NORTEL NETWORKS™

Nortel Networks Multiservice Switch 7400/15000/20000

Upgrading Software

NN10600-272

Document status: Standard
Document issue: sPCR6.1S1
Document date: February 2005
Product release: sPCR6.1
Job function: Upgrades
Type: NTP
Language type: US English

Contents

About this document

NN10600-272 *Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software* provides procedural and conceptual information on how to upgrade Nortel Networks Multiservice Switch node software. This document is intended for any user who has the responsibility of performing or planning a software upgrade on Multiservice Switch network devices.

This guide assumes you have an advanced knowledge of Multiservice Data Manager, Unix, Multiservice Switch software, and Multiservice Switch network architecture.

What's new in this document

The following feature was added to this document:

- Fabric card NTHR16EA (page 6)

Other changes made to this document include the following:

- The section Performing a hitless software migration (page 39) was updated for CR Q00983787.
- The section Performing initial software migration tasks (page 35) was updated to include information about having two options if migrating directly from a pre-PCR 6.1 release to a PCR 6.1 with patches. Also, information was included about performing hitless software migration from pre-PCR6.1 to PCR6.1 without a specific pre-PCR6.1 patch, in regards to the ethernet application.
- The sections Performing a hitless software migration (page 39) and Performing a service-interrupting software migration (page 46) were updated to include information about verifying the edit view, current view, and committed view commands patched AV.
- The section Performing auto patch application (page 69) was updated to correct information pertaining to the Auto-patch feature.
- The section Performing hitless software FP patching (page 71) was updated to change a step pertaining to the patched AV.

Fabric card NTHR16EA

The following section was updated

- Applying a software patch (page 67)

Procedure conventions

This document uses the following procedure conventions:

- The commands used in the procedures contain full component and attribute names. You can abbreviate the component and attribute names when you enter commands, however this document does not provide the abbreviations. For more information on abbreviating component and attribute names, see NN10600-060 *Nortel Networks Multiservice Switch 7400/15000/20000 Component Reference*. All component and attribute names are formatted in italics.
- The introduction of every procedure states whether you must perform the procedure in operational mode or provisioning mode. For more information on these modes, see Operational mode (page 6) or Provisioning mode (page 6).

Operational mode

Procedures contained within this document can either be performed in operational mode or provisioning mode. When you initially log into a node, you are in operational mode. Nortel Networks Multiservice Switch nodes use the following command prompt when you are in operational mode:

```
#>
```

where:
is the current command number

In operational mode, you work with operational components and attributes. In operational mode, you can

- list operational components and display operational attributes to determine the current operating parameters for the node
- control the state of parts of the node by locking and unlocking components
- set certain operational attributes and enter commands to perform diagnostic tests

Provisioning mode

To change from operational mode to provisioning mode, use the start Prov command. Only one user can be in provisioning mode at a time. Nortel Networks Multiservice Switch nodes use the following command prompt whenever you are in provisioning mode:

```
PROV #>
```

where:
is the current command number

In provisioning mode, you work with the provisionable components and attributes which contain the current and future configurations of the node. You can add and delete components, and display and set provisionable attributes. You can also verify your changes and then activate them as the new node configuration. You end provisioning mode and return to operational mode using the end Prov command.

For information on operational and provisionable attributes, see NN10600-060 *Nortel Networks Multiservice Switch 7400/15000/20000 Component Reference*.

Completing configuration changes

Several procedures in this document ask that you complete the configuration changes. When you complete the configuration changes, you are activating the configuration changes, confirming that you want to activate them, and saving the changes. Follow this procedure in provisioning mode when asked to complete the configuration changes. See the section Provisioning mode (page 6) for more information.

1. Verify that the provisioning changes you have made are acceptable:

   ```
   check Prov
   ```

   Correct any errors and then verify the provisioning changes again.

2. If you want to store the provisioning changes in a file, save the provisioning view with portable formats:

   ```
   save -f(<filename>) -portable Prov
   ```

3. If you want these changes as well as other changes made in the edit view to take effect immediately, activate and commit the provisioning changes:

   ```
   activate Prov
   confirm Prov
   c
   ommit Prov
   ```

4. End the provisioning session:

   ```
   end Prov
   ```

Software upgrade

Upgrade software to add new functionality and reliability to Nortel Networks Multiservice Switch nodes by activating a new version of software.

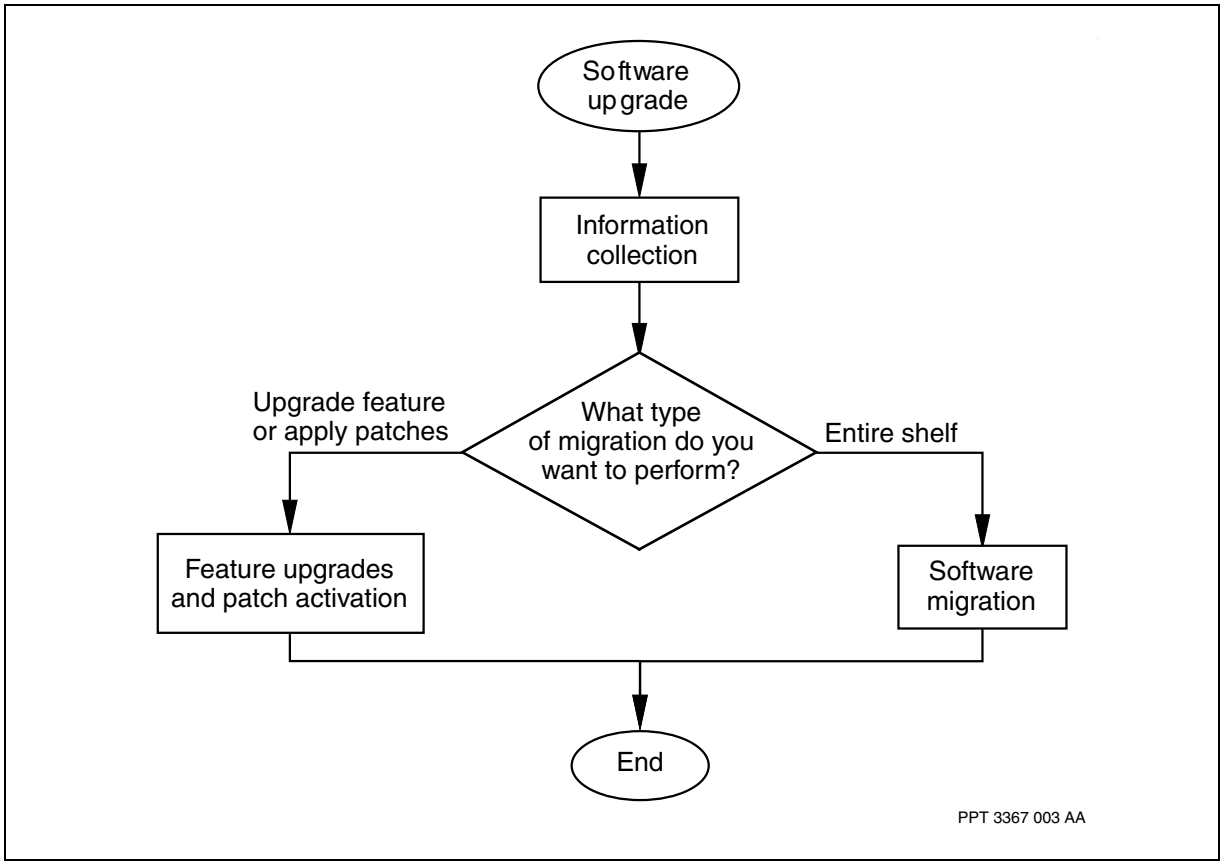
Prerequisites to software upgrade

- Contact your Nortel Networks technical representative prior to migrating software. For information on how to contact Nortel Networks technical support, refer to NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.
- There is new software available and a requirement for that new software has been determined.
- Determine the correct version of software or fabric card firmware you are migrating to and download it from the software distribution site. Refer to NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation* for more information on downloading software.

Software upgrade tasks

This work flow shows you the sequence of procedures you perform to upgrade software on a Nortel Networks Multiservice Switch node. To link to any procedure, go to Software upgrade task navigation (page 10).

Software upgrade tasks



Software upgrade task navigation

- Information collection (page 11)
- Software migration (page 19)
- Feature upgrades and patch activation (page 61)

Information collection

Collect information to identify and avoid any compatibility issues that could prevent completing a software migration successfully.

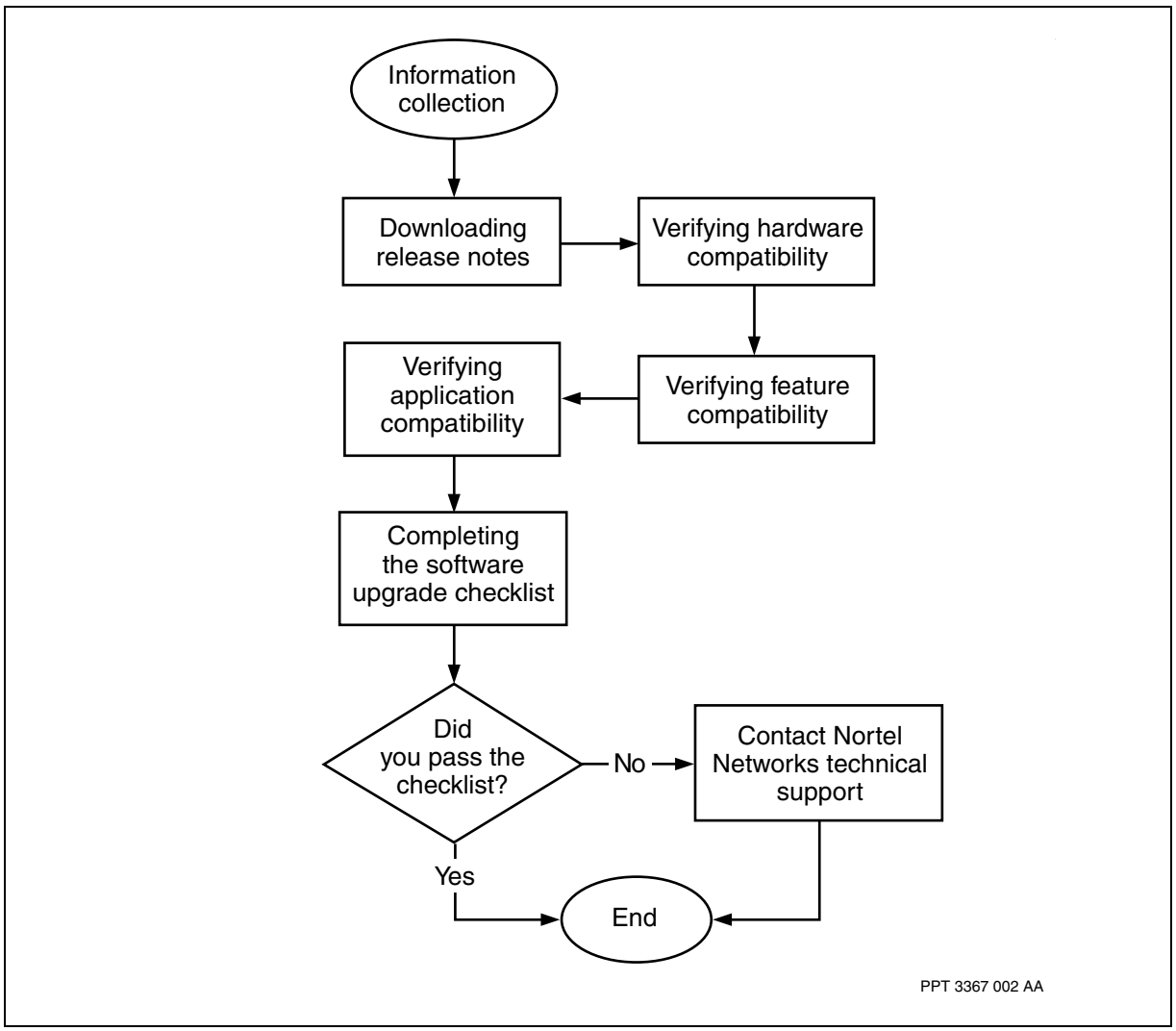
Prerequisites to information collection

- You have confirmed which release of software is active on the node.
- The node is operating without errors or failures.

Information collection procedures

This task flow shows you the sequence of procedures you perform to collect information about the upgrade. To link to any procedure, go to Information collection procedure navigation (page 12).

Information collection procedures



Information collection procedure navigation

- Downloading release notes (page 13)
- Verifying hardware compatibility (page 14)
- Verify feature compatibility (page 15)
- Verifying application compatibility (page 16)
- Completing the software upgrade checklist (page 17)
- Contact Nortel Networks technical support. For details on how to contact your Nortel Networks representative, see NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.

Downloading release notes

Download *Nortel Networks Multiservice Switch Release Notes* to collect specific information affecting hardware and services for each of the Nortel Networks Multiservice Switch node carrier releases (PCRs) involved in the migration.

Procedure steps

Step	Action
1	Got to Nortel Networks public website. http://www.nortelnetworks.com/
2	In the section titled “Support” click on Technical Documentation.
3	Click on the node product name in the list of products.
4	Click on the “documentation” link for the specific product you are upgrading.
5	Select and download all the documentation you require. Some documentation may require you to register and log in using your user ID and password.

--End--

Verifying hardware compatibility

Verify hardware compatibility to confirm that your hardware configuration will support all the software versions that will be used in the migration.

Procedure steps

Step	Action
1	Note the product engineering codes (PECs) of all the processor cards used in the node that is the target of the upgrade. `d shelf card/<card_no> *`
2	Review the hardware compatibility section of *Nortel Networks Multiservice Switch Release Notes* for each release in your migration path to determine if there are any other hardware considerations.
3	Compare your hardware configuration to the minimum supported hardware information in *Nortel Networks Multiservice Switch Release Notes* of each release in the migration path.

--End--

Variable definitions

Variable	Value
<card_no>	is the slot number that the card is inserted into.

Verify feature compatibility

Verify feature compatibility to confirm that your configuration of services and features will not be negatively affected by the software migration.

Procedure steps

Step	Action
1	Create a list of all Nortel Networks Multiservice Switch features loaded on the node that is the target of the upgrade.
2	Refer to *Nortel Networks Multiservice Switch Release Notes* for each PCR in your migration path to confirm there are no known compatibility issues.
3	If you have any doubt about the compatibility between your existing features and your migration path, contact your Nortel Networks Service Representative before beginning the migration.

--End--

Verifying application compatibility

Verify application compatibility to confirm that any third party software being used will not interfere with the software migration.

Procedure steps

Step	Action
1	List all the non-Nortel Networks Multiservice Switch applications you are using with the node that is the target of the upgrade.
2	Refer to the technical documentation of the non-Multiservice Switch software for any known compatibility issues with the PCR versions in your migration path.
3	Refer to *Nortel Networks Multiservice Switch Release Notes* of each PCR in your migration path to confirm there are no known compatibility issues.
4	Contact your Nortel Networks Service Representatives and inform them of your specific scenario to ensure there are no known compatibility issues.

--End--

Completing the software upgrade checklist

Complete the software upgrade checklist to confirm that all potential complications have been considered and eliminated.

Procedure steps

Step	Action
1	Complete the checklist Node software upgrade checklist (page 17) by referring to the information discovered while performing the Information collection procedures (page 12).

--End--

Procedure job aid

Node software upgrade checklist

Task	Complete
Migration plan including acceptance criteria and fall back strategy (backup & restore)	
Migration plan reviewed and verified by migration prime as well as operational and engineering resources	
Migration operator has complete knowledge of node applications, features, and software.	
Migration operator has complete knowledge of migrating software versions.	
Nortel Networks Multiservice Switch Release Notes for all releases in the migration path have been reviewed for potential impacts to the migration plan.	
Network health has been analyzed to verify no known problems exist.	
Network management platform meets minimum hardware requirements.	
Network management software is compatible with each release in the migration plan.	
Network statistical data is collected. (Install NetRx if required. See http://www.nortelnetworks.com)	
Node hardware is compatible with all releases in the migration path.	
Node software is compatible with all releases in the migration path.	
Non-Multiservice Switch applications are compatible with all releases in the migration path.	
All provisioning files have been saved (backed up).	
Network configuration changes are prohibited.	

(1 of 2)

Node software upgrade checklist (continued)

Task	Complete
The software version you are migrating to has been downloaded and installed on the node.	
The software patches you are applying have been downloaded and installed on the node.	
The file system is organized and the migration operator know which software versions are applicable to the migration path.	
The software version currently running on the node is:	
The intended software version after migration is:	
The software patches you are applying are:	
The PCRs between the intended software release and the current PCR operating on the node.	
(2 of 2)	

Software migration

Migrate software to save the current configuration and activate the new version. Monitoring, aborting, or confirming the migration success is part of the software migration task.

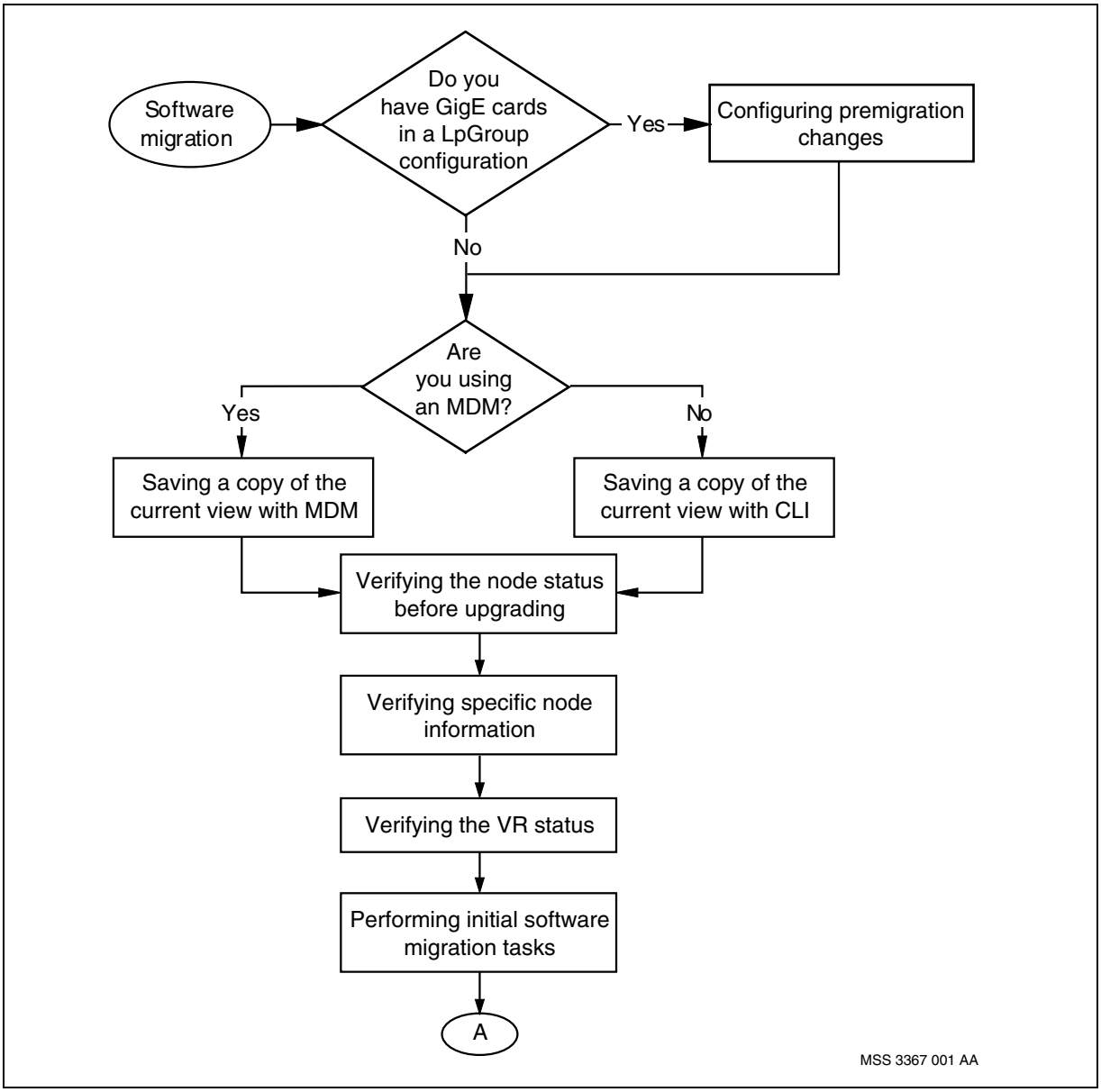
Prerequisites for software migration

- The committed view, the current view, the edit view, and the last used view must be identical. If these views are not the same, see NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation* for information on making them the same.
- Refer to the description of each FP card type in NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference* to understand any FP-specific migration considerations that may affect how the migration occurs.

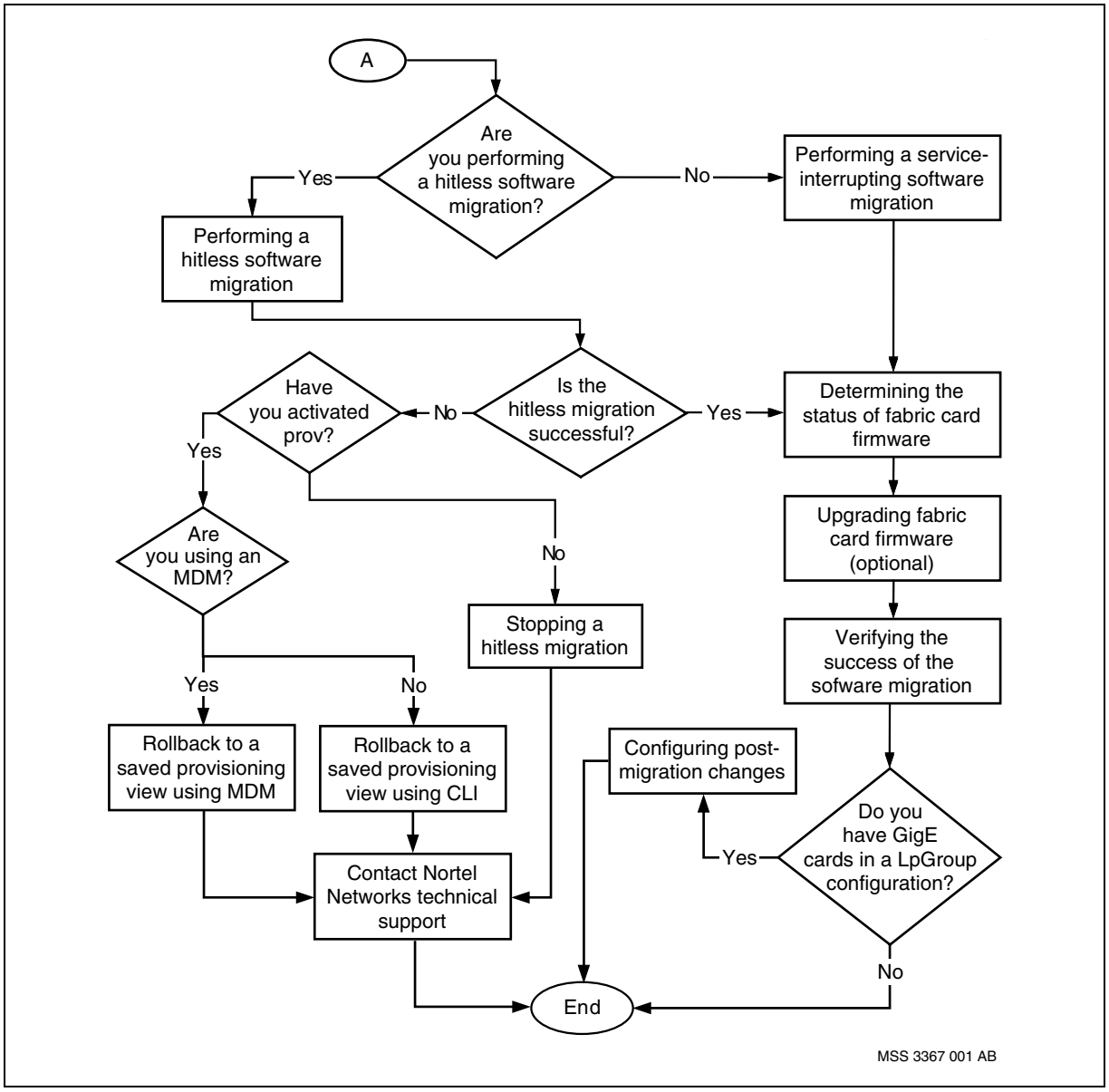
Software migration procedures

This task flow shows you the sequence of procedures you perform to migrate software. To link to any procedure, go to Software migration procedure navigation (page 21).

Software migration procedures



Software migration procedures (continued)



Software migration procedure navigation

- Configuring pre-migration changes (page 23)
- Saving a copy of the current view with Multiservice Data Manager (page 24)
- Saving a copy of the current view with CLI (page 26)
- Verifying the node status before upgrading (page 28)
- Verifying specific node information (page 31)
- Verifying the VR status (page 33)

- Performing initial software migration tasks (page 35)
- Performing a hitless software migration (page 39)
- Performing a service-interrupting software migration (page 46)
- Stopping a hitless software migration (page 49)
- Rollback to a saved provisioning view using Multiservice Data Manager (page 50)
- Rollback to a saved provisioning view using CLI (page 53)
- Determining the status of fabric card firmware (page 55)
- Upgrading Multiservice Switch 15000 and Multiservice Switch 20000 fabric card firmware (page 56)
- Verifying the success of the software migration (page 58)
- Configuring post-migration changes (page 59)
- Contact Nortel Networks technical support. For details on how to contact your Nortel Networks representative, see NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.

Configuring pre-migration changes

Configure pre-migration changes to reduce Hitless Software Migration (HSM) outage.

Procedure steps

Step	Action
1	Create a static ARP entry for all adjacent routers attached to all GigE ports. **`add Vr/<vr_name> Ip Arp HostEntry/<host_address>,na physAddress/<MAC_address>`**
2	Create a static ARP entry for this node, on each adjacent router attached to the GigE port.
	--End--

Variable definitions

Variable	Value
<host_address>	is the IP address of the static host being defined.
<MAC_address>	is the 48-bit MAC address of the host being defined. It is formatted as zero to eight pairs of hex digits separated by dashes. The default address is 00-00-00-00-00-00-00-00.
<vr_name>	is the name of the virtual router (Vr)

Saving a copy of the current view with Multiservice Data Manager

Save a copy of the current view with Nortel Networks Multiservice Data Manager to copy service data and application version information so if you must revert to a previous software load, you will not need to re-configure the old software release manually.

Prerequisites

- If you need to revert to a saved view of an older version of Nortel Networks Multiservice Switch software, when the node restarts, it restarts in the operational state it was in when you saved that view.
- The backup site can be the Multiservice Data Manager server or a Software Distribution Site (SDS) configured to store backed-up node service data.
- Verify that the backup site has enough space to accommodate the backup.
- The Backup server, the Restore server, the Passport Backup provider, the Passport Restore provider, and the Data Synchronization server must all be running on the Multiservice Data Manager workstation for the Passport Service Data Backup and Restore tool to function properly.

Procedure steps

Step	Action
1	Open a Multiservice Data Manager window: **`/opt/MagellanNMS/bin/nmstool &`** The copyright dialog and the Multiservice Data Manager window open.
2	Click *OK* to close the copyright dialog.
3	From the Multiservice Data Manager window, select Configuration > Passport Devices > Administration > Passport Service Data Backup/ Restore. The Passport Backup and Restore window opens with the Backup Configuration tab displayed.
4	Click Add. The Add Device dialog opens and displays a list of available nodes or node groups. This list of nodes or groups is obtained from the HGDS server.
5	Select the node. To select a node from within a group, click on the + beside a groupname to expand the displayed list.
6	Click the button box with incremental displayed. This provides a dropdown box containing the alternate backup mode full. Select full.
7	Configure the node's access information.

If a node userID and password were previously set as the defaults for node access from this MDM workstation, the button Use default will be checked. If the default userID and password are applicable to this node, click OK and go to the next step.

If a default node userID and password were not previously set for node access from this Multiservice Data Manager workstation or if the default userID and password are not applicable to this node, type a User ID and Password in the provided data entry boxes. The Use default button is un-checked. Click OK.

8 Click *Backup*.

When the back up completes successfully, a message is displayed in the Message area. If the back up is unsuccessful, an error dialog is displayed that specifies the device and the reason for the failure.

9 When the back up is finished, click *File > Exit* to close the window.

--End--

Saving a copy of the current view with CLI

Save a copy of the current view with CLI to copy service data and application version information so if you must revert to a previous software load, you will not need to re-configure the old software release manually.

Prerequisites

- If you need to revert to a saved view of an older version of the node software, when the node restarts, it restarts in the operational state it was in when you saved that view.
- The view to be saved must have a value of either commit or portable.
- You must have write permissions on the node.
- You must understand FTP.
- You must save and restore all views in binary format.

Procedure steps

Step	Action
1	Display on-switch provisioning to determine the filenames of the current, committed, and last viewed provisioning files that you need to copy: **`display -o prov`** The current view and committed view must be the same before performing the software upgrade.
2	List the directories for the provisioning views that you can back up: **`listfile -path(provisioning) fs`**
3	List the provisioning files within your chosen directory that you need to back up: **`listfile -path("/provisioning/<filename>.<type>.<num>") fs`** You will need to back up all of the files in the directory, including portable, view, and lp0 through lp15 depending on the type of node.
4	If needed, create a directory on the Multiservice Data Manager server to save the view: **`mkdir <prov_dir>.<type>.<num>`**
5	On the Multiservice Data Manager server, change to the directory you wish to save the provisioning files in: **`cd <prov_dir>.<type>.<num>`**
6	From the Multiservice Data Manager server, FTP to the node: **`ftp <nodename>`**

7 Change to the provisioning directory:

```
ftp> cd provisioning
```

8 List the files in the directory:

```
ftp> ls
```

9 Change to the directory that contains the view:

```
ftp> cd <filename>.<type>.<num>
```

10 List the files in the directory:

```
ftp> ls
```

11 Change the file transfer mode to binary:

```
ftp> binary
```

12 Transfer each file in the directory:

```
ftp> get <prov_files>
```

You must transfer all files from the directory. These files include portable, view, and lp0 through lp15 depending on node type.

13 Quit your FTP session:

```
ftp> quit
```

--End--

Variable definitions

Variable	Value
<filename>	is the name of the file that contains the committed or portable provisioning data. The variable must be between 1 and 13 characters in length. Current and edit are not valid names.
<nodename>	is the name of the node.
<num>	is the number of the file that contains the provisioning data. This number must be a 3 digit sequence.
<prov_dir>	is the name of the workstation directory to save the committed or portable provisioning view. The variable must be between 1 and 13 characters in length. Current and edit are not valid names.
<prov_files>	are the names of the provisioning files.
<type>	is the type of the file, either full or part, that contains the provisioning data.

Verifying the node status before upgrading

Verify the status of the node before upgrading to ensure that the node does not have any alarms raised, and that it has been configured correctly. In addition, by recording the current status, you can compare it to the status following the upgrade to verify that the upgrade proceeded correctly

Prerequisites

- If your network has a lot of live connections, displaying the status of the logical processors, SONET ports, and ATM interfaces will result in large amounts of output.
- Save the information gathered in the following procedure to verify the success of the upgrade. To save the information to a file if you are using Nortel Networks Multiservice Data Manager Command Console, select *Log to File* from the File menu and set the options in the Log to File dialog as required. If you are not using Multiservice Data Manager Command Console, use the standard UNIX logging functionality.
- If any of the components displayed in the following procedure are not enabled or have alarms, investigate the cause and correct the problem before proceeding with the hitless software migration. The node you are upgrading and all of the nodes connected to it must be free of alarms.

Procedure steps

Step	Action
1	Verify that the disk and file systems are synchronized: **`display FileSystem syncStatus`**
2	Verify that the syncProgress between the disk and the file system is 100%: **`display FileSystem syncProgress`**
3	Verify that all logical processors on the system are enabled and without alarms: **`display Lp/* osistate`**
4	Verify that all the SONET or SDH ports configured on the system are enabled and without alarms: **`display Lp/* Sonet/* osistate`** **`display Lp/* Sdh/* osistate`**
5	Verify that all service interfaces configured on the system are enabled and without alarms: For example: **`display AtmIf/* osistate`**
6	Verify all trunks or any other services are running correctly.

For example:

display trk/*

7 Ensure that there is no provisioning activity on the control processors by verifying that the standbyCpAtctivity value is none:

display prov standbyCpActivity

8 Ensure that there is no provisioning activity on the control processors by verifying that the standbyCpAtctivityProgress value is n/a:

display prov standbyCpActivityProgress

9 If this is a remote migration, verify that the active control processor has Ethernet connections available:

display Lp/0 Oamenet/<enet_port> activeStatus

10 If this is a remote migration, verify that the standby control processor has Ethernet connections available:

display Lp/0 Oamenet/<enet_port> standbyStatus

--End--

Variable definitions

Variable	Value
<enet_port>	is the port number of the OAM Ethernet port on the control processors.

Procedure job aid

Example of osistate display

```
5> display Lp/* Sonet/* osistate

Lp/* Sonet/*
```

Example of system display showing all components enabled and no alarms.

```
+==+=====+=====+====+=====+=======+=======+=======+=======+====+=====
|Lp |Sonet|osiAdmin|osiOper|osiUsage|osiAvail|osiProc|osiCntr|osiAlarm|osiStby|osiUnknw
+==+=====+=====+====+=====+=======+=======+=======+=======+====+=====
|2  | 1   |unlck  |ena    |busy    |        |       |       |nSet    |false
|2  | 2   |unlck  |ena    |busy    |        |       |       |nSet    |false
|3  | 1   |unlck  |ena    |busy    |        |       |       |nSet    |false
|3  | 2   |unlck  |ena    |busy    |        |       |       |nSet    |false
|8  | 0   |unlck  |ena    |busy    |        |       |       |nSet    |false
|8  | 1   |unlck  |ena    |busy    |        |       |       |nSet    |false
|8  | 2   |unlck  |ena    |busy    |        |       |       |nSet    |false
|8  | 13  |unlck  |ena    |busy    |        |       |       |nSet    |false
|9  | 0   |unlck  |ena    |busy    |        |       |       |nSet    |false
|9  | 1   |unlck  |ena    |busy    |        |       |       |nSet    |false
|9  | 3   |unlck  |ena    |busy    |        |       |       |nSet    |false
|9  | 13  |unlck  |ena    |busy    |        |       |       |nSet    |false
```

Verifying specific node information

Verify specific Nortel Networks Multiservice Switch 15000 or Multiservice Switch 20000 node information before upgrading to ensure that the node does not have any alarms raised and that it has been configured correctly.

Attention: This procedure is only applicable to Multiservice Switch 15000 and Multiservice Switch 20000 nodes.

Procedure steps

Step	Action

CAUTION

Possibility of a non-hitless software migration

Any card that does not have equipment protection enabled will undergo a regular software upgrade during the migration and experience an outage. If there is a card that has equipment protection configured on it, but has a value of *nset* displayed in the *osiStby* column, that protection pair will also undergo a service outage.

Investigate why that value is being displayed and correct the problem before proceeding with a hitless software migration.

1 Verify that the equipment protection has been configured properly:

```
display Shelf Card/* SparedServices
```

All cards configured with equipment protection should have a value of serv. All standby function processors should have a value of hot indicating hot standby. The main control processor must have a value of cold indicating cold standby.

2 Display the *Laps* components:

```
display Laps/*
```

3 For each *Laps* component, remove the manual overrides related to the automatic selection of the active line of a link protected by line automatic protection switching (LAPS):

```
clear Laps/<laps_inst>
```

Issuing this command clears the effects of the *protectionLockout Laps* and the *switch Laps* commands and ensures that all higher priority commands are nulled before the migration.

4 Verify that the *lop, ais, rfi, slm, txAis* and *txRdi* attributes of the *Laps* components have a value of *off*:

```
display Laps/* Sts/0
```

5 Verify that the *Laps* components are enabled and without alarms:

```
display Laps/* osistate
```

--End--

Variable definitions

Variable	Value
<laps_inst>	is the instance value of the *Laps* component whose manual overrides you want to remove. This instance value is an integer between 0 and 15999.

Verifying the VR status

Verify the status of the Virtual Router (VR) before upgrading so that if problems arise, you can compare the VR status before the upgrade to the status of the VR following the upgrade.

Procedure steps

Step	Action
1	Display and record the virtual router instance values: **`list VirtualRouter/*`**
2	Display and record the virtual router protocol port instance values: **`list VirtualRouter/0 ProtocolPort/*`**
3	Display and record information about the OamEnet logical interfaces for all the *VirtualRouter* and *ProtocolPort* instances in case problems occur during the migration and you need to reconfigure this component: **`display -p VirtualRouter/<vr_inst> ProtocolPort/ <pp_num> Ipport LogicalIf/*`** You will need to record the *address, netMasks, broadcastAddress* and the *linkDestinationAddress* attribute values.
4	Display and record information about the static routes of all *VirtualRouter* instances, in case problems occur during the migration and you need to reconfigure this component: **`display -nt VirtualRouter/<vr_inst> Ip Static Route/*`**
5	Verify that all protected static routes are enabled and 'card protected'. **`display VirtualRouter/<vr_inst> Ip Static Route/* operationalState, protectionLevel`**
6	Display and record information about the static route next hop of all *VirtualRouter* instances, in case problems occur during the migration and you need to reconfigure this component: **`display -nt VirtualRouter/<vr_inst> Ip Static Route/* Nh/*`**

--End--

Variable definitions

Variable	Value
<pp_num>	is the instance value of the *ProtocolPort* component.
<vr_inst>	is the instance value of the *VirtualRouter* component.

Performing initial software migration tasks

Perform initial software migration tasks in order to change the software version to allow for new or improved functionality without causing a loss of service.

Attention: This procedure is applicable for both hitless software migrations and service-interrupting migrations.

Prerequisites

WARNING

Calls in progress are dropped

A hitless migration strategy removes inactive control and function processors from service. As a result, redundancy in the event of failure of the active shelf components is not available and some transient calls are dropped. Stable calls are unaffected by the migration.

A service-interrupting migration strategy removes function processors from service. As a result active calls are dropped during the migration.

Undertake the procedures required by this strategy during low-traffic periods.

CAUTION

Loss of stable SVC connections may occur

When you perform the hitless software migration, a loss of SVC connections may occur. Although stable SVC calls should remain active in a redundant processor configuration, exercise caution when performing this upgrade.

Undertake the procedures required by this strategy during low-traffic periods.

- The migration will take between fifteen minutes, and three-and-a-half hours of time, depending on the number of calls and components that have been provisioned on the node.
- It is recommended that you perform this upgrade using the Command Console tool on Nortel Networks Multiservice Data Manager server rather than through a Telnet session. By using the Command Console, you ensure that you will remain connected to the node, and can monitor the CP switchover. For more information on opening the Command Console, see 241-6001-303 *Nortel Networks Multiservice Data Manager Customization and Administration*.

- While you perform software migration tasks, the system may interrupt the process to display warnings or notifications. Some of these notifications may require you to confirm your intent before continuing. Respond as required by the online instructions.
- For a hitless software migration, the node must contain two control processors (CP). One CP must be active and the other CP must be in standby mode. For a service-interrupting software migration, two CPs are not required, but recommended, as loss of service will be minimized if the node contains two CPs.
- Hitless software migration only applies to FPs in a one-for-one equipment sparing configuration. The active FPs must be provisioned for one-for-one equipment sparing. During the software migration, equipment protection is unavailable for those cards whose standby card is part of the migration shelf.

Procedure steps

Step	Action
1	Enter provisioning mode so that you can issue the appropriate commands: **`start -force prov`**

Attention: If the system indicates that the edit view and the current view are the same, proceed to step 3.

Step	Action
2	Copy the current view into the edit view to ensure that they are identical: **`copy prov`**

Attention: If you were cross-referenced to this step as a method to abort the migration before activation, no outage will occur as you have not yet started the hitless software migration.

Step	Action
3	Save the current software provisioning. **`save -c -file(<filename>) prov`** Make note of the filename you choose as pre-caution for Rollback.
4	Display the current software application version list: **`display -c Software avList`** The release is indicated by the version number after the underscore. For example, *CD01S1E* is PCR software release 4.1.1. There may be different versions of the software applications on the node.

WARNING

avList requires the same number of applications

The new sw avList must contain the same number of applications as the old avList of the release you are migrating from in order for the upgrade to be hitless.

For example, the fabric application, while it is not required to be set on the new sw avList, if it was on the previous sw avList, it would cause the number of applications listed to be different, making the upgrade non-hitless.

5 Remove the fabric package from the application version list.

```
set Software avList ~fabric_<old_VersionNumber>
```

6 Activate and confirm these changes:

```
activate prov
confirm prov
```

7 Replace all of the old application versions in the application version list with the new application versions of the release you are migrating to:

```
set Software avList ! <new_applications>
```

Attention: Do not set the software applications for the fabric. Refer to Upgrading Multiservice Switch 15000 and Multiservice Switch 20000 fabric card firmware (page 56) for more information about upgrading the fabric firmware.

Attention: The ethernet application is required in PCR6.1 to load software on 4pGigE function processors. However, since the ethernet application is not present in pre-PCR6.1 releases, customers cannot perform hitless software migration from pre-PCR6.1 to PCR6.1 without a specific pre-PCR6.1 patch. Refer to Clarify Bulletin 2004005174 for further information about this patch, or contact Nortel Networks Global Network Technical Support.

8 Check that the new applications are in the application version list and that, other than the load name, the applications are the same as those listed in step 4:

```
display Software avList
```

Attention: If you are migrating directly from a pre-PCR6.1 release to PCR6.1 with patches, there are two options available, as described below.

Option 1: Apply a specific pre-PCR6.1 migration patch, download patch_CF01xxx, then migrate directly to PCR6.1 with patches following the procedure below. Contact Nortel Networks Global Network Product Support to obtain the appropriate pre-PCR6.1 migration patch. The patch format will be baseFT420A_XXXXXX for Multiservice Switch 15000 and Multiservice Switch 20000, and base7T420A_XXXXXX for Nortel Networks Multiservice Switch 7400. The patch Readme file will contain download and activation instructions.

Option 2: Without the pre-PCR6.1 migration patch, patches cannot be applied simultaneously with software migration to PCR6.1. You must first migrate to the appropriate PCR6.1 release with no patches, download the patch AV (e.g. patch CF01D), add the patch AV to the "sw avl", and then apply the patches. Hence, for this option, Step 9 would be:

```
set Software patchlist !
```

9 If there is a patch required for the release you are migrating to, apply the patches needed to the patchlist:

```
set Software patchlist ! <patches>
```

10 Verify the patches that are going to be applied:

```
display Software patchlist
```

--End--

Variable definitions

Variable	Value
<new_applications>	is a space-separated, case-sensitive list of application versions. The release is indicated by the version number after the underscore.
<patches>	is a space-separated, case-sensitive list of patches.

Performing a hitless software migration

Perform a hitless software migration to change the software version currently in use on the node to allow for new or improved functionality without causing a loss of service.

Prerequisites

CAUTION
Risk of loss of service
Do not activate a hitless software migration when migrating software versions of a feature. The impact on service cannot be predicted if both migrations are attempted at the same time.

Procedure steps

Step	Action
1	Verify that the *editViewChangedComponents* attribute indicates that you have made only one provisioning change, or two provisioning changes if one of those changes was to clear a patchlist and set a new one: `display -o prov`

WARNING
Risk of interruption of all calls in progress
The software upgrade for the node is hitless only if the new provisioning view contains only the new AVL. If the system indicates that more than one provisioning change has occurred, and one of those two changes was not clearing a patchlist and setting a new one, the node will go through a normal software migration that is not hitless and all calls are interrupted.

If more than one provisioning change has occurred, repeat step 2 of the procedure Performing initial software migration tasks (page 35) and then perform the procedure Verifying the node status before upgrading (page 28) again.

WARNING

Proceeding with a non-hitless software migration

The node will go through a normal software migration that is not hitless and all calls on the node are interrupted if the system returns the following message:

```
All applications will experience service
outage.
```

If this happens, abort the hitless software migration. For more information, see Stopping a hitless software migration (page 49).

2 Perform a semantic check:

```
check prov
```

The node continues with a hitless software migration if the system returns the following message:

```
Some applications may experience service outage.
```

Here is a sample output from the switch:

```
Lp/0
   Warning:
      Reason: Lp 0 (card 1) will be reset when this view
      is activated.
Lp/3
   Warning:
      Reason: Lp 3 (card 3) will be reset when this view
      is activated.
Prov
   Warning:
      Activation will disrupt service for the following
      component(s):
            Lp/0
            Lp/3
   Warning:
      Activation will result in a software migration
      system reload. Some applications may experience
      service outage.
```

3 Save the edit view with portable formats:

```
save -f(<filename>) -portable prov
```

WARNING
Unexpected messages about the logical processors
If the system gives you unexpected messages about the logical processors during the migration, abort the migration. For more information, see Stopping a hitless software migration (page 49).

4 Apply the changes and start the migration:

```
activate prov
```

A warning is generated indicating that a new component is being created for the hitless software migration.

If there are any logical processors that cannot participate in the hitless software migration because of provisioning reasons (for example, they are unspared or in a 1forN configuration) or because of operational reasons (for example, a standby card is unavailable), the system identifies these logical processors.

If the list of logical processors changes during the software migration, the system generates a *Migration Visible Alarm*, which pauses the software migration. You can choose to abort the migration at this time. For more information, see Stopping a hitless software migration (page 49). To continue with the migration, type *continue prov*.

5 To monitor the progress of the migration, enter the following command:

```
display -o prov
```

The results of this command are constantly updated in operational mode. Even when the node is reconnecting, you can use this command to monitor the upgrade.

You can continue to issue this command up until you lose connectivity to the node. When the active control processor begins to load the software, connectivity is lost. Once you lose connectivity, you will need to log back into the node (see step 6). If you are using Nortel Networks Multiservice Data Manager Command Console, the connection to the node is automatically re-established, but you will need to get back into provisioning mode. For more information, see Performing initial software migration tasks (page 35).

6 If using Telnet, when prompted, log in to the node with the appropriate permissions.

CAUTION
Risk of loss of service
You must enter the confirm prov command. If you do not enter this command, the shelf resets and you can cause a loss of all services.

7 Within 20 minutes of activating the new software and completing the software migration, confirm the changes to avoid a non-hitless rollback to the previously committed configuration:

```
confirm prov
```

8 Enter provisioning mode:

```
start -force prov
```

9 Check and confirm the changes made. Refer to Completing configuration changes (page 7) for details.

You may see warnings during the semantic check, but they will not disrupt service.

A committed file is required in case of a node reset, at which time the committed view will be reloaded.

10 Verify that the edit view, current view, and committed view are the same:

```
display -o prov
```

If they are not, issue the following commands:

```
check prov
save prov
act prov
confirm prov
commit prov
```

11 Exit provisioning mode once the migration is complete:

```
end prov
```

--End--

Variable definitions

Variable	Value
<filename>	is the name of the file to which you are saving the view. You should make this file name easily identifiable.

Procedure job aid

Impact of an error condition on a node during a hitless software migration

Phase	Error condition	Result and action
1) Active CP pre-work	Criteria for activate prov is not met.	Command failed.
	Cannot save temp file.	Command failed. Check disk usage and tidy disk if necessary.
	Active CP crashes (service shelf).	CP switchover. Take action based on responses or alarms received as a result of the failed activity.
2) CP migration	Cannot load new software.	Command failed. Take action based on responses or alarms received as a result of the failed activity.
	Cannot build migration provisioning view.	Command failed. Take action based on responses or alarms received as a result of the failed activity.
	Cannot save commit formats.	Command failed. Check disk usage and tidy disk if necessary, or take action based on responses or alarms received as a result of the failed activity.
	Cannot deliver shelf management data.	Command failed. Take action based on responses or alarms received as a result of the failed activity.
3) FP migration	Cannot load new software.	FP failed. Take action based on responses or alarms received as a result of the failed activity.
	An application does not acknowledge the provisioning data entry.	Application failed. Take action based on responses or alarms received as a result of the failed activity.
	An application negatively acknowledges the provisioning data delivery.	Application failed. Take action based on responses or alarms received as a result of the failed activity.
	An application cannot achieve synchronization of dynamic data.	Application failed. Take action based on responses or alarms received as a result of the failed activity.
4) Migration switchover	Active CP crashes (service shelf).	Continue with software migration.
5) Post-migration switchover	Former migrating CP cannot become active.	Service shelf outage. The system rolls back to the committed provisioning view. No operator action.

(1 of 3)

Impact of an error condition on a node during a hitless software migration (continued)

Phase	Error condition	Result and action
	Former migrating FP cannot become active.	FP outage. The new provisioning view is maintained. Respond to alarms generated by the system.
	Operator does not or cannot confirm provisioning changes.	Service shelf outage. The system rolls back to the committed provisioning view. No operator action.
	The newly active CP crashes (with or without standby CP available).	Service shelf outage. The system rolls back to the committed provisioning view. No operator action.
	FP crashes.	Normal recovery procedure. The FP resets, reloads software, reloads provisioning data, and restarts applications. The new provisioning view is maintained.
	Former service shelf FPs/CP cannot reload with new software.	Equipment sparing is not restored. The new provisioning view is maintained. Respond to alarms generated by the system.
	Disk synchronization failed or unexpectedly lost.	Respond to alarm generated by the system. The commit prov command is not accepted until disk synchronization is achieved or the standby CP is removed from service.
Any phase	Any FP crash (service shelf).	The system performs the appropriate recovery procedure, depending on the type of sparing that is available for an FP crash, either processor sparing or a card restart. The software migration activation continues.

(2 of 3)

Impact of an error condition on a node during a hitless software migration (continued)

Phase	Error condition	Result and action
1-3	Disk synchronization failed or unexpectedly lost.	A hardware disk failure has occurred, or the CP's disks are not the same size and the total data on the disk exceeds the size of the smallest disk. It is normal to lose disk synchronization when the standby CP is reset to reload new software. Disk synchronization must be regained before the migration switchover can occur. Take action based on responses or alarms received as a result of the failed activity.
2-3	Active CP crashes (service shelf).	If both of the following conditions are true, then this error triggers migration switchover: - disks are synchronized - Lp/0 is ready for migration switchover. FPs that have not completed their FP migration phase are reset. FPs that have completed their FP migration phase switchover to the new software. If either of the conditions are not true, then the system rolls back to the committed provisioning view. A service shelf outage occurs.
(3 of 3)		

Performing a service-interrupting software migration

Perform a service-interrupting software migration to change the software version the node is using to allow for new or improved functionality in a situation where the upgrade is expected to cause a service outage.

Prerequisites

CAUTION
Loss of service
Do not activate a service-interrupting software migration when migrating software versions of a feature. The impact on service cannot be predicted if both migrations are attempted at the same time.

- Limit the impact of the service interruption by temporarily redirecting traffic to other nodes in your network.

Procedure steps

Step	Action
1	Verify that the *editViewChangedComponents* attribute indicates that you have made only one provisioning change, or two provisioning changes if one of those changes was to clear a patchlist and set a new one: **`display -o prov`**
2	Perform a semantic check: **`check prov`** A warning that you are proceeding with a non-hitless migration should appear.

WARNING
Proceeding with a non-hitless software migration
The node will go through a normal software migration that is not hitless and all calls on the node are interrupted if the system returns the following message:

```
All applications will experience service
outage.
```

Step	Action
3	Save the edit view with portable formats: **`save -f(<filename>) -portable prov`**
4	Apply the changes and start the migration:

```
activate prov
```

5 To monitor the progress of the migration, enter the following command:

```
display -o prov
```

The results of this command are constantly updated in operational mode. Even when the node is reconnecting, you can use this command to monitor the upgrade.

You can continue to issue this command up until you lose connectivity to the node. When the active control processor begins to load the software, connectivity is lost. Once you lose connectivity, you will need to log back into the node (see step 6). If you are using Nortel Networks Multiservice Data Manager Command Console, the connection to the node is automatically re-established, but you will need to get back into provisioning mode. For more information, see Performing initial software migration tasks (page 35).

6 If using Telnet, when prompted, log in to the node with the appropriate permissions.

7 Within 20 minutes of activating the new software and completing the software migration, confirm the changes to avoid a non-hitless rollback to the previously committed configuration:

```
confirm prov
```

8 Enter provisioning mode:

```
start -force prov
```

9 Check and confirm the changes made. Refer to Completing configuration changes (page 7) for details.

You may see warnings during the semantic check, but they will not disrupt service.

A committed file is required in case of a node reset, at which time the committed view will be reloaded.

10 Verify that the edit view, current view, and committed view are the same:

```
display -o prov
```

If they are not, issue the following commands:

```
check prov
save prov
act prov
confirm prov
commit prov
```

11 Exit provisioning mode once the migration is complete:

```
end prov
```

--End--

Variable definitions

Variable	Value
<filename>	is the name of the file to which you are saving the view. You should make this file name easily identifiable.

Stopping a hitless software migration

Stop a hitless software migration to abort the migration and keep the provisioning view before the software application version list was changed. To abort an upgrade without causing a service outage, this procedure must be performed during the migration-switchover phase.

Prerequisites

WARNING
Service outage
If you issue the *stop prov* command after the migration-switchover phase, it will cause a service outage.

Procedure steps

Step	Action
1	Stop the migration: `stop prov`
2	To resume a hitless software migration after issuing the *stop prov* command, wait until both control processors' LEDs are green, with one flashing and one solid and see Performing a hitless software migration (page 39).

--End--

Rollback to a saved provisioning view using Multiservice Data Manager

Rollback to a saved provisioning view using Nortel Networks Multiservice Data Manager to abort an upgrade and revert to a previous working provisioning file on the node using the Passport/SNMP Devices Backup and Restore tool. Aborting an upgrade minimizes the impact of problems you are encountering during the upgrade. and is suggested if service windows close, failures occur on other nodes, or an unexpected MigrationVisibleAlarm is raised.

Prerequisites

WARNING

Reverting to an earlier software version is not hitless

After the originally-active CP and FPs have been reset, reverting back to the old configuration view is not hitless. At this point, any downgrade to the old configuration view results in a loss of call processing. While loading the old software and configuration view, the following events occur: call processing is initially maintained while the previous software load is loaded into one of the control processors. The function processors then go out of service, resulting in a loss of calls.

WARNING

Loss of provisioning changes

If you revert the node to an earlier version of the software, provisioning changes made to the upgraded version are lost.

- You must ensure the FPs and CPs in the node are compatible with the level of software to which you are reverting.
- You must refer to the *Nortel Networks Multiservice Switch Release Notes* of the PCR you are reverting to and identify any hardware or software considerations.
- The node restarts in the operational state it was in when you saved the current view if you revert to a saved view of an older software version.
- The Backup server, the Restore server, the Passport Backup provider, the Passport Restore provider, and the Data Synchronization server must all be running on the Multiservice Data Manager workstation for the Service Data Backup and Restore tool to function properly.

Procedure steps

Step	Action
1	Open a Multiservice Data Manager window: **`/opt/MagellanNMS/bin/nmstool &`** The copyright dialog and the Multiservice Data Manager window open.
2	Click *OK* to close the copyright dialog.
3	From the Multiservice Data Manager window, select Configuration > Passport Devices > Administration > Passport Service Data Backup/ Restore. The Passport Backup and Restore window opens with the Backup Configuration tab displayed.
4	Click the Restore tab.
5	Click Add. The Add Device dialog opens and displays a list of the nodes that have previously been backed-up.
6	Select the node.
7	Click the button box with incremental displayed. This provides a dropdown box containing the alternate backup mode full. Select full.
8	Configure the node access information. If a node userID and password were previously set as the defaults for node access from this Multiservice Data Manager workstation, the button Use default will be checked. If the default userID and password are applicable to this node, click OK and go to the next step. If a default node userID and password were not previously set for node access from this Multiservice Data Manager workstation or if the default userID and password are not applicable to this node, type a User ID and Password in the provided data entry boxes. The Use default button is un-checked. Click OK.
9	Click *Restore*. When the backup completes successfully, a message is displayed in the Message area. If the backup is unsuccessful, an error message is displayed that specifies the device and the reason for the failure. After restoring the data, you need to make the restored configuration data active.
10	When the view restore is finished, click *File > Exit* to close the window.
11	Log back in to the node.
12	Download to the node any required application software missing from the node's disk.

13 Enter provisioning mode so that you can issue the appropriate commands:

```
start prov
```

14 Activate the previously saved view:

```
reloadCp -file (<filename>) lp/0
```

If there is only one CP on the shelf, use the -force command:

```
reloadCp -force -(<filename>) lp/0
```

Network connectivity is lost and the node starts reloading the old software.

WARNING

Possible loss of calls

After activating the previously saved view, the following events occur: call processing is initially maintained while the previous software load is loaded into one of the control processors. The function processors then go out of service, resulting in a loss of calls.

15 Reconnect to the node.

16 Confirm the provisioning changes:

```
confirm prov
```

17 Save the view:

```
save prov
```

18 Commit the provisioning changes:

```
commit prov
```

19 Exit provisioning mode once the migration is complete:

```
end prov
```

--End--

Variable definitions

Variable	Value
<filename>	is the name of the previously saved view.
<IPAddress>	is the IP address of the node to which you want to connect.

Rollback to a saved provisioning view using CLI

Rollback to a saved provisioning view using CLI to revert the node to a provisioning view that was saved while running a previous version of the software and have already issued the *activate prov* command.

Prerequisites

WARNING

Reverting to an earlier software version is not hitless

After the originally-active CP and FPs have been reset, reverting back to the old configuration view is not hitless. At this point, any downgrade to the old configuration view results in a loss of call processing. While loading the old software and configuration view, the following events occur: call processing is initially maintained while the previous software load is loaded into one of the control processors. The function processors then go out of service, resulting in a loss of calls.

WARNING

Loss of provisioning changes

If you revert the node to an earlier version of the software, provisioning changes made to the upgraded version are lost.

- You must ensure the FPs and CPs on the shelf are compatible with the level of software to which you are reverting.
- If you need to revert to a saved view of an older version of node software, when the node restarts, it restarts in the operational state it was in when you saved the current view.

Procedure steps

Step	Action
1	Log in to the node with the appropriate permissions.
2	Enter provisioning mode so that you can issue the appropriate commands: `start prov`
3	Activate the previously saved view: `reloadCp -file (<filename>) lp/0` If there is only one CP in the node, use the -force command:

```
reloadCp -force –(<filename>) lp/0
```

Network connectivity is lost and the node starts reloading the old software.

WARNING

Possible loss of calls

After activating the previously saved view, the following events occur: call processing is initially maintained while the previous software load is loaded into one of the control processors. The function processors then go out of service, resulting in a loss of calls.

4 Reconnect to the node.

5 Confirm and save the provisioning changes Refer to Completing configuration changes (page 7) for details.

--End--

Variable definitions

Variable	Value
<filename>	is the name of the previously saved view.
<IPAddress>	is the IP address of the node to which you want to connect.

Determining the status of fabric card firmware

Determine the status of fabric card firmware to identify whether the firmware should be, or must be, upgraded.

Prerequisites

- Both fabric cards must be installed and in-service.

Procedure steps

Step	Action
1	Display the attributes of the fabric banks: **Display -n shel f fabricCard/* banks**
2	Display the correct value of the firmware version: **display shelf fabricCard/<fabcard_inst> recommendedVersionToInstall**
3	Compare the attributes of the fabric banks to the recommended version. If the versions are different, you must decide whether to upgrade the firmware to match. Check for alarm 7002 0005 or 7002 0007 and do the remedial action. If the versions are the same, no upgrade is required.

--End--

Variable definitions

Variable	Value
<fabcard_inst>	is the instance value of the fabric card.

Upgrading Multiservice Switch 15000 and Multiservice Switch 20000 fabric card firmware

Upgrade Nortel Networks Multiservice Switch 15000 or Multiservice Switch 20000 fabric card firmware to take advantage of enhancements and new functionality and to improve the node's operating efficiency.

Prerequisites

- For Multiservice Switch 20000 nodes, the fabric card firmware must be fabric driver 7.9 to complete your software migration or fabric replacement successfully. For Multiservice Switch 7400 and Multiservice Switch 15000 nodes firmware replacement is encouraged, but is not necessary to complete your software migration or fabric replacement successfully.
- To upgrade the firmware on one fabric card, both fabric cards in the node must be installed and operational.
- The fabric card that is receiving the new firmware version must be locked.
- The fabric card that is not receiving the new firmware version must be unlocked and enabled.
- You do not need to upgrade the fabric card firmware every time you upgrade the control processor (CP) and function processor (FP) software. However, an alarm is raised by the system whenever a newer version of the fabric card firmware is available, and Multiservice Switch 15000 nodes operate more efficiently if you upgrade the firmware when the alarm is raised. To see if you need to upgrade the transport fabric firmware, refer to *Nortel Networks Multiservice Switch Release Notes*.
- The new fabric card firmware must be downloaded from the Nortel Networks Multiservice Data Manager server acting as the software distribution site (SDS). For more information on how to download from the SDS, see NN10600-270 *Nortel Networks Multiservice Switch 7400/ 15000/20000 Software Installation*.

Procedure steps

Step	Action
1	Display the fabric driver version currently installed: **`display shelf fabric/x recommendedVersionToInstall`** If the response is: **`recommendedVersionToInstall = Fabric software version is up to date.`** Then an upgrade does not need to be performed. If the response is a load number, you need to upgrade the firmware.

2 Lock the fabric card:

```
lock shelf fabricCard/<fabcard_inst>
```

3 Install the new firmware:

```
install -file(<load>) shelf fabricCard/<fabcard_inst>
```

Wait a few minutes for the firmware to be installed, and for the system to notify the operator of any errors.

4 Display the attributes of the fabric banks:

```
display shelf fabricCard/<fabcard_inst> banks
```

5 Verify that the fabric card operates correctly with the new firmware:

```
start shelf fabricCard/<fabcard_inst> test
```

The test results show if the fabric card is operating correctly. See NN10600-520 *Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* for assistance in understanding the test results.

6 If there are problems with the upgraded fabric card, It might be necessary to make the fixed bank the bankOnShelfRestart using the following command:

```
set shelf fabricCard/<fabcard_inst> bankOnShelfRestart
fixed
```

If the writable bank is set as the committed bank and it becomes corrupted, the fabric card might not come up. If the writable bank is corrupted, it must be replaced. Contact your Nortel Networks representative.

7 Unlock the fabric card to return it to service:

```
unlock shelf fabricCard/<fabcard_inst>
```

--End--

Variable definitions

Variable	Value
<fabcard_inst>	is the instance of the fabric card, *X* for a card in the upper position, or *Y* for a card in the lower position.
<load>	is the software load version of the firmware AV. For example, install CE01B for fabric_CE01B.

Verifying the success of the software migration

Verify the success of the software migration to confirm that the migration was completed correctly and that the node is functioning the same as before the upgrade.

Prerequisites

- If your network has many live connections, displaying the status of the logical processors, SONET ports, and ATM interfaces will result in large amounts of output.
- If any of the components displayed in the following procedure are not enabled or have alarms, investigate the cause and attempt to correct the problem.

Procedure steps

Step	Action
1	Open and locate the log file where the information that was collected before performing the migration is stored.
2	Compare the information in the log file to the information collected in this procedure.
3	Display the status of the logical processors: **`display Lp/* osistate`**
4	Display the status of the SONET ports: **`display Lp/* sonet/* osistate`**
5	Display the status of the service interfaces: For example: **`display AtmIf/* osistate`**
6	Display the status of the node equipment protection. **`display Shelf Card/* SparedServices`**

--End--

Configuring post-migration changes

Configure post-migration changes to reduce Hitless Software Migration (HSM) outage.

Procedure steps

Step	Action
1	Delete a static ARP entry for all adjacent routers attached to all GigE ports. **`del Vr/<vr_name> Ip Arp HostEntry/<host_address>,na`**
2	Delete a static ARP entry for this node, on each adjacent router attached to the GigE port.

--End--

Variable definitions

Variable	Value
<host_address>	is the IP address of the static host being defined.
<vr_name>	is the name of the virtual router (Vr).

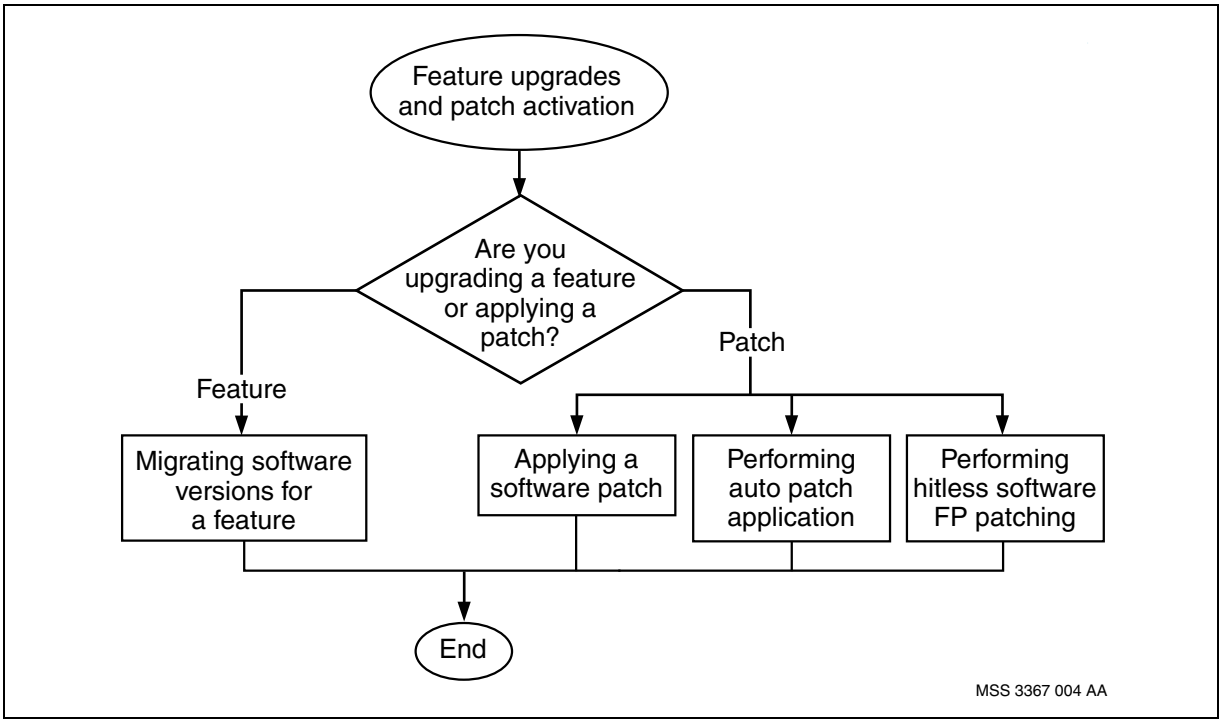
Feature upgrades and patch activation

Upgrade features and activate patches to provide improvements to the software without upgrading the software on the entire node.

Feature upgrades and patch activation procedures

This task flow shows you the sequence of procedures you perform to perform feature upgrades or patch activation. To link to any procedure, go to Feature upgrades and patch activation procedure navigation (page 62).

Feature upgrades and patch activation procedures



Feature upgrades and patch activation procedure navigation

Migrating software versions for a feature

Migrate software versions for a feature to perform an incremental upgrade or downgrade of the version of feature software that is being used on multi-processor function processor cards like the 6mPktServ.

Prerequisites

CAUTION
Loss of service
Do not activate any other software migration when migrating software versions of a feature. The impact on service cannot be predicted if two or more migrations are attempted at the same time.

CAUTION
Loss of service
Do not migrate software versions of a feature during peak hours. Software migration results in a temporary capacity decrease or service outage, and can take between 3 to 12 hours to complete depending on the number of function processors affected. Minimize loss of service by migrating software versions of a feature during off-peak hours.

CAUTION
Loss of accounting records
A software migration activation can result in accounting records being discarded. To minimize accounting data loss, do not schedule a software migration during a time-of-day accounting (TODA) update. Schedule software migration to occur when call clear rates are low and the records from the previous TODA have been spooled to disk.

- No external interface modifications may be performed during the upgrade.
- The software migration must not affect the control processors.
- The node to be upgraded must be physically installed, operational, and running Nortel Networks Multiservice Switch software. All affected function processors should also be operating without errors.
- The alarm display should be visible on the operator console.
- During a software version migration, equipment protection is unavailable for cards whose standby card is being upgraded.

- Obtain a copy of the *Nortel Networks Multiservice Switch Release Notes* that correspond to the version of software you are migrating to.
- The software version must be certified as being backward compatible by Nortel Networks.
- The software release you are migrating to must be compatible with all the processor cards of the node. Refer to NN10600-551 *Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference* to verify minimum software requirements of function processors. Refer to NN10600-120 *Nortel Networks Multiservice Switch 15000/20000 Hardware Description* and NN10600-170 *Nortel Networks Multiservice Switch 7400 Hardware Description* to verify minimum software requirements for control processors.
- The current provisioning view must be the committed view.

Procedure steps

Step	Action
1	Start the provisioning view. `start prov`

Attention: There is no command to stop the software migration once it has started. Refer to the Procedure job aid (page 65) for information on handling alarms and errors during the feature software migration.

2	Display the software application version list (AVL). `d sw avl`
3	Note the application version that you are replacing.
4	Replace the old application version with the version you are migrating to. `set sw avl ~<old_av_version> <new_av_version>`
5	Display the edited AVL to verify the proper version has been set. `d sw avl`

CAUTION
Loss of service
To prevent a complete node outage the current view must be committed before a CP failure. Rollback to the previous committed view and a node outage will occur if the active CP fails before the current view is committed.

6 Verify and activate the provisioning changes. Refer to Completing configuration changes (page 7) for details.

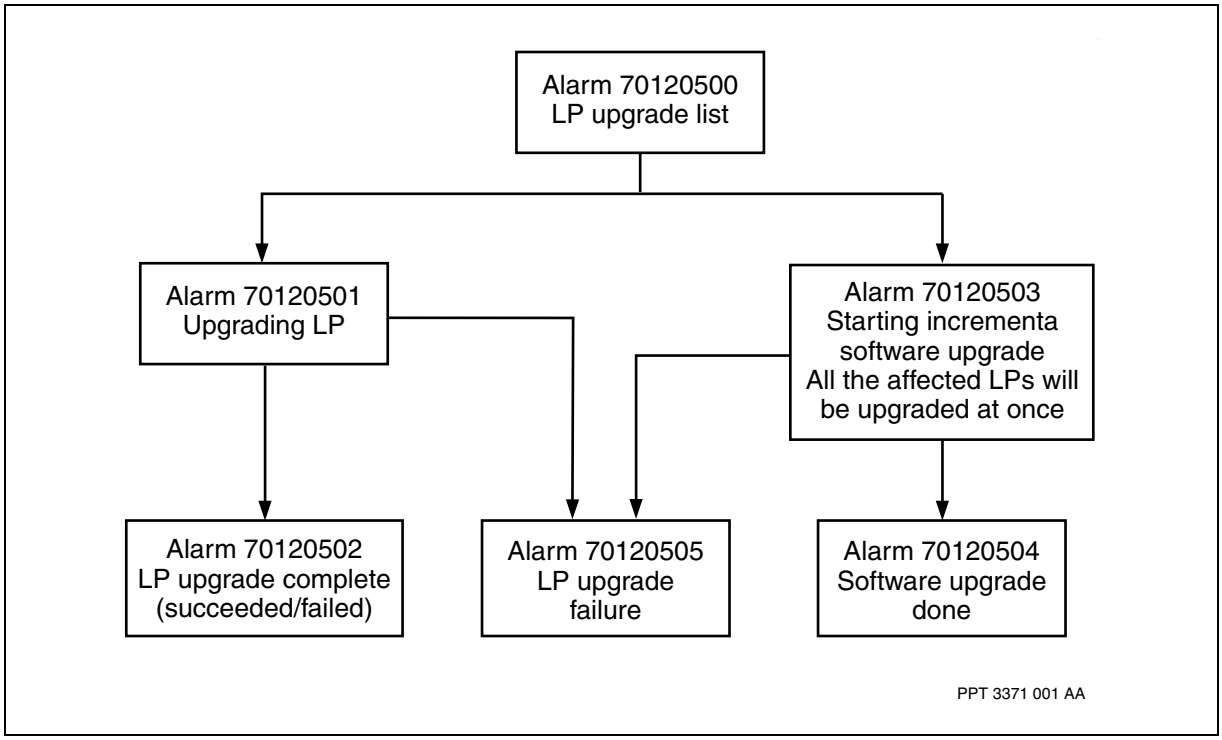
--End--

Variable definitions

Variable	Value
<new_av_version>	is the version of the software feature you are migrating to.
<old_av_version>	is the version of the software feature currently installed.

Procedure job aid

Multiservice Switch node alarm sequence during a feature software migration



Impact of an error condition on a feature software migration

Error condition	Result and action
criteria for activate prov not met	Command failed.
cannot save temp file	Command failed. Check disk usage and tidy disk if necessary.

(1 of 2)

Impact of an error condition on a feature software migration (continued)

Error condition	Result and action
cannot load new software	Command failed. Take action based on responses or alarms received as a result of the failed activity.
cannot build migration provisioning view	Command failed. Take action based on responses or alarms received as a result of the failed activity.
cannot save commit formats	Command failed. Check disk usage and tidy disk if necessary, or take action based on responses or alarms received as a result of the failed activity
an application cannot complete upgrade	An alarm is generated to inform operator. No action required. Card will be declared as potentially failing its upgrade. Note that in most cases the card will have successfully upgraded.
active CP crashes	CP swtichover. An automatic audit will take place. All cards that are part of the feature software migration are reset to load the committed view.
standby CP crashes	Continue the feature software migration.
LP upgrade failure	An alarm is generated to inform operator. Manually reset the LP. If the LP fails to recover once it has been reset then roll back to the previous software version by repeating Migrating software versions for a feature (page 63) and specifying the previous working version of software. If the operator chooses to prevent migration from occurring on the remaining processors that are scheduled to be migrated. Start Migrating software versions for a feature (page 63) again but specify the previous working version of software. The processors will not reload if the software version specificed in the AVL matches the version currently loaded. The processors that have already migrated will once again start to reload the software version specified in the changed AVL.

(2 of 2)

Applying a software patch

Apply a software patch to update existing software and allow for improved functionality or to assist with the diagnosis a current problem.

Prerequisites

WARNING

Calls in progress are dropped

This strategy removes inactive control and function processors from service. As a result, redundancy in the event of failure of the active components is not available and some transient calls are dropped. Stable calls are unaffected by the migration.

Undertake the procedures required by this strategy during low-traffic periods.

CAUTION

Loss of stable SVC connections may occur

A loss of SVC connections may occur. Although stable SVC calls should remain active in a redundant processor configuration, exercise caution when performing this upgrade.

Undertake the procedures required by this strategy during low-traffic periods.

- For auto patch application, the Patch Av must be downloaded from the Multiservice Switch SDS in order to view patches on-switch.
- The node must contain two control processors (CP). One CP must be active and the other CP must be in standby mode.
- When applying the patch for a fabric card NTHR16EA:
  - — the node must contain two CP3s, one active and one standby, if the patch is a disruptive patch
  - — the patch should be activated before the fabric is unlocked, otherwise ignore the alarm 7002 0005 for a mismatch when the other fabric in the node is not an EA version
  - — both CP3s are loaded at the same time when the patch is activated and service is unaffected, if the patch is a non-disruptive patch
  - — a fabric firmware mismatch is handled automatically, as normal, although if you are prompted to upgrade the fabric driver (version 21.1 or later)
- While you perform software migration tasks, the system may interrupt the process to display warnings or notifications. Some of these notifications

may require you to confirm your intent before continuing. Respond as required by the online instructions.

Procedure steps

Step	Action
1	Enter provisioning mode so that you can issue the appropriate commands: **`start -force prov`**
2	Display the current software patchlist: **`display -c sw patl`** Fabric card NTHR16EA has patch identifier baseFTxxxxA_yyyyyy, where xxxx is the sequence number and yyyyyy is the load name.
3	Apply the required patches to the patchlist: **`set sw patl ! <patches>`**
4	Verify the patches that are going to be applied: **`display sw patl`**
5	Verify and activate the provisioning changes. Refer to Completing configuration changes (page 7) for details.

--End--

Variable definitions

Variable	Value
<patches>	is a space-separated, case-sensitive list of patches.

Performing auto patch application

Perform auto-application of Multiservice Switch patches to obtain all the patches for a single software release with the delivery of a single AV (application Version), the Patch Av. This AV contains all the patches for a given release, including any patches that have been built specifically for a patched Av. The Patch AV does not need to be provisioned in the Sw avList in order to view the patches contained within it; however, it must be provisioned in the Sw avl in order for patches to be added to the Sw patchList.

Prerequisites

- The Patch Av must be downloaded from the Multiservice Switch SDS in order to view the patches on-switch.

Attention: Modifications must also be made on Multiservice Data Manager to enable auto-patching. Refer to the chapter entitled "Using the Auto-Patch tool" in NTP 241-6001-303 *Nortel Networks Multiservice Data Manager Customization and Administration* to enable the auto-patch process on MDM.

Procedure steps

Step	Action
1	Download the Patch Av from the Multiservice Switch SDS in order to view the patches on the switch: **set sw dld avl patch_<release version>** **set sw dld processorTargets ! i960 ppc** **start -h(IP address of SDS) -u(userID) -p(password) sw dld**
2	Enter provisioning mode so that you can issue the appropriate commands.
3	Add the Patch Av to the Sw Avl. **set sw avl patch_<release version>**
4	Display the status for the current patches: **display sw av/patch_<release version> patch/***
5	Determine what *patchVersion* files are on the switch: **list sw av/patch_<release version> patchVersion/***
6	Optionally, set the *patchVersion*: **set sw autopatch patchVersion <patchVersion file>**
7	Display the patches for each *patchVersion* file: **display sw av/patch_<release version> patchVersion/***

8 Determine which *patchVersion* is currently selected:

```
display sw autopatch patchVersion
```

If the response is latest, then the latest *patchVersion* file is used.

9 Insert another *patchVersion* if required:

```
set sw autopatch patchVersion <new patchVersion>
```

10 List the selected patches that can be provisioned:

```
check sw autopatch
```

11 Optionally, print an extended output:

```
check -all sw autopatch
```

12 Apply all or some of the proposed patches in the *patchList*:

```
set sw patchList <patch1> <patch2> ...
```

--End--

Variable definitions

Variable	Value
<new patchVersion>	is a patchVersion other than the latest version.
<patch1> <patch2>	is a patch number in the patchList.
<patchVersion file>	is the Patch Version file associated with the Patch AV.
<release version>	is the patch release version.

Performing hitless software FP patching

Perform hitless software FP patching to update existing software, and to allow for improved functionality or to assist with the diagnosis of a current problem, without causing a loss of service.

Prerequisites

WARNING

Calls in progress are dropped

This strategy removes inactive control and function processors from service. As a result, redundancy in the event of failure of the active components is not available and some transient calls are dropped. Stable calls are unaffected by the migration.

Undertake the procedures required by this strategy during low-traffic periods.

CAUTION

Loss of stable SVC connections may occur

A loss of SVC connections may occur. Although stable SVC calls should remain active in a redundant processor configuration, exercise caution when performing this upgrade.

Undertake the procedures required by this strategy during low-traffic periods.

- While you perform hitless software FP patching tasks, the system may interrupt the process to display warnings or notifications. Some of these notifications may require you to confirm your intent before continuing. Respond as required by the online instructions.
- For hitless software FP patching, the active FPs must be provisioned for one-for-one equipment sparing. During the software patch, equipment protection is unavailable for those cards whose standby card is being patched.

Procedure steps

Step	Action
1	Ensure the edit view is equal to the current view: **`cas> display prov editViewAddedComponents, editViewDeletedComponents, editViewChangedComponents`** If the edit view is equal to the current view, then the attribute values for the displayed attributes are all zero. If the edit view is not equal to the current

view (that is, one or more of the displayed attributes is non-zero) then continuing with this procedure results in a non-hitless software patch activation. The copy prov command can be used from within provisioning mode to make the edit view equal to the current view.

The provisioning changes currently in the edit view are lost when the copy prov command is used.

2 Enter provisioning mode so that you can issue the appropriate commands:

```
start prov
```

3 Display the current application version list:

```
display sw avl
```

4 Display the current software patchlist:

```
display sw patl
```

5 For a patch that is to be provisioned in the software patchlist, verify that it is an FP reset patch. TAP patches provisioned in conjunction with FP reset patches can also be applied as part of hitless software patching:

```
display sw avl patl patchType
```

For CP reset patches, HSM will be done, if possible.

6 Provision the Patched Application Version (patched AV):

```
set sw avl~<current av> <patched AV>
```

7 Provision the patch:

```
set sw patl ! <patches>
```

8 Verify that the provisioning changes are semantically correct:

```
prov> check prov
```

If an HSP will occur then the following response is generated:

```
Activation will result in a software patch activation.
Some applications may experience service outage.
```

If an HSP cannot occur, then the system will do an HSM, if possible. This is indicated by the presence of the following HSM response:

```
Activation will result in a software migration
activation. Some applications may experience service
outage.
```

If neither an HSP nor HSM can be done, then a non-hitless software patch is performed. This non-hitless software patch activation is indicated by the absence of either of the above responses. (Note that a separate response will indicate which FPs will be reset.)

9 Activate the provisioning changes:

```
prov> activate prov
```

A response is issued indicating which LPs will take part of HSP:

```
The following LPs will participate in software patching:
<list of LPs....>
```

10 Prior to starting the software patch activation, verify all provisioned cards involved in the HSP are operational. for all cards that are involved in the HSP, use the following command:

CAS> display Shelf Card/x osiState

11 Verify that both electrical FPs in a 1:1 sparing configuration are EP operational. for each Lp that is involved in the HSP, use the following command:

CAS> display Lp/x mainCardStatus, spareCardStatus

12 Verify that both LPs in a 1+1 FP sparing configuration are EP operational

CAS> display Shelf Card/x SparedServices operState, availStatus

13 Verify that all load-shared Lps are operational. For each unspared Lp that is involved in the HSP, use the following command:

CAS> display Lp/x mainCardStatus

The response should be *active*.

14 Confirm the provisioning:

cas> confirm prov

If the provisioning is not confirmed within 20 minutes of the completion of the software patch activation then a rollback to the committed provisioning view occurs. This results in reloading the entire shelf in a non-hitless manner.

15 Exit provisioning mode:

cas> end prov

--End--

Variable definitions

Variable	Value
<patches>	is a space-separated, case-sensitive list of patches.
<patched AV>	is the Patched Application version.

Procedure job aid

Impact of an error condition on a hitless software patch

Phase	Error condition	Result and action
beginning of HSP	Criteria for activate prov is not met.	Command failed, hitless recovery.
Phase 0: Tap-only patching	Cannot load new software.	Command failed, the card(s) which can not load is reset (existing behavior for TAP patching mechanism).
	A swerr or engineering alarm occurs on a card that is, or is being, patched.	Software patch activation is paused and a partial response is generated. Operator makes the decision to stop (roll back) or to continue with possible service impact.
Phase 1: Incremental FP Patching	A load shared card can not de-load.	Software patch activation is paused and a partial response is generated. Operator makes the decision to stop (roll back) or to continue with possible service impact.
Phase 1: Incremental FP Patching (continued)	Cannot load new software.	Command failed, hitless recovery for 1:1 and 1+1 cards, potential service impact for load shared cards.
	An application does not acknowledge the successful patch loading.	Software patch activation is paused and a partial response is generated. Operator makes the decision to stop (roll back) or to continue with possible service impact.
	An application negatively acknowledges the patch loading or it is unable to become ready for Switchover.	Software patch activation is paused and a partial response is generated. Operator makes the decision to stop (roll back) or to continue with possible service impact.
	A swerr or engineering alarm occurs on a card that is, or is being, patched.	Software patch activation is paused and a partial response is generated. Operator makes the decision to stop (roll back) or to continue with possible service impact.

(1 of 2)

Impact of an error condition on a hitless software patch (continued)

Phase	Error condition	Result and action
Phase 2: Spared FP switchover	Former standby FP (in 1:1 or 1+1 configuration) cannot become active.	Appropriate alarms generated, recovery sequence as follows: For 1:1 and 1+1 sparing - If an active card fails, the sparing is lost (the standby is already upgraded); If a standby card fails, service outage occurs. Manual recovery results in service outage for patched AVs and FP reset patches; Operator commands are re-enabled.
Phase 3: Post-FP switchover	Operator does not or cannot confirm provisioning changes.	Rollback to committed provisioning view (node outage).
Phase 3: Post-FP switchover (continued)	Former active FP (in 1:1 or 1+1 configuration cannot become standby	Appropriate alarms generated, recovery sequence as follows: For 1:1 and 1+1 sparing - If an active card fails, the sparing is lost (the standby is already upgraded); If a standby card fails, service outage occurs. Manual recovery results in service outage for patched AVs and FP reset patches; Operator commands are re-enabled For unsparing - a manual recovery is required.
	An unspared FP fails to load the patch software.	Appropriate alarms generated, service impact.
Any phase	Any FP involved in HSP crashes.	The appropriate recovery procedure is applied, depending on what type of sparing is available for when the FP crashes. This could mean processor sparing or a card restart. HSP automatically rolls back if in Phase 0 or Phase1.
	Active CP crashes.	The following recovery procedure is applied during HSP: Phase 0: all FPs participating in this phase are reset (this is equivalent to existing behavior for TAP patch activation); Phase 1: all FPs that have been or are being patched are reset; Phase 2 and Phase 3: any FPs that need to be patched but haven't been patched yet are reset.

(2 of 2)

Stopping or pausing a hitless software patch

Stop hitless software FP patching to roll back the system to the previous configuration, or pause software FP patching to either abort or continue with the hitless software patch.

This procedure must be run at any time prior to the Controlled-Switchover phase.

The pause option is not applied if a patch affects only load shared cards (HSP completes with phase 1).

Procedure steps

Step	Action
1	To stop the hitless software patch: **`stop prov`**
2	To pause the hitless software patch: **`activate -pause prov`**
3	To continue with a paused hitless software patch: **`continue (-force) prov`** Without the -force option, this command will only continue the software upgrade if the conditions that caused the upgrade to pause have cleared. The -force option forces the upgrade to resume, even if pausable conditions still persist.

--End--

Software migration fundamentals

Nortel Networks Multiservice Switch systems provide the capability of upgrading software three different ways, depending on your configuration. You may perform a complete migration that temporarily removes your node from service, or you may choose to perform a hitless software migration that has the potential to not interrupt services. Multiservice Switch systems also offer a migration that upgrades the software for a specific feature without upgrading the software for the entire node. This section describes the types of software migration and their associated processes.

Navigation

Service-interrupting software migration for Multiservice Switch nodes

A service-interrupting software migration causes the whole Nortel Networks Multiservice Switch node, and all of its applications, to go out-of-service during the migration. To reduce the time that the node is out-of-service during a service-interrupting software migration, processing occurs on the standby CP before the node goes out of service, if the node contains a standby CP. No processing occurs on the standby FPs during the software migration before the node goes out of service. When the node goes out of service, all cards reset to shutdown and reload with the new version of software.

Phases of a service-interrupting software migration activation on Multiservice Switch nodes

Phase	Activity
1) Active CP pre-work	The edit view is saved in a temporary file.
Criteria for protected static route is not met	Command failed. Check next hops of protected static routes.
2) CP migration	a) The standby CP is reset to activate new software and start up in migration mode.
	b) The new provisioning view migrates to the migrating CP. For more information, see “View migration during a software migration” (page 6).
	c) Committed formats of the migrated view are saved on the migrating CP.
Attention: Disk synchronization occurs in the background during this phase. This phase is not complete until disk synchronization is also complete.	
3) Migration switchover	When the system notifies the active CP that phase two is complete, the following occurs:
	a) The active CP resets to load new software. This allows the standby CP to become active and start providing service.
	b) When the system indicates that the active CP has reset, the FPs reset in order to load the new software when they restart.
4) Post-migration switchover	The node is running the new software, however only the CP is operating.
	The restarting FPs activate new firmware, new software, and their provisioning data is activated.
	FP applications initialize with provisioning data and re-establish permanent connections at maximum call setup rate.
	Network management connectivity is re-established.
	The operator must complete provisioning by confirming the provisioning changes. This phase is completed once the operator commits the new provisioning view.

Operator control during a service-interrupting software migration

To monitor the provisioning activity and its progress during a service-interrupting software migration on any Nortel Networks Multiservice Switch node, issue the following command:

```
display -o prov
```

If you have configured a spare CP but it is unavailable, the migration activation fails. To force the migration activation to continue, reset the shelf by issuing the following command:

```
continue -force provisioningSystem
```

Hitless software migration for Multiservice Switch 15000 and Multiservice Switch 20000 nodes

Hitless software migration for Nortel Networks Multiservice Switch 15000 and Multiservice Switch 20000 nodes allows the active CP and the active FPs to operate using the old version of software while a new version of software is being loaded and provisioned on the standby CP and standby FPs. The standby cards that are being loaded with the new version of software are referred to as the migrating cards. The active cards remain active until the migrating cards have completed software migration and are ready to take over.

You can perform a hitless software migration only when you migrate from a software version that contains the hitless software migration functionality to a later release.

A successful hitless software migration requires preparation and an understanding of how the hitless software migration works.

- What happens during a hitless software migration? (page 79)
- Hitless software migration equipment protection and sparing (page 82)
- Operator control during a hitless software migration (page 85)

What happens during a hitless software migration?

During a hitless software migration, the Nortel Networks Multiservice Switch 15000 or Multiservice Switch 20000 shelf logically splits into two shelves: the service shelf and the migration shelf. The service shelf contains the active FPs and is controlled by the active CP. The migration shelf contains the migrating FPs and is controlled by the migrating CP.

When the migration shelf is ready, the active CP and FPs shut down and the migration shelf becomes the new active shelf. This is called migration switchover. The CP and FPs in the former service shelf then reset and are loaded with the new version of software.

There are five phases to a hitless software migration:

- Phase 1 — Preparation of the CP (page 80)
- Phase 2 — CP migration (page 80)
- Phase 3 — FP migration (page 81)
- Phase 4 — Migration switchover (page 81)
- Phase 5 — Post-migration (page 82)

Phase 1 — Preparation of the CP

As the hitless software migration begins, the following occurs:

1 The edit view is saved in a temporary file.

2 Hitless CP switchover is disabled.

3 The card availability status of the standby CP is set to migrating. The standby CP resets to load new software.

4 The system responds to the *activate prov* command indicating that a software migration activation is to be performed.

5 Certain operator commands are automatically disabled.

6 The *Prov Migration* component is created and a SET warning alarm is issued against this component indicating that a software migration is being performed.

Attention: The disabled operator commands remain disabled by the system until after the migration switchover or hitless recovery.

Phase 2 — CP migration

After the system raises the SET warning alarm to complete phase 1, the following occurs:

1 The migrating CP is reset to load new software and start up in migration mode.

2 The LED of the migrating CP changes to fast, pulsing green.

3 The new provisioning view migrates to the migrating CP.

4 Committed formats of the migrated view are saved on the migrating CP.

5 The active CP splits the physical shelf into two logical shelves: the service shelf and the migration shelf. The active CP also prepares for the FP migrations according to the following criteria:

For an FP with a one-for-one spare and whose standby FP is operational, the active FP remains under the control of the active CP in the service shelf. The standby FP is selected to be part of the migration shelf under the control of the migrating CP. The standby FP's card availability status is set to migrating. The standby FP resets to load new software. At this point, equipment protection is disabled.

For FPs that are part of an LP pair configuration and with both FPs operational, the active FP remains under the control of the active CP in the service shelf. The FP that contains the standby application instances is selected to be part of the migration shelf under the control of the migrating CP. Any unspared services on this standby FP are dropped and reestablished after migration switchover. The active CP sets the card's

availability status to migrating, then resets the LP to initiate the FP migration phase. At this point, equipment protection and inter-card APS is lost.

For FPs that fit neither of the previous criteria, the FPs remain under the control of the active CP in the service shelf. These FPs are reloaded with new software after the migration switchover occurs.

6 Provisioning data is delivered within the migrating CP.

7 Applications that run on the CP, such as ATM routing, are partially initialized.

Attention: Disk synchronization occurs in the background during this phase. This phase is not complete until disk synchronization is also complete.

Phase 3 — FP migration

After the system partially initializes the CP applications to complete phase 2, the following occurs:

1 The migrating FPs load new software and start up in migration mode.

2 The LEDs of the migrating FPs change to fast, pulsing green.

3 Provisioning data is delivered on the migrating FPs.

4 The migrating FPs are loaded with dynamic service data for switched services, such as ATM SVCs.

Phase 4 — Migration switchover

After the system notifies the active CP that phase 3 is complete, the following occurs:

1 The CPs close all spooled files. For example, billing and statistics.

2 All processors in the service and migration shelves are notified to switchover:

Processors within the service shelf reset to load new software.

The CP and FPs in the migration shelf become the service shelf. FPs providing switched services, such as ATM SVCs, re-establish signalling and routing functions. The CP and FPs with the new software start providing service.

The sparing panel and single-FP line APS are switched over.

Final port initialization is completed.

3 The shelf becomes one when all CPs and FPs are running the new software. The shelf is no longer logically split into two parts.

In order to abort a hitless software migration, you must issue the *stop prov* command. To do so without causing a service outage, you must issue this command during the migration-switchover phase. By issuing the command during this phase, you can roll back to the view before the software application version list was changed and the software migration remains hitless.

Phase 5 — Post-migration

After all CPs and FPs are running the new software and phase 4 is complete, the following occurs:

1 The restarting CP and FPs load new firmware, new software, and their provisioning data is activated.

2 FP applications initialize with provisioning data and re-establish permanent connections at maximum call setup rate. Dynamic service data is loaded from the active FPs.

3 Network management connectivity is re-established.

4 Equipment protection and inter-card APS are re-established.

5 The operator commands which are disabled during the software migration are now available.

6 The operator must complete provisioning by confirming the provisioning changes. This phase is completed once the operator commits the new provisioning view.

Hitless software migration equipment protection and sparing

During a software migration, equipment protection is unavailable for cards whose standby card is part of the migration shelf.

In a one-for-n equipment sparing configuration, all of the FPs that make up that configuration remain part of the service shelf, along with the initially active CP and the active FPs that make up a one-for-one equipment sparing configuration. When the service shelf goes down and the migration shelf takes over, all services running on the FPs in the one-for-n configuration go out of service.

During a software migration, ensure that all components supporting the service intended to be hitless are enabled. A check of all components should be performed prior to activating the migration provisioning to minimize any impacts to associated services.

Nortel Networks Multiservice Switch 15000 and Multiservice Switch 20000 node software applications and features fall into three behavior categories during hitless software migration:

- hot standby. For a definition and description of hot standby, see NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.
- warm standby. For a definition of warm standby, see NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.
- cold standby. For a definition of cold standby, see NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.

Hot and warm standby are used to provide hitless software migration and to provide hitless services in case of an FP switchover. By definition, cold standby applications and features cannot offer hitless software migration or hitless services in the case of an FP switchover.

See Hot standby applications and features (page 83) for a list of hot standby applications and features as they apply to hitless software migration. See Warm standby applications and features (page 84) for a list of warm standby applications and features as they apply to hitless software migration. Any application or feature that is not listed in Hot standby applications and features (page 83) or Warm standby applications and features (page 84) either does not apply to Multiservice Switch 15000 and Multiservice Switch 20000 nodes, or is a cold standby application or feature.

Hot standby applications and features

Application	Feature
atmBearerService	atmBearerService
base	aps atmCore
atmNetworking	atmIisp atmPnni atmUni
aal1Ces	aal1Ces
(1 of 2)	

Hot standby applications and features (continued)

Application	Feature
pvg	vgsAtmDc vgsAtmG729 vgslpG729 vgsAtm vgslp
Attention: Applications aal1Ces and PVG support hot equipment protection (HEP) and hitless software migration (HSM) for a 1 + 1 sparing configuration on the Multiservice Switch 15000 Media Gateway node. Application PVG supports HEP and HSM for voice services processor 2 (VSP2)(NTHW87) or voice services processor 3 (VSP3) (NTHW84)FP cards when used with 4-port OC-3/STM-1Ch TDM/CES FP cards. The PVG application with VSP2/VSP3 FP cards is only hitless when used in conjunction with application aal1Ces (but not vice versa). Application PVG also supports HEP and HSM for voice processor 3 with optical TDM interface (VSP3-o) (NTHW77) FP when used with ATM FP cards that are carrier grade compliant. The PVG application with VSP3-o FP cards supports HEP on the Multiservice Switch 15000 MG node using a 1 + 1 sparing configuration for the TDM ports and using dual LP equipment protection (DLEP) sparing through component *Vsp DualLpEquipmentProtection (Dlep)*. The PVG application with VSP3-o FP cards does not use application aal1Ces when in a hitless configuration.	
(2 of 2)	

Warm standby applications and features

Application	Feature
base	aal1Ces imaAtmForum
atmNetworking	atmApi dprsMcsAgent dprsMcsEp dprsMcsEpIntercept porsApi routingGateway
callRedirection	callRedirection
(1 of 2)	

Warm standby applications and features (continued)

Application	Feature
frameRelay	frameRelayAtm frameRelayAtmNiwf frameRelayAtmIsdn frameRelayDte frameRelayNni frameRelayUni frameRelayUniPvcSvc frf5EndPoint frsVirtualFramer ppp
huntGroupSystem	huntGroupSystem
ip	ip
networking	callServer dpnRouting ipiFr
serviceTrace	frameRelayNniTrace frameRelayUniTrace frTraceRcvr x25TraceRcvr
trunks	atmTrunks porsTrunks
WanDte	LocalMedia AtmMpe
Attention: LAN applications are considered warm standby.	
(2 of 2)	

Operator control during a hitless software migration

To monitor the provisioning activity and its progress during a hitless software migration on any Nortel Networks Multiservice Switch node, issue the following command:

```
display -o prov
```

During a hitless software migration on Multiservice Switch 15000 and Multiservice Switch 20000 nodes, you can use progress indication attributes to monitor the main phases and activities of a software migration, or to assist

with gathering performance measurements. You can also use progress indication attributes to obtain information on activity that is temporarily blocking the progress of the software migration, for example, disk synchronization or automatic pause. Use the following progress indication attributes to determine the progress of provisioning system commands during a hitless software migration:

```
provisioningActivity, activityProgress,
standbyCPActivity, standbyCPActivityProgress
```

To determine the stage of a provisioning procedure during a hitless software migration, use the following progress indication attributes:

```
checkRequired, confirmRequired
```

Operator control allows you to stop a hitless software migration on Multiservice Switch 15000 and Multiservice Switch 20000 nodes before the start of the migration switchover phase by issuing the following command:

```
stop provisioningSystem
```

In addition to a manual stop, if an application does not behave properly during a migration switchover, then the hitless software migration automatically pauses before migration switchover occurs. This pause allows you to review all visible migration alarms before continuing or stopping the hitless software migration. To continue the hitless software migration, issue the following command:

```
continue provisioningSystem
```

To disable the automatic pause, issue the following command at the beginning of the software migration:

```
activate -noPause provisioningSystem
```

Software patches

Nortel Networks Multiservice Switch software patches may be used to fix a known software problem or as a diagnosis tool.

There are three patch types:

- TAP patches
- Reset patches
- Patched Avs

With the introduction of the patch auto-application feature, the delivery of Multiservice Switch patches has been automated. The application of patches is accomplished with the delivery of a single Av, the Patch Av. This Av contains all the patches for a given release, including any patches that have been built specifically for a patched Av based on the release.

It is not necessary for the Patch Av to be present in the Sw Avl in order for patches to be seen and associated with the application that they are patching. However, in order to provision patches, the Patch Av must be added to the Sw Avl. In order to view patches on-switch, the Patch Av must be downloaded from the Passport SDS site.

Patch auto-application is a scheduled process that applies released Multiservice Switch patches to customer's switches. The scheduling of the patch download is controlled by the MDM. At the appointed time, the MDM will trigger the switch to download the latest version of the Patch Av.

At this time, only TAP patches are eligible for auto-application. Such patches currently make up approximately 70% of all Multiservice Switch patches generated. Reset patches, while delivered with the Patch Av, must always be manually applied, regardless of their status.

Patches which have been declared obsolete are not eligible for auto-application regardless of their patch type.

Refer to Patch types and effects (page 87) for a list of the patch types and their activation and removal effects.

Patch types and effects

Type	Platform	Activation	Removal
TAP	All	hitless	hitless
FP reset	15000	FP migration - HSP	FP migration - HSP
	7000	FP disruptive	FP disruptive
CP Reset	15000	Shelf migration - HSM	Shelf migration - HSM
	7000	Cold restart	Cold restart
Modified Application Version	15000	Shelf migration – HSM	Cold restart
	7000	Cold restart	Cold restart

For more information on patches, see NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*. See the *Nortel Networks Multiservice Switch Release Notes* for the restrictions on particular patches.

Hitless Software FP Patching for Multiservice Switch 15000 and Multiservice Switch 20000 nodes

Hitless Software FP Patching (HSP) for Nortel Networks Multiservice Switch 15000 and Multiservice Switch 20000 nodes provides FP reset patches and patched applications on only those cards whose software is modified. HSP supports incremental upgrading of load-shared cards. That is, for each logical pool of load-shared cards, one card in the pool is upgraded at a time.

Note that the HSP feature does not make any applications hitless, but instead provides a framework that allows applications to achieve the same level of outage for patching FPs that they would experience for an FP equipment protection switchover. This feature also does not convert existing load-shared upgrade mechanisms, such as the PSFP ISU, to HSP.

What happens during a hitless software FP patch application?

During a hitless software FP patch application, the cards whose software is modified are upgraded incrementally in a 1:1 or 1+1 FP sparing configuration. Standby cards are patched first, followed by a controlled switchover of the affected FPs, after which the previously active cards are patched.

There are four phases to a hitless software FP patch application:

- Phase 0 — TAP-only Patching (page 88)
- Phase 1— Incremental FP patching (page 88)
- Phase 2 — Controlled Switchover (page 89)
- Phase 3 — Post Switchover (page 90)

Phase 0 — TAP-only Patching

This phase applies to all cards which require non disruptive patching (or patching without card reset). This implies adding or/and removing of TAP patches only.

Both CP and FP cards could be part of this phase, regardless of their sparing configuration. This includes cards in 1:1, 1+1 and 1:N sparing model, as well as load-shared and unspared cards. All cards are upgraded at the same time, which is equivalent to the TAP patching mechanism prior to this feature implementation.

During this phase, activity and progress information is available for querying the Prov and Prov Patch components.

Phase 1— Incremental FP patching

During this phase, activity and progress information is available for querying the Prov and Prov Patch components. The following activities are performed:

For load-shared cards, upgrading occurs one card at a time for the cards in a single load shared pool. The following procedure is applied for each one of the load shared cards:

1 The card is locked, giving an opportunity for the active services on this card to be transferred to other card(s) in the same load shared pool.

Attention: Disk synchronization occurs in the background during this phase. This phase is not complete until disk synchronization is also complete.

2 The card is reset to load the patched software.

3 After the card acknowledges the successful completion of the reload, proceed with the next load shared card.

4 There is a maximum of 10 minutes time interval for each load shared card to acknowledge that has loaded successfully and it is providing service expected. If this time limit is reached, then the HSP pauses.

5 The HSP pauses if a pausable condition occurs on a card that is being patched.

6 Disk synchronization occurs in the background during this phase. This phase is not complete until disk synchronization is also complete

For 1:1 and 1+1 spared cards:

1 The standby card in each 1:1 or 1+1 pair is reset to load the patched software. At this point equipment protection and inter-card automatic protection switching (APS) redundancy are lost.

2 The HSP pauses at the end of this phase if a pausable condition occurs on a card that has been patched.

3 Equipment protection and inter-card APS are re-established.

Phase 2 — Controlled Switchover

Once the Controlled Switchover phase starts, the HSP can no longer pause, or be stopped by the operator. The Prov Patch component is removed, and alarm 7000 0033 is cleared. Activation is considered complete, even though patching of the final set of cards (active-unspared and active-spared) may still be ongoing.

This phase applies to the previously active spared FPs which are to be patched.

At this point all the corresponding standby cards have been reloaded with the new software. After all of the standby FPs declare themselves ready for switchover, the active mate cards are reset which triggers the spared (already patched) cards to start providing service. The performance impact is equivalent to the EP equipment protection impact for these cards.

Phase 3 — Post Switchover

During this last phase of HSP the following occurs:

1 The previously active cards in a 1:1 or 1+1 sparing configuration reload with the new software and become standby.

2 The Unspared FPs which are taking part of HSP are reset. These cards are reset last in order to reduce possible service outage in case of a HSP failure at any previous phase (that is, to reduce unnecessary roll back due to an HSP failure).

Operator control during a hitless FP patch application

A dynamic component, *ProvPatch*, is created at the start of a software patch activation, and is removed at the successful completion of the HSP (after the controlled switchover) or at the unsuccessful completion of the HSP.

To view the state of the software patch activation, issue the following command in operational mode:

```
CAS> display prov patch
```

If the OSI state is ‘unlocked, enabled, active’ then the software patch activation is progressing. If the OSI state is ‘unlocked, disabled, idle’ then the software patch activation is paused waiting for operator intervention. If the component does not exist then a software patch activation is not being performed.

To view the summary progress of the software patch activation, issue the following command in operational mode:

```
CAS> display prov activityProgress
```

To view the more detailed progress, issue the following command:

```
CAS> display prov patch cardsBeingMigrated,
cardsToMigrate, cardsMigrated
```

Feature software migration

A feature software migration is the upgrade or downgrade of the software version for a specific feature. A feature software migration does not change the software loaded on the control processors and is independent from the base software loaded on the node.

A feature software migration loads the specified version of software on each LP, one function processor at a time. All FPs may be updated simultaneously in a critical condition, defined by the provisioned features.

Fabric firmware upgrade

Upgrade fabric card firmware to ensure the version in the control processors (CPs) matches or is compatible with the firmware in a replaced or upgraded fabric card. A fabric card firmware upgrade may be available with the software release you are upgrading to. The alarm 7002 0005 or 7002 0007 prompts you to upgrade the fabric card firmware when an update is available.

All software running onNortel Networks Multiservice Switch 15000 and Multiservice Switch 20000 nodes is compatible with any firmware running on the fabric cards. It is not necessary to upgrade the firmware on the fabric cards every time you upgrade the software on the CP. However, upgrading the fabric card firmware allows you to take advantage of enhancements and new functionality and to improve the node's operating efficiency.

The alarms also indicate which firmware to install on the fabric card. For more information on alarms, see NN10600-500 *Nortel Networks Multiservice Switch 6400/7400/15000/20000 Alarms Reference*. You can install new fabric card firmware at any time during normal node operation.

View migration during a software migration

Each version of software has an associated component model. This component model defines the components and attributes you can use with that software version. Often, the component model changes between software versions.

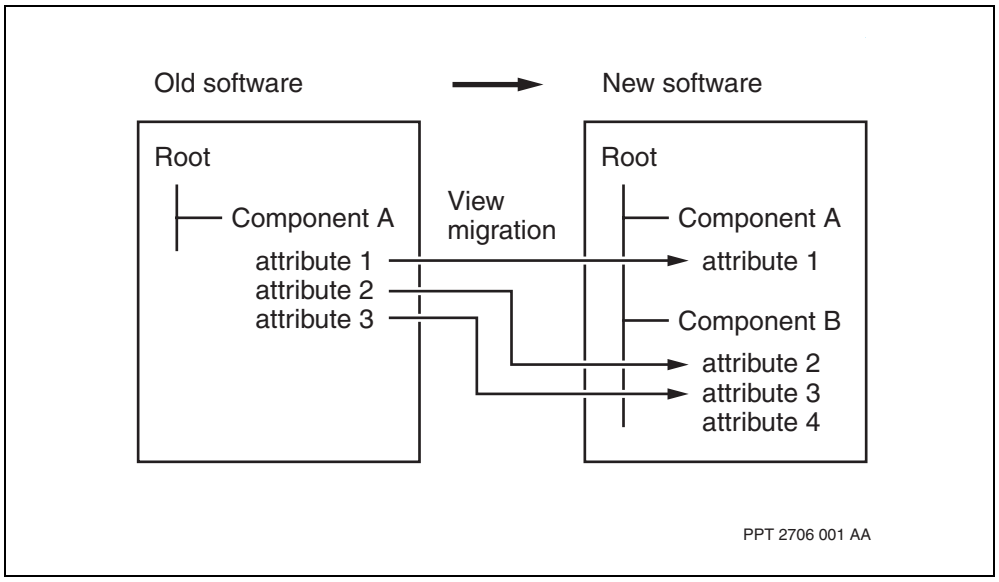
The current view and the edit view store their provisioned data using the component model of the currently running software. When you update the application version list of the edit view and activate it, you change the currently running software and move from one component model to another.

If you are upgrading the software, that is you are updating the application version list (AVL) with newer application software, the node automatically converts the provisioned data stored in the activated view so it fits into the newer software's component model. This conversion process is called view migration.

Attention: View migration occurs only during a software migration. It does not occur during a software reversion.

The figure View migration during a software migration (page 92) shows an example where the component model of the new software has a new component (B) with a new attribute (4) and attributes (2 and 3) from an old component (A). The provisioned data from the old component model is automatically moved so that it fits into the new component model.

View migration during a software migration



Nortel Networks Multiservice Switch 7400/15000/20000

Upgrading Software

Publication: NN10600-272
Document status: Standard
Document issue: sPCR6.1S1
Document date: February 2005
Product release: sPCR6.1
Job function: Upgrades
Type: NTP
Language type: US English