Nortel Communication Server 1000

Patching Fundamentals

Release: 6.0
Document Revision: 01.03

www.nortel.com

NN43001-407

Nortel Communication Server 1000
Release: 6.0
Publication: NN43001-407
Document release date: 12 June 2009

Contents

New in this release 7
Features 8
Other changes 9
Revision history 9

How to get help 11
Getting help from the Nortel Web site 11
Getting help over the telephone from a Nortel Solutions Center 11
Getting help from a specialist by using an Express Routing Code 12
Getting help through a Nortel distributor or reseller 12

Introduction 13
Subject 13
Legacy products and releases 13
Applicable systems 14
Intended audience 14
Conventions 14
Related information 14

Overview 17
Remote broadband connection 18
Linux patches 18
Serviceability updates 19
Naming conventions 20
Patches 20
Service packs 21
Patch loading and unloading sequence 24
Obsolete patches 24
Patch dependencies 25
Patching impacts 25

Patching Manager overview 27
Central and Local Patching Managers 27
Applications 28
Patching permissions and roles 30
Patching job queuing 31

Concurrent patching operation from Patch Manager user interfaces 32
Patch libraries 32
In Progress status information 33
Clearing patch activities 34
Recovery from failures 35
Limitations 36

Central Patching Manager 39
Download and save patches, serviceability updates, and service packs 39
Access the Central Patching Manager 42
Add a service pack to the central patch library 45
View service pack details 47
Delete a service pack from the central patch library 50
Add a patch to the central patch library 51
View patch details 53
Delete a patch from the central patch library 55
Activate a service pack 56
Activate patches 63
Deactivate a patch 70

Local Patching Manager 77
Download and save patches, serviceability updates, and service packs 78
Access the Local Patching Manager 78
Add a service pack 80
View service pack details 82
Delete a service pack 84
Activate a service pack 85
Add a patch 90
View patch details 91
Activate patches 92
Deactivate a patch 96
Delete a patch 98

CLI commands 101
Target patch and serviceability update commands 103
- pstat 104
- plis 104
- pload 105
- pins 106
- poos 107
- pout 107

Target service pack commands 108
- issp 108
- spstat 109
- spload 110

spins 110
spout 111

Patch maintenance 113

New in this release

The following sections detail what's new in *Patching Fundamentals* (NN43001-407) for Nortel Communication Server 1000 Release 6.0:

- "Features" (page 8)
- "Other changes" (page 9)

Features

Patching Fundamentals (NN43001-407) is new for CS 1000 Release 6.0.

Other changes

Revision history

June 2009	Standard 01.03. This document is updated for Communication Server 1000 Release 6.0.
May 2009	Standard 01.02. This document is updated for Communication Server 1000 Release 6.0.
May 2009	Standard 01.01. This document is a new NTP for Communication Server 1000 Release 6.0.

How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the telephone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Introduction

This document contains the following topics:

- "Overview" (page 17)
- "Patching Manager overview" (page 27)
- "Central Patching Manager" (page 39)
- "Local Patching Manager" (page 77)
- "CLI commands" (page 101)
- "Patch maintenance" (page 113)

Subject

This document describes how to patch your system using Linux patching and Linux CLI commands. For information about Call Server patching, see *Element Manager System Reference - Administration* (NN43001-632). For information about VxWorks patching, see the Enterprise PEP Solution Library (ESPL) Web site.

ATTENTION
Before patching your system using the Patching Manager, make sure you consider concurrent coordinated patching of your entire system (in particular, with the Call Server).

Legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 6.0 (or later) software. For more information about legacy products and releases, click the Technical Documentation link under Support & Training on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

Intended audience

This document is intended for individuals who administer CS 1000 systems.

Conventions

Terminology

In this document, the following systems are referred to generically as system:

- Communication Server 1000E (CS 1000E)
- Communication Server 1000M (CS 1000M)

Unless specifically stated otherwise, the term Element Manager refers to the CS 1000 Element Manager.

Related information

This section lists information sources that relate to this document.

Technical documentation

This document references the following technical documents:

- *Unified Communications Management Common Services Fundamentals* (NN43001-116)
- *Subscriber Manager Fundamentals* (NN43001-120)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *SIP Line Fundamentals* (NN43001-508)
- *Network Routing Service Fundamentals* (NN43001-564)
- *Element Manager System Reference - Administration* (NN43001-632)

Online

To access Nortel documentation online, click the Technical Documentation link under Support & Training on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Overview

Patching Manager supports patching for all Linux-based elements in CS 1000 Release 6.0. This includes patching of Linux base components (operating system, base layer, and base applications) on these elements (except for Call Server on the Co-resident Call Server and Signaling Server).

> ***Note:*** Element Manager supports patching for the Call Server (on VxWorks or Linux) and other VxWorks devices (such as media cards).

Linux base supports three corrective content categories:

- Patch—Patches are used to fix bugs or for diagnostic purposes. In some instances, you can apply this category of patch without a program restart.
- Serviceability update—A serviceability update (SU) is a full-application RPM Package Manager (RPM) package distribution that you apply to a specific application, and replaces previous serviceability updates. An RPM is a Linux software standard for software updates.
- Service packs—A service pack (SP) is a single file that contains a bundle of multiple patches and serviceability updates for a specific product release.

This chapter contains the following topics:

- "Remote broadband connection" (page 18)
- "Linux patches" (page 18)
- "Serviceability updates" (page 19)
- "Patches" (page 20)
- "Service packs" (page 21)
- "Patch loading and unloading sequence" (page 24)
- "Obsolete patches" (page 24)

- “Patch dependencies” (page 25)
- “Patching impacts” (page 25)

Remote broadband connection

To successfully patch your system, you must have a secure remote broadband connection. This remote broadband connection is required to transfer files and to connect to the UCM interface.

Patches, serviceability updates, and services pack range in file size. Patches are small (a few kilobytes) while service packs can be 100 megabytes (MB) or greater in size. You need a secure broadband connection to successfully transfer these files to your target system.

Linux patches

Linux patching involves the patching of a specific version of an RPM. The RPM is the base building block of the Linux patching process.

RPM patches are issued only as serviceability updates and each serviceability update can contain only one RPM. Serviceability updates have the same file name as the RPM file that it contains; however, the serviceability update has a different file extension.

Patches are created and distributed against a specific RPM name and release. Patches have unique patch names, which are automatically generated by the patch library. Binary patches are linked to the RPM using the patch header.

All other patches on Linux (such as JAR, WAR, and FRU) are treated in the same manner and each is tied to a specific version or release of an RPM.

As a result, only two types of corrective content distributions exist for Linux:

- “Serviceability updates” (page 19)
- “Patches” (page 20)

ATTENTION
In this document, the term patch or patches includes both patches and serviceability updates (SUs) unless explicitly mentioned otherwise because patches and SUs are applied in the same way.

Linux also supports service packs. A service pack is a single file containing multiple patches and serviceability updates for a specific product release. For more information, see “Service packs” (page 21).

Patches cannot cross RPM boundaries. For example, a JAR patch cannot replace files in several RPMs. Patches and serviceability updates do not change the release of applications on the target.

Serviceability updates

Linux serviceability updates (SUs) are used to deliver new and updated RPMs to the target server.

A serviceability update contains the following:

- A header—The header information contains the product releases to which the SU is applicable. When the SU is loaded, the product release of the target is validated. If there is no match, the SU does not load.
- Two optional script files—A pre-patch script file (preScript.pl) and post-patch script file (postScript.pl). These files are predefined and are case sensitive.
- One optional readme file
- One RPM file

After the patch command finishes, if a post-patch script file is included with the patch, it loads and runs. If the post-patching script fails, then an attempt is made to reverse the operation. For example, if the script operation was an installation, then the script attempts to take it out of service.

In some cases, reversing the script may not succeed; for example, trying to remove an SU that is not removable. The SU has identification in the header on whether they are removable. Only kernel RPMs are known not to be removable. If you need to return to a previous state, Nortel must provide another SU to reverse the changes.

Because serviceability updates only replace RPMs, the version of the applications does not change.

ATTENTION
The **`swVersionShow`** command is not always affected by installing a serviceability update.

Serviceability updates are stored in the Serviceability Updates section of the patch library. (Patches are stored in a different area.) Serviceability updates are linked to the patching section of the patch library as releases of software. Each RPM is treated as its own release so patches can link it. The serviceability update is also linked in patch library to each product release for which it is applicable.

Naming conventions

The file name for a serviceability update is identical to the name of the RPM it contains. The file extension is changed from .rpm to .XXX.ntl (XXX is a unique number assigned by patch library and is the patch library issue of the SU). This naming convention follows the standard for RPM files but also allows for differences for Nortel purposes.

ATTENTION
Do not rename a serviceability update. The patching framework validates the serviceability update file name against the header contents.

The serviceability update file name contains the RPM name and release information for the RPM which, by default, is the name and release of the SU. The SU naming convention can therefore take into account third-party RPMs and Nortel-generated RPMs. Because the SU contains a new version of an RPM, this version replaces the version on the target and appears in commands that display RPM information. If there is any change (other than a RPM change), then the patch library issue is changed.

For example, the RPM file name for the minicom RPM is minicom-2.1-3.rpm

The first serviceability update issued is called minicom-2.1-3.000.ntl.

If there is a change and the readme file has to be modified, then the SU is upissued in patch library. The new SU is named minicom-2.1-3.001.ntl.

The naming convention identifies the exact contents of the file while preserving the RPM. As a result, an SU can be upissued and all patches still apply to the original minicom RPM with no changes or the need to be re-released.

If the minicom RPM changes release then all the patches are no longer applicable because all patches link to the RPM contained in the serviceability update.

For example, if the minicom RPM was changed to minicom-2.1-4, then the new serviceability update is called minicom-2.1-4.000.ntl.

Patches

Three types of patches are available:

- File Replacement Update (FRU)—An FRU is a simple patch type in that no extra packages must be generated for target file updates. An

FRU can be used for replace files, but files cannot be removed from the target machine using a FRU patch.

- Java Archive (JAR)—A JAR patch aggregates many files into one. Software developers generally use .jar files to distribute Java classes and associated metadata. Due to the way CS 1000 makes use of the J2EE (JBoss) applications, then it uses hierarchical class loaders. Therefore, the JAR is currently distributed using the FRU mechanism.
- Web Application Archive (WAR)—A WAR patch is a JAR file used to distribute a collection of JavaServer Pages, servlets, Java classes, XML files, tag libraries, and static Web pages (HTML and related files) that together constitute a Web application.

A patch contains the following:

- Header—The patch header contains information about applications and the product release.
- Optional scripts—Patches have optional scripts that function the same as the optional scripts for SUs.

Patches must be created against a specific name and version of an RPM. This information is in the file name of the RPM. The RPM file name is stored in the patch header and links the patch to the specific RPM for which it was created.

ATTENTION
Do not rename patches. The patching framework validates the patch file name against the header contents.

Linux patches are stored in the patch library in the same location as patches for the VxWorks platforms. Patches are stored against the RPM name and release they are linked to. In the patch library, links exist from the RPM to all related patches.

When you load a patch, the version and name of the RPM (which the patch is linked to) is checked. If the RPM name does not exist or if the RPM version does not match, then the patch is not loaded. Patching Manager filters out patches with a patch header product release that does not match the product release of the target.

Service packs

A service pack (SP) is a single file containing multiple patches and serviceability updates for a specific product release. The files are bundled in the service pack and a list of files is placed in the header. The service pack can also have optional script files attached that are similar to the scripts attached to an individual patch or serviceability update.

Individual patches and serviceability updates are extracted from the service pack and automatically placed in service. All patches and serviceability updates from the elements which are not in the header of the service pack are removed. The removal occurs automatically without prompting the user for input.

A service pack file has a .ntl file extension.

ATTENTION
Do not change the .ntl file extension. A service pack file name can be renamed to help you keep track of your updates using your preferred naming conventions. However, you must not change the .ntl file extension.

A service pack file can be large if it includes serviceability updates. Use the Meridian ISSP Report and Conflict Checker (MIRCC) to reduce the size of the service pack file. The MIRCC is on the ESPL. Service Packs can be dynamic and tailored to specific installations in the patch library similar to the deplist process by the use of the MIRCC tool. You can use the **`issp`** command on the target to list all installed RPMs, patches, and serviceability updates. MIRCC uses this information to include only the necessary files in the service pack to make the target current. The header file for the service pack contains the list of all serviceability updates and patches that MIRCC determined are needed to be running on the target. However, because the target can already have some of these files installed, only the missing files are included in the service pack. When the service pack reaches the target, the header information is used to determine which patches remain on the target element, which are removed, and which require updating.

Three types of service packs are available:

- Standard service pack—A standard service pack contains the generally available and emergency patches for a specified release.
- Standard + Site-specific service pack—A site-specific service pack contains additional patches or serviceability updates that are not in the standard service pack. These can be debug or limited customer-specific patches. The site-specific service pack may be missing patches or serviceability updates that are in the standard service pack. This can occur, for example, if an added serviceability updates replaces another serviceability updates that is in the standard service pack. Another case is if an added patch conflicts with another patch that is in the standard service pack.
- Target-specific service pack—A target-specific service pack is generated for a specific element. The service pack is obtained by passing in ISSP command output from the target element to the MIRCC tool. Any debug or limited customer-specific patches that are on the target are retained.

The first two types of service packs contain all the actual patches and serviceability updates for all applications. The target-specific service pack has a header that indicates all the required patches and serviceability updates for the target element. This list depends on the applications installed on the target element. The target-specific service pack only contains actual patches and serviceability updates that are not already present on the target element.

Consider the following when you apply service packs to target elements:

- If a target element has any debug or limited customer-specific patches, then application of a standard service results in removal of these patches. Either a site-specific service pack containing these special patches must be used, or a target-specific service must be generated for the target element.

  ATTENTION
  Applying a service pack will remove customer patches.

- A target-specific service pack is intended for a specific target element. However, you can apply such service packs to other targets but there may be errors. If the other targets do not have the same applications as on the intended target, then patches or serviceability updates may be missing and are not applied. If the other targets do not have the same patches and serviceability updates already installed as on the intended target, and these are still required, there are errors because these items are not in the service pack. This could include debug or limited customer-specific patches that are only on the intended target prior to generating the target-specific service pack. If other targets have other debug or limited customer-specific patches that are not on the intended target, these are removed after you apply the service pack.

Individual patches and serviceability updates contain which applications are stopped and started when they are placed in service. When a service pack is placed in service, the following events occur:

- Applications are stopped as requested by each patch or serviceability update.
- Applications do not start until the entire service pack is loaded.
- A list of applications to restart is maintained as each patch and serviceability update is loaded.
- Applications start automatically at the end of the service pack installation.

A service pack cannot be backed out. To reverse the changes put in by a service pack, you can do the either of the following:

- Reapply a previous service pack for the current release (if available)—If the service pack is updating from a previous service pack, then you can reapply that previous service pack. The previous service pack being reapplied must contain all removed patches.
- Note all the changes made by the service pack—Note the patches and serviceability updates that were added, the patches that were removed, and then reverse the changes. You may need to obtain individual patches from the patch library to complete this process.

Patch loading and unloading sequence

Use the following steps to load a service pack on the target using either the patch command line interface (CLI) commands or the Patching Manager application:

1. Remove all serviceability updates that are no longer needed or will be replaced. (The unload utility removes all patches associated with the RPM contained within the serviceability update which is being removed.)
2. Unload all patches that are no longer needed.
3. Load new serviceability updates.
4. Load new patches.

Note: Operations such as application stop, start, restart, and system reboot are analyzed for service pack-contained patches and serviceability updates, and they are optimized to be invoked only once.

Obsolete patches

The Patch Management Enhancement Feature in Release 6.0 provides functionality to remove obsolete patches automatically on the VxWorks platform. The header of the patch contains a list of patches that the current patch makes obsolete. The patches in this header list must be removed before this patch is placed in service. A patch can only obsolete another patch on the same RPM.

To achieve this same functionality in the Linux platform, the patches must be removed manually when you apply individual patches. When using the Patching Manager, you are provided with this information in a service impact. You must manually remove that particular patch by using the Deactivate button within the Central Patching Manager or the Local Patching Manager. For service packs, obsolete patches are automatically removed from the target.

In Patching Manager, you can find patch obsolescence details in two ways:

- You can view individual patch details by clicking the patch name hyperlink. The obsolete patch name is in the Obsolete field on the Patch Details page. If the patch does not make another patch obsolete, then the Obsolete field says None.
- The number of patches which need to become obsolete is indicated after preprocessing the patches selected by the user. You can find the information for the patches that must become obsolete on the Patching Job Details page by clicking the Patching Status Summary hyperlink. Under the Action column, note the patch names that have Deactivate (Obsolete) displayed for the patch name.

  Note: After preprocessing individual patches, the Patching Manager provides the following message: The obsolete patches need to be deactivated before activating the selected patches.

Patch dependencies

Patches are loaded one at a time in a serial fashion. As a result, patches can only have one dependant patch. If the dependant patch (for the patch currently being loaded) is not already loaded, then the current patch is not loaded. A dependent patch must be on the same RPM.

Patching impacts

Patching operations generally require application restarts or reboots. These actions occur automatically when the service pack or patches are applied, or when patches are removed.

If any Linux base application is restarted as the result of patching operations, this results in all Nortel applications being restarted. The Call Server running on a CP PM Co-resident Call Server and Signaling Server is included as a Nortel application. Use Base Manager to determine the Nortel applications running on a target.

When the Patching Manager is used for patching, two processing methods are available:

- Review impact for each target and run individually—With this manual processing method, the impact of applying the selected service pack or patch is analyzed. This is the default method. A patching plan is created and presented for each selected target element. After you review the patching plan, you must manually initiate the patching

operation for each element. You must take appropriate steps (such as idling down) prior to initiating patching to avoid user impact.

- Run all automatically—With this automatic processing method, each target element is patched automatically as soon as the analysis is complete.

WARNING
Service impacts are not considered with the automatic method. For example, applications can restart as part of this operation.

In the manual mode, application restarts or reboots are flagged. Review the potential impacts and take the necessary steps before you start patching.

ATTENTION
Nortel recommends using the manual mode of patching so you can review the impacts. The automatic mode is useful if you are patching during a maintenance window, when service impacts are permitted.

You may need to gracefully idle down the system or transfer operations to other redundant devices prior to patching. Impacts may extend to other systems in cases of network-wide virtual office or branch office scenarios. Some other applications can issue alarms or logs related to applications being restarted.

WARNING
Special attention is required if a CP PM Co-resident Call Server and Signaling Server is being patched. A reboot or restart of any Linux base application results in a restart of the Call Server component, with significant operational impact. Furthermore, any changes that were made to the Call Server configuration but not saved using an equipment data dump (EDD) would be lost. If required, the EDD must be performed prior to patching.

Patching Manager overview

The Patching Manager provides a graphical user interface (GUI) to upload and manage patches and service packs on the Linux targets in the enterprise network. The Patching Manager facilitates the centralized deployment of patches to all target Linux elements within the Unified Communications Management (UCM) security domain. For more information about UCM, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

This chapter contains the following topics:

- “Central and Local Patching Managers” (page 27)
- “Applications” (page 28)
- “Patching permissions and roles” (page 30)
- “Patching job queuing” (page 31)
- “Concurrent patching operation from Patch Manager user interfaces” (page 32)
- “Patch libraries” (page 32)
- “In Progress status information” (page 33)
- “Clearing patch activities” (page 34)
- “Recovery from failures ” (page 35)
- “Limitations” (page 36)

Central and Local Patching Managers

You can use Patching Manager on the primary security server to remotely deploy patches from a central location to other Linux servers on the same UCM domain (using the Central Patching Manager). You can also install patches locally. Local patching is accessible from the Base Manager of each Linux Element (using the Local Patching Manager).

Two interfaces support patch management:

1. Central Patching Manager—The Central Patching Manager is accessible from Primary UCM server. Central Patching Manager obtains the list of all Linux servers (or Linux Base Elements) in the same security domain from the UCM framework and can patch all Linux elements in the same security domain. For more information, see "Central Patching Manager" (page 39).
2. Local Patching Manager—The Local Patching Manager is accessible from the UCM Base Manager of each Linux element. You can access Base Manager using a central UCM logon or a local logon to the element. For more information, see "Local Patching Manager" (page 77).

WARNING
You cannot patch using Central Patching Manager and Local Patching Manager at the same time. You should not use the CLI patching commands while either the Central or Local Patching Manager are being used.

Patching Manager does not support patching of the Call Server, Media Gateway Controllers, and media cards. Element Manager supports Call Server and media card patching.

Applications

Patching Manager is a centralized patch deployment application used to patch all software components that run on the Linux elements (except for the Co-resident Call Server). The following table shows the list of software components that can be patched.

Table 1
List of applications

Application	Description
Signaling Server (SS)	The Signaling Server includes the following applications: • UNIStim Line Terminal Proxy Server (UNIStim LTPS) • H.323 Gateway (H.323 GW) • Session Initiation Protocol Gateway (SIP GW) • Failsafe Network Routing Service • MySQL For more information about the Signaling Server, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Table 1
List of applications (cont'd.)

Application	Description
Personal Directory (PD)	The Personal Directory allows a user to enter or copy names to a personal directory, and to edit and delete those entries. For more information about the Personal Directory application, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).
Network Routing Service (NRS)	The Network Routing Service includes the following: • SIP Proxy/Redirect Server • Gatekeeper (GK) • Network Connection Server (NCS) • NRS Manager (NRSM) • MySQL For more information about the NRS, see *Network Routing Service Fundamentals* (NN43001-564).
SIP Line (SIPL)	SIP Line Service fully integrates Session Initiation Protocol (SIP) endpoints in the CS 1000 system and extends the CS 1000 telephony features to the SIP clients. SIP Line is a stand-alone application. For more information about SIP Line, see *SIP Line Fundamentals* (NN43001-508).
Element Manager (EM)	Element Management includes the following: • Element Manager (EM) with Phone configuration • MySQL For more information about Element Manager, see *Element Manager System Reference - Administration* (NN43001-632).
Subscriber Manager (SM)	Subscriber Manager provides a centralized location for the management of subscriber information for enterprise services. For more information about Subscriber Manager, see *Subscriber Manager Fundamentals* (NN43001-120).
All other Linux applications, such as Deployment Manager, Base Manager, Patching Manager, IPSec configuration, SNMP Profile Manager.	Other Linux applications running on UCM elements.

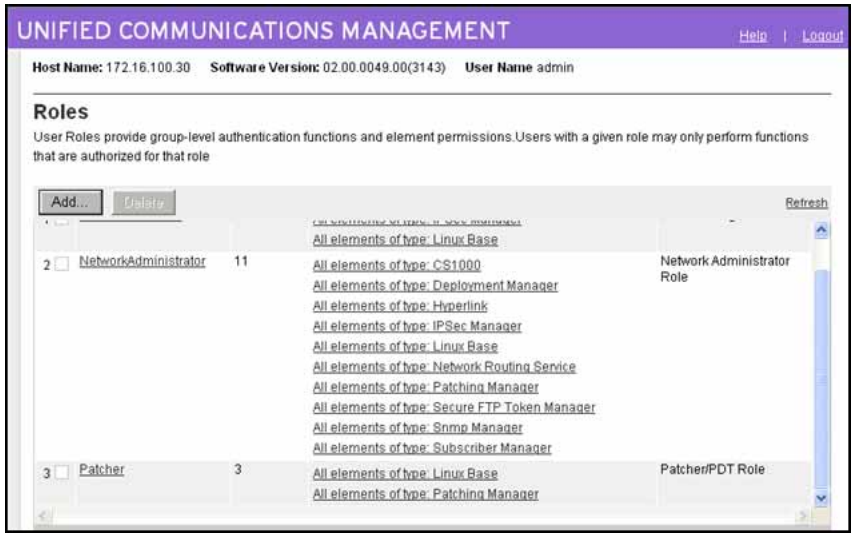
Table 1
List of applications (cont'd.)

Application	Description
Unified Communications Manager (UCM)	UCM provides an intuitive, common interface to manage and run managed elements. UCM is a container that stores several system management elements in a single repository. You have access to all network system management elements in UCM. For more information about UCM, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).
Operating System (Linux Base)	The CS 1000 Linux base system provides a Linux server platform for applications on a Pentium server. The platform can support Session Initiation Protocol Network Redirect Server (SIP NRS) and Unified Communications Management (UCM). For more information about the Linux base, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Patching permissions and roles

Central Patching Manager access is controlled by being allowed access to All Elements of type: Patching Manager for a role assigned to the user. UCM includes two built-in roles that provide this access: NetworkAdminstrator and Patcher.

Figure 1
Roles



In the UCM navigation tree, the Patches link does not appear if the user does not have a role with this access (All Elements of type: Patching Manager). To view the UCM navigation tree, see (Figure 5 "UCM navigation tree (Patches selected)" (page 43)).

The default account, called Admin, has the default NetworkAdminstrator role. To use the default Patcher role, create an account and assign the Patcher role to that account. You can also create a new role with All Elements of type: Patching Manager access and assign the role to a user.

For more information about accounts and roles, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Patching job queuing

To avoid excessive Primary UCM server resource consumption and network activity, only a limited number of patching operations can run concurrently. The activities are classified as follows:

- preprocessing to analyze the impact of patch application or deactivation, and which patches are applicable to targets
- actual application or deactivation of patches

Two queues are maintained for these two classes of activities. The queues hold the patching activities of all users and are maintained on a first in, first out (FIFO) basis. There is a limit imposed of three concurrent activities. For example, there can be two targets that are being preprocessed and another target being patched. If there is a mixture of preprocessing and patching activities, at least one patching activity will be running.

The sequence of patching is that preprocessing always occurs first for a target, followed by patching of the target.

- For automatic mode of patch application, the activity is first in the preprocessing queue and later in the patching queue.
- For manual processing, the activity enters the patching queue after the user verifies the impact and proceeds with activation or deactivation.

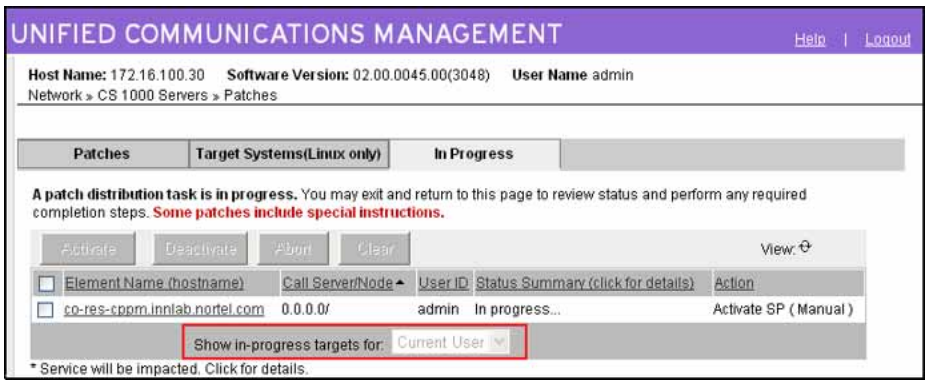
You may experience delays to their patching activities at times. For example, one user may have queued up patching activities for several targets. A second user initiating patching will find that activities are not started until the queued activities of the first user have completed. The In Progress tab is used to view all patching activities for all users. This can be used to estimate when activities would be initiated.

Concurrent patching operation from Patch Manager user interfaces

Multiple patch administrators can perform patching operations on various Linux targets through different UCM sessions. Up to five administrators can perform patching operations at a time. However, different administrators are blocked from patching the same target at the same time.

Any administrator with patching permissions can see the current patching operations being performed by any other administrator. An administrator can take over any patching operation initiated by another administrator (for example, clearing completed operations, proceeding with patching). In such cases, a warning is issued that another administrator had control, and if the user proceeds they are designated as the new owner of the activity for that target.

Figure 2
Show in-progress targets list



Patch libraries

Nortel supports the Enterprise Solutions PEP Library (ESPL), which provides online access to Nortel-approved Product Enhancement Package (PEP) solutions for Enterprise products. Use the ESPL Web site to first download and save patches, serviceability updates, and service packs to your local PC. The patches, serviceability updates, and service packs must then be added to the patch libraries using the Central or Local Patching Manager interfaces.

Normally a single UCM security domain exists for every customer enterprise network. As a result, there is a central patch library on the Primary UCM server for that UCM domain. Use the Central Patching Manager to add patches, serviceability updates, and service packs to the central patch library.

The Local Patching Manager works with patches, serviceability updates, and service packs in the normal storage locations as the equivalent CLI patching commands. No patch library maintained by the Local Patching Manager. Each Linux target element has a folder to store patches, serviceability updates, and service packs. No patch libraries are maintained on the element but you can use the Local Patching Manager to add and install any patch, serviceability update, or service pack on the target.

In Progress status information

In both the Central and Local Patching Manager, an In Progress tab appears when patching activity is taking place. This tab provides status information about the patches, serviceability updates, and service packs being activated or deactivated on the target elements. In particular, the Status Summary column on this tab provides status information.

Figure 3 "In Progress tab - Status Summary column" (page 33) shows the some of the provided status information. Note that some statuses appear as hyperlinks. Click the link to obtain additional status information.

Table 2 "Status information" (page 34) lists and describes the statuses displayed on the In Progress tab.

Figure 3
In Progress tab - Status Summary column

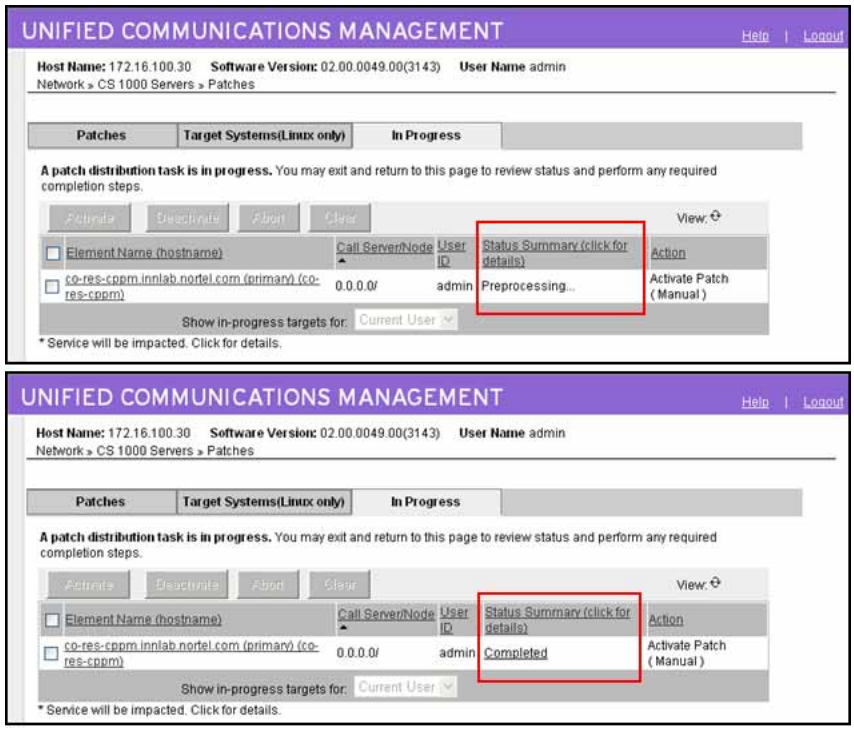


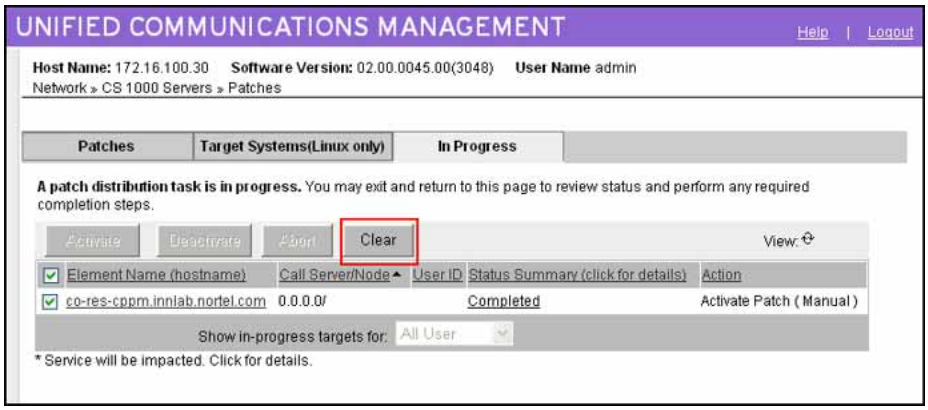
Table 2
Status information

Status	Description
Queued for Analysis	The target is placed into queue for analysis before preprocessing the selected patches with the target information.
Preprocessing	Currently preprocessing the selected patches with the target information. If there are activities queued up then it could take some time for the preprocessing to be done.
No Impact	This status is set after preprocessing (during patch activation process), if the selected patches are already in service on the target or the patch is not applicable if the required RPM is not installed.
Ready to load	The target is ready for patch activation process; this occurs once the preprocessing completes successfully.
No action required: Patches absent	This status is set after preprocessing (during patch deactivation process), if the selected patches are not already in service.
Ready to deactivate	The target is ready for patch deactivation process. This status appears after the preprocessing completes successfully.
Queued for patching	The target is placed into queue either for patch activation or deactivation process.
In progress	Either patch activation or deactivation is in progress on the target.
Completed	Either patch activation or deactivation completed successfully.
Partially Completed	Either patch activation or deactivation completed with partial success.
Failed	Either patch activation or deactivation failed.

Clearing patch activities

All patching activities on a target element must be cleared on the element before further patching activities can start (such as patch activation or deactivation). Use the Clear button to end the patching activities for a selected target element.

Figure 4
Clear button



Patching activation and deactivation operations cannot occur on an element if the element is cleared. (That is, the target element should not appear on the In Progress tab.)

If any user is patching a target element (including yourself or another user), you cannot initiate new patching activities on that element. The patching must be cleared before you attempt to perform patching activities.

If any patching activities are in progress that are not cleared, then the In Progress tab appears when you log on to UCM (in addition to the Patches and Target Systems tabs). The In Progress tab shows the active patching activities on the elements (for you or for any other patching administrator).

The Clear button must not be used for targets unless the patching operation is finished. If a patching operation is taking excessively long, there could be rare cases that some internal error occurred and the patching status will never be updated. In this case, the Clear button may be used to clear out the information for the operation. A warning appears indicating that patching may still be in progress. The patching operation may have been completed or there could have been failures. After the clear, review the patching status on the target using Base Manager or the CLI, and perform the required actions.

Recovery from failures

When patching activities fail, you may need to perform manual clean up activities on the patching targets. The following situations require such clean up:

- Failure of service pack activations
- Failure of patch or serviceability updates activation or deactivation

These operations have several stages, such as a patch first being placed into a loaded state and then installed. If the failure occurs at a specific point, patches may move to a particular stage and have to be cleaned up. If a service pack is being activated, a failure at the loading stage can result in some patches being loaded. The service pack does not move to the installation stage if there are loading errors, so the patches are left in that state. Similarly, there can be deactivation failures that result in patches being left in a loaded state or not deleted. Patches that are being activated, can also be left in a loaded state if installation fails.

The following are related clean up activities. These relate to activities done using a service pack (if applicable) or individual patches:

- Patches or serviceability updates that are to be activated, deactivated, or obsoleted could be left in a loaded state. These patches or serviceability updates would have to be installed or unloaded as required.
- Some patches can be transferred and show up as Unloaded, but not loaded. Cleanup or activation would be required as appropriate.
- Patches to be deactivated may be in Unloaded state and have to be removed.
- When a service pack is applied, some installed patches may have been automatically removed because they were rendered obsolete. If the service pack installation fails it is necessary to reapply the patches that were removed.

Many of these activities may be accomplished using Local Patching Manager. For more information, see “Local Patching Manager” (page 77).

Limitations

The following limitations exist for the Central Patching Manager and Local Patching Manager:

- You cannot use Central and Local Patching Manager at the same time. You should not use CLI patching commands while either the Central or Local Patching Manager are being used.
- You can only patch the Primary UCM server by itself. If patching activities on other target elements are in progress, you cannot select or patch the primary UCM server.
- You must clear all patching activities on all targets before you can patch the Primary UCM server. That is, you must select an element and then click the Clear button.
- In Central Patching Manager, if you select the Primary UCM server on the Target Systems tab, then you cannot select any other element at the same time.

- If an element is currently being patched by another user, you cannot select that element (check box is dimmed) until activities for the element are cleared.
- If another user is registering or deploying new elements in Deployment Manager, these elements do not automatically show up in Central Patching Manager. Use the Refresh icon to display the list of active elements in the Central Patching Manager.

Central Patching Manager

The Central Patching Manager interface runs on the Primary UCM Security server and is accessible by logging on to UCM. A central patch library is available to which patches and service packs can be uploaded to the library and centrally deployed on all Linux elements in the security domain. The central patch library consists of patches, serviceability updates, and service packs on the Primary UCM Security server. You can add and remove patches, serviceability updates, and service packs from the central patch library.

ATTENTION
In this document, the term patch or patches includes both patches and serviceability updates (SUs) unless explicitly mentioned otherwise because patches and serviceability updates are applied in the same way.

This chapter provides procedures to perform the following in the Central Patching Manager:

- Add, activate, deactivate, and delete patches.
- Add, activate, and delete service pack. (Service packs cannot be deactivated; however, individual patches that are part of a service pack can be deactivated.)

You must have patching permissions to access the Central Patching Manager. For more information, see “Patching permissions and roles” (page 30).

Download and save patches, serviceability updates, and service packs

The Enterprise Solutions PEP Library (ESPL) provides online access to Nortel-approved Product Enhancement Package (PEP) solutions for Enterprise products.

- Patches are stored in the Communication 1000 /Meridian 1 Patch Tools section of the ESPL. Use Procedure 1 “Downloading and saving

patches" (page 40) to download the required FRU and WAR patches and save them on your client PC.

- Serviceability updates are stored in the Serviceability Updates and Loadware/Firmware Distribution Tools (CS1000) section of the patch library. Use Procedure 2 "Downloading and saving serviceability updates" (page 41) to download the required RPM SUs and save them on your client PC.
- Service packs are stored in the PEP Dependency Tools section of the ESPL. Use Procedure 3 "Downloading and saving service packs" (page 41) to download the required SPs and save them on your client PC.

Use the following procedure to download patches and save them on your client PC.

Procedure 1
Downloading and saving patches

Step	Action
1	Navigate to the ESPL on the Nortel Web site: www.nortel.com/espl
2	Log on with your User ID and Password.
3	On the Enterprise Solutions PEP Library page, click **Click Here**.
4	Scroll to **Communication Server 1000 / Meridian 1 PEP Tools**.
5	For the **PEP SEARCH** option, click **Click Here**.
6	Enter the search criteria for the patch that you need.
7	Click **Search**.
8	Select the required patch to download and save it to your PC.
9	Note the location in which you save the file on your PC. You need to know the location of the file when you add the file to the central patching library.

--End--

Use the following procedure to download serviceability updates and save them on your client PC.

Procedure 2
Downloading and saving serviceability updates

Step	Action
1	Navigate to the ESPL on the Nortel Web site: www.nortel.com/espl
2	Log on with your User ID and Password.
3	On the Enterprise Solutions PEP Library page, click **Click Here**.
4	Scroll to **Serviceability Updates and Loadware/Firmware Distribution Tools (CS1000)**.
5	For the **SU/LW/FW File Search** option, click **Click Here**.
6	Enter the search criteria for the serviceability update that you need.
7	Click **Search**.
8	Select the required serviceability update to download and save it to your PC.
9	Note the location in which you save the file on your PC. You need to know the location of the file when you add the file to the central patching library.

--End--

Use the following procedure to download service packs and save them on your client PC.

Procedure 3
Downloading and saving service packs

Step	Action
1	Navigate to the ESPL on the Nortel Web site: www.nortel.com/espl
2	Log on with your User ID and Password.
3	On the Enterprise Solutions PEP Library page, click **Click Here**.
4	Scroll to **PEP Dependency Tools**.
5	For the **RLS 6.0 Linux Production Service Packs** option, click **Click Here**.
6	Enter the search criteria for the service pack that you need.
7	Click **Submit**.
8	Select the required service pack to download and save it to your PC.

9	Note the location in which you save the file on your PC. You need to know the location of the file when you add the file to the central patching library.

--End--

Access the Central Patching Manager

Users must have patch administrator permissions (the patchAdmin permissions) to access Central Patching Manager. For more information, see “Patching permissions and roles” (page 30).

Use the following procedure to access the Central Patching Manager.

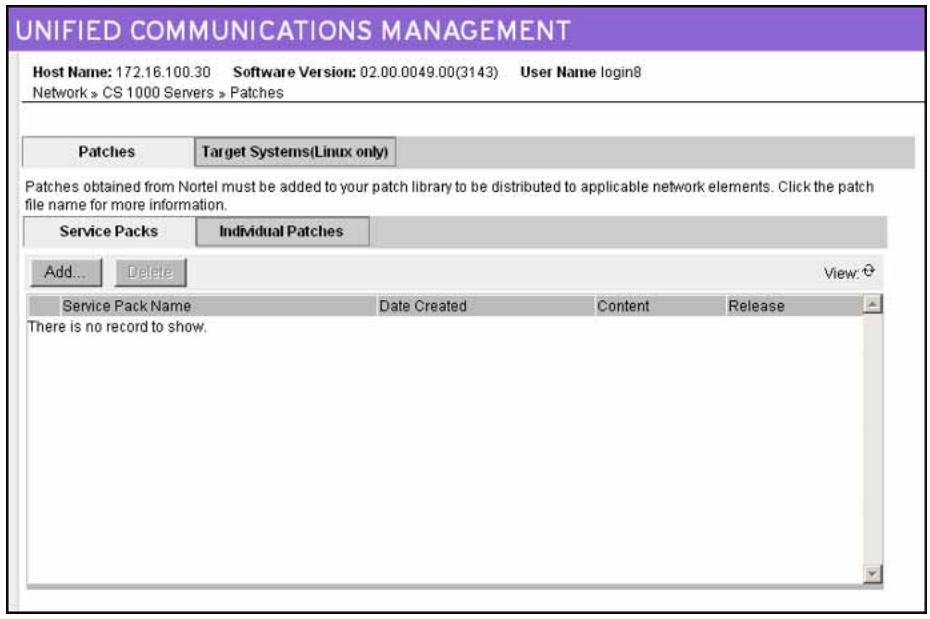
Procedure 4
Accessing the Central Patching Manager from the Primary UCM Server

Step	Action
1	Start your browser.
2	In the **Address** field of the browser, enter the Fully Qualified Domain Name (FQDN) of the server (or if the FQDN is not known then enter then IP address). • If the FQDN is entered, go to Step 4. • If the IP address is entered, go to Step 3.
3	Click the **Go to central login for Single Sign-On** link (on the left side of the Unified Communications Management (UCM) page).
4	Log in to UCM using an account with patching privileges. The UCM interface appears.
5	In the UCM navigation tree, select **Network > CS 1000 Services > Patches**.

Figure 5
UCM navigation tree (Patches selected)

The Central Patching Manager appears. See Figure 6 "Central Patching Manager" (page 44).

Figure 6
Central Patching Manager



The Central Patching Manager has two main tabs at the top of the page: Patches and Target Systems (Linux Only).

ATTENTION
If any in progress patching activities are active (not cleared), a third tab called In Progress appears when you log on to UCM and shows the active patching activities on the elements (for you or any other patch administrator). The In Progress tab appears only when patch distribution is in progress (and then the tab is selected by default).

The Patches tab has two sub-tabs for Service Packs and Individual Patches.

- Service Packs: On the Service Packs tab, you can add service packs to the central patch library or delete them from the central patch library. You can also view service patch details for added service packs. You can perform the following procedures from the Service Pack tab:
  - — Procedure 5 “Adding a service pack” (page 45)
  - — Procedure 6 “Viewing service pack details” (page 47)
  - — Procedure 7 “Deleting a service pack” (page 50)
- Individual Patches: On the Individual Patches tab, you can add patches or serviceability updates to the central patch library or you can delete them from the central patch library. You can also view patch details for added patches. You can perform the following procedures from the Individual Patches tab:

— Procedure 8 “Adding a patch” (page 51)

— Procedure 9 “Viewing patch details” (page 53)

— Procedure 10 “Deleting a patch” (page 55)

The Target Systems (Linux only) tab shows a list of elements that can be patched. This page provides a list of patchable targets (Linux Base Elements) with Call Server and Cluster association, applications, and release details for each target element. You can click an Element Name and then Base Manager opens and displays information about currently deployed patches. You can perform the following procedures from the Target Systems tab:

- Procedure 11 “Activating a service pack” (page 56)
- Procedure 12 “Activating patches” (page 63)
- Procedure 13 “Deactivating a patch” (page 70)

--End--

Add a service pack to the central patch library

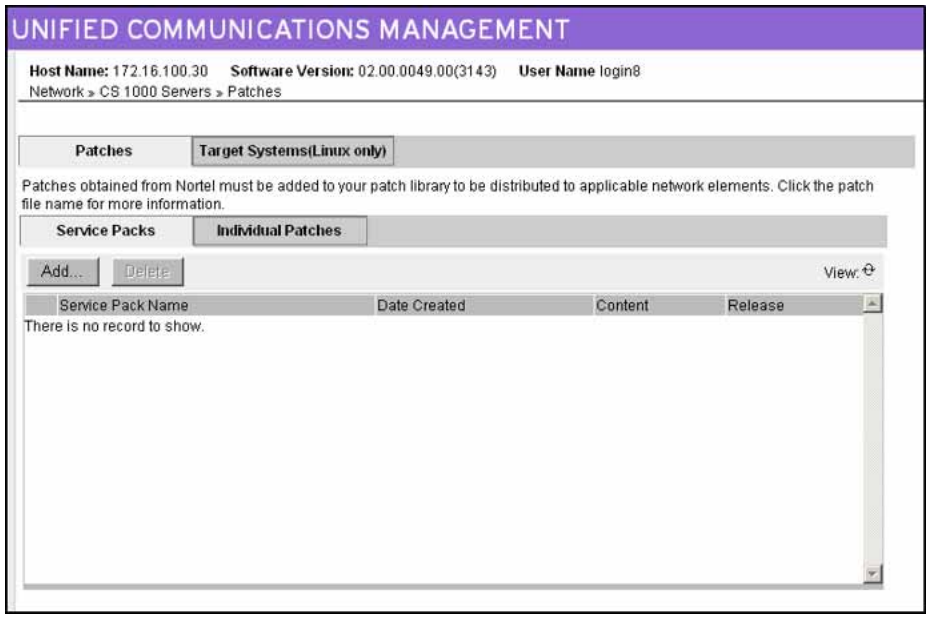
Use the following procedure to add a service pack to the central patch library. The file name of a service pack is similar to Nortel_Service_Pack_Linux_6.00_12.ntl. You must have downloaded and saved the service pack to a location accessible from your local PC before you can add it to the central patch library. For more information, see Procedure 3 “Downloading and saving service packs” (page 41).

Note: Uploading a large service pack can take a significant amount of time (15-30 minutes or longer) depending on the size of the service pack.

Procedure 5
Adding a service pack

Step	Action
1	In the Patching Manager, ensure the **Patches** tab is selected.
2	Select the **Service Packs** tab.

Figure 7
Patches tab - Service Packs tab



3 Click **Add**.

The New Service Pack page appears.

Figure 8
New Service Pack

4 Click **Browse**.

The Choose File dialog box appears.

5 In the **Choose File** dialog box, browse to the find the service pack on your client PC.

6 Select the service pack file, and click **Open**.

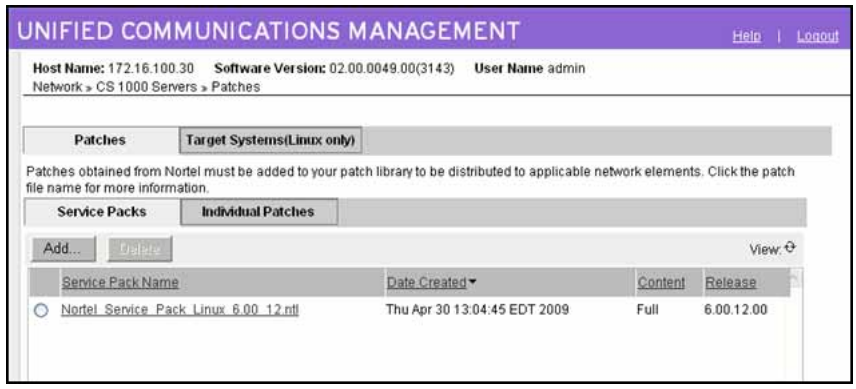
The file appears in the File field.

7 Click **Upload**.

The upload progress is indicated by a status bar at the bottom of the screen. The Central Patching Manager validates the file and then the service pack file appears on the Service Pack tab. The

Service Pack tab displays the new service pack and its details. For more information, see “View service pack details” (page 47).

Figure 9
Service pack added



--End--

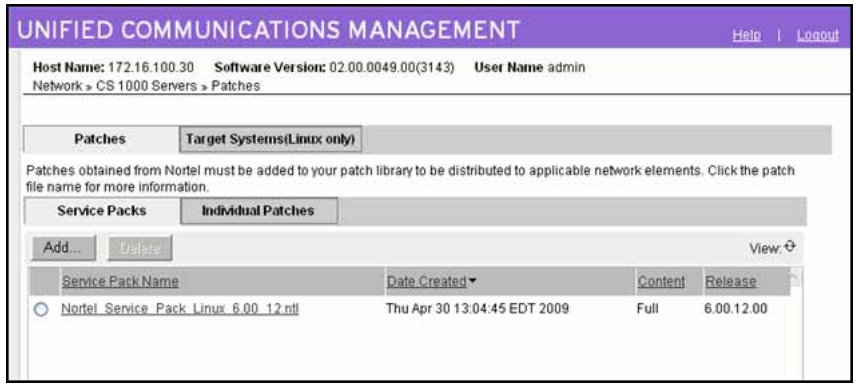
View service pack details

Use the following procedure to view the details about a service pack and the individual patches and serviceability updates that it contains. The Service Pack Details page displays important details about a service pack and patches such as header information.

Procedure 6
Viewing service pack details

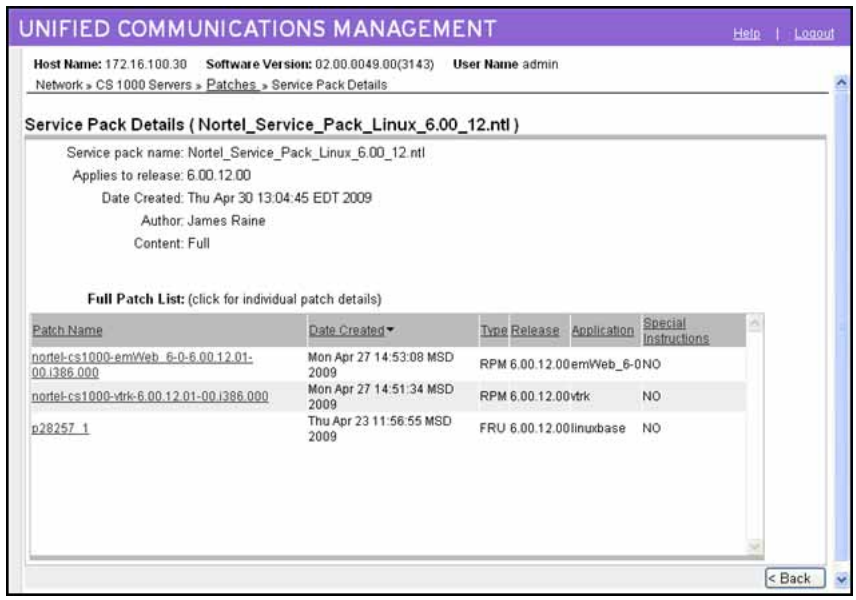
Step	Action
1	In the Central Patching Manager, select the **Patches** tab.
2	Select the **Service Packs** tab.
3	To view details of the service pack, under the **Service Pack Name** column, click the name of the service pack file.

Figure 10
Service Packs tab



The Service Pack Details (sp_name) page appears; sp_name is the name of the service pack.

Figure 11
Service Pack Details page



4 On the **Service Pack Details (sp_name)** page, review the detailed information about the service pack.

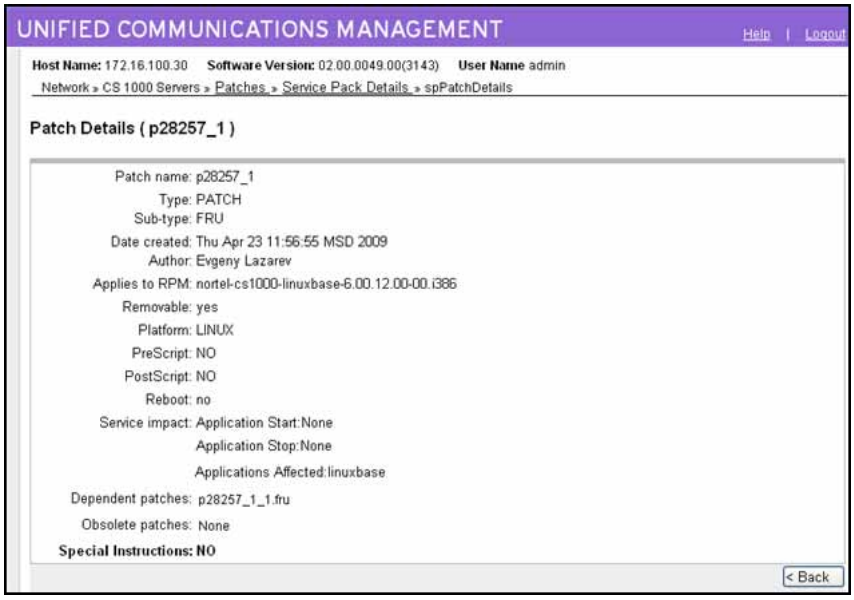
The page provides the following information about the service pack:

- Patch Name—The name of the patches or serviceability updates within the service pack.
- Date Created—The date the patch or serviceability update was created.
- Type—The patch or SU type.
- Release—The software release that the patch or serviceability update is applies to.
- Application—The applications affected by the patch
- Special Instructions—Whether there are special instructions. YES appears if the patch has special instructions and NO appears if the patch has no instructions.

5 To review an individual patch in the service pack, under **Patch Name**, click the name of the patch.

The Patch Details (patch_name) page appears; patch_name is a name of a patch in the service pack. The Patch Details page provides information such as patch name, type and sub-type, general patch information, service impacts, dependent patches, obsolete patches, special instructions, and other details from the patch header.

Figure 12
Patch Details



6 To return to the **Service Pack Details** page, click **Back** on the **Patch Details** page.

7 To return to the **Service Packs** tab, click **Back** on the **Service Pack Details** page.

--End--

Delete a service pack from the central patch library

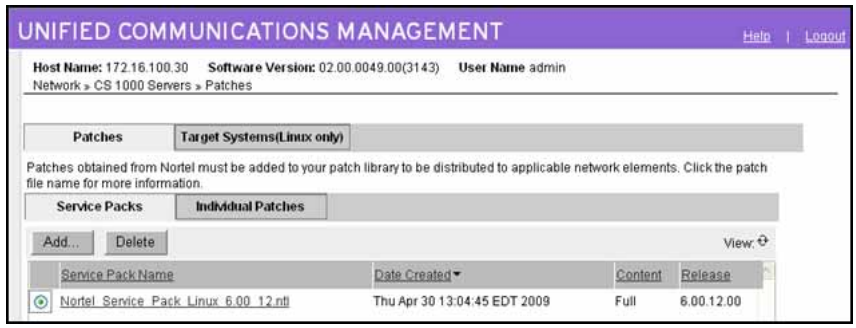
Use this procedure to delete a service pack from the central patch library. Deleting a service pack from the central patch library does not delete it from any target.

ATTENTION
A service pack cannot be recovered after it is deleted.

Procedure 7
Deleting a service pack

Step	Action
1	In the Patching Manager, ensure the **Patches** tab is selected.
2	Select the **Service Packs** tab.
3	Select the option button for the service pack you want to delete.

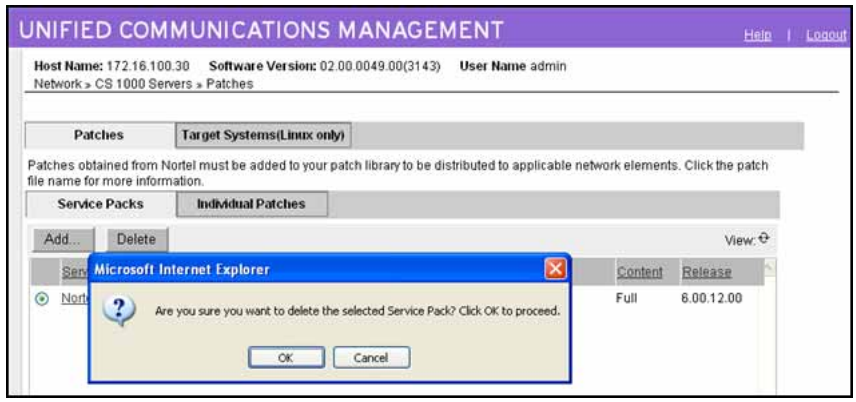
Figure 13
Select service pack



4 Click **Delete**.

A dialog box appears prompting you to confirm the service pack deletion.

Figure 14
Confirm deletion



5 Click **OK** to confirm the deletion of the service pack.

The service pack is removed from the list on the Service Packs tab.

--End--

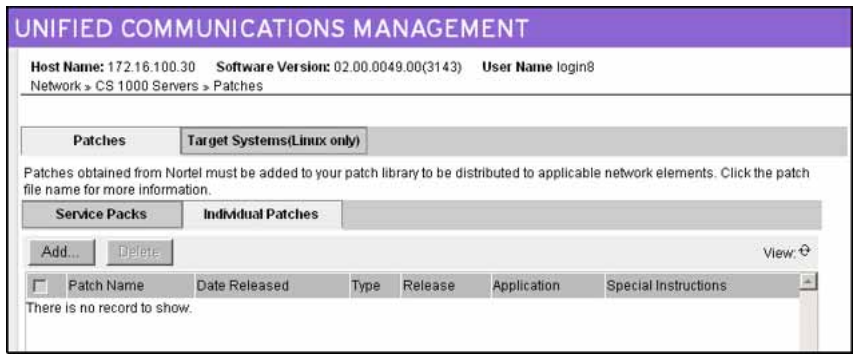
Add a patch to the central patch library

Use the following procedure to add a patch to the central patch library. You must have downloaded and saved the patch that you need to your local PC before you can add it to the central patch library. For more information, see Procedure 1 “Downloading and saving patches” (page 40).

Procedure 8
Adding a patch

Step	Action
1	In the Central Patching Manager, select the **Patches** tab.
2	Select the **Individual Patches** tab.

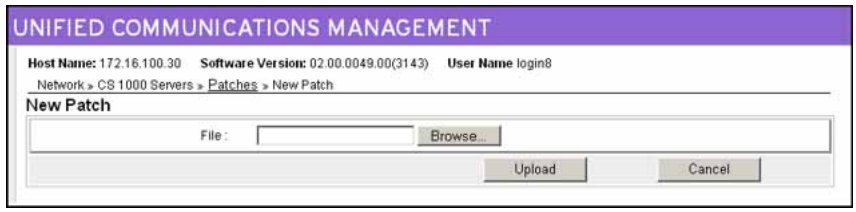
Figure 15
Patches tab - Individual Patches tab



3 Click **Add**.

The New Patch page appears.

Figure 16
New Patch



4 Click **Browse**.

The Choose File dialog box appears.

5 In the **Choose File** dialog box, browse to the find the downloaded patch on your client PC. Patch files have an .ntl file extension.

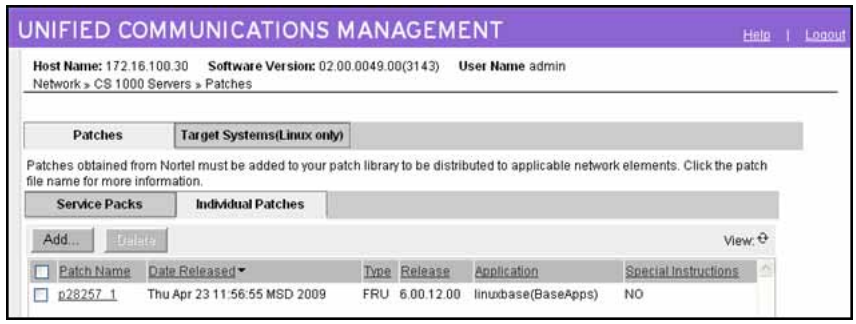
6 Select the patch file, and click **Open**.

The file appears in the File field.

7 Click **Upload**.

The upload progress is indicated by a status bar at the bottom of the window. The Central Patching Manager validates the file and then the patch file appears on the Individual Patches tab.

Figure 17
Added patch



The Individual Patches tab displays the new patch and its details:

- Patch Name—The name of the patch or serviceability update.
- Date Released—The date and time the patch was released. Patches are sorted based on the Date Release column.
- Type—The type of patch. A patch appears as type FRU or WAR. A serviceability update appears as type RPM.
- Release—The software release number.
- Application—The application for which the patch applies.
- Special Instructions—Whether there are special instructions. YES appears if the patch has special instructions and NO appears if the patch has no instructions.

For more information about viewing the patch details, see "View patch details " (page 53).

--End--

View patch details

Use the following procedure to view the details about a specific patch that is in the central patch library. The Patch Details page displays important details about the patch such as header information.

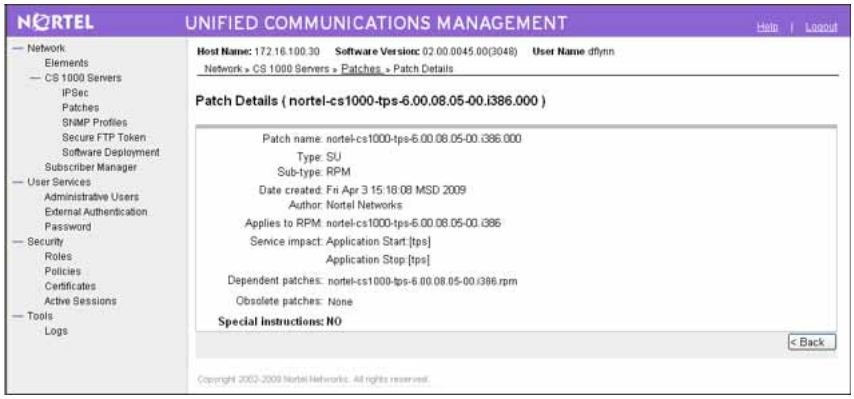
Procedure 9
Viewing patch details

Step	Action
1	In the Patching Manager, select the **Patches**.
2	Select the **Individual Patches** tab.

3 To view details for a patch, under the **Patch Name** column, click the patch name.

The Patch Details (patch_name) page appears; patch_name is the name of the patch.

Figure 18
Patch Details (patch_name)



4 On the **Patch Details (patch_name)** page, review the detailed information about the patch.

The Patch Details page provides the following information:

- Patch name—The name of the patch.
- Type—Patch or SU (Serviceability Update)
- Sub-type— If the type is patch, then the subtype is FRU or WAR. If the type is SU, then the subtype is RPM.
- Date created—The date and time the patch was created.
- Author—The author appears.
- Applies to RPM—Provides the RPM name and version to which the patch applies. For a serviceability update, the field provides the new version of the RPM that is contained in the serviceability update.
- Removable—Whether the patch is removable or not.
- Platform—The platform appears.
- PreScript—Whether there is a prepatch script file.
- PostScript—Whether there is a postpatch script file.
- Reboot—Whether a system reboot is required.
- Service impact—Provides a list of service impacts. For example, if an application must stop or start.

- Dependent patches—Because patches are loaded one at a time in a serial fashion, patches can have only one dependant patch. If the dependant patch (for the patch being loaded) is not already loaded then the patch will not load. A dependent patch can only be on the same RPM.
- Obsolete patches—The most recently uploaded patch makes any listed patch obsolete.
- Special instructions—Lists any special instructions or considerations for the patch; otherwise, NO is displayed.

5 To return to the **Individual Patches** tab, click **Back** on the **Patch Details** page.

--End--

Delete a patch from the central patch library

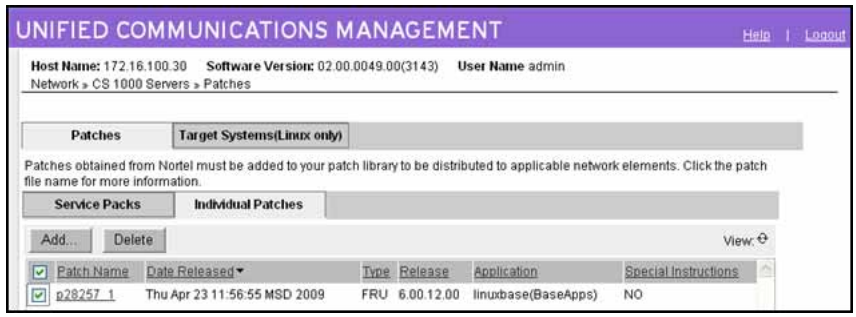
Use this procedure to delete a patch from the central patch library. Deleting a patch or serviceability update from the central patch library does not deactivate or delete it from any target.

ATTENTION
Patches and serviceability updates cannot be recovered after they are deleted.

Procedure 10
Deleting a patch

Step	Action
1	In the Patching Manager, select the **Patches** tab.
2	Select the **Individual Patches** tab.
3	Select the check box for the patch or serviceability update you want to delete.

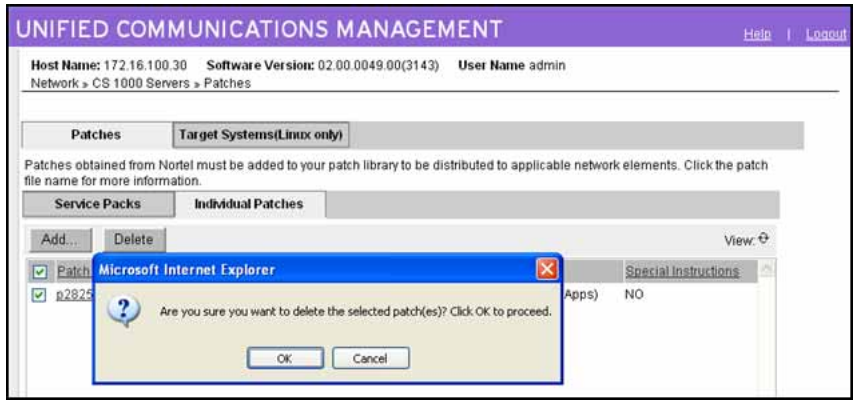
Figure 19
Select patch



4 Click **Delete**.

A dialog box appears prompting you to confirm the patch deletion.

Figure 20
Confirm patch deletion



5 Click **OK** to confirm the deletion of the patch.

The patch is removed from the list.

--End--

Activate a service pack

Use the following procedure to apply a service pack to one or multiple elements. The service pack must be in the Central Patching Library.

Procedure 11
Activating a service pack

Step	Action
1	In the Patching Manager, select the **Target Systems (Linux only)** tab.
2	From the list of elements, select the check box for one or more elements for which you want to apply the service pack.

ATTENTION
If you select the Primary UCM server on the Target Systems tab, no other element can be selected at the same time.

If an element is being patched by another user, you cannot select that element (check box is dimmed) until all patching activities for that element are cleared.

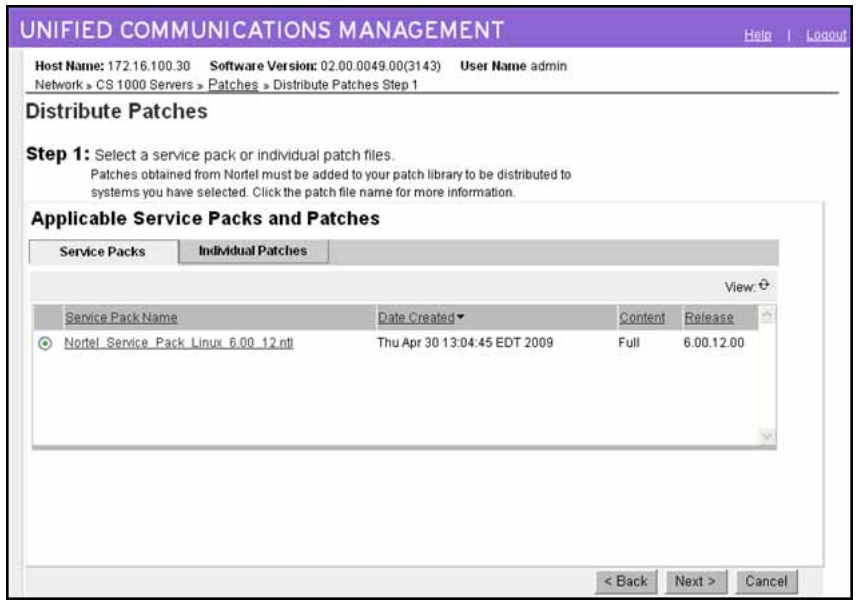
Figure 21
Select element to receive service pack

The Activate button is enabled.

3 Click **Activate**.

The Distribute Patches Step 1 page appears. Applicable service packs are displayed on the Service Packs tab (based on the release of the selected elements and the applications installed on them).

Figure 22
Distribute Patches Step 1 page



4 On the **Distribute Patches Step 1** page, ensure the **Service Packs** tab is selected.

5 Select the applicable service pack to apply on the elements.

ATTENTION
You can select only one of the following to activate at any one time:

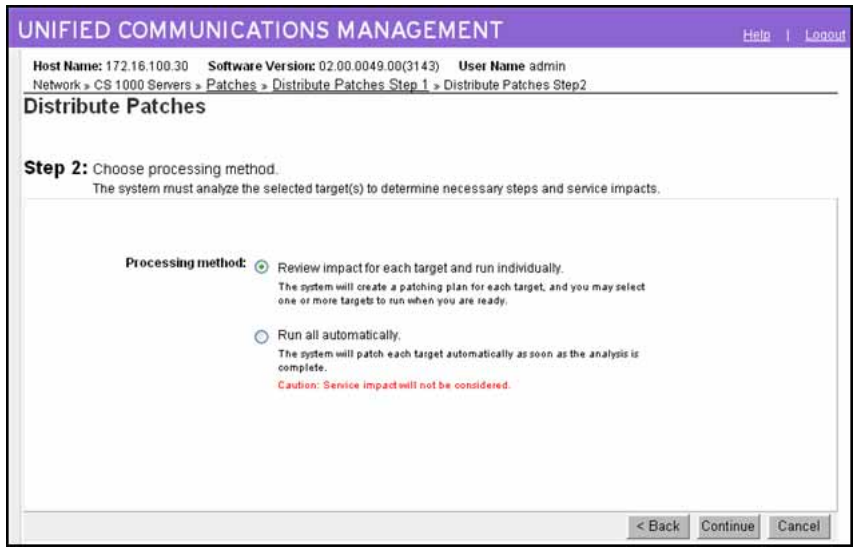
- A single service pack
- Multiple patches and serviceability updates

You cannot mix activation of service packs with patches and serviceability updates.

6 Click **Next**.

The Distribute Patches Step 2 page appears.

Figure 23
Distribute Patches Step 2



7 On the **Distribute Patches Step 2** page, select the **Processing method**.

- **Review impact for each target and run individually**—With this manual processing method, the impact of applying the selected service pack or patch is analyzed. This is the default method. A patching plan is created and presented for each selected target element. After you review the patching plan, you must manually initiate the patching operation for each element. You must take appropriate steps (such as idling down) before you start patching to avoid user impact.

WARNING
If you are patching the Primary UCM server then this is the only option. Nortel strongly advises that you review the impact of patching the Primary UCM server and be aware of any application restart or reboot. If there is an indication of a JBoss restart or reboot during the patching operation, then the Web session will be dropped. You must then log on again.

WARNING
When you review the impacts for a given target, if there is an indication of a JBoss-Quantum restart or reboot during the patching operation, be aware that all Nortel applications will also be restarted.

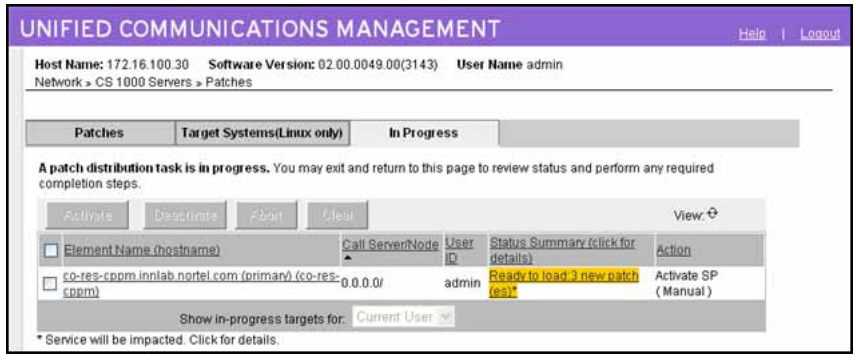
- **Run all automatically**—With this automatic processing method, each target element is patched automatically as soon as the analysis is complete.

WARNING
Service impacts are not considered with the automatic method. For example, applications can restart as part of this operation.

8 Click **Continue**.

The In Progress tab appears and shows the number of patches which are ready to load (under the Status Summary column).

Figure 24
In Progress tab



ATTENTION
Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

9 If you selected the **Review impact for each target and run individually** option in Step 7, the targets are analyzed based on the current patch information obtained from the target and the service pack to be applied. Complete Step 10 to Step 13 and then proceed to Step 14.

OR

If you selected the **Run all automatically** option in Step 7, the targets are analyzed based on the current patch information obtained from the target and the service pack to be applied. Unless there are errors detected, the patch application proceeds automatically without waiting for your user input. Proceed to Step 14.

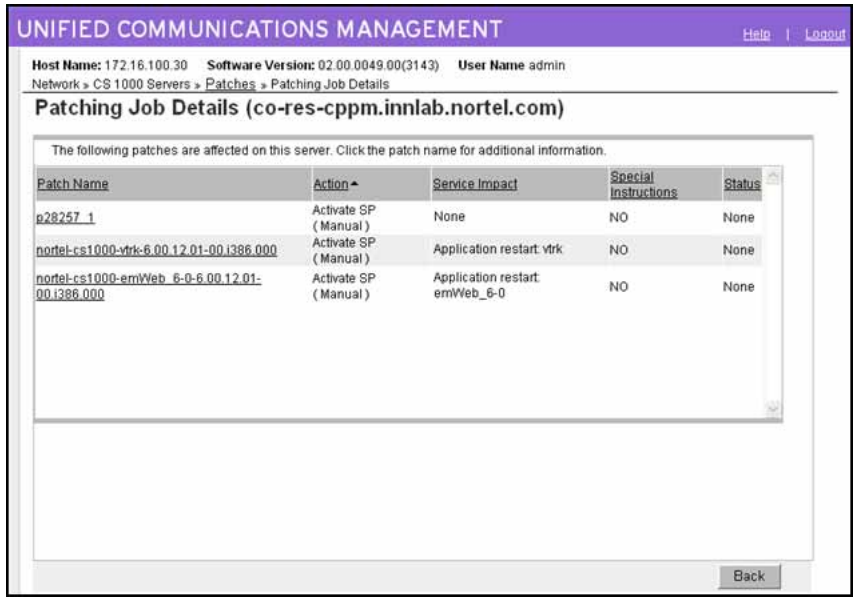
10 Wait for the status to change in the **Status Summary** column. The Status Summary provides information about the patch activation progress. For more information about the statuses displayed, see Table 2 "Status information" (page 34).

Use the Refresh icon to see the progress updates.

11 Under the **Status Summary** column, click the **Ready to Load** link for each target element to view the patching plan details for that target.

The Patching Job Details page appears for the selected element and displays the list of patches and serviceability updates within the service pack.

Figure 25
Patching Job Details page

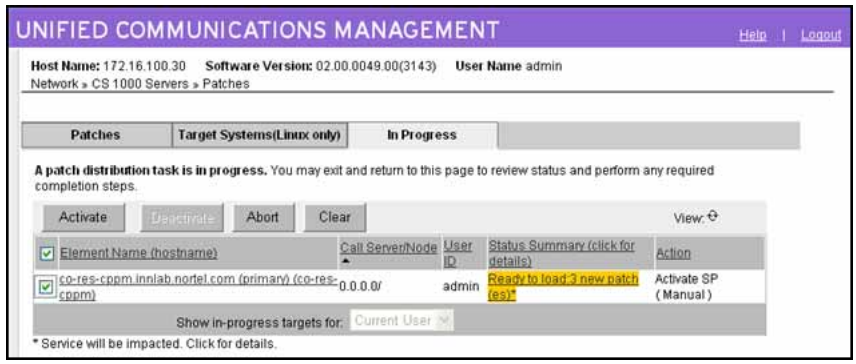


To view details for a specific patch, click the link under the **Patch Name** column. The Patch Details page appears.

12 After you review the identified service impacts in the patching plan, click **Back** on the **Patch Details** page, and then click **Back** again on the **Patching Job Details** page to return to the **In Progress** tab.

13 Select the check box for the target element and then click **Activate** to apply patches within the service pack.

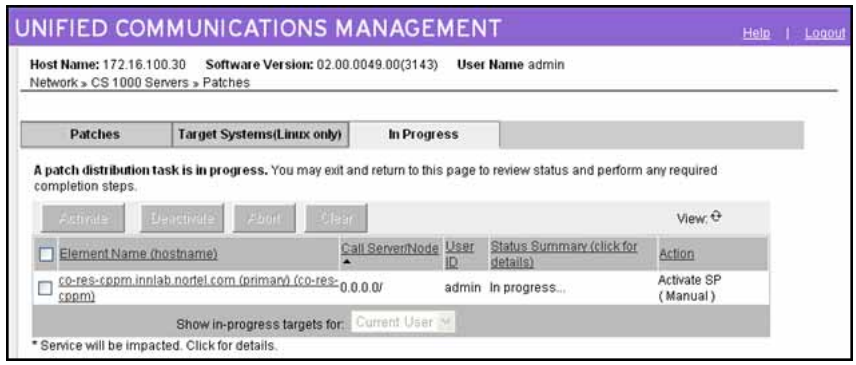
Figure 26
Activate service pack on target element



14 Wait while the updates are applied to the target element.

Note: Depending on the size of the service pack, it can take some time to activate a service pack.

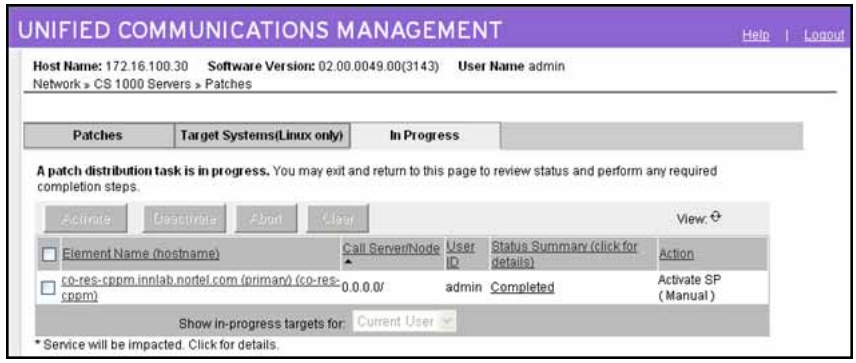
Figure 27
Service pack activation in progress



15 Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

16 Wait until the updates are completed on the target. The **Status Summary** column indicates when the service pack activation is **Completed**.

Figure 28
Activation complete



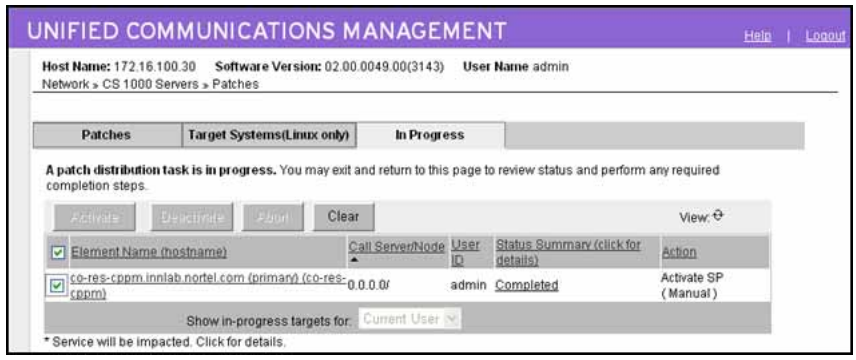
17 To view the results, under the **Status Summary** column, click the **Completed** link.

The Patching Job Details (target_name) page appears and the Status column indicates that the patch succeeded. For a service pack, the underlying operations and an overall result is provided.

18 On the **Patching Job Details (target_name)** page, click **Back**.

19 After you review your patching results and are satisfied with the results, select the check box for the target element, and then click **Clear** to end the patching process for the target element. You must click Clear before you can perform any other patch operations for this target element.

Figure 29
Clear button enabled



Further patching activation and deactivation operations cannot be performed on the element until it is cleared.

The In Progress tab disappears when all activities for all elements are cleared.

--End--

Activate patches

Use the following procedure to apply a patch to one or more target elements.

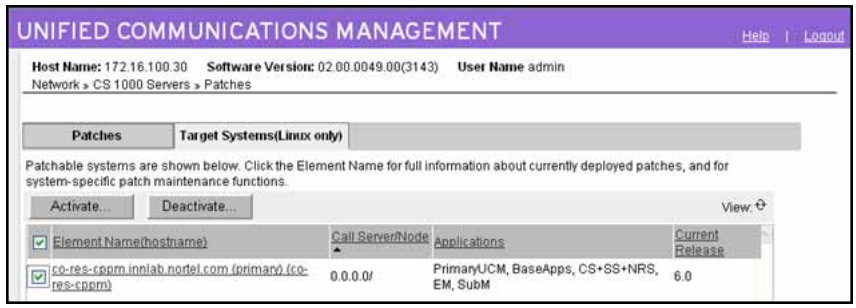
Procedure 12
Activating patches

Step	Action
1	In the Patching Manager, select the **Target Systems (Linux only)** tab.
2	From the list of elements, select the check boxes for one or more elements for which you want to apply the patches.

ATTENTION
If you select the Primary UCM server on the Target Systems tab, no other element can be selected at the same time.

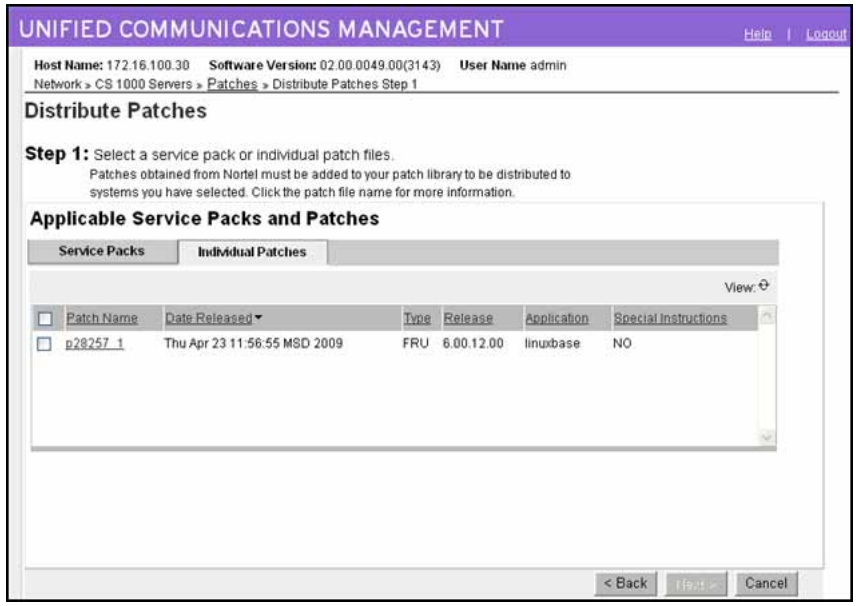
If an element is currently being patched by another user, you cannot select that element (check box is dimmed) until all patching activities for that element have been cleared.

Figure 30
Select target element



3	Click **Activate**. The Distribute Patches Step 1 page appears.
4	On the **Distribute Patches Step 1** page, select the **Individual Patches** tab. Applicable patches and serviceability updates are displayed (based on the release of the selected elements).

Figure 31
Distribute Patches Step 1 page



5 Select the check boxes for the patches to apply on the elements.

ATTENTION
You can select only one of the following to activate at any one time.

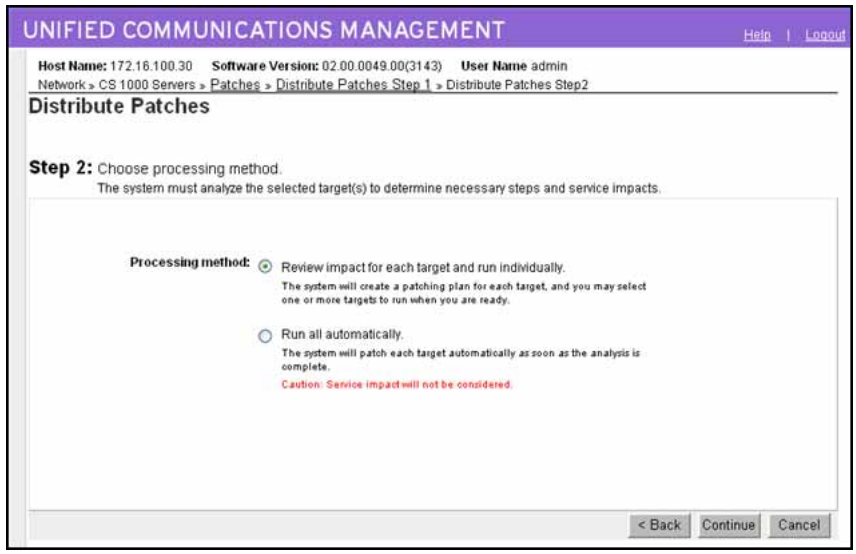
- A single service pack.
- Multiple patches and serviceability updates

You cannot mix activation of service packs with patches and serviceability updates.

6 Click **Next**.

The Distribute Patches Step 2 page appears.

Figure 32
Distribute Patches Step 2



7 On the **Distribute Patches Step 2** page, select the **Processing method**.

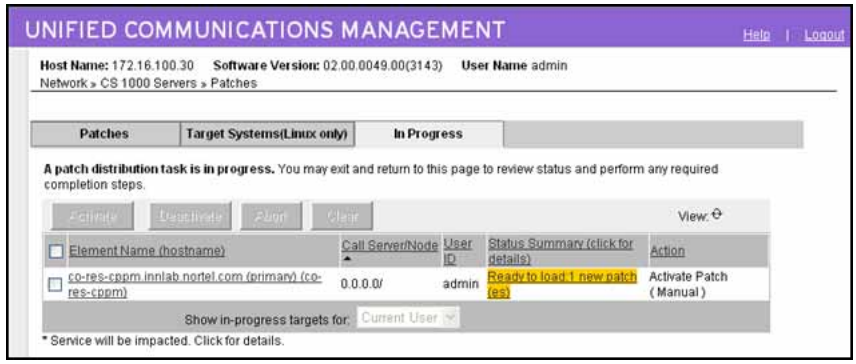
- **Review impact for each target and run individually**—With this manual processing method, the impact of applying the selected patch or serviceability update is analyzed. This is the default method. A patching plan is created and presented for each selected target element. After you review the patching plan, you must manually initiate the patching operation for each element. You must take appropriate steps (such as idling down) before you start patching to avoid user impact.
- **Run all automatically**—With this automatic processing method, each target element is patched automatically as soon as the analysis is complete.

WARNING
Service impacts are not considered with the automatic method. For example, applications can restart as part of this operation.

8 Click **Continue**.

The In Progress tab appears.

Figure 33
In Progress tab



ATTENTION
Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

9 If you selected the **Review impact for each target and run individually** option in Step 7, the targets are analyzed based on the current patch information obtained from the target and the new patches to be applied. Complete Step 10 to Step 13 and then proceed to Step 14.

OR

If you selected the **Run all automatically** option in Step 7, the targets are analyzed based on the current patch information obtained from the target and the new patches to be applied. Unless there are errors detected, the patch application proceeds automatically without waiting for your user input. Proceed to Step 14.

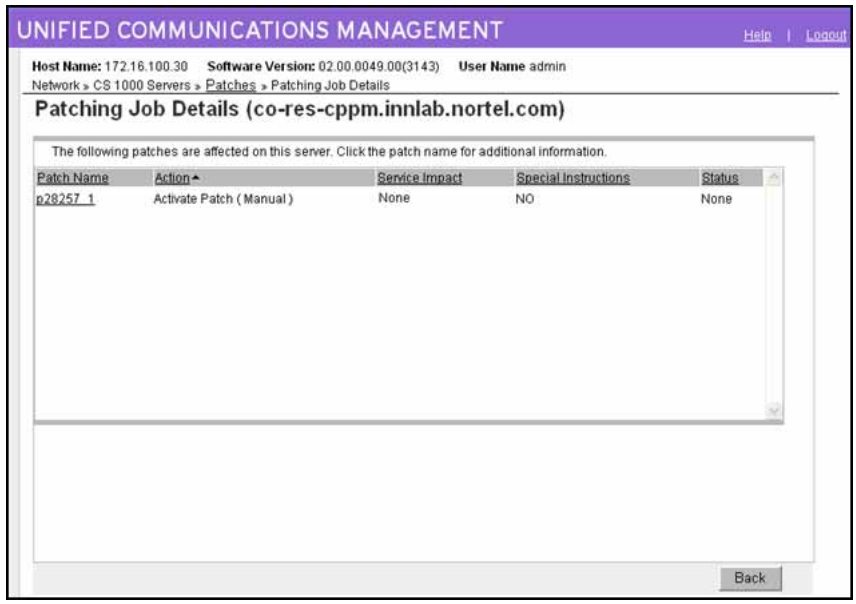
10 Wait for the status to change in the **Status Summary** column. The Status Summary provides information about the patch activation progress. For more information about the statuses displayed, see Table 2 "Status information" (page 34).

Use the Refresh icon to see the progress updates.

11 Under the **Status Summary** column, click the **Ready to Load** link for each target element to view the patching plan details for that target.

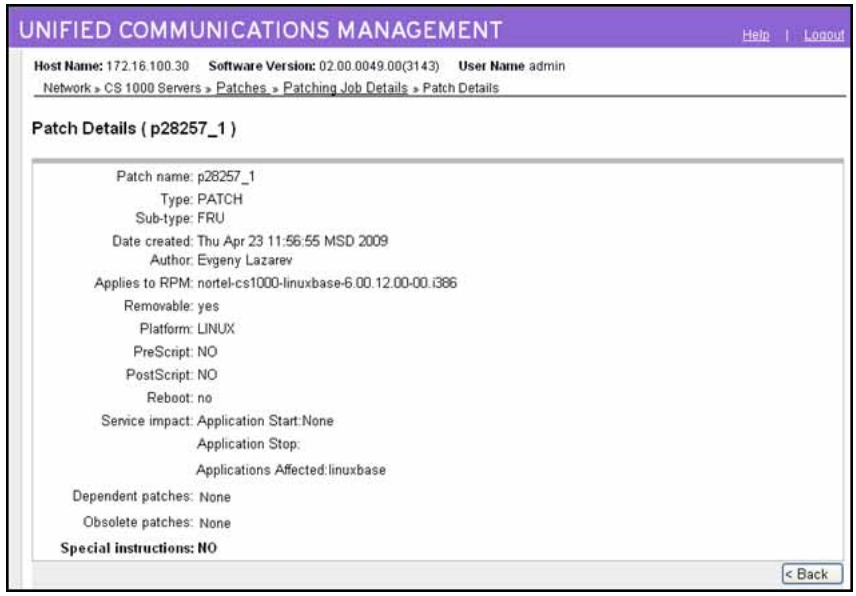
The Patching Job Details page appears.

Figure 34
Patching Job Details



To view the patch details, click the link under the **Patch Name** column. The Patch Details page appears.

Figure 35
Patch Details



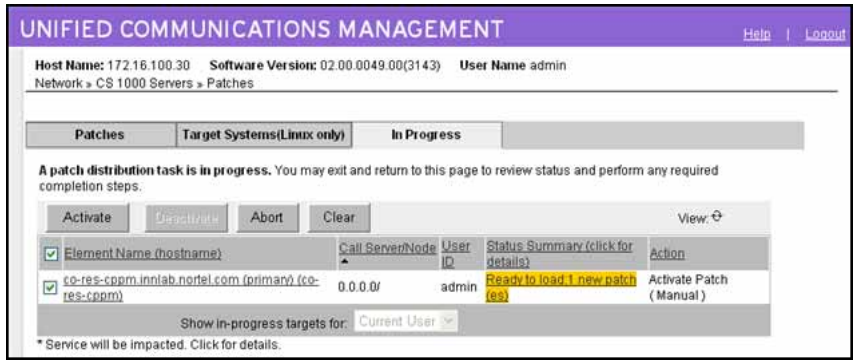
12 After you review the identified service impacts in the patching plan, click **Back** on the **Patch Details** page, and then click **Back**

again on the **Patching Job Details** page to return to the **In Progress** tab.

13 Select the check box for the target element.

The Activate button is enabled.

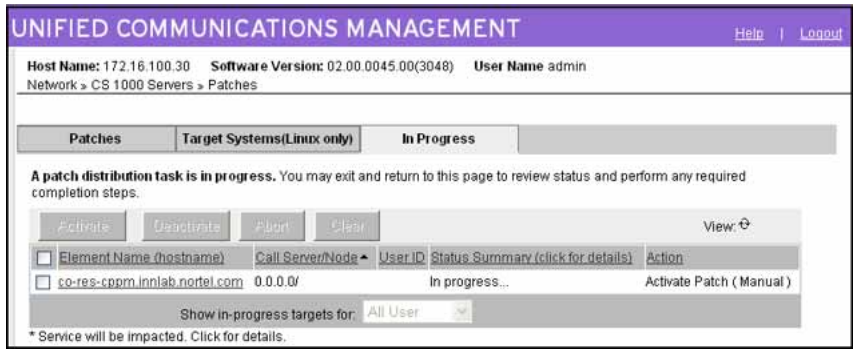
Figure 36
Select target element



14 Click **Activate** to start applying patches.

15 Wait while the updates are applied to the target. The **Status Summary** column provides information about the patch activation progress. For more information about the statuses displayed, see Table 2 "Status information" (page 34).

Figure 37
Activation in progress

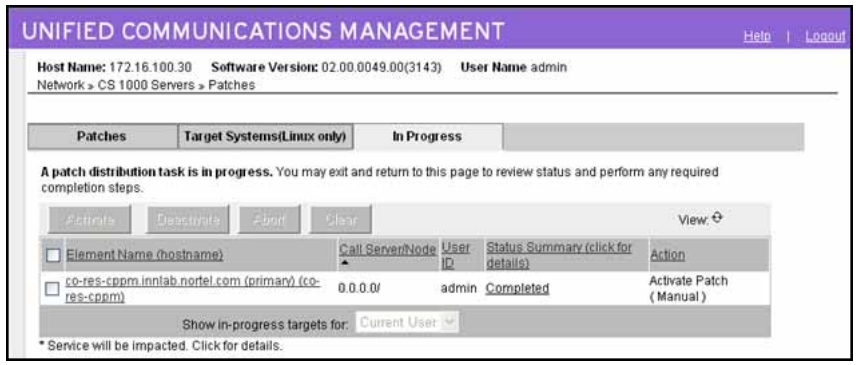


16 Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

17 Wait for the process to complete.

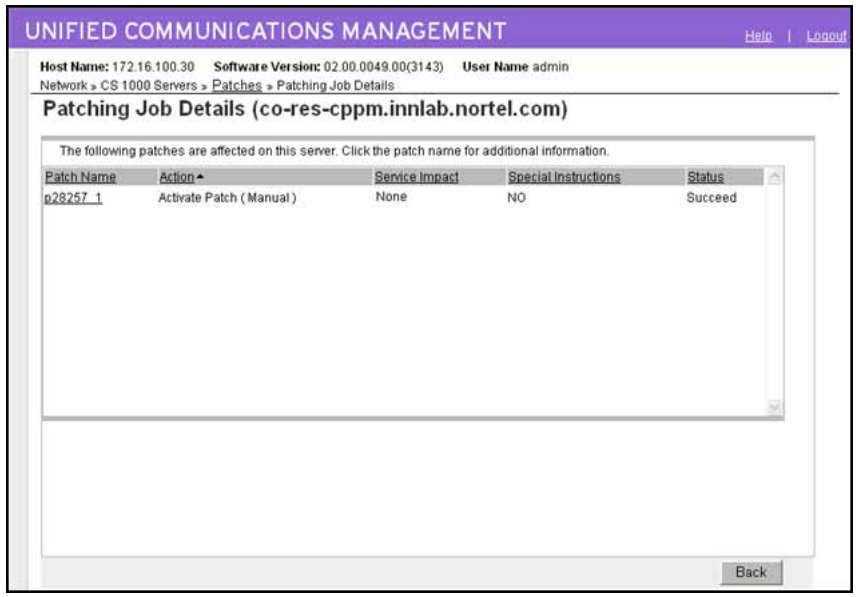
18 To view the results, under the **Status Summary** column, click the **Completed** link.

Figure 38
Activation completed



The Patching Job Details (target_name) page appears and the Status column indicates that the patch succeeded.

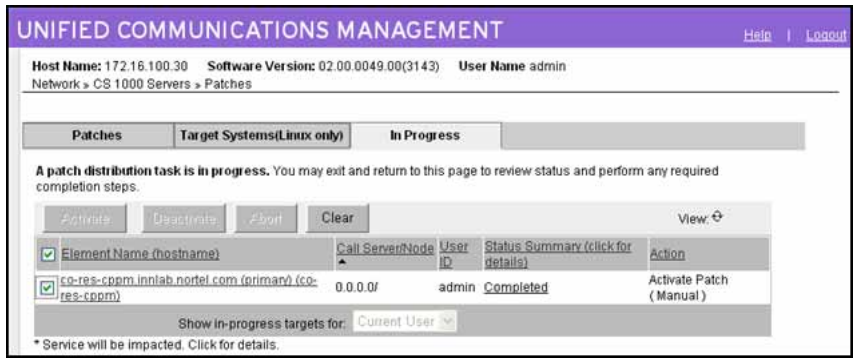
Figure 39
Patching Job Details



19 On the **Patching Job Details (target_name)** page, click **Back**.

20 After you review your patching results and are satisfied with the results, select the element and then click **Clear** to end the patching process for the select target. You must click Clear before you can perform any other patch operations for this target element.

Figure 40
Clear button enabled



Further patching activation and deactivation operations cannot be performed on the element until it is cleared.

The In Progress tab disappears when all activities for all elements are cleared.

--End--

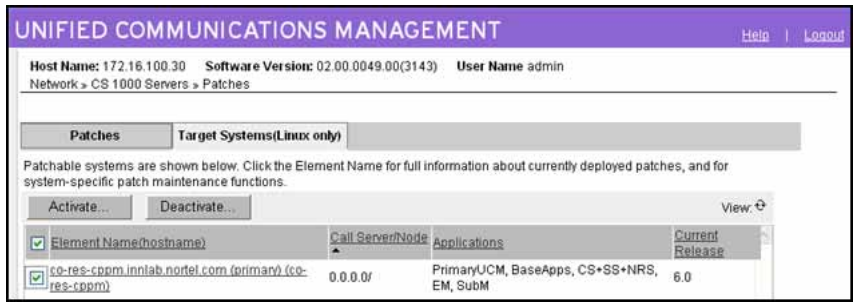
Deactivate a patch

Use the following procedure to deactivate a patch or serviceability update. Service packs cannot be deactivated; however, you can deactivate items that were installed using a service pack.

Procedure 13
Deactivating a patch

Step	Action
1	In the Patching Manager, select the **Target Systems (Linux only)** tab.
2	From the list of elements, select the check box for one or more elements for which you want to deactivate patches.

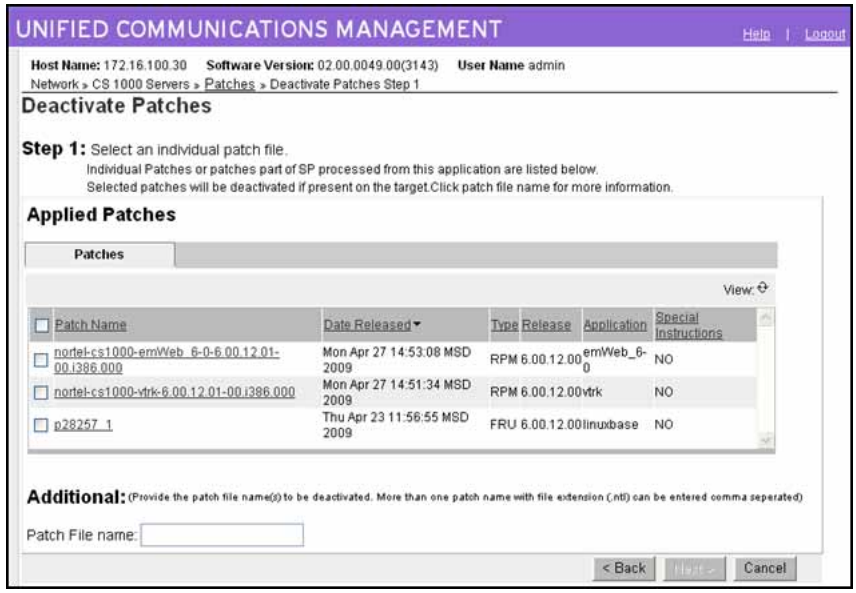
Figure 41
Element to deactivate



3 Click **Deactivate**.

The Deactivate Patches Step 1 page appears. This page displays a list of all patches or serviceability updates (that are available for deactivation) that have been applied by Central Patching Manager. These patches or serviceability update may have been applied individually or using a service pack. If the patch or serviceability update was never processed using Patching Manager, then the names of such patches (separated by commas) may be entered in the box at the bottom. Only patches applicable to the selected elements are displayed based on release and installed applications. However, some patches may not be in service on the selected elements; there will be an indication of no operation to be performed for these elements.

Figure 42
Deactivate Patches Step 1

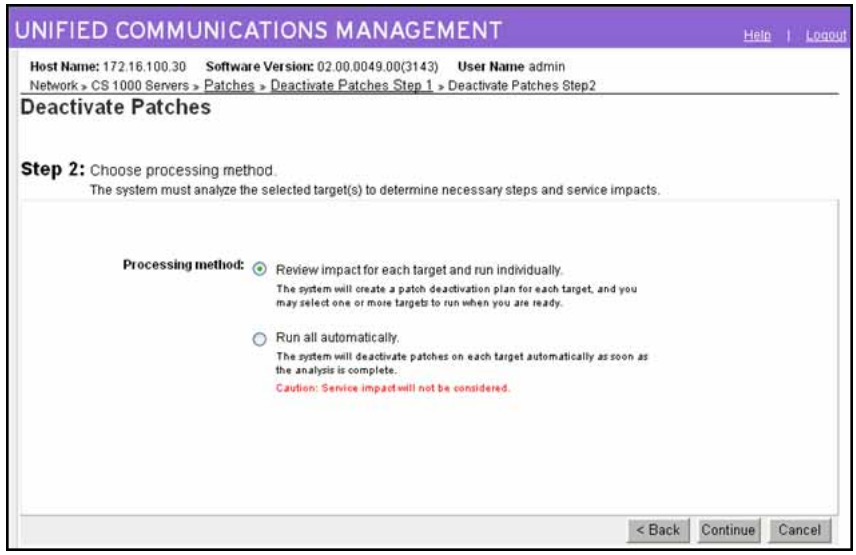


4 On the **Deactivate Patches Step 1** page, from the **Applied Patches** list, select the patches to deactivate.

5 Click **Next**.

The Deactivate Patches Step 2 appears.

Figure 43
Deactivate Patches Step 2



6 On the **Deactivate Patches Step 2** page, select the **Processing method**:

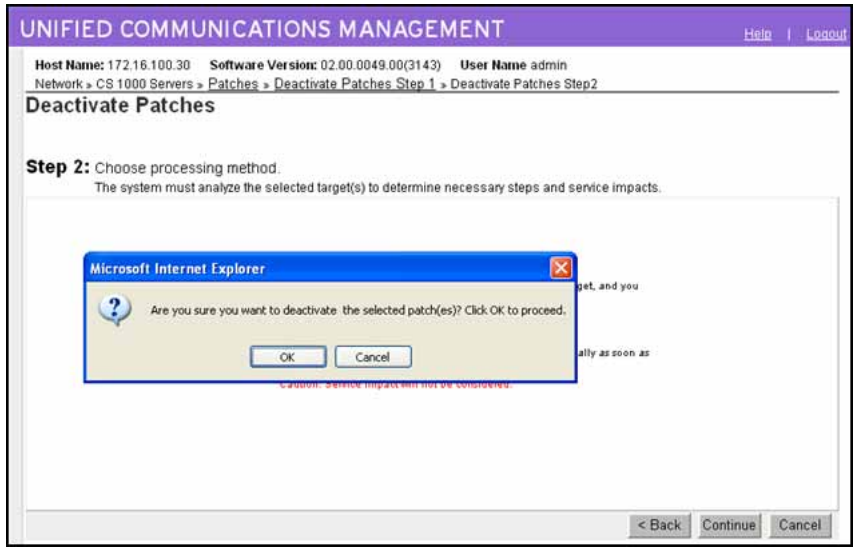
- **Review impact for each target and run individually**—With this manual processing method, a patch deactivation plan is presented for each target. Review the patch deactivation plan. You must select each target and manually initiate the patch deactivation.
- **Run all automatically**—With this automatic processing method, the patch deactivation occurs automatically as soon as the analysis is complete. In Automatic mode patch deactivation on each target occurs automatically as soon as the analysis is complete.

WARNING
Service impacts are not considered with the automatic method.

7 Click **Continue**.

A dialog box appears prompting you to confirm the patch deactivation.

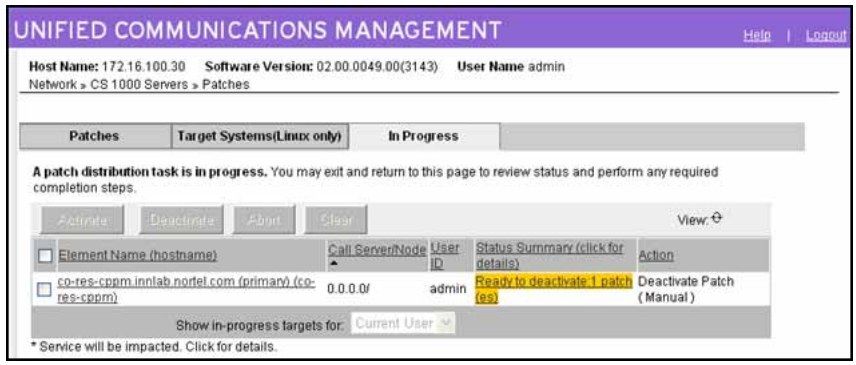
Figure 44
Confirmation dialog box



8 Click **OK** to confirm the patch deactivation.

The In Progress tab appears.

Figure 45
In Progress tab



ATTENTION
Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

9 If you selected the **Review impact for each target and run individually** option in Step 6, the targets are analyzed based on

the current patch information obtained from the target. Complete Step 10 to Step 14, and then proceed to Step 15.

OR

If you selected the **Run all automatically** option in Step 6, the targets are analyzed based on the current patch information obtained from the target. Unless there are errors detected, the patch deactivation proceeds automatically without waiting for your input. Wait while the patches are deactivated on the target. Proceed to Step 15.

10 Under the **Status Summary** column, click the **Ready to Deactivate** link for each target to view the patching deactivation plan details for that target.

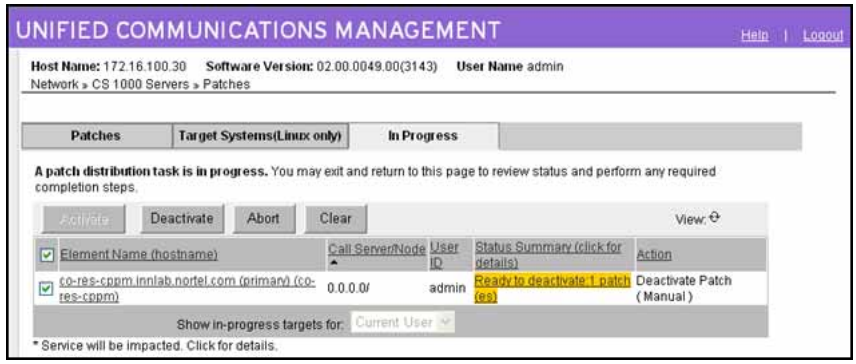
The Patching Job Details page appears for the patch.

11 After you review the identified service impacts in the patching deactivation plan, click **Back**.

12 Select the check box for the target element.

The Deactivate button is enabled.

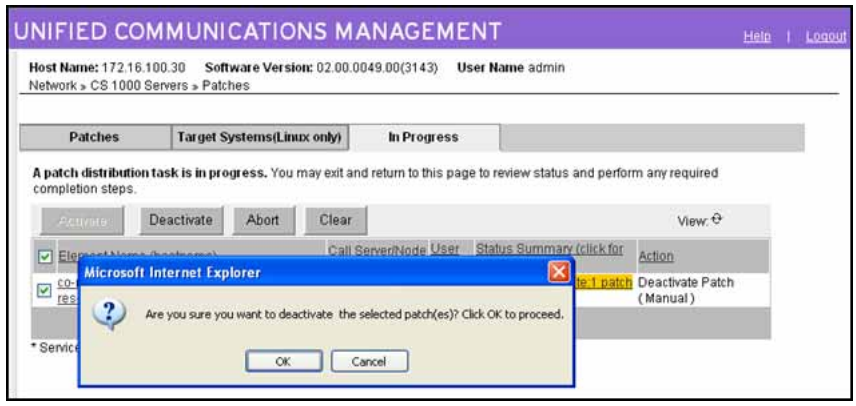
Figure 46
Deactivate button enabled



13 Click **Deactivate** to start the patch deactivation.

A dialog box appears prompting you to confirm the patch deactivation.

Figure 47
Confirm deactivation



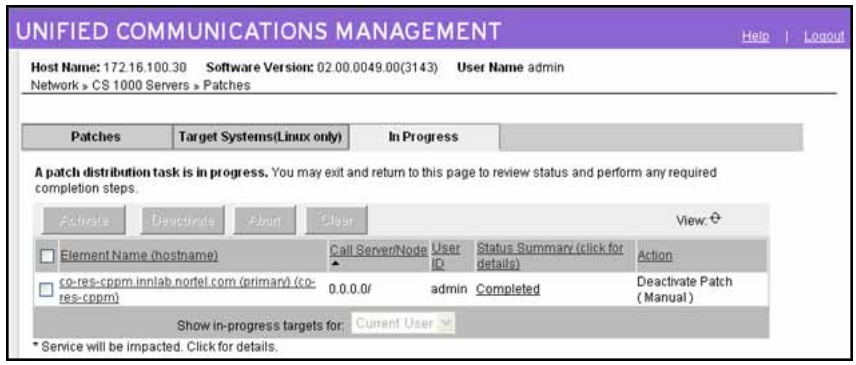
14 Click **OK** to confirm the patch deactivation.

15 Wait while the patch is deactivated on the target. The **Status Summary** column provides information about the patch deactivation progress.

16 Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

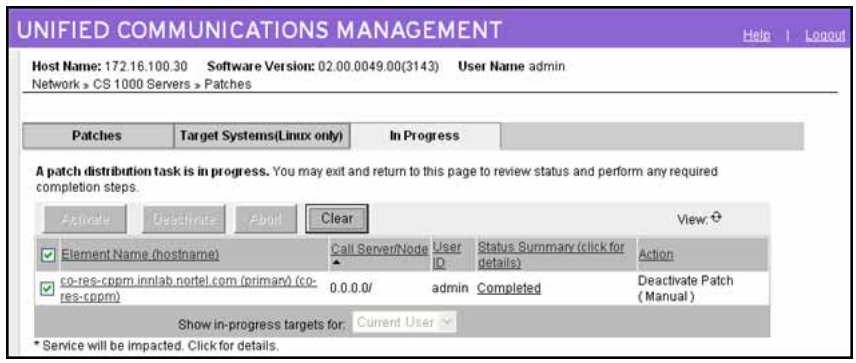
17 Wait for the process to complete. The Status Summary column indicates the process is **Completed**.

Figure 48
Deactivation completed



18 After you review your patching results and are satisfied with the results, select the check box for the target element and then click **Clear** to end the patching process for the selected target. You must click Clear before you can perform any other patch operations for this target element.

Figure 49
Clear button enabled



Further patching activation and deactivation operations cannot be performed on the element until it is cleared.

The In Progress tab disappears when all activities for all elements are cleared.

--End--

Local Patching Manager

The Local Patching Manager interface runs directly on each Linux element and supports patching only for that specific element. The Local Patching Manager provides a list of patches on the server with the status (such as Unloaded, Loaded, and In-Service). It also provides storage space management for patches.

Patching can occur on a single-target basis using the Local Patching Manager (within Base Manager). The Local Patching Manager can be used to augment the Central Patching Manager in the following ways:

- To view the current state of a patch.
- To remove existing patches to avoid conflicts (if necessary).
- To remove patches in failure scenarios.

Base Manager can be used for related activities, such as the following:

- Application maintenance for starting, stopping, and restarting before and after patching. (This process depends on the instructions in each patch.)
- To reboot the server (if necessary).

When patching finishes, generally all application restarts or reboot occur automatically. It is necessary to take manual action only if indicated in the special instructions for the patch. Manual actions may be necessary in case of patching errors. For example, if a patch deactivation fails, then an application may be stopped and not restarted. The patch details show applications to restart and the status of these applications can be checked to see if action is required.

ATTENTION
In this document, the term patch or patches includes both patches and serviceability updates (SUs) unless explicitly mentioned otherwise because patches and SUs are applied in the same way.

This chapter provides procedures to perform the following in the Local Patching Manager:

- Add, activate, deactivate, and delete patches.
- Add, activate, and delete service pack. (Service packs cannot be deactivated; however, patches that are part of a service pack can be deactivated.)

Download and save patches, serviceability updates, and service packs

The Enterprise Solutions PEP Library (ESPL) provides online access to Nortel-approved Product Enhancement Package (PEP) solutions for Enterprise products. To download the required patches, serviceability updates, and service packs and save them on your client PC, see "Download and save patches, serviceability updates, and service packs" (page 39).

Access the Local Patching Manager

You can access Local Patching Manager by being redirected from the UCM network level or from Element Manager (using a log in to the UCM framework). For these cases, the role of the user governs whether access is permitted to local patching capabilities. Access to the Local Patching Manager is controlled by the permission for the element. The patchAdmin permission must be assigned for the element (either individually or in All elements of type: Linux Base). This element-level permission is allocated to a role, which in turn is assigned to a user.

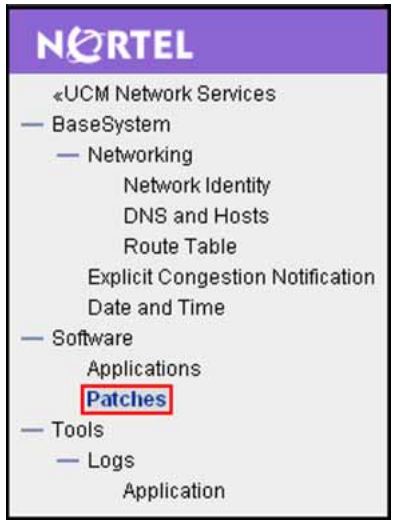
You can also access the Local Patching Manager using local login to Base Manager. When a local log on is performed (this could be with an emergency account), you have complete access to all Base Manager functionality, including patching

Use the following procedure to access the Local Patching Manager.

Procedure 14
Accessing the Local Patching Manager from the Base Manager

Step	Action
1	Log on to UCM.
2	In the **Elements** pane, under the **Element Name** column, select the element you want to patch. Base Manager appears for the element.
3	In the Base Manager navigation tree, select **Software > Patches**.

Figure 50
Base Manager navigation tree: Patches



You can also access the Local Patching Manager in the following ways:

- In the UCM Central Patching Manager, select the Targets Systems (Linux only) tab, and then select an element name to open the Local Patching Manager for that element.
- When Base Manager is accessed with a local logon (using local or emergency account).

The Local Patching Manager (within Base Manager) appears for the element. The page is called Patches (element host name) where element host name is the name of the server.

Figure 51
Local Patching Manager

The Local Patching Manager has two main tabs: Service Packs and Individual Patches.

On the Service Packs tab, you can add or delete service packs. After you add service pack, you can view details for the service pack. Service packs can also be activated on the Service Packs tab but cannot be deactivated. You can perform the following procedures on the Service Packs tab:

- Procedure 15 “Adding a service pack” (page 80)
- Procedure 16 “Viewing service pack details” (page 82)
- Procedure 17 “Deleting a service pack” (page 84)
- Procedure 18 “Activating a service pack” (page 86)

On the Individual Patches tab, you can add or delete patches or serviceability updates. You can also view details for the patches you have added on the element. Patches and serviceability updates can be both activated and deactivated. (This tab is selected by default.) You can perform the following procedures on the Individual Patches tab:

- Procedure 19 “Adding a patch” (page 90)
- Procedure 20 “Viewing patch details” (page 92)
- Procedure 21 “Activating patches” (page 93)
- Procedure 22 “Deactivating a patch” (page 96)
- Procedure 23 “Deleting a patch” (page 98)

--End--

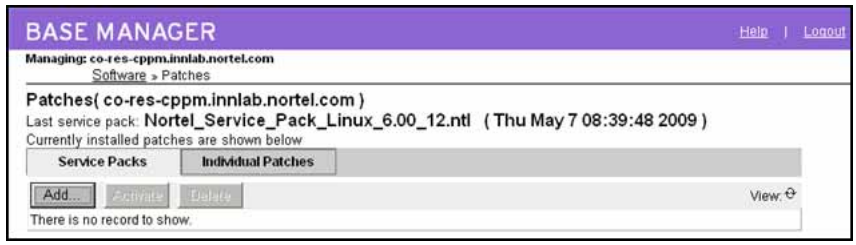
Add a service pack

Use the following procedure to add a service pack to the element.

Procedure 15
Adding a service pack

Step	Action
1	In the Local Patching Manager, select the **Service Packs** tab.

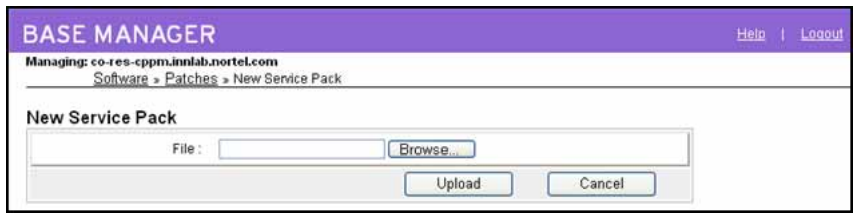
Figure 52
Service Packs tab



2 Click **Add**.

The New Service Pack page appears.

Figure 53
New Service Pack



3 Click **Browse**.

The Choose File dialog box appears.

4 In the **Choose File** dialog box, browse to the find the service pack on your client PC.

5 Select the service pack file, and click **Open**.

The file appears in the File field.

6 Click **Upload**.

The Local Patching Manager validates the file. The service patch file appears on the Service Pack tab. The Service Pack tab displays the new service pack and it details.

Figure 54
Added service pack

For more information, see "View service pack details" (page 82).

--End--

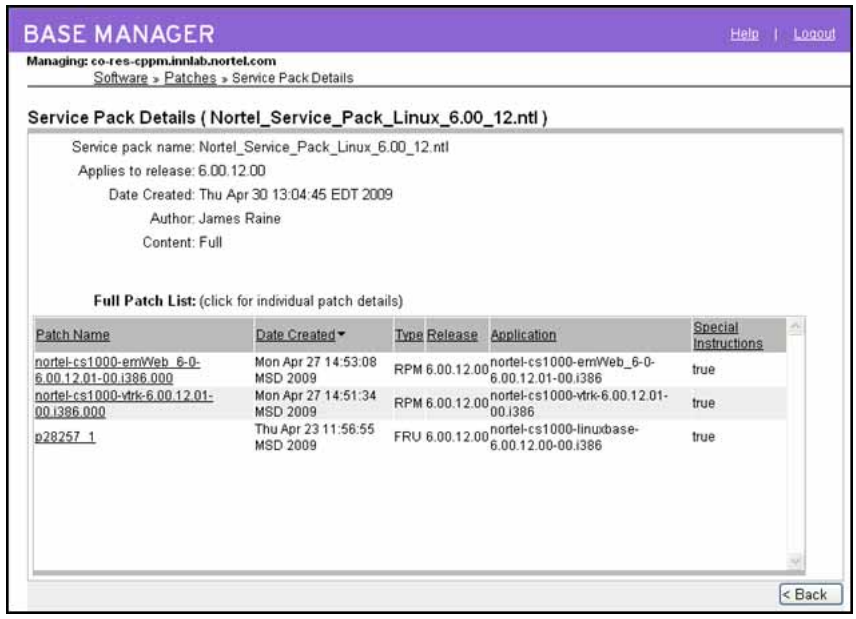
View service pack details

Use the following procedure to view the details about a service pack and the individual patches that it contains. The Service Pack Details page displays important details about a service pack and patches such as header information.

Procedure 16
Viewing service pack details

Step	Action
1	In the Local Patching Manager, select the **Service Packs** tab.
2	To view details of the service pack, under the **Service Pack Name** column, click the name of the service pack file. The Service Pack Details (sp_name) page appears; sp_name is the name of the service pack.

Figure 55
Service Pack Details

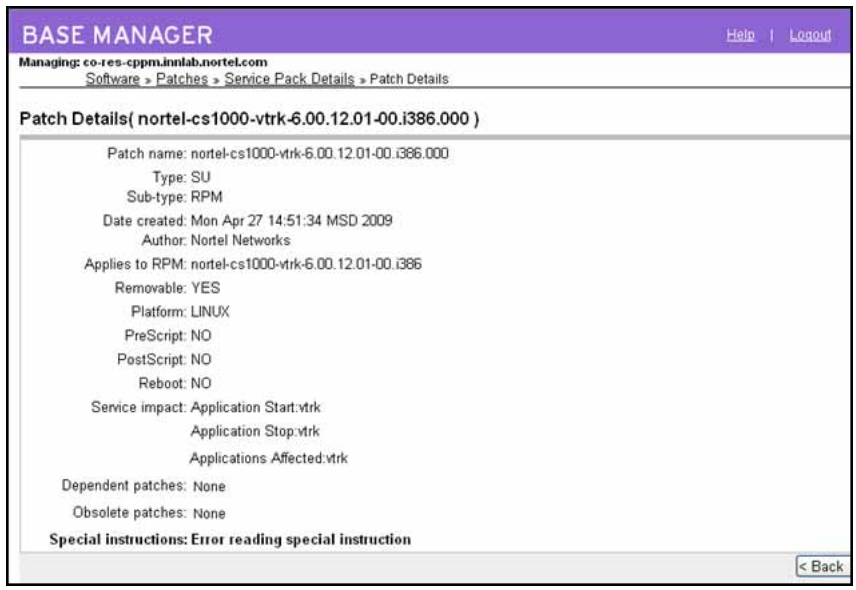


3 On the **Service Pack Details (sp_name)** page, review the detailed information about the service pack.

4 To review an individual patch in the service pack, under **Full Patch List**, click the name of the patch.

The Patch Details (patch_name) page appears. This page provides details such as patch file name, service impact, dependent patches, obsolete patches special instructions, and other details from the patch header.

Figure 56
Patch Details



5 To return to the **Service Pack Details** page, click **Back** on the Patch Details page.

6 To return to the **Service Packs** tab, click **Back** on the Service Pack Details page.

--End--

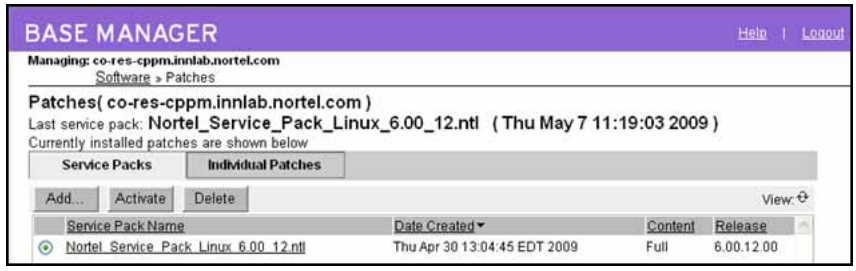
Delete a service pack

Use this procedure to delete a service pack from the element. Service packs stay on the target element until you manually remove them. Deleting a service pack does not delete or deactivate the patches or serviceability updates that were included within service pack.

Procedure 17
Deleting a service pack

Step	Action
1	In the Local Patching Manager, select the **Service Pack** tab.
2	Select the option button for the service pack you want to delete.

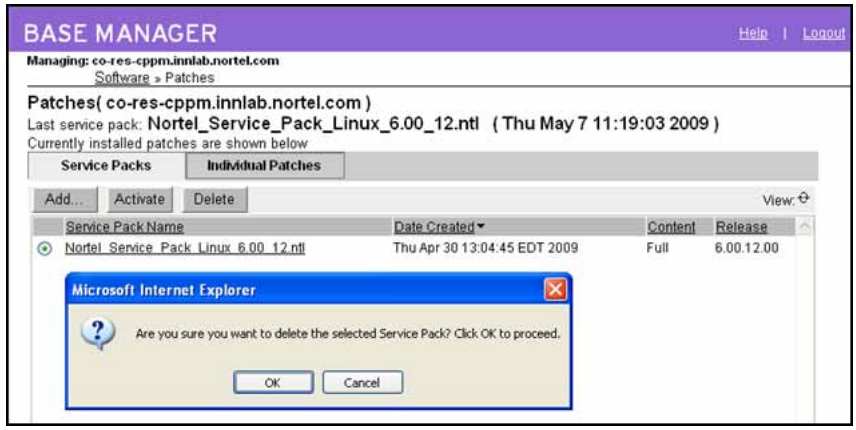
Figure 57
Select service pack



3 Click **Delete**.

A dialog box appears prompting you to confirm the service pack deletion.

Figure 58
Confirm service pack deletion



4 Click **OK** to confirm the deletion of the service pack.

The service pack is removed from the list on the Service Packs tab.

--End--

Activate a service pack

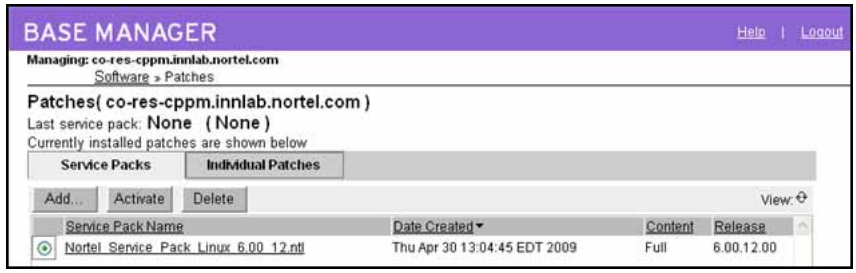
Use the following procedure to apply a service pack to the element. When you activate a service pack, all the applicable patches and serviceability updates within the service pack are loaded and placed in service.

Note: You can activate only one service pack at a time. You cannot activate a service pack together with patches or serviceability updates.

Procedure 18
Activating a service pack

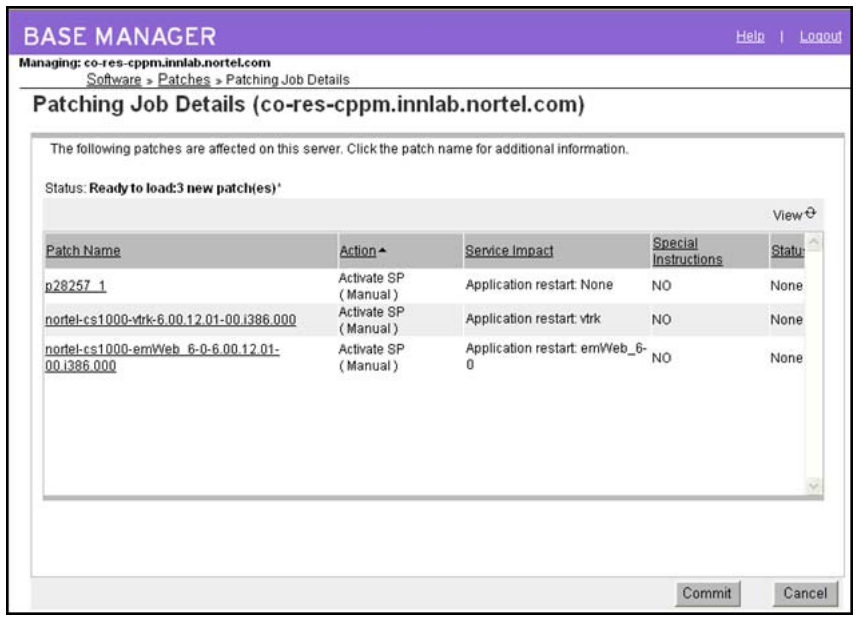
Step	Action
1	In the Local Patching Manager, select the **Service Packs** tab.
2	From the list of service packs, select the option button for the service pack you want to activate on the element.

Figure 59
Select the service pack



3	Click **Activate**. The Patching Job Details page appears. The status changes from Queued for Patching to Ready to Load: x new patches (x is the number of patches in the service pack).

Figure 60
Patching Job Details - Ready to load



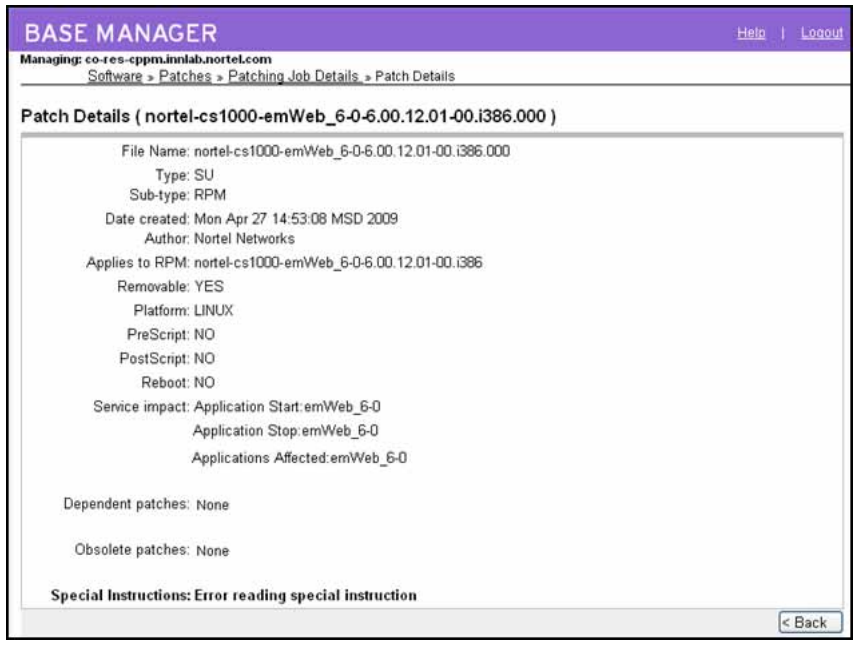
4 In the **Service Impact** column, review the service impacts for the patches and serviceability updates.

5 In the **Special Instructions** column, verify whether any patches have Special Instructions equal to **YES**. Review the patch if there are special instructions.

6 To review the details for a specific patch, under the **Patch Name** column, click the link for the patch.

The Patch Detail (patch_name) page appears.

Figure 61
Patch Details (patch_name)

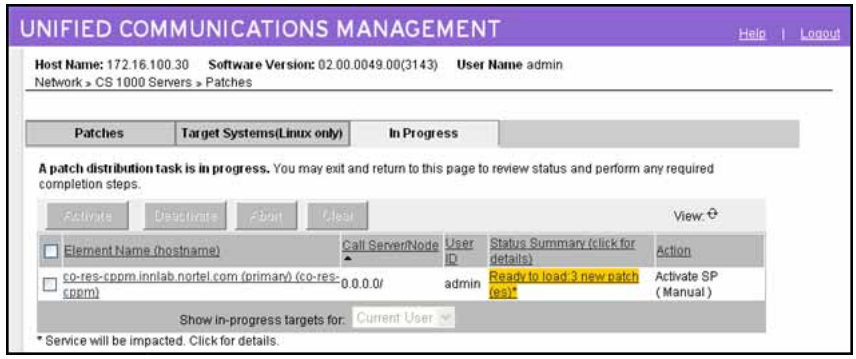


7 Click **Back** to return to the **Patching Job Details** page.

8 Click **Commit**.

The status changes from Queued for Patching to In Progress. For more information, see Table 2 "Status information" (page 34).

Figure 62
Patching Job Details - In Progress

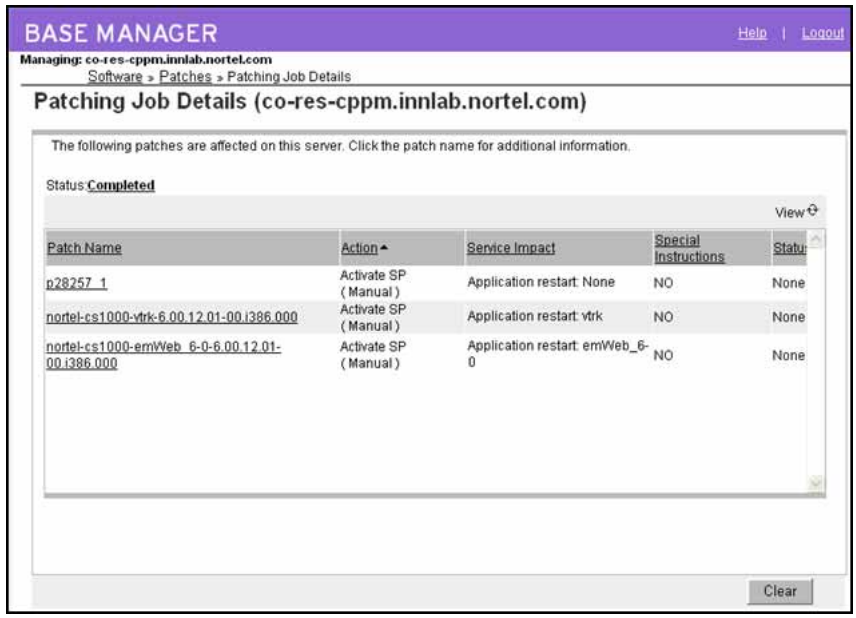


9 Wait while the service pack is activated.

The time required to activate a service pack depends on the number patches in the service pack.

When the service pack is activated, the Status field changes to Completed (at the top of the window). The overall status for the service pack activation is provided as a link at the top of the page.

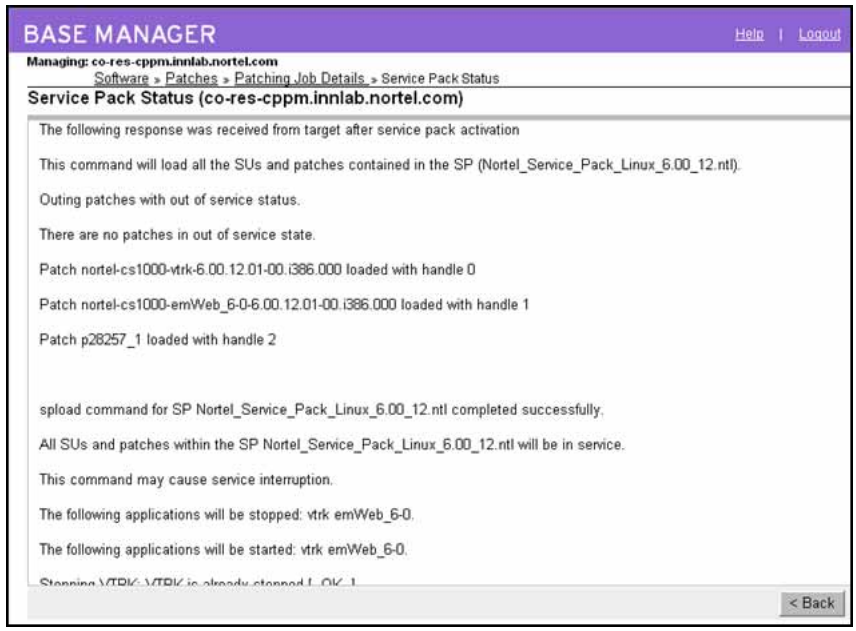
Figure 63
Activation complete



10 Click the **Completed** status link.

The Service Pack Status page appears and the output from the underlying base service pack installation appears.

Figure 64
Service Pack Status



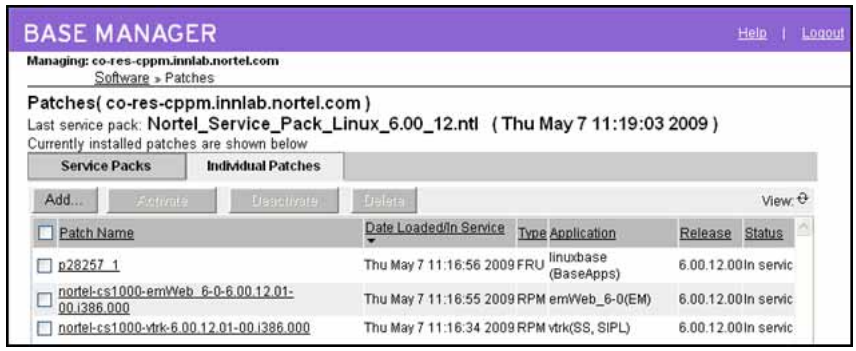
11 Click **Back** to return to the Patching Job Details page.

12 On the Patching Job Details page, click **Clear**.

The Service Pack tab appears.

13 Select the **Individual Patches** tab, in the **Status** column, verify that the patches are **In service**.

Figure 65
In service patches



--End--

Add a patch

Use the following procedure to add a patch to the element.

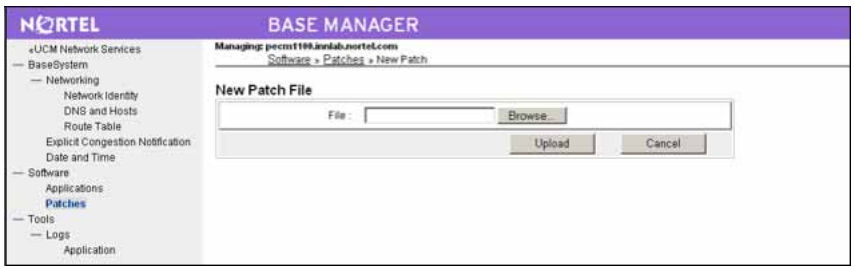
Procedure 19
Adding a patch

Step	Action
1	In the Local Patching Manager, ensure the **Individual Patches** tab is selected.

Figure 66
Individual Patches tab

2	Click **Add**. The New Patch File page appears.

Figure 67
New Patch File



3 Click **Browse**.

The Choose File dialog box appears.

4 In the **Choose File** dialog box, browse to the find the patch on your client PC.

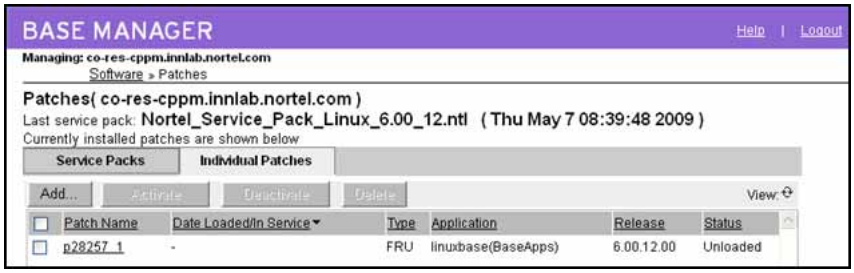
5 Select the patch file, and click **Open**.

The file appears in the File field.

6 Click **Upload**.

The Patching Manager validates the file. The patch file appears on the Individual Patches tab. The Individual Patches tab displays the new patch and it details. New patches are in an Unloaded state.

Figure 68
Added patch



For more information, see "View patch details" (page 91).

--End--

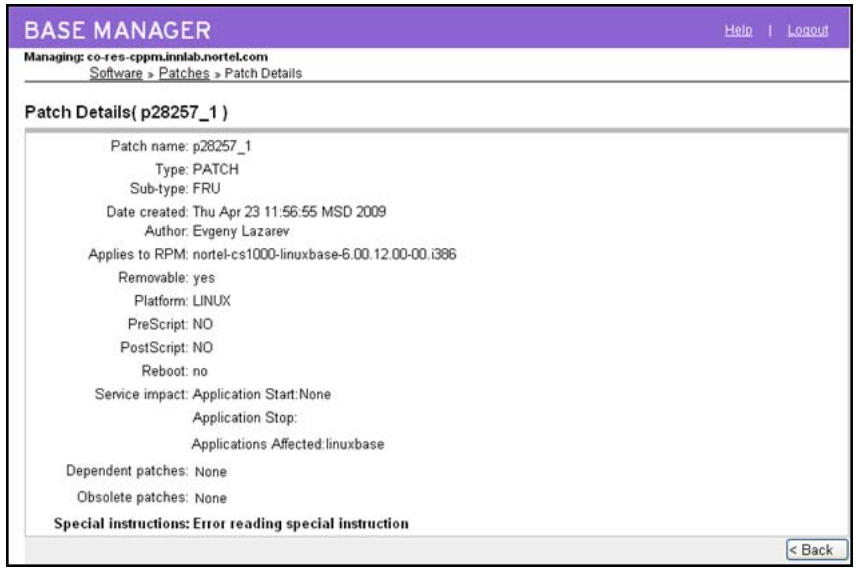
View patch details

Use the following procedure to view the details about a specific patch. The Patch Details page displays important details about the patch from the header information.

Procedure 20
Viewing patch details

Step	Action
1	In the Local Patching Manager, select the **Individual Patches** tab.
2	To view details for a patch, under the **Patch Name** column, click the name patch. The Patch Details (patch_name) page appears; patch_name is the name of the patch.

Figure 69
Patch Details



3	On the **Patch Details (patch_name)** page, review the detailed information about the patch.
4	To return to the Individual Patches tab, click **Back** on the Patch Details page.

--End--

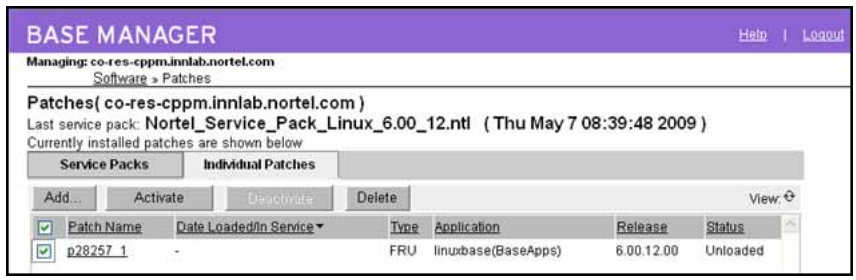
Activate patches

Use the following procedure to apply a patch or multiple patches to the element. Activating a patch loads the patch and places it in service.

Procedure 21
Activating patches

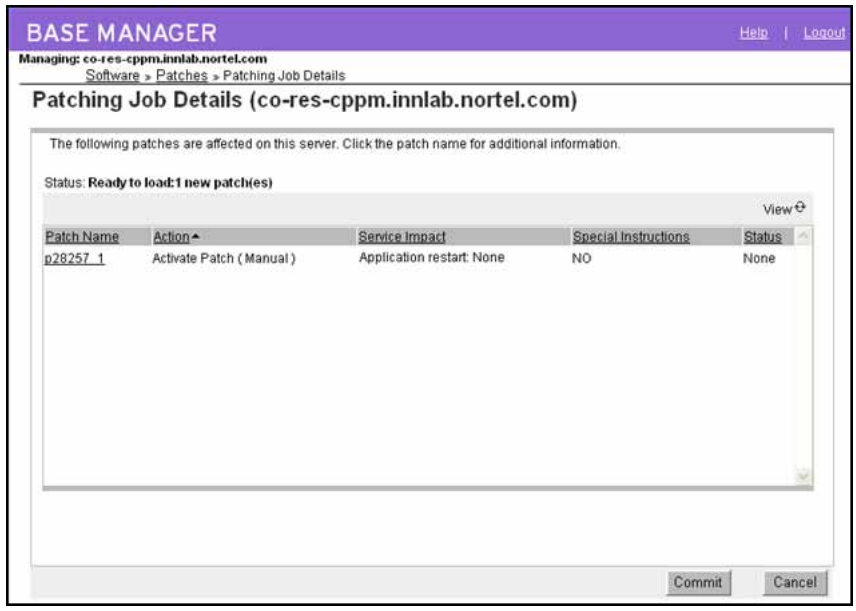
Step	Action
1	In the Local Patching Manager, select the **Individual Patches** tab.
2	From the list of patches, select the check box for the patches you want to activate on the element.

Figure 70
Select patch to activate



3	Click **Activate**. The Patching Job Details page appears. The status changes from Preprocessing to Ready to Load. For more information, see Table 2 "Status information" (page 34).

Figure 71
Patching Job Details - Ready to Load



New patches are in Loaded status. You can select any patches that are loaded (but not in service) and place them in service. Patches may have been placed in the Loaded state by the CLI, by failure of service pack activation, or if an issue arises with installing the patch after it is loaded.

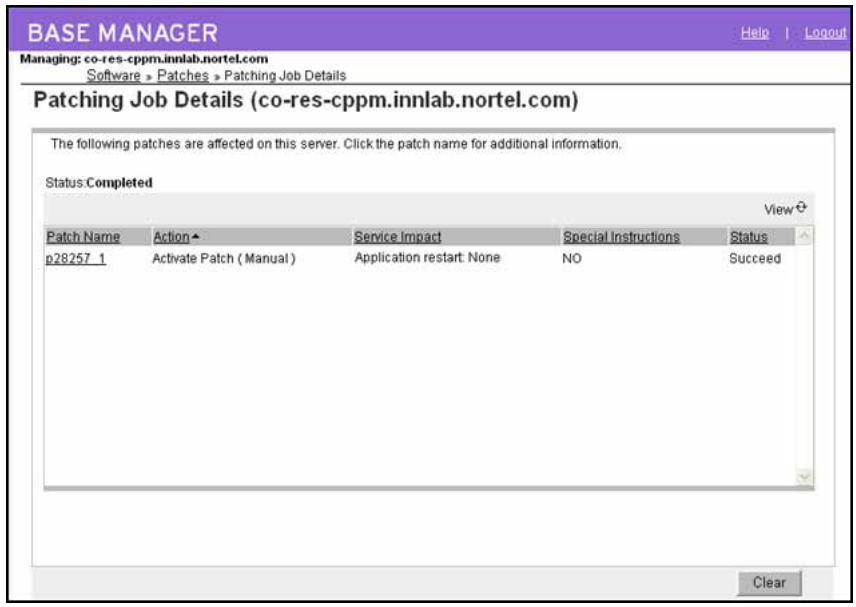
4 Click **Commit**.

The status changes from Queued for Patching to In Progress.

5 Wait while the patch is activated.

When the patch is activated, the status changes to **Completed** (at the top of the window) and the Status column indicates that the patch succeeded.

Figure 72
Patching Job Details - Completed

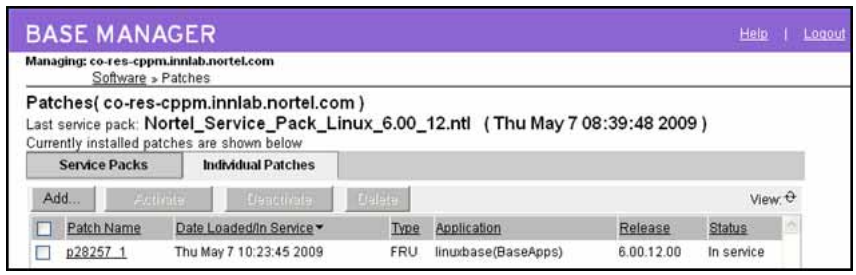


6 Before proceeding with additional patch activation, click **Clear** to end the patching process.

The Individual Patches tab appears.

7 On the **Individual Patches** tab, under the **Status** column, verify that the patch is **In Service**.

Figure 73
In service patch



--End--

Deactivate a patch

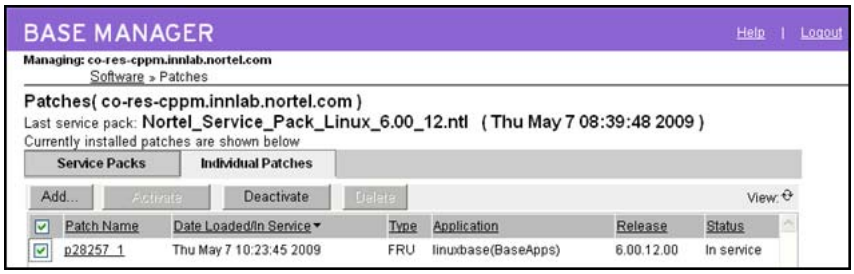
Use the following procedure to deactivate a patch or serviceability update. When a patch is deactivated, is it taken out of service and is unloaded.

Note: You cannot deactivate service packs; however, patches that are part of a service pack can be deactivated.

Procedure 22
Deactivating a patch

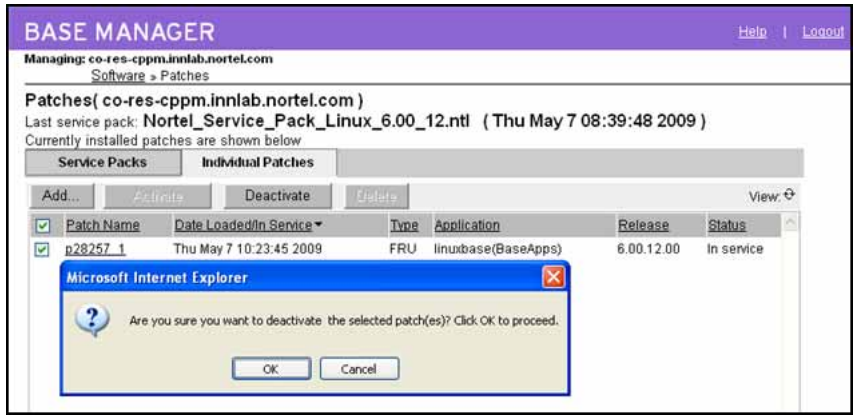
Step	Action
1	In the Local Patching Manager, select the **Individual Patches** tab.
2	From the list of patches, select the check box for patch you want to deactivate. (The status of the patch must be In Service.) The Deactivate button is enabled.

Figure 74
Select patch to deactivate



3	Click **Deactivate**. A dialog box appears prompting you to confirm the deactivation of the patch.

Figure 75
Confirm deactivation



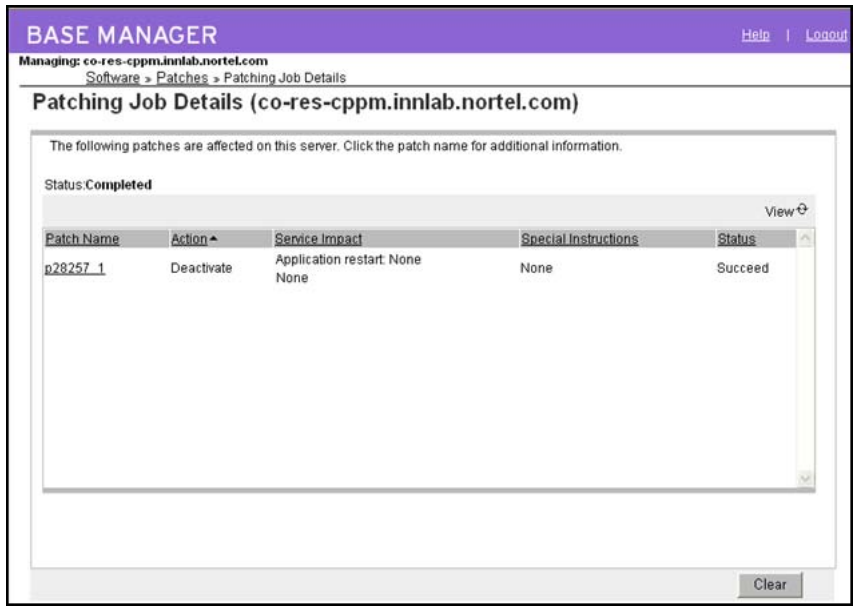
4 Click **OK** to confirm the patch deactivation.

5 Wait for the deactivation process to complete.

The Patching Job Details appears.

6 On the Patching Job Details page, verify that the **Status** is **Completed** and that the **Status** column displays **Succeed**.

Figure 76
Deactivation Complete

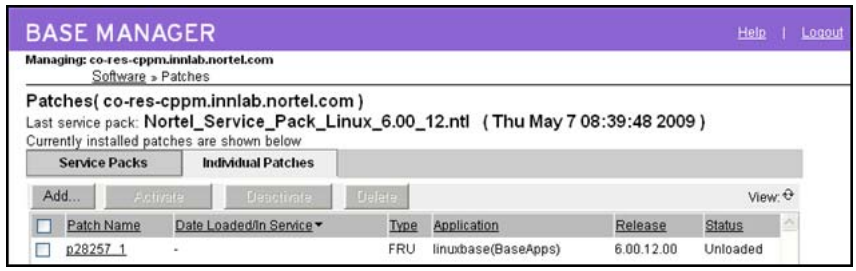


7 On the Patching Job Details page, click **Clear**.

The Individual Patches tab appears.

8 Verify that the **Status** column says **Unloaded** for the patch you deactivated.

Figure 77
Unloaded patch



--End--

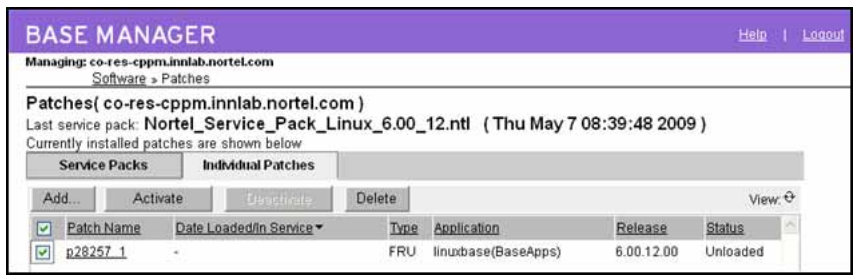
Delete a patch

Use this procedure to delete a patch from the element. A patch must have an Unloaded status to be deleted.

Procedure 23
Deleting a patch

Step	Action
1	In the Local Patching Manager, ensure the **Individual Patches** tab is selected.
2	Select the check box for the patch you want to delete and verify that the patch has an **Unloaded** status.

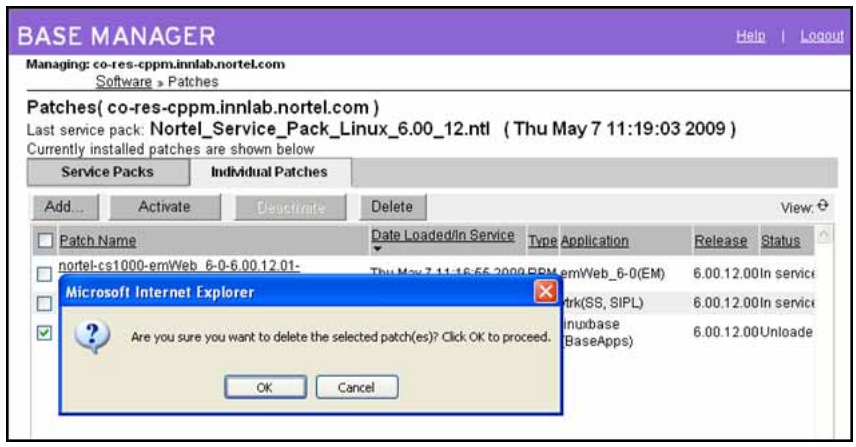
Figure 78
Select patch



3 Click **Delete**.

A dialog box appears prompting you to confirm the deletion of the patch.

Figure 79
Confirm deletion



4 Click **OK** to confirm the patch deletion.

The patch is removed from the list.

--End--

CLI commands

This chapter describes the Command Line Interface (CLI) commands for Linux patching.

You must have an account with the patching permissions to run these CLI commands.

The CLI commands are available for patches, serviceability updates, and service packs. For more information, see the following:

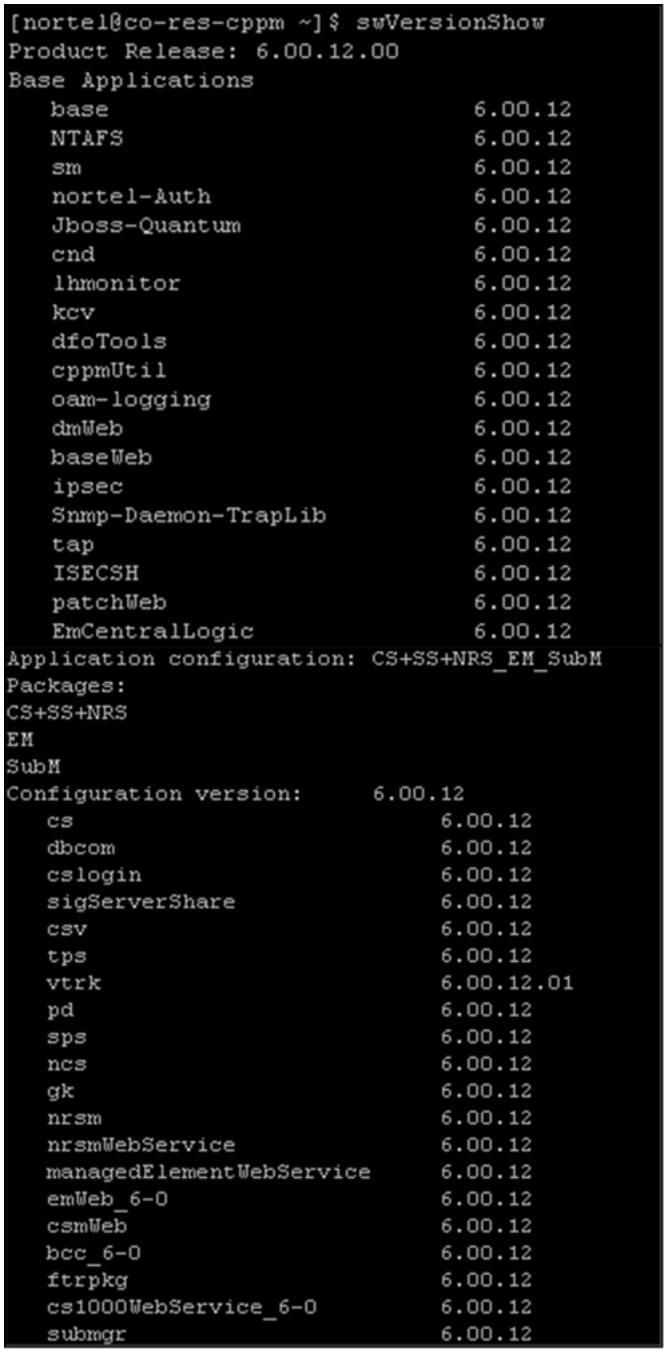
- “Target patch and serviceability update commands” (page 103)
- “Target service pack commands” (page 108)

Use the following procedure to issue patching CLI commands.

Patching using the CLI

Step	Action
1	Log on using the **admin2** account.
2	After you log on, enter the CLI command **`swVersionShow`** and press **Enter**. The installed applications and the application version numbers are displayed, as shown in Figure 80 "Installed applications and version numbers" (page 102). Figure 80 "Installed applications and version numbers" (page 102) contains the base or application name in the left column and the corresponding version number in the right column. Note the Product Release that you are patching. You must use the correct version number to retrieve the correct patch or serviceability update from the ESPL. **ATTENTION** The application version returned by the **`swVersionShow`** command may not match the versions of RPMs constituting the application. Always refer to the RPM versions returned by the **`issp`** command when determining patch applicability.

Figure 80
Installed applications and version numbers



```
[nortel@co-res-cppm ~]$ swVersionShow
Product Release: 6.00.12.00
Base Applications
   base                          6.00.12
   NTAFS                         6.00.12
   sm                            6.00.12
   nortel-Auth                   6.00.12
   Jboss-Quantum                 6.00.12
   cnd                           6.00.12
   lhmonitor                     6.00.12
   kcv                           6.00.12
   dfoTools                      6.00.12
   cppmUtil                      6.00.12
   oam-logging                   6.00.12
   dmWeb                         6.00.12
   baseWeb                       6.00.12
   ipsec                         6.00.12
   Snmp-Daemon-TrapLib           6.00.12
   tap                           6.00.12
   ISECSH                        6.00.12
   patchWeb                      6.00.12
   EmCentralLogic                6.00.12
Application configuration: CS+SS+NRS_EM_SubM
Packages:
CS+SS+NRS
EM
SubM
Configuration version:     6.00.12
   cs                              6.00.12
   dbcom                           6.00.12
   cslogin                         6.00.12
   sigServerShare                  6.00.12
   csv                             6.00.12
   tps                             6.00.12
   vtrk                            6.00.12.01
   pd                              6.00.12
   sps                             6.00.12
   ncs                             6.00.12
   gk                              6.00.12
   nrsm                            6.00.12
   nrsmWebService                  6.00.12
   managedElementWebService        6.00.12
   emWeb_6-0                       6.00.12
   csmWeb                          6.00.12
   bcc_6-0                         6.00.12
   ftrpkg                          6.00.12
   cs1000WebService_6-0            6.00.12
   submgr                          6.00.12
```

3 Retrieve a patch, serviceability update, or service pack file from the ESPL. For more information, see “Download and save patches, serviceability updates, and service packs” (page 39).

4 Upload the serviceability updates and patch files to the Linux server and save it in the /var/opt/nortel/patch folder. Service packs are uploaded to the Linux server and are saved in the /var/opt/nortel/sp folder.

Secure File Transfer Protocol (SFTP) and Secure Copy (SCP) are the supported methods of patch file transfer.

The patch file transfer is initiated from the Linux server or from an external computer.

- To initiate the patch file transfer from within the Linux server:
  - Log on to the Linux server as admin2.
  - Enter the **`sftp`** or **`scp`** CLI command.
  - Enter the **`get`** command (for **`sftp`**) or the **`scopy`** command (for **`scp`**) to transfer the patch to the Linux server.
- To initiate the patch file transfer from an external machine:
  - Initiate an SFTP or Secure Shell (SSH) program.
  - Provide the IP address (or host name) of the Linux server, the Nortel user ID, and password as parameters.
  - Enter the **`put`** command (for **`sftp`**) or the **`scopy`** command (for **`scp`**) to transfer the patch to the Linux server.

5 Perform the required on-target patch management CLI commands. The on-target patch management CLI provides an interface command set similar to the CS 1000 patcher. For more information, see the following:

- “Target patch and serviceability update commands” (page 103)
- “Target service pack commands” (page 108)

--End--

Target patch and serviceability update commands

The following CLI commands are available for patches and serviceability updates:

- “pstat” (page 104)
- “plis” (page 104)
- “pload” (page 105)
- “pins” (page 106)

- “poos” (page 107)
- “pout” (page 107)

pstat

Syntax: **pstat <handle> -l, --list -a, --all -h, --help**

Parameter	Description
<handle>	Prints status information about the patches and serviceability updates with <handle>.
--list or -l	Lists all installed in-service patches and serviceability updates.
--all or -a	Lists all in-service and out-of-service patches and serviceability updates in detail.
--help or -h	Prints information about the pstat command.

Description: Prints a status summary of all installed patches and serviceability updates (loaded, in-service, and out-of-service patches and serviceability updates).

Example 1: Print the information for all installed in-service patches and serviceability updates.

```
$ pstat -l
Product Release:  6.00.00.00
In service patches:  1

PATCH#  NAME      IN_SERVICE  DATE    SPECINS  TYPE  RPM
1       p20002_1  yes         10/07   no       FRU   mlocate-0.15-1.el5
Applied service updates:  1

SU#  IN_SERVICE  DATE    SPECINS  REMOVABLE  NAME
4    yes         10/07   no       yes        acl-2.2.39-2.1.el5.001
```

plis

Syntax: plis <patch_handle> --help

Parameter	Description
<patch_handle>	Prints status information about the patch with <patch_handle>.
--help	Prints information about the plis command.

Description: Print detailed information about a specific patch.

Example 1: Print information for the patch with 1 handle.

```
$ plis 1
Handle: 1
Type: PATCH
Filename: p19000_1.ntl
Dependency: None
CR number: Q000000000
Engineer: John Doe
Created: Tue Sep 16 15:49:33 2008
Loaded: Tue Sep 23 12:21:59 2008
Patch is in-service In-service date: 10/03/07 01:24:08
Special Instructions: no
Applications stopped: None
Applications started: None
Requires reboot: No
PrePatch script: No
PostPatch script: No
Patch member type: JAR RPM: nortel-cs1000-vtrk-6.00.00-
00.i386.rpm
```

pload

Syntax: **pload [--all] <patch_name>.ntl --help**

Parameter	Description
--all	Loads all patches from the patch directory.
<patch_name>.ntl	Loads the patch called <patch_name> from the patch directory.
--help	Prints information about the pload command.

Description: The **pload** command loads a patch from a disk file and updates the on-switch database with the specific patch information.

The /var/opt/nortel/patch directory must contain the patch file to load.

The patch type includes the following:

- Patch—WAR or FRU. The format of patch name is pxxxxx_x.ntl.
- Serviceability Update (SU)—The format of SU name is <any_SU_name>.ntl.

Example 1: Use the following command to load the p20002_1.ntl patch.

```
$ pload p20002_1.ntl
Loading patch /var/opt/nortel/patch/p20002_1.ntl
Patch handle is:  1
```

Example 2: Use the following command to load all patches.

```
$ pload --all
Loading patch /var/opt/nortel/patch/p19000_1.ntl
Patch handle is:  0

Loading patch /var/opt/nortel/patch/p20002_1.ntl
Patch handle is:  1
```

pins

Syntax: **pins <patch_id> --all --help**

Parameter	Description
<patch_id>	Activates the patch with <patch_id> handle (as identified by pload or pstat commands).
--all	Activates all loaded patches.
--help	Prints information about the pins command.

Description: The **pins** command places a patch in service. The patch is placed into service for all processes to which it applies.

The patch must load (using the **pload** command) before the patch can be placed in service. The patch cannot be placed in service if it conflicts with another patch. The patch conflict checking includes application checking and patch element checking.

Example 1: Activate a patch with 4 handle (patch_id = 4).

```
$ pins 4
Patch handle:  4
All Nortel applications will be stopped.
Do you want to continue (Y/N) [N]? y
...
```

poos

Syntax: **poos <patch_id> --all >> --help,-h**

Parameter	Description
<patch_id>	Deactivates the patch with <patch_id> handle.
--all	Deactivates all patches.
--help or -h	Prints information about the poos command.

Description: Removes a patch from service. The patch is removed from service for all processes in which it was in service. A patch is always retained until the **poos** CLI command explicitly puts the patch out of service.

Note: In some cases, you cannot remove a patch (that is, the **poos** CLI command fails).

Example 1: Deactivate all patches.

```
$ poos --all
Patch handle:  0
Performing the uninstallation:
The patch 0 has been deactivated successfully
Patch handle:  1
Performing the uninstallation:
The patch 1 has been deactivated successfully
Patch handle:  2
Performing the uninstallation:
The patch 2 has been deactivated successfully
```

pout

Syntax: **pout <patch_id> --all --help**

Parameter	Description
<patch_id>	Unloads the patch with <patch_id> handle.
--all	Unloads all out of service patches.
--help	Prints information about the pout command.

Description: Unloads a patch that was loaded using the **pload** command and cleans up the on-switch database of the specific patch information.

Example 1: Unload the patch with 0 handle.

```
$ pout 0
Patch 0 has been removed successfully
```

Target service pack commands

The following CLI commands are available for service packs:

- “issp” (page 108)
- “spstat” (page 109)
- “spload” (page 110)
- “spins” (page 110)
- “spout” (page 111)

Note: There is no **spoos** command because service packs cannot be deactivated. For more information about service packs, see “Service packs” (page 21).

issp

Syntax: **issp [-h, --help]**

Parameter	Description
--help or -h	Prints the information for the issp command.

Description: Print a list of installed RPMs, serviceability updates, and patches.

Example 1: Print a list RPMs, SUs, and patches in a service pack.

```
$ issp
START:
##################
Release:  6.00.00.00
Machine:  i686
HostName:  abc.domain.name.com
##################
RPMs:
pcre-devel-4.5-3.2.RHEL4
PyQt-3.13-1
qt-designer-3.3.3-9.3
kdebase-devel-3.3.1-5.8
kdesdk-3.3.1-2
tetex-afm-2.0.2-22.EL4.7
linuxdoc-tools-0.9.20-14
docbook-utils-pdf-0.6.14-4
compat-libstdc++-296-2.96-132.7.2
```

```
libdbi-0.6.5-10.RHEL4.1
gsl-1.5-2.rhel4
unixODBC-kde-2.2.11-1.RHEL4.1
cyrus-sasl-ntlm-2.1.19-5.EL4
rusers-0.17-41.40.1
compat-gcc-32-c++-3.2.3-47.3
zsh-4.2.0-3.EL.3
am-utils-6.0.9-15.RHEL4
elfutils-libelf-devel-0.97-5
tftp-0.39-1
##################
SUs:
basesystem-8.0-5.1.1.001 Start:nrsm Stop:nrsm Reboot:no
 Spec:no
kernel-headers-2.6.18-53.el5.002 Start: Stop: Reboot:no
 Spec:Yes
zlib-1.2.3.3.003.001 Start:dbcom,sps,ncs Stop:ncs,dbcom
,sps Reboot:yes Spec:no
mktemp-2.0-0.0.0.005.001 Start: Stop: Reboot:yes Spec y
es
##################
Patches:
p12345_1 Start:dbcom Stop:dbcom Spec:no
p22345_1 Start: Stop: Spec:no
p53233_1 Start:dbcom,sps Stop:dbcom,sps Spec:yes
##################
EOF:
```

spstat

Syntax: **spstat [-l, --list] [-h, --help]**

Parameter	Description
--list or -l	Lists patch activity done for the currently loaded or in-service service pack.
--help or -h	Prints the information for the spstat command.

Description: Prints a status summary of all loaded and in-service service packs.

Example 1: Print a summary of installed and in-service service packs.

```
$ spstat 0
The following SP is in loaded status:  cs1000e_1.ntl Loaded
by user nortel on
```

```
Sat Mar 22 00:49:24 2008.
The following SP is in-service cs1000e_1.ntl Loaded by user
nortel on Sat Mar 20 01:11:33 2008.
```

spload

Syntax: **spload <service_pack_file_name>.ntl --help**

Parameter	Description
<service_pack_file_name>.ntl	Loads a service pack called <service_pack_file_name> into the system. The format of service pack file name is pxxxxx_x.ntl.
--help	Prints information about the spload command.

Description: Loads a service pack (a set of patches and serviceability updates) into the system database. The service pack content types includes the following:

- Patches—WAR or FRU
- Serviceability Updates

If not path is specified for the <service_pack_file_name>, the /var/opt/nortel/patch folder must contain the service pack file. If a path is given when specifying <service_pack_file_name>, then the service pack file must be in the path.

Example 1: Load the service pack called p20002_1.ntl.

```
$ spload p20002_1.ntl
Loading patch /var/opt/nortel/patch/p19000_1.ntl
Patch handle is:  0

Loading patch /var/opt/nortel/patch/p20002_1.ntl
Patch handle is:  1
...
```

spins

Syntax:**spins [--help]**

Parameter	Description
--help	Prints information about the spins command.

Description: Places a service pack in service. Only one service pack can be placed in service at one time. The **spload** command must have ran successfully for this command to work.

Example 1: Place a service pack in service.

```
$ spins
Performing the installation:
Name : nortel-cs1000-solid
Relocations: (not relocatable)
Version : 5.25.06
Vendor: (none)
Release : 00.4.50.0090
Build Date: Fri 12 Oct 2007 05:43:58 PM MSD
Install Date: (not installed)
Build Host: zbvwh0ja.ca.nortel.com
Group : Application Software
Source RPM: nortel-cs1000-solid-5.25.06-00.4.50.0090.src
.rpm
Size : 17825125
License: Commercial
Signature : (none)
URL : www.nortel.com
Summary : change summary
Description : Solid database server boost engine
distributed with nortel CS1000 product.
Do you want to continue? (Y/N) [Y]?
Performing new RPM patch installation...
Preparing... ##########################################
# [100%]
1:nortel-cs1000-solid ##################################
######### [100%]
executing Solid DB post install...
Installation nortel Solid database server completed.
Installing the Solid database server package done Done.
The RPM patch installation is completed.
The patch 2 has been activated successfully.
Patch handle: 1
Performing the installation:
The patch 1 has been activated successfully.
Patch handle: 0
Performing the installation:
Warning: installing a new file. Please pay attention to
the /etc/test1 file attributes
The patch 0 has been activated successfully.
Patch handle: 3
...
```

spout

Syntax: **spout [--help]**

Parameter	Description
--help	Prints information about the spout command.

Description: Unloads a service pack (the set of patches and serviceability updates) from the system database. The **sploa**d command must have ran successfully for this command to work. The **spins** command cannot have been run on this service pack.

Example 1: Unload the service pack.

```
$ spout
Patch 0 has been removed successfully
Patch 1 has been removed successfully
Patch 2 has been removed successfully
Patch 3 has been removed successfully
...
```

Patch maintenance

You must perform regular maintenance to remove patches, serviceability updates, and service packs to avoid excessive storage consumption. Another reason to clean up unused patches, serviceability updates, and service packs is that they are included when the element is backed up and this can result increased backup times and storage consumption.

When service packs are applied using Patching Manager or CLI, they are not automatically deleted. If application of a service pack results in automatic removal of patches or serviceability updates, these are also not deleted. Deactivation of patches or serviceability updates using Patching Manager results in complete removal of these items.

Use the Local Patching Manager on an element to identify and remove any patches or serviceability updates that are not in service. The Local Patching Manager can also be used to remove service packs.

> ***Note:*** After a service pack is applied, you can remove the service pack without affecting the patches and serviceability updates that were installed as part of the service pack.

Clean up must be done on the UCM and all target elements being patched. The **`sysBackup`** command backs up all patches, serviceability updates, and service packs that accumulate on the target elements making the backup files very large and slow to backup.

For more information about deleting service packs, patches, and serviceability updates, see the following:

- Central Patching Manager
  - “Delete a service pack from the central patch library” (page 50)
  - “Delete a patch from the central patch library” (page 55)
- Local Patching Manager
  - “Delete a service pack” (page 84)
  - “Delete a patch” (page 98)

Nortel Communication Server 1000

Patching Fundamentals

Release: 6.0
Publication: NN43001-407
Document revision: 01.03
Document release date: 12 June 2009

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com