to display patches and packages applied on the CBM 850 on page 133

Note 2: Ensure that you have logged into the active node of the cluster, using the IP address of the <u>active</u> node, and not the cluster IP address. Connection through the cluster IP address is lost if a reboot and SwAct are required during the patching transaction.

2   Enter the password for the "emsadm" user.

3   Back up the CBM 850 filesystems by performing the procedure, Performing a backup of file systems on an SSPFS-based server on page 50

4   Use the following table to determine your next step.

If	Do

you want to apply a single patch	At the prompt, apply the patch:
	
	patchctrl -f <full_path>/<patch_file>
	
	where
	
	<full_path>
	is the full path specifying the directory containing the patch file to be applied
	
	<patch_file>
	is the patch file within the <full_path> specified that you want to apply on the system
	
	Example:
	The patch to be applied is NTL075810-01.patch and is located in the /home/patches directory. The command to apply this patch would be as follows:
	
	`patchctrl -f`
	`/home/patches/NTL075810-01.patch`
	
	Note: If patchctrl is invoked from within the directory containing the patch, you do not need to enter the full pathname of the file. Instead, you may enter the file name.

you want to apply a directory with one or more patches within it	At the prompt, apply the patch: **patchctrl -d <full_path_to_patch_directory>** *where* **<full_path_to_patch_directory>** is the full path specifying the directory containing the patch(es) file to be applied **Example:** The patch to be applied is NTL075810-01.patch and is located in the /home/patches directory. The command to apply this patch would be as follows: `patchctrl -d /home/patches` **Note:** If patchctrl is invoked from within the directory containing the patch directory, you do not need to enter the full pathname of the directory. Instead, you may enter either the directory name, or "." (period).

Note 1: Ensure that you do not enter the patchctrl command from within a replicated file system.

Note 2: If "inactive-apply" patches are found, the system prompts you to indicate the node on which to apply the patch, or patches, first. You should always enter "Inactive". You should contact your next level of support if you want to apply the patch, or patches, on the Active node first.

Note 3: If any of the patches you are applying require a system reboot, the system will notify and prompt you to authorize the reboot before beginning the patch application. If multiple patches are being applied, the system will reboot the node only one time, after all of the patches have been applied on that node. If you do not authorize the reboot, the patching transaction is stopped, without applying any patches to either node of the system, and you are returned to the command line.

Note 4: When any of the patches you are applying require a system reboot (which only occurs when they are being applied on the inactive node first), after the reboot you will be prompted to authorize a SwAct (software activation) to the other node of the cluster. The patch, or patches, are then applied on the node made inactive by the SwAct (originally active node of the cluster). Finally, the system prompts you to authorize a reboot of this newly-inactive node. You must enter "Yes" and authorize the reboot; if you do not authorize the reboot, the system will be left in an unsupported state.

Note 5: You may receive a prompt from the patchctrl tool warning you that the patches you are about to apply require a reboot on the active node, which will result in a swact, a loss of connection, and the software on the nodes being out of sync. The prompt recommends that you apply the patches on the inactive node first by including the "i" option in the patchctrl command.

In this event, it is recommended that you abort the current patching operation by entering Abort, and then enter the following command, which includes the "i" option, to perform the patching operation:

patchctrl -i <-f or -d> <full_path>/<patch_file>

where:

  -i

is the "i" option, indicating that the patchctrl command is to be performed on the inactive node.

If you wish, instead, to continue the patching operation without first aborting and entering the patch command with the "i" option, you should contact your next level of support.

5   Using the procedure, <u>Using the Queryloads tool to display patches and packages applied on the CBM 850 on page 133</u> verify that the patches were applied.

6   Back up the CBM 850 filesystems by performing the procedure, <u>Performing a backup of file systems on an SSPFS-based server on page 50</u>

7   You have completed this procedure.

Purpose

This procedure enables you to remove a patch that you have applied to a CBM 850 cluster. The procedure enables you to choose to remove the patch either from both nodes of the cluster or only from the inactive node of the cluster.

Note: 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.

Procedure

Removing a patch 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 "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

Note: If an "emsadm" user has not been configured, perform the procedure Creating a user allowed to perform patching on a CBM on page 148

2   Enter the password for the "emsadm" user.

3   Using the Queryloads tool, identify the patch to be removed. For the procedure used to do this, see Using the Queryloads tool to display patches and packages applied on the CBM 850 on page 133.

4   Use the following table to determine your next step.

If	Do
you want to remove the patch from both nodes of the cluster	step 5
you wish to remove the patch only from the inactive node of the cluster	step 8

5   Remove the patch from both nodes of the cluster:

```
patchctrl -r <patch_id>
```

where

> **<patch_id>**
>   is the ID of the patch to be removed from the system.
>
> **Example**
> The patch to be removed is NTMTCE208208-01. The command to remove this patch from both nodes of the cluster would be as follows:
>
> ```
> patchctrl -r NTMTCE208208-01
> ```

6   After the patchctrl command is accepted, you may then be prompted by the system to authorize a reboot. Use the following table to determine your next step.

If	Do
you are prompted by the system to authorize a reboot because the patch requires a reboot	step 7
you are not prompted by the system to authorize a reboot because none of the patches require reboot	Wait for the following activities to occur: 1. The patch is first removed from the active node and is then removed from the inactive node of the cluster. 2. The patchctrl program exits. Go to step 9

7   Respond to the system prompt to perform a reboot.

If you enter	system response
Abort	The system prompts you again, to ensure that you want to abort the patching transaction. If you choose to abort the patching transaction, the patchctrl program exits without removing the patch. Go to step 9
No	The system displays a message indicating that the patch cannot be removed without a reboot, and the patchctrl program exits without removing the patch. Go to step 9
Yes	1. The patch is removed from the inactive node. 2. The inactive node reboots. 3. You are prompted to authorize a SwAct to the other (currently active) node. 4. The patch is removed from the newly inactive (previously active) node. 5. You are prompted by the system to authorize a reboot of this node. You <u>must</u> respond Yes; otherwise, if you do not authorize the reboot, the system will be left in an unsupported state. 6. Go to step 9

8   Remove the patch only from the inactive node of the cluster:

`patchctrl -i -r <patch_id>`

where

> **<patch_id>**
> is the ID of the patch to be removed from the inactive node.

> **Example**
> The patch to be removed is NTMTCE208208-01. The command to remove this patch only from the inactive node would be as follows:

`patchctrl -i -r NTMTCE208208-01`

The patch is removed only from the inactive node of the cluster

9   You have completed 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.

> *Note:* 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.

Procedure

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

   > *Note:* If an "emsadm" user has not been configured, perform the procedure Creating a user allowed to perform patching on a CBM on page 52

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 5
List in XML format all installed packages or only installed packages that you specify	step 6

Query	Do
Store package information in a file that you designate	step 7
List in text format all installed patches (including Sun patches) or only installed patches that you specify	step 8
List in XML format all installed patches (including Sun patches) or only installed patches that you specify	step 9
Store patch information in a file that you designate	step 10
List packages or patches missing from the baseline	step 11
You want to obtain usage help for the Queryloads tool	step 12

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.

Example

```
CBM00070    Core and Billing Manager    7.0.0
```

Go to step 13.

5   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 a
you want to list all packages installed on the inactive node	step b
you want to list all packages installed on the active node	step c
you want to list only packages that you specify, that are installed on both nodes	step d
you want to list only packages that you specify, that are installed on the inactive node	step e
you want to list only packages that you specify, that are installed on the active node	step f

a List all packages installed on both nodes:

```
queryloads -m packages
```

Go to step 13

b List all packages installed on the inactive node:

```
queryloads -m packages -n inactive
```

> *Note:* 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 13

c List all packages installed on the active node:

```
queryloads -m packages -n active
```

Go to step 13

d 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.

The table below 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 SUNWlpmsg	SUN

a.The entry for <unique_package_identifier> is case-sensitive.

Go to step 13.

e List only packages that you specify, that are installed on the inactive node:

```
queryloads -m packages -n inactive | grep
<unique_package_identifier>
```

where

<unique_package_identifier>
is the identifier of the package you want to list.

Note 1: 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.

Note 2: The table in step 5d shows sample unique_package_identifiers.

Go to step 13.

f List only packages that you specify, that are installed on the active node:

```
queryloads -m packages -n active | grep
<unique_package_identifier>
```

where

<unique_package_identifier>
is the identifier of the package you want to list.

Note: The table in step 5d shows sample unique_package_identifiers.

Go to step 13.

6 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 a
you want to list all packages installed on the inactive node	step b
you want to list all packages installed on the active node	step c
you want to list only packages that you specify, that are installed on both nodes	step d
you want to list only packages that you specify, that are installed on the inactive node	step e
you want to list only packages that you specify, that are installed on the active node	step f

a List all packages installed on both nodes:

```
queryloads -m packages -x
```

Go to step 13.

b List all packages installed on the inactive node:

`queryloads -m packages -x -n inactive`

> *Note:* 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 13.

c List all packages installed on the active node:

`queryloads -m packages -x -n active`

Go to step 13.

d 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 table below 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 SUNWlpmsg	SUN

a.The entry for <unique_package_identifier> is case-sensitive.

Go to step 13.

e List only packages that you specify, that are installed on the inactive node:

`queryloads -m packages -x -n inactive | grep <unique_package_identifier>`

where

> **<unique_package_identifier>**
> is the identifier of the package you want to list.

Note 1: 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.

Note 2: The table in step 6d shows sample unique_package_identifiers.

Go to step 13.

f List only packages that you specify, that are installed on the active node:

```
queryloads -m packages -x -n active | grep
<unique_package_identifier>
```

where

> **<unique_package_identifier>**
> is the identifier of the package you want to list.

Note: The table in step 6d shows sample unique_package_identifiers.

Go to step 13.

7 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.

Go to step 13.

8 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
```

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 a
you want to list all patches (including Sun patches) installed on the inactive node	step b
you want to list all patches (including Sun patches) installed on the active node	step c
you want to list only patches that you specify, that are installed on both nodes	step d
you want to list only patches that you specify, that are installed on the inactive node	step e
you want to list only patches that you specify, that are installed on the active node	step f

a List all patches installed on both nodes:

queryloads -m patches

Go to step 13.

b List all patches installed on the inactive node:

queryloads -m patches -n inactive

Note: 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 <u>13</u>.

c List all patches installed on the active node:

`queryloads -m patches -n active`

Go to step <u>13</u>.

d 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 table below 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.

Go to step <u>13</u>.

e List only patches that you specify, that are installed on the inactive node:

`queryloads -m patches -n inactive | grep <unique_patch_identifier>`

where

<unique_patch_identifier>
is the identifier of the patch you want to list. The table in step <u>8d</u> shows sample unique_patch_identifiers.

Note: 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 13.

f List only patches that you specify, that are installed on the active node:

```
queryloads -m patches -n active | grep
<unique_patch_identifier>
```

where

<unique_patch_identifier>
is the identifier of the patch you want to list. The table in step 8d shows sample unique_patch_identifiers.

Go to step 13.

9 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>
```

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 a
you want to list all patches (including Sun patches) installed on the inactive node	step b
you want to list all patches (including Sun patches) installed on the active node	step c

If	Do
you want to list only patches that you specify, that are installed on both nodes	step d
you want to list only patches that you specify, that are installed on the inactive node	step e
you want to list only patches that you specify, that are installed on the active node	step f

a   List all patches installed on both nodes:

queryloads -m patches -x

Go to step 13.

b   List all patches installed on the inactive node:

queryloads -m patches -x -n inactive

> *Note:* 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 13.

c   List all patches installed on the active node

queryloads -m patches -x -n active

Go to step 13.

d   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 table
    below 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.

Go to step 13.

e List only patches that you specify, that are installed on the
    inactive node:

**queryloads -m patches -x -n inactive | grep
<unique_patch_identifier>**

where

    <unique_patch_identifier>
        is the identifier of the patch you want to list. For a list of
        sample unique_patch_identifiers, see step 9d.

    Note: 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 13.

f List only patches that you specify, that are installed on the
    active node:

**queryloads -m patches -x -n active | grep
<unique_patch_identifier>**

where

    <unique_patch_identifier>
        is the identifier of the patch you want to list. For a list of
        sample unique_patch_identifiers, see step 9d.

Go to step 13.

10   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.

Go to step 13.

11   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`

Go to step 13.

12   At the prompt, invoke the queryloads tool:

`queryloads -h`

13 You have completed this procedure.

Purpose

An SDM610 alarm is raised by the Software Inventory Manager (SIM) in response to patching events. Minor SDM610 alarms are raised when either a patch application fails or a reboot fails during patching. A minor SDM610 alarm is also raised when a SwAct to the companion node in a CBM 850 cluster during patching fails. If a failed patch is subsequently successfully applied, a log is raised and the alarm is cleared. Up to five failed patch minor SDM610 alarms can be raised. When a sixth failed patch occurs, a critical SDM610 alarm is raised and the patching tool exits.

It is recommended that you always attempt to clear alarms by re-applying failed patches. If this does not clear an alarm, you should then contact your next level of support for assistance. When necessary, minor alarms can be cleared through the SIM "simAlarmClear" tool.

This procedure describes how to clear SDM610 alarms on a CBM 800 or on a CBM 850 cluster.

> *Note:* 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.

Procedure

Clearing an SDM610 alarm

At your workstation

1 Open a connection to the CBM using SSH, if one is not already established, and log in as the "emsadm" user. If you are addressing an alarm raised in a CBM 850 cluster, connect to the node (either active or inactive) on which the problem occurred.

```
ssh -l <emsadm_user> <ip_address>
```

where

   <emsadm_user>
   is the emsadm user login name

   <ip_address>
   is the IP address of the CBM

> *Note:* If an "emsadm" user has not been configured, perform the procedure Creating a user allowed to perform patching on a CBM on page 148

2 Enter the password for the "emsadm" user.

3 If you want to view the current alarms, use the queryflt tool:

`queryflt`

4 Use the following table to determine your next step.

If	Do
you want to clear an SDM610 notification alarm	step 5
you want to clear an SDM610 count alarm	step 6
you want to clear an SDM610 alarm for a specific patch	step 7

5 At the command line prompt, type:

`simAlarmClear -t notification`

When the alarm has been cleared, it will no longer appear in the "queryflt" command output.

Go to step 8.

6 At the command line prompt, type :

`simAlarmClear -t count`

When the alarm has been cleared, it will no longer appear in the "queryflt" command output.

Go to step 8.

7 At the command line prompt, type:

`simAlarmClear -t <patch ID>`

where

<patch ID>
is the patch ID from the alarm you wish to clear.

Example
To clear an SDM610 alarm for patch ID "NTBMI077595-01", you would enter:

simAlarmClear -t NTBMI077595-01

When the alarm has been cleared, it will no longer appear in the "queryflt" command output.

8 You have completed this procedure.

Creating a user allowed to perform patching on a CBM

Purpose

This procedure enables you to create a new user who is allowed to perform patching procedures on a CBM 800 or CBM 850 node.

Note: 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.

Procedure

Creating a user allowed to perform patching on a CBM

At your workstation

1   Open an SSH connection to the CBM and log in as the root user. If you are creating a user for a CBM 850 cluster, connect first to the active node of the cluster. You will later need to connect to the companion node of the cluster and perform this procedure a second time.

`ssh -l root <ip_address>`

where

<ip_address>
is the IP address of the CBM 800 or CBM 850

2   Enter the password for the root user.

3   Add the user:

`/usr/sbin/useradd -g emsadm -m -d /export/home/<user_name> -s /bin/ksh <user_name>`

where

<user_name>
is the name of the new user you want to create

Note: "EMSADM" should not be used as the actual name for the emsadm user you are creating.

4   Create a password for the user you just added:

`passwd <user_name>`

where

<user_name>
is the user name you added in the previous step

5   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.

6   When prompted, enter the password again for verification.

7   If you are creating users for a CBM 850 cluster, execute the following command:

```
tar -cf - /export/home/<user_name> | ssh
<inactive ip address> "tar -xf - "
```

>   ***Note:*** Note that the <u>tar -xf -</u> sequence above has no space between - and xf (-xf) and that a space separates -xf and the following -.

8   You have completed 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.

Network protocols

Insecure		*Secure*
Telnet	⟶	ssh
ftp	⟶	sftp
rcp	⟶	scp
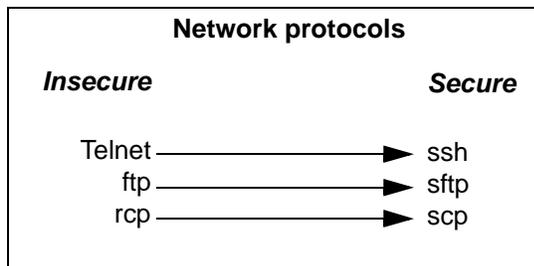
The suite of OpenSSH tools is as follows:

- 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 securely 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

Editing and viewing object properties using Java Web Client

Application

Use this procedure to edit or view the properties of objects that are displayed in the IEMS topology using Java Web Client.

Prerequisites

None

Action

At the IEMS workstation

1   Launch the IEMS Java Web Start Client. Refer to Launching IEMS Java Web Start Client in.

2   Select the required object in the Integrated EMS Topologies tree under Applications.

> ***Note:*** The properties of an object from the Inventory panel of Integrated EMS tree can also be viewed. To view the Inventory object properties, select the object in the Integrated Topologies tree under Applications to open the Inventory view. Double-click the required row in the Inventory view.

3   Right-click the map symbol and select the **Managed Object Properties** menu item or double-click the map symbol to open the Object Properties window.

> ***Note:*** The object properties displayed can differ for each component.

A window similar to the following figure opens.

4   Modify the object properties listed in the table below if required.

Managed object properties in Java Web Client

Field	Description
Name	Displays a unique name for the object
Display Name	Edit the name displayed in the topology for the object
Type	Displays the type of object (element manager, EMS, EMS platform or NE)
Status	Displays the status of the object
IP-Address	Edit the IP address of the object

Managed object properties in Java Web Client

Field	Description
Platform	Select the platform where the object resides from the drop-down list
Managed	Indicates whether the object is managed or unmanaged
Time Zone	Select the time zone of the geographical location where the object exists from the drop-down list
Device Version	Select the device version of the managed object from the drop-down list
Enable System Unmanage	Enable or disable the System_Unmanaged state. Refer to the System_Unmanaged state section of Configuring the Message Overload Controller parameters in *Integrated EMS Fault Management*, NN10334-911.
Poll Interval	Edit the Poll Interval for status updates
Status Change Time	Displays the last status change time of the object

Note: For the following objects, only the Display Name and the Managed field can be modified.

- SDM platform, APS EMS application, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Proxy, Media Gateway 7480/15000, MSS 15000

5   Select your next step.

If	Do
you do not want to modify any other properties	go to step 6
you want to view or modify the fault interface or performance interface properties	go to step 8

6   Click the **Modify** button to update the changes.

7   Go to step 16.

8   Click the **Next** button to proceed to the Fault Interface window.

A window similar to the following figure opens.

9   Edit or view the fault interface properties of the object as required.

> *Note:* The Details panel dynamically changes according to the fault interface of the EMS/NE.

10   Select your next step.

If	Do
you do not want to modify any other properties	step 11
you want to view or modify the performance interface properties	step 13

11   Click the **Modify** button to update the changes.

12   Go to step 16.

13   Click the **Next** button to proceed to the Performance Interface window.

A window similar to the following figure opens.

14   Edit or view the performance interface properties of the object as required.

15   Click the **Modify** button to update the changes.

16   You have completed this procedure.

Editing and viewing object properties using Web Client

Application

Use this procedure to modify or view the properties of an object in the IEMS topology using Web Client.

Prerequisites

None

Action

At the IEMS workstation

1   Launch the IEMS Web Client. Refer to Launching the IEMS Web Client.

2   Select the **Integrated EMS Topologies** tab.

3   Navigate to the required topology node in the Integrated EMS Topologies tree.

4   Click the map symbol label to open the **General Information** window.

> ***Note:*** The object properties displayed can differ for each component.

A window similar to the following figure opens.

5   Select each vertical tab and modify the object properties listed in the table below if required.

Managed object properties in Web Client

Field	Description
General	
Name	Displays the unique object name of the managed object
Device Type	Displays the type of object (element manager, EMS, EMS platform or NE)
Status	Displays the status of the object
Is Managed?	Indicates whether the object is managed or unmanaged
Display Name	Displays the name or label displayed in map symbol
Device Version	Select the version of the device from the drop-down list

Managed object properties in Web Client

Field	Description
IP Address	Modify the IP address of the object
Web User name	Enter your web user name
Web Password	Enter your web password
Monitoring	
Last Status Update Time	Displays the time when the status of the managed object last changed
Last Status Change Time	Displays the time when the status of the managed object last changed
Status Polling Interval (secs)	Modify the Poll Interval for status updates

Managed object properties in Web Client

Field	Description
Fault Interface If the details are present for the selected object, the details can be modified. **Performance Interface** If the details are present for the selected object, the details can be modified.	

6   Click the **Update Object** button to update the changes.

7   You have completed this procedure.