Core and Billing Manager 800 Upgrades

Introduction

Software upgrades for the Core and Billing Manager are delivered in the form of software packages and software patches. The software packages for installation 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. Patches are applied safely to applications that are running on the CBM: 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.

This NTP contains the procedures for patching the CBM 800 using functionality provided by the Software Inventory Manager (SIM). The tasks you can perform using these procedures are described in the following sections:

Applying and removing CBM software packages

Although many software packages are applied to a CBM node during CBM installation, some software packages require manual configuration and must be applied to the CBM 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, through the "packages" level of the cbmmtc user interface. When you remove a software package, 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

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.

Setting up patching rules using patch filters

There are three types of patches that can be applied on the CBM 800: active 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 schedule through the SIM patching tool, "patchconfig".
- "Manual" patches cannot be applied automatically and, thus, cannot be scheduled.
- "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. After these patches have been moved to this special directory, the release notes that accompany the patches can be extracted and displayed by the SIM patching tools.

The SIM patching tools can be used to override the embedded 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 800, two types of filters can be set: manual filters and the *reboot filter. When a manual filter is set, active-apply patches matching specified criteria will always be treated as manual-apply patches. When the *reboot filter is set, any active-apply patch requiring a system reboot when the patch is applied is made a manual-apply patch.

Manual-apply and interactive patches cannot be filtered to become active-apply patches. In 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 800.

Setting up automatic patching schedules and applying patches on the CBM

Automatic patching is the recommended method of applying patches on the CBM 800. 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.

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 filter file is consulted. Any patches that match the criteria of a manual filter (that is, the *reboot or alphanumeric text string filters) defined on the system 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 800.
- The system automatically reboots if at least one of the patches that was applied required a reboot.

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

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 through the procedure, Manually applying patches to a CBM 800 on page 34. 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.

Clearing patching alarms

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 minor alarm is cleared automatically when a patch is successfully applied while the alarm is raised. 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

The SIM tool can be used to remove applied patches from the CBM. 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.

Querying the system for patch and package information using Queryloads

The SIM "Queryloads" tool provides an interface used for gathering information about patches and software application packages installed on the system. The tool can also be used to obtain patch and software package baseline information. Information can be compiled either as a formatted report or as raw XML data.

Guide to the SIM patching tool procedures

The following table provides a list of the procedures you can perform using the package and patching tools.

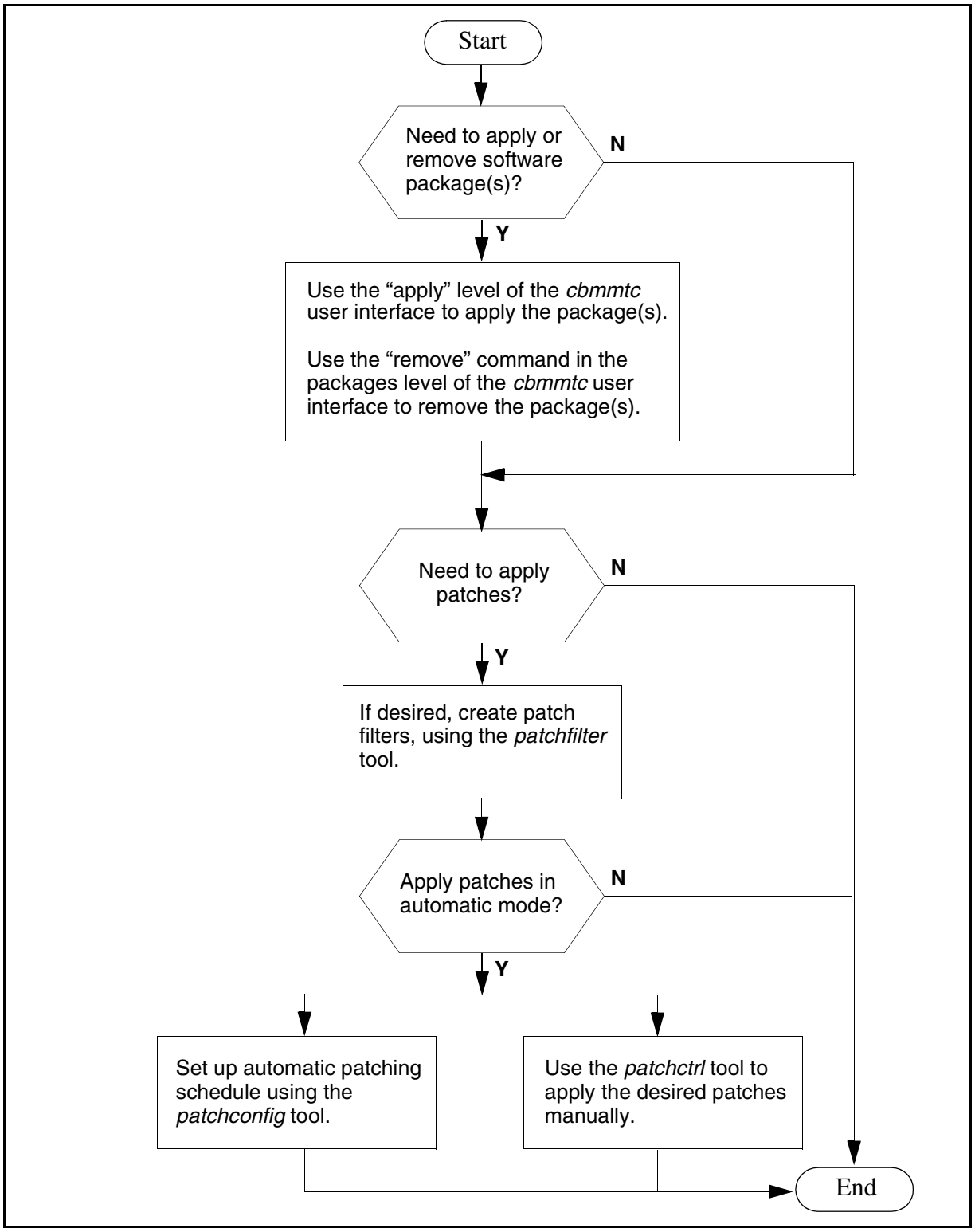
Procedure
Installing optional software on a CBM 800 on page 8
Installing the SBA and AFT software packages on a CBM 800 on page 12
Applying software packages on a CBM 800 on page 14
Removing software packages from a CBM 800 on page 20
Viewing software transaction history and logs on the CBM 800 on page 24
Delivering patches to a CBM 800 on page 26
Setting up patch filters for a CBM 800 on page 28
Setting up automatic patching on a CBM 800 on page 32
Manually applying patches to a CBM 800 on page 34
Using the Queryloads tool to display patches and packages applied on the CBM 800 on page 38
Making the CBM 800 patch-current after optional software package installation on page 46
Creating a user allowed to perform patching on a CBM on page 54
Clearing an SDM610 alarm on page 48

The following flowchart shows the basic task flow for patching and updating using the SIM patching tool procedures. To perform the tasks

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

Note: SSH is the preferred method for connecting to the CBM 800 in order to perform these tasks. For information about SSH, refer to OpenSSH overview on page 51.

Basic task flow for patching and updating using the SIM patching tool procedures



Purpose

This is a generic procedure that is used for the installation of optional software packages on the CBM 800.

Note: If you are installing SBA and AFT software packages, use the procedure Installing the SBA and AFT software packages on a CBM 800 on page 12.

Procedure

Installing optional software on a CBM 800

At your workstation

1 Open a connection to the CBM 800 using SSH and log in as the root user:

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

where

<ip_address>
is the IP address of the CBM 800

2 Enter the password for the root user.

3 Apply the software application package by performing the procedure Applying software packages on a CBM 800 on page 14. Since CD-ROM is used for CBM 800 package installations, specify /cdrom/cdrom/applications/cbm/packages as the source directory when you perform that procedure.

Note: For a list of valid applications (filesets), see Filesets available for the CBM 800 on page 9.

4 Configure the software application using the procedures found in *Core and Billing Manager 800 Configuration Management*, NN10360-511.

5 Ensure that the CBM is patch-current by performing the procedure, Making the CBM 800 patch-current after optional software package installation on page 46.

6 You have completed this procedure.

Filesets available for the CBM 800

The following table lists filesets (applications) included in the CBM00070 load. The table also shows which filesets are included with the CBM 800 at the time of installation (Base) and which filesets you may install later (non-base).

Filesets available for the CBM 800 (Sheet 1 of 2)

Fileset	Description	Type
SDM_BASE.version_20.81 .0.0	Load Lineup Information	Base
NT_SIM.tools	Patching Tools	Base
SDM_ACE	SDM ACE distribution	Non-base
SDM_AFT.DMS500	SBA Automatic File Transfer	Non-base
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	Base
SDM_BASE.logs	Log Delivery Service	Non-base
SDM_BASE.mtce	Platform Maintenance	Base
SDM_BASE.omsl	OM Access Service	Base
SDM_BASE.tasl	Table Access Service	Base
SDM_BASE.util	Platform Utilities	Base
SDM_DEBUG.tools	SDM/CBM Debug Helper Tools	Base
SDM_FTS.package	Solaris FTS/MTS Streams Modules	Base
SDM_GDB.gdb	Gnu Debugger	Base
SDM_FTP.proxy	FTP Proxy	Non-base

Note: Base = included with the CBM 800; Non-base = package that can be applied

Filesets available for the CBM 800 (Sheet 2 of 2)

Fileset	Description	Type
SDM_SBA.DMS500	SDM Billing Application	Non-base
SDM_SCFT.scft	Core File Transfer	Non-base
Note: Base = included with the CBM 800; Non-base = package that can be applied		

Installing the SBA and AFT software packages on a CBM 800

Purpose

This procedure explains how to install the SuperNode Billing Application (SBA) and Automatic File Transfer (AFT) software packages on the CBM 800.

Procedure

Installing the SBA and AFT software packages on a CBM 800

At your workstation

1 Open a connection to the CBM 800 using SSH and log in as the root user:

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

where

<ip_address>
is the IP address of the CBM 800

2 Enter the password for the root user.

3 Using the procedure Applying software packages on a CBM 800 on page 14, apply the SBA and AFT software packages located in the /cdrom/cdrom/applications/cbm/packages directory of the CD-ROM.

4 Create the required logical volumes for the SBA application.

Note: Ensure that you create logical volumes only for the type of stream that you are configuring.

For ama strreams:

```
# makelv /cbmdata/00/billing/ama 1024
# chmod ug=rwx,o=/cbmdata/00/billing/ama
# chown maint:maint /cbmdata/00/billing/ama
```

For occ streams:

```
# makelv /cbmdata/00/billing/occ 1024
# chmod ug=rwx,o=/cbmdata/00/billing/occ
# chown maint:maint /cbmdata/00/billing/occ
```

For smdr streams:

```
# makelv /cbmdata/00/billing/smdr 1024
# chmod ug=rwx,o=/cbmdata/00/billing/smdr
```

```
# chown maint:maint /cbmdata/00/billing/smdr
```

5 To configure the SBA for operation, refer to NTP NN10357-811, *Core and Billing Manager 800 Accounting* for the procedures to use.

6 To configure AFT for operation, refer to NTP NN10357-811, *Core and Billing Manager 800 Accounting* for the procedures to use.

7 Ensure that the CBM is patch-current by performing the procedure, Making the CBM 800 patch-current after optional software package installation on page 46.

8 You have completed this procedure.

Applying software packages on a CBM 800

Purpose

This procedure enables you to apply software packages to a CBM 800.

Note: If you are installing SBA and AFT software packages, use the procedure Installing the SBA and AFT software packages on a CBM 800 on page 12.

Procedure

Applying software packages on a CBM 800

At your workstation

1 Open a connection to the CBM 800 using SSH and log in as the root user:

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

where

<ip_address>
is the IP address of the CBM 800

2 Enter the password for the root user.

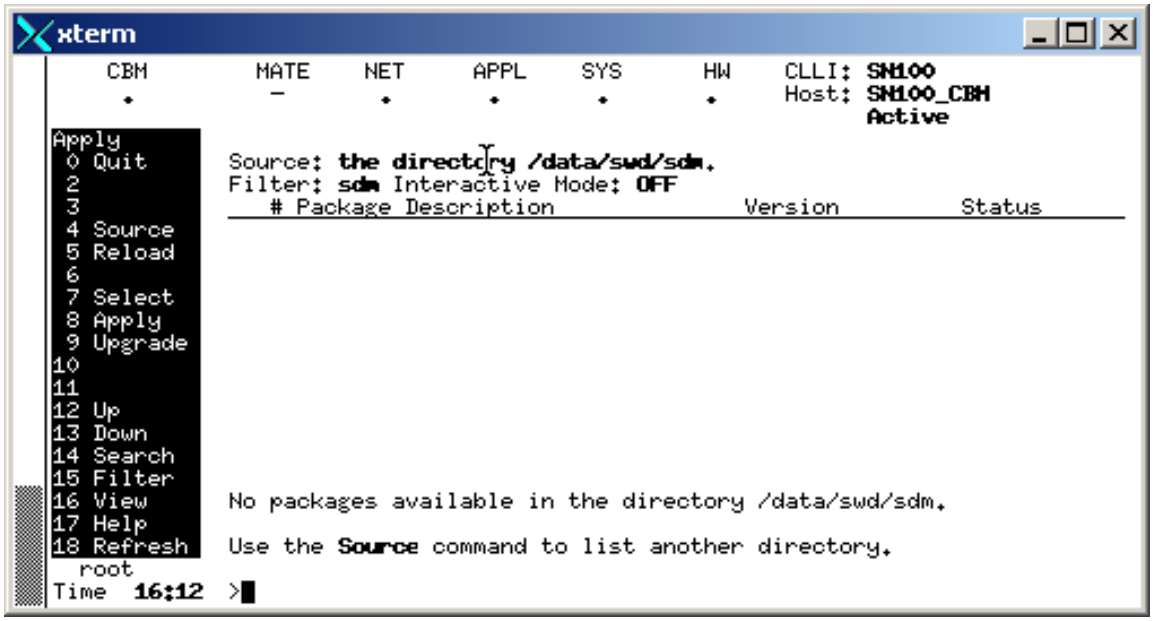
3 From the command line prompt, access the apply level of the cbm maintenance interface:

```
# 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
you wish to continue the package application	step 4
you wish to exit from the cbm maintenance interface	step 8

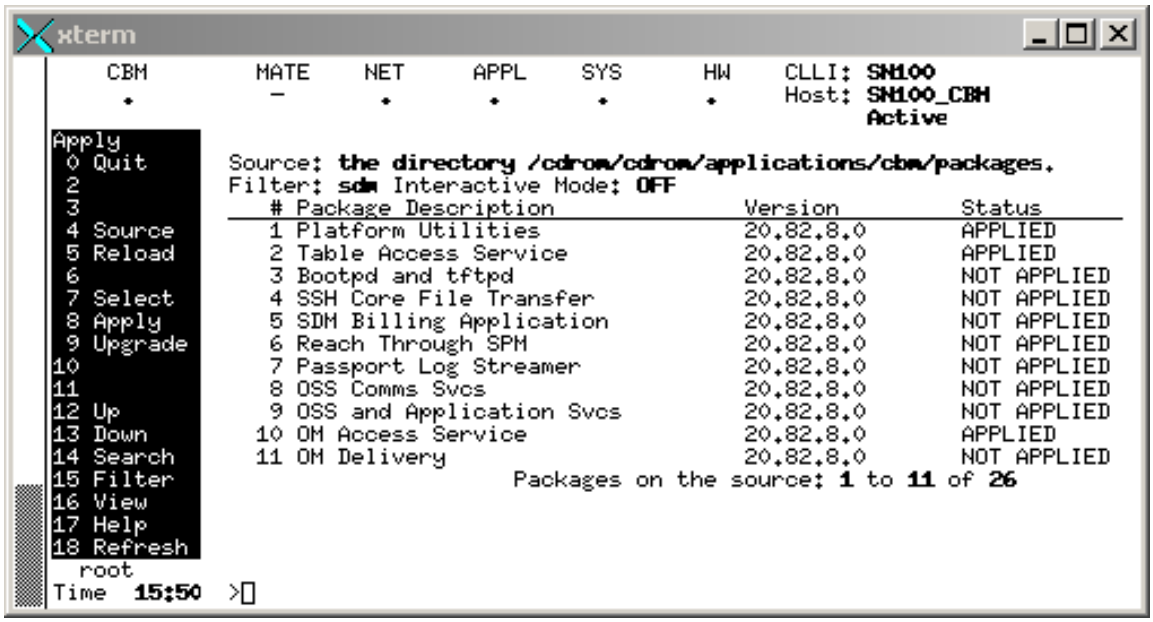
4 Insert the CD-ROM into the CD drive if the CD-ROM is not already present in the drive.

5 At the command line located at the bottom of the screen, type:

```
> source /cdrom/cdrom/applications/cbm/packages
```

The system displays the apply level screen of the cbm maintenance interface, which shows a list of all packages in the source directory (CD-ROM) that you specified.

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



6 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

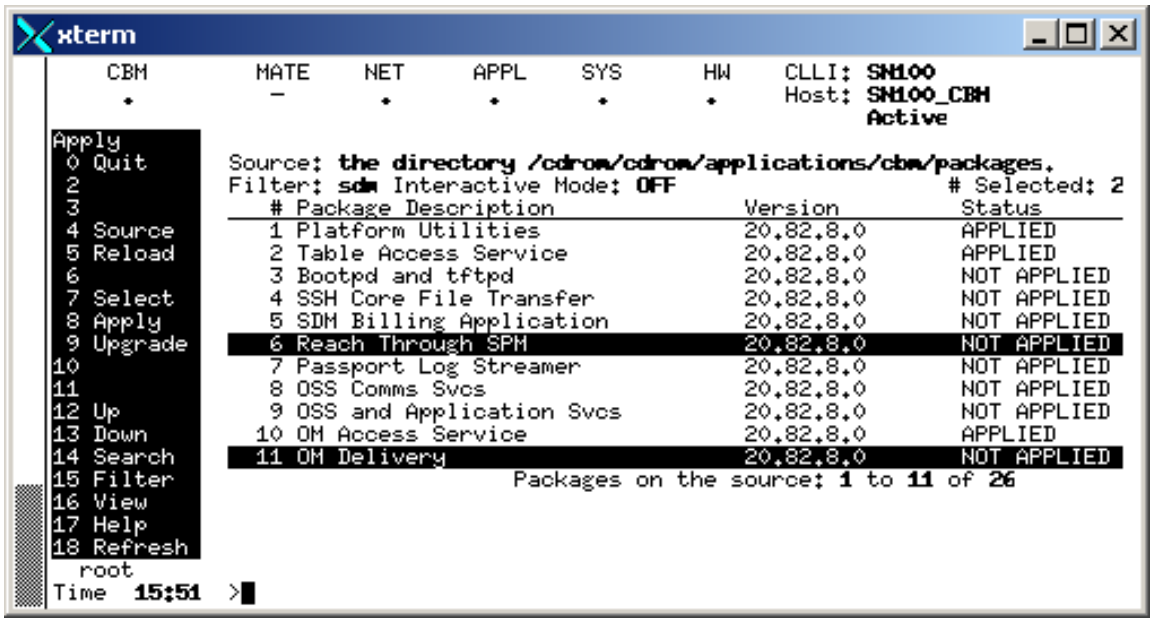
<package number>
is the number associated with a package, that you noted. Each package number is separated by preceding and succeeding spaces.

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



Note: If you wish to de-select any packages that you selected, re-enter the select command for the packages you wish to de-select. The highlighting on the packages that you de-select will be removed.

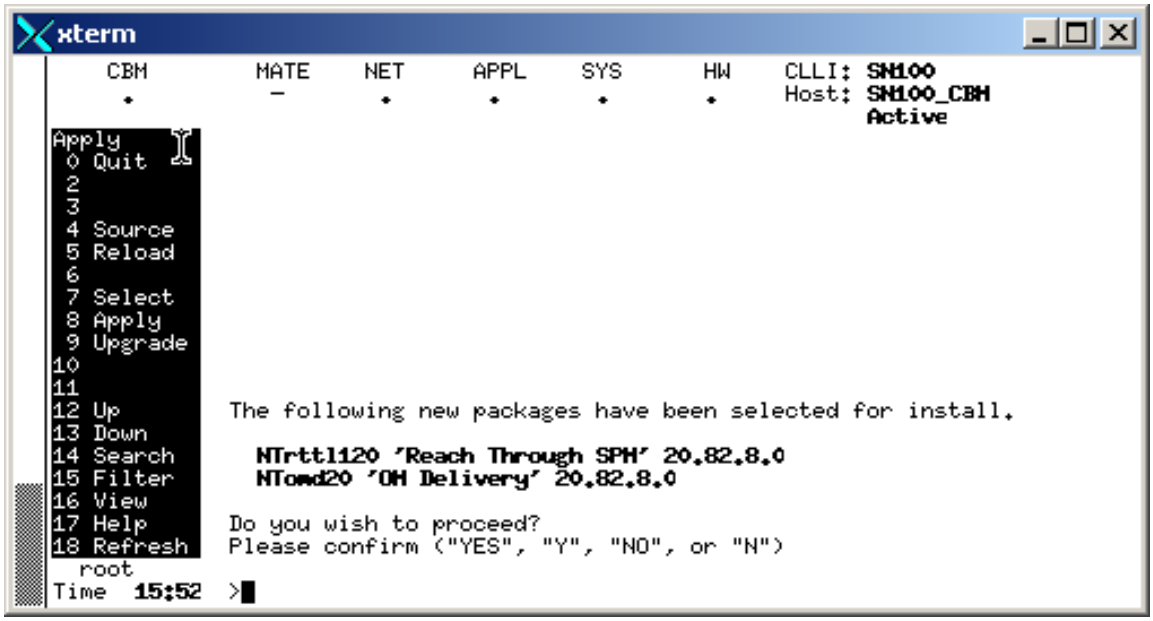
7 Apply the selected packages:

```
> 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

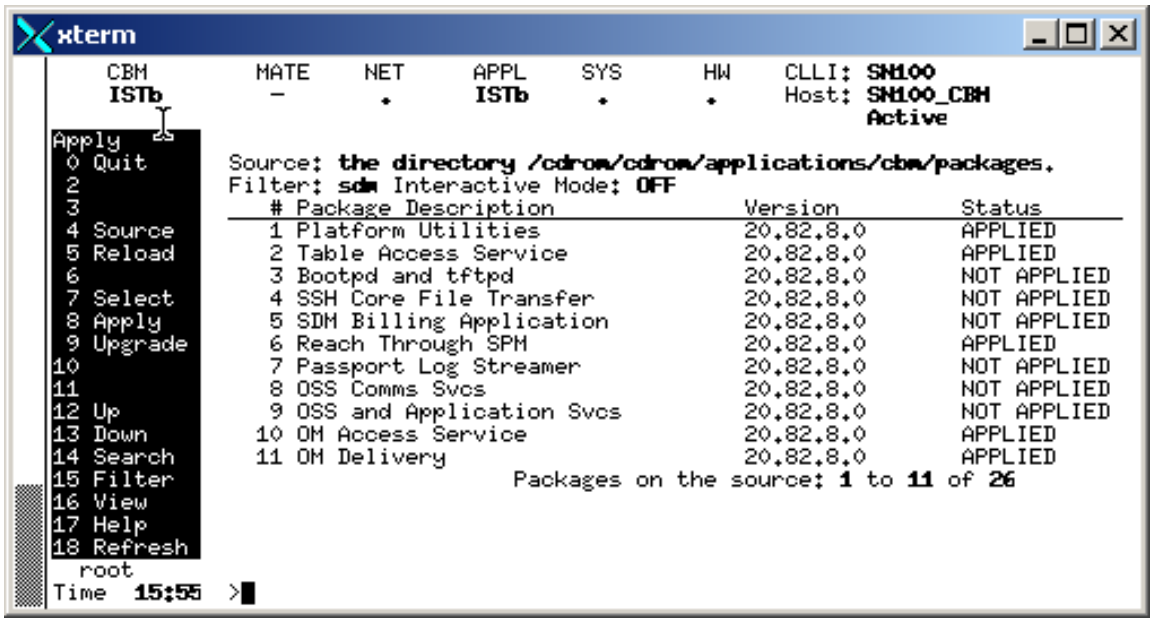


If	Do
you wish to continue the package application	step 7a
you do not wish to continue the package application	step 7b

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



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 wish to view details about the CBM package application, perform the procedure Viewing software transaction history and logs on the CBM 800 on page 24

Go to step 8.

b Type no in response to the prompt.

8 Exit from the cbm maintenance interface:

```
> quit all
```

9 You have completed this procedure.

Removing software packages from a CBM 800

Purpose

This procedure enables you to remove software packages from a CBM 800.

Note: 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.

Procedure

Removing software packages from a CBM 800

At your workstation

1 Open a connection to the CBM 800 using SSH and log in as the root user:

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

where

<ip_address>
is the IP address of the CBM 800

2 Enter the password for the root user.

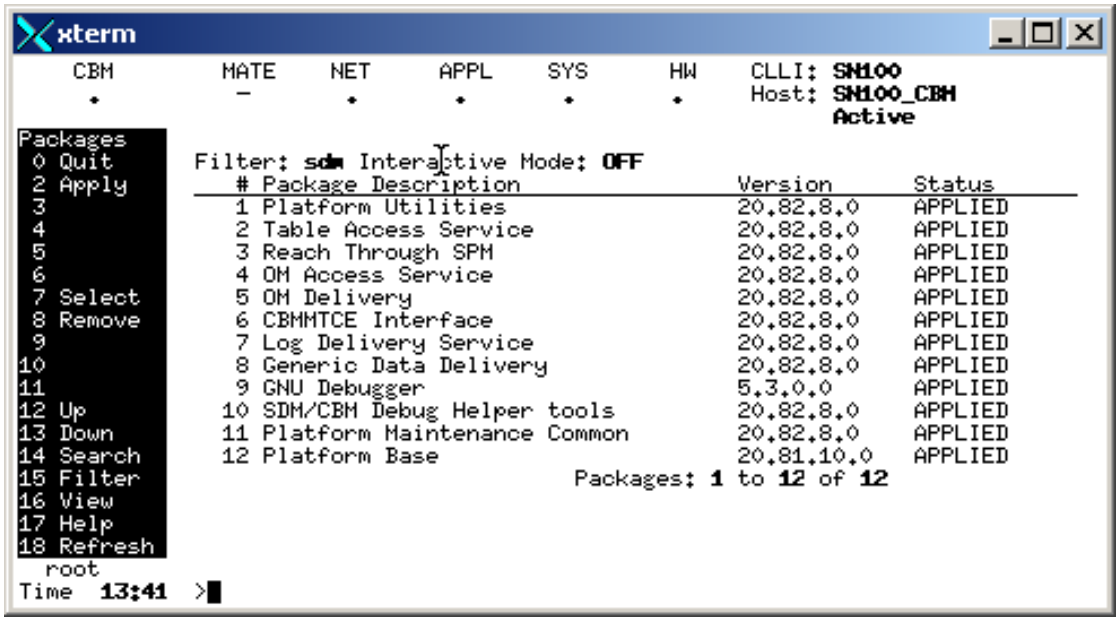
3 From the command line prompt, access the packages level of the cbm maintenance interface:

```
# cbmmtc packages
```

The system displays the packages level screen of the cbm maintenance interface, which 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 screen display showing packages, with Applied status, available for removal



4 In the list of packages, 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

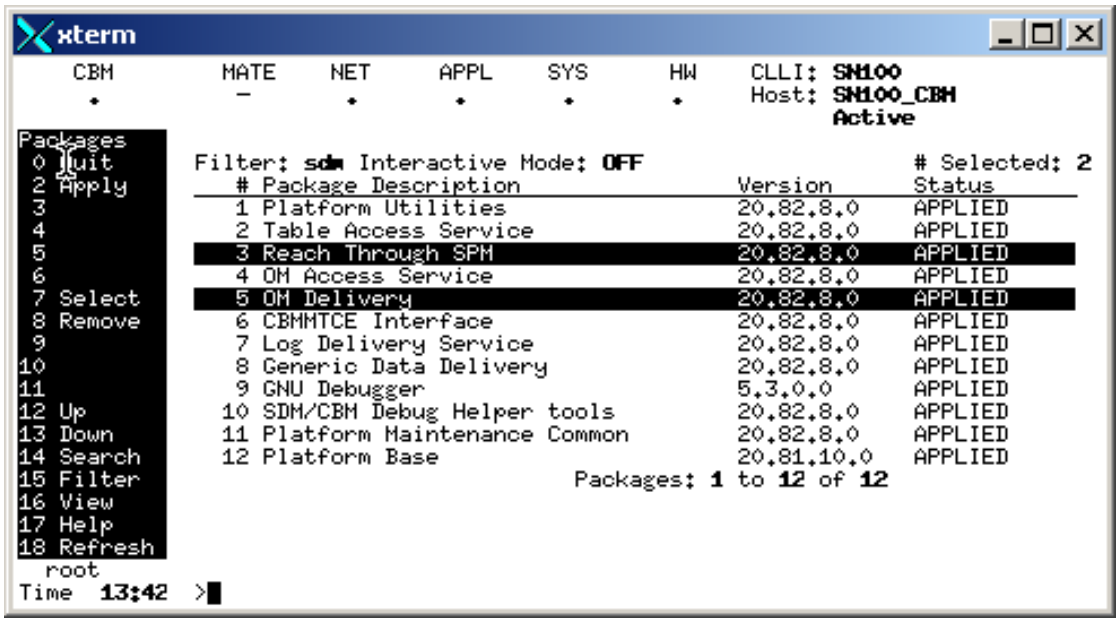
<package number>
is the number associated with a package, that you noted. Each package number is separated by preceding and succeeding spaces.

Example
To select Reach Through SPM, which is number 3 in the sample screen display shown in step 3, and OM Delivery, which is number 5 in the sample screen display, enter

```
> select 3 5
```

If the command is successful, the package you selected will be highlighted on the cbmmtc packages screen.

Example of the cbm maintenance interface packages level screen display showing packages that you have selected for removal



Note: If you wish to de-select any packages that you selected, re-enter the select command for the packages you wish to de-select. The highlighting on the packages that you de-select will be removed.

5 Remove the package(s):

```
> remove
```

Note: 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.

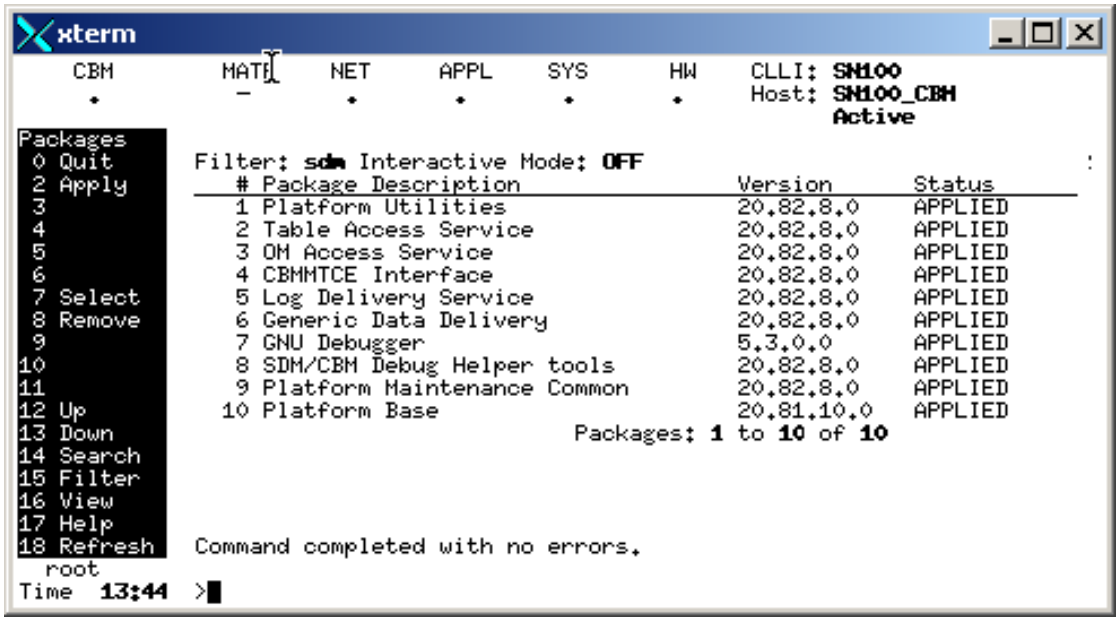
The system will prompt you once to ensure that you want to continue with the package removal.

If	Do
you wish to continue the package removal	step 5a
you do not wish to continue the package removal	step 5b

a Type yes in response to the prompt.

The status of the package application will be displayed on the cbmmtc packages screen.

Example of the cbm maintenance interface packages level screen display showing the remaining packages on the CBM after the packages removal



If the removal was successful, the package will no longer appear in the packages list that displays when you enter the cbmmtc packages command. If the removal was not successful, the package will still appear in the packages list, with the status “Applied”, or with the status “Partial” if an error occurred when the package removal was attempted.

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.

If you wish to view details about the CBM package removal, perform the procedure Viewing software transaction history and logs on the CBM 800 on page 24.

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.

Viewing software transaction history and logs on the CBM 800

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 800.

Procedure

Viewing software transaction history and logs on the CBM 800

At your workstation

1 Determine the first step to perform.

If	Do
you are already connected to a CBM 800	step 4
you are not connected to a CBM 800	step 2

2 Open a connection to the CBM 800 using SSH and log in as the root user:

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

where

<ip_address>
is the IP address of the CBM 800

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 Access the cbmmtc user interface:

```
# cbmmtc
```

6 Type the following on the command line:

```
> history
```

The system displays the information about the package transactions you have performed, including a log file and the

results of the individual operations. 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 800

Purpose

This procedure describes how patches can be delivered to a CBM 800.

The recommended method of software delivery is electronic software delivery (ESD), through FTP. Patches that are to be automatically applied should be transferred to the /swd/fixes/incoming directory on the CBM node. Patches that are to be manually applied should be placed in a directory that can be used for patching. This directory must not be one in the /swd/fixes directory.

Procedure

Delivering patches to a CBM 800

At your workstation

1 Open a connection to the CBM 800 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 CBM 800

Note: If an "emsadm" user has not been configured, perform the procedure Creating a user allowed to perform patching on a CBM on page 54

2 Enter the password for the "emsadm" user.

3 Determine the next step to perform.

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

4 At the prompt, electronically transfer (ftp) the patches to the /swd/fixes/incoming directory on the CBM 800.

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 800 on page 28, 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 800 and removing previously configured schedules on page 32, then go to step 8.

6 At the prompt, electronically transfer (ftp) the patches to the CBM 800. Place the patches in a directory other than in those under the /swd/fixes directory, that can be used for patching.

7 Perform the procedure Manually applying patches to a CBM 800 on page 34.

8 You have completed this procedure.

Setting up patch filters for a CBM 800

Purpose

This procedure enables you to set up a patch filter for a CBM 800. 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 redefined as a “manual apply” patch even though the patch was packaged as an “active apply” patch.

Procedure

Setting up patch filters for a CBM 800

At your workstation

1 Open a connection to the CBM 800 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 CBM 800

Note: If an “emsadm” user has not been configured, perform the procedure Creating a user allowed to perform patching on a CBM on page 54

2 Enter the password for the “emsadm” user.

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

```
# patchfilter
```

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

If	Do
you wish to add a filter	step 5
you wish to remove a filter	step 8
you wish to abort the program	step 12
you wish to save the filter	step 11

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 active-apply patches that require a reboot of the system when the patches are applied. When you configure the *reboot filter for a manual filter, all active-apply patches requiring a system reboot will be made manual-apply patches.
- an alphanumeric text string can be created that represents the desired behavior of the filter. Any active-apply patches matching the filters will be made manual-apply patches.

Note: Patches matching the *reboot filter or an alphanumeric text string filter are automatically moved to the /swd/fixes/manual directory when the automatic patching schedule is invoked. You must then apply these patches manually using the procedure, Manually applying patches to a CBM 800 on page 34 at another time.

The following table provides examples of possible alphanumeric text string filter names that might be created.

Desired filter behavior	Patch name	Examples of possible filter names[a]
To filter all patches that update a specific software package	NTBMI077505-01 (patch applying to package NTbmi7)	NTbmi, ntbmi, NTbmi07, bmi
To filter all Nortel patches	Not applicable	NT, nt, Nt, nT
To filter a particular patch	NTSIM077505-07	NTSIM077505-07, NTsim077505-07
To filter all patches with a specific version identifier	NTSIM077505-03 (version 3 of an NTsim7 patch)	-03

a.The patchfilter tool is case insensitive.

7 Use the following table to determine your next step.

If	Do
you wish to add another filter	step 5
you wish to save your changes and exit from the patchfilter program	step 11
you wish to remove a filter	step 8
you wish to abort the program without first saving any changes	step 12

8 In response to the prompt, type:

```
> remove
```

9 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.

10 Use the following table to determine your next step.

If	Do
you wish to remove another filter	step 8
you wish to save your changes and exit from the patchfilter program	step 11
you wish to add a filter	step 5
you wish to abort the program without first saving any changes	step 12

11 To save your changes, type:

```
> save
```

Go to step 13.

12 In response to the prompt, type:

```
> abort
```

13 You have completed this procedure. Proceed to Setting up automatic patching on a CBM 800 on page 32.

Setting up automatic patching on a CBM 800

Purpose

This procedure enables you to set up an automatic patching schedule for “active-apply” patch types, on a CBM 800.

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

Procedure

Setting up automatic patching on a CBM 800 and removing previously configured schedules

At your workstation

1 Open a connection to the CBM 800 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 CBM 800

Note: If an “emsadm” user has not been configured, perform the procedure Creating a user allowed to perform patching on a CBM on page 54

2 Enter the password for the “emsadm” user.

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

```
# patchconfig
```

If	Do
you want to set a patching schedule	step 4

If	Do
you want to remove the currently defined patching schedule and exit from the patchconfig tool	step 7
you want to abort the patchconfig program without setting a patching schedule	step 8

4 In response to the prompt, enter your choice for a daily, weekly, or monthly patching schedule.

If	Do
you want to continue setting the patching schedule	step 5
you wish to abort the patchconfig program at this point, without saving any changes you have made	step 8

5 In response to the prompts, select the time of day (hour and minute) that the patches should be applied on the node.

If	Do
you have selected Daily and entered the hour and minute at the appropriate prompts	step 9
you wish to continue setting either a weekly or monthly patching schedule	step 6
you wish to abort the patchconfig program at this point, without saving any changes you have made	step 8

6 In response to the prompt, select the day of the week, if you are setting a weekly patching schedule, or the day of the month, if you are setting a monthly patching schedule, that the patches are to be applied on the node.

If you have selected either a weekly or a monthly schedule, go to 9.

7 Enter none

Go to step 9

8 Enter abort and then enter yes in response to the confirmation request to abort.

9 You have completed this procedure.

Manually applying patches to a CBM 800

Purpose

This procedure enables you to manually apply patches to a CBM 800. You apply the patches using the “patchctrl” tool, which can be invoked from any directory. The patchctrl tool applies a single patch or multiple patches located in a source directory that you specify. You may apply two types of patches: “active apply” patches or “manual apply” patches.

Note: “Interactive” patches are not applied on the system but are, instead, moved by the patchctrl 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 on the node.

Procedure

Manually applying patches to a CBM 800

At your workstation

1 Open a connection to the CBM 800 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 CBM 800

Note: If an “emsadm” user has not been configured, perform the procedure Creating a user allowed to perform patching on a CBM on page 54

2 Enter the password for the “emsadm” user.

3 Use the following table to determine the next step.

If	Do
you want to apply a single patch	step a
you want to apply a directory with one or more patches within it	step b

a 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 wish 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
```

Go to step 4

b 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 either the patch directory or patch file, you do not need to enter the full pathname of the directory or file.

Instead, you may enter either the directory name, or "." (period) if you use the "-d" command option, or the file name if you use the "-f" command option.

4 After the patchctrl command is accepted, you will then be prompted by the system to authorize a reboot if one is required.

If	Do
you are prompted to confirm a reboot because one or more patches being applied require a reboot of the node	step 5
you are not prompted to confirm a reboot because none of the patches being applied require reboot of the node	step 6

5 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. If you choose to abort the patching, the patchctrl program exits without applying the patches.
No	The system displays a message indicating that the patches cannot be applied without a reboot, and the patchctrl program exits without applying the patches.
Yes	The node will reboot. If multiple patches are being applied, the system will reboot the node only one time, after all of the patches have been applied.

6 You have completed this procedure.

Using the Queryloads tool to display patches and packages applied on the CBM 800

Purpose

This procedure shows how to use the Queryloads tool to display information about patches that have been applied to a CBM 800 node. For several of the queries, the tool allows you to select either a formatted report display or a raw XML data display.

Procedure

Using the Queryloads tool to display patches and packages applied on the CBM 800

At your workstation

1 Open a connection to the CBM 800 using SSH and log in as the "emsadm" user:

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

where

<ip_address>
is the IP address of the CBM 800

<emsadm_user>
is the emsadm user login name

Note: If an "emsadm" user has not been configured, perform the procedure Creating a user allowed to perform patching on a CBM on page 54

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 all packages installed on the system, or list only packages installed on the system that you specify, displayed in text format.	step 5
List all packages installed on the system, or list only packages installed on the system that you specify, displayed in xml format	step 6

Query	Do
Store package information in a file that you designate	step 7
List all patches (including Sun patches) installed on the system, or list only patches installed on the system that you specify, displayed in text format	step 8
List all patches (including Sun patches) installed on the system, or list only patches installed on the system that you specify, displayed in xml format	step 9
Store patch information in a file that you designate	step 10
List packages or patches missing from the baseline	step 11
You wish 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 next step.

If	Do
you want to list all packages, displayed in text format	step a
you want to list only packages that you specify, displayed in text format	step b

a List all packages:

```
# queryloads -m packages
```

The system displays all packages installed on the system, in text format.

Go to step 13

b List only packages that you specify:

```
# 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 SUNWIpmsg	SUN

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

The system displays the package you have specified, in text format.

Go to step 13.

6 Use the following table to determine the next step.

If	Do
you want to list all packages, displayed in xml format	step a
you want to list only packages that you specify, displayed in xml format	step b

a List all packages:

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

The system displays all packages installed on the system, in xml format.

Go to step 13.

b List only packages that you specify:

```
#  queryloads -m packages -x | grep
<unique_package_identifier>
```

where

<unique_package_identifier>
is the identifier of the package you want to list. For a list of sample unique_package_identifiers, see step 5b.

The system displays the package that you have specified, in xml format.

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 Use the following table to determine the next step.

If	Do
you want to list all patches (including Sun patches), displayed in text format	step a
you want to list only patches that you specify, displayed in text format	step b

a List all patches:

 # queryloads -m patches

The system displays each patch and the packages to which the patch is applied, in text format.

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
```

Go to step 13.

b List only patches that you specify:

 # 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, ntbmi, NTbmi07, bmi
A specific patch	NTSIM077505-07	NTSIM077505-07, NTsim077505-07
Nortel patches	Not applicable	NT, nt, Nt, nT
SUN patches	112162-03::SUNWcarx, SUNWcsr	SUN

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

The system displays the patch and the packages to which the patch is applied, in text format.

Go to step 13.

9 Use the following table to determine the next step.

If	Do
you want to list all patches (including Sun patches), displayed in xml format	step a
you want to list only patches that you specify, displayed in xml format	step b

a List all patches:

```
# queryloads -m patches -x
```

The system displays each patch and the packages to which the patch is applied, in xml format.

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>
```

Go to step 13.

b List only patches that you specify:

```
# queryloads -m patches -x | 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 8b.

The system displays the patch you have specified and the packages to which the patch is applied, in xml format.

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

<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 CBM0070

Go to step 13.

12 At the prompt, invoke the queryloads tool:

```
# queryloads -h
```

13 You have completed this procedure.

Making the CBM 800 patch-current after optional software package installation

Purpose

This procedure describes how to make the CBM 800 patch-current after software packages have been installed.

Prerequisites

Before performing this procedure, ensure that you have completed installing all of the desired optional software packages on the node.

Procedure

Making the CBM 800 patch-current after optional software package installation

At your workstation

1 Open a connection to the CBM 800 using SSH and log in as the root user:

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

where

<ip_address>
is the IP address of the CBM 800

2 Enter the password for the root user.

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

4 If there are patches present in the /cdrom/cdrom/applications/cbm/packages directory of the CD-ROM, then apply all of the patches by performing the procedure, Manually applying patches to a CBM 800 on page 34. When performing the procedure, use the directory command option (-d) and the directory name, /cdrom/cdrom/applications/cbm/patches.

Note: Patches will only be applied for corresponding packages that are installed on the system. You will see patch application failures for patches whose packages are not yet installed on the system. This is normal system behavior.

5 Complete the installation by configuring the applications that you have installed and by ensuring that the file system is sane.

6 You have completed this procedure.

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

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.

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 54

2 Enter the password for the “emsadm” user.

3 If you wish 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.

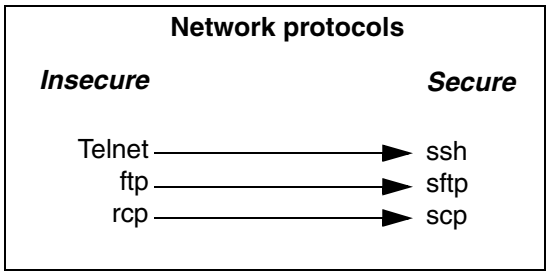
8 You have completed this procedure.

OpenSSH overview

Functional description

ATTENTION
This document is an overview only of the OpenSSH functionality. Nortel Networks does not provide any detailed usage information or client installation procedures. For this information, refer to the official OpenSSH website located at http://www.openssh.com/.

OpenSSH is an open source version of the Secure Shell (SSH) protocol suite of network connectivity tools. Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. OpenSSH is a suite of tools that provides strong authentication and secure communications over unsecure channels.



The suite of 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 (via the SSH standard). SSH clients are supplied bundled with some operating systems, but may need to be obtained separately. The following

table lists some sources for SSH clients (sources are not limited to those listed in this table).

Sources for SSH clients

Source	Type
PUTTY	freeware
OpenSSH	freeware
SSH Inc.	commercial
Secure CRT	commercial
WinSCP	freeware

- scp (secure copy) - improved (secure) functionality of rcp (remote copy)

  Using scp, you can securily copy files to and from the core manager or a remote system. Scp uses ssh for data transfer, and uses the same authentication and provides the same security as SSH.

- sftp (secure file transfer program) - a replacement for ftp

  Using sftp, you can perform secure file transfers. Sftp is an interactive program that connects and logs into the specified host, then enters an interactive command mode.

- sshd (OpenSSH SSH daemon) - the server-side daemon

  Sshd is the daemon program for SSH. Together these programs provide secure encrypted communications between two hosts over an insecure network.

Note: The functionality of OpenSSH does not interfere with existing networking services, such as telnet, FTP, DCE, NTP, or SFT.

The implementation of OpenSSH on the 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

Note: The administrator on the SDM and the client must be familiar with the key authentication method, before using it.

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

Note 1: For detailed instructions on the use of key authentication, refer to the official OpenSSH website http://www.openssh.com/.

Note 2: 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 Upgrades document to install the OpenSSH fileset.

For more information, you can 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

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.

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
/cbmdata/users/<user_name> -s /bin/ksh
<user_name>
```

where

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

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, perform steps 1 through 6 on the inactive node of the cluster.

8 You have completed this procedure.