NORTEL NETWORKS

Passport 7400, 15000, 20000

Software Upgrade

241-5701-272

Passport 7400, 15000, 20000

Software Upgrade

Publication: 241-5701-272
Document status: Standard
Document version: 5.2S3
Document date: March 2004

Printed in Canada

Publication history

March 2004

5.2S3 Standard
General availability. Contains information on Passport 7400, Passport 15000, and Passport 20000 for the PCR5.2 release.

Contents

About this document 13
Who should read this document and why 13
What you need to know 13
How this document is organized 13
What's new in this document 14
Voice services processor 3 with optical TDM interface (2pOc3ChSmIrVsp3) 14
Text conventions 14
Related documents 15
How to get more help 16

Chapter 1

Software upgrade 17
Prerequisites to software upgrade 17
Software upgrade work flow 17

Chapter 2

Information collection 19
Downloading release notes 22
Verifying hardware compatibility 23
Verify Passport feature compatibility 24
Verifying non-Passport application compatibility 25
Completing the Passport software upgrade checklist 26

Chapter 3

Software migration 29
Saving a copy of the current view with Preside MDM 32
Saving a copy of the current view with CLI 35
Verifying the Passport status before upgrading 38
Performing a hitless software migration 43
Performing a service-interrupting software migration 52
Stopping a hitless software migration 60
Rollback to a saved provisioning view using Preside MDM 61
Rollback to a saved provisioning view using CLI 65
Determining the status of fabric card firmware 67
Upgrading Passport 15000 or 20000 fabric card firmware 68
Verifying the success of the software migration 70

Chapter 4

Feature upgrades and patch activation 71
Applying a software patch 73
Migrating software versions for a feature 75

Chapter 5

Software migration overview 81
Service-interrupting software migration for Passport 81
Operator control during a service-interrupting software migration 83
Hitless software migration for Passport 15000 and 20000 83
What happens during a hitless software migration? 83
Phase 1 — Preparation of the CP 84
Phase 2 — CP migration 84
Phase 3 — FP migration 86
Phase 4 — Migration switchover 86
Phase 5 — Post-migration 87
Hitless software migration equipment protection and sparing 87
Operator control during a hitless software migration 91
Software patches 92

Feature software migration 93
Fabric firmware upgrade 93
View migration during a software migration 94

List of figures

Figure 1 Software upgrade work flow 18
Figure 2 Information collection task flow 20
Figure 3 Software migration task flow 30
Figure 4 Example of osistate display 42
Figure 5 Feature upgrades and patch activation task flow 72
Figure 6 Passport alarm sequence during a feature software migration 78
Figure 7 View migration during a software migration 95

List of tables

Table 1 Passport software upgrade checklist 26
Table 2 Impact of an error condition on a Passport hitless software migration 49
Table 3 Impact of an error condition on a Passport hitless software migration 56
Table 4 Impact of an error condition on a feature software migration 79
Table 5 Phases of a service-interrupting software migration activation on Passport 82
Table 6 Hot standby applications and features 88
Table 7 Warm standby applications and features 89

About this document

The following topics are discussed in this section:

- "Who should read this document and why" (page 13)
- "What you need to know" (page 13)
- "How this document is organized" (page 13)
- "What's new in this document" (page 14)
- "Text conventions" (page 14)
- "Related documents" (page 15)
- "How to get more help" (page 16)

Who should read this document and why

This NTP is intended for any user who has the responsibility of performing or planning a software upgrade on a Passport.

What you need to know

Users of this NTP must have an advanced knowledge of Preside Multiservice Data Manager, Unix, the Passport software, and their network architecture.

How this document is organized

241-5701-272 *Passport 7400, 15000, 20000 Software Upgrade* contains the following sections:

- "Software upgrade" (page 17)
- "Information collection" (page 19)
- "Software migration" (page 29)

- “Feature upgrades and patch activation” (page 71)
- “Software migration overview” (page 81)

What’s new in this document

The following feature was added to this document:

- “Voice services processor 3 with optical TDM interface (2pOc3ChSmIrVsp3)” (page 14)

Other changes made to this document include the following.

- For CR Q00770163, the section “Prerequisites to software upgrade” (page 17) was updated with information about how to download new software and fabric firmware.

Voice services processor 3 with optical TDM interface (2pOc3ChSmIrVsp3)

The following section was updated for this feature:

- “Hot standby applications and features” (page 88)

Text conventions

This document uses the following text conventions:

- `nonproportional spaced plain type`

  Nonproportional spaced plain type represents system generated text or text that appears on your screen.

- **`nonproportional spaced bold type`**

  Nonproportional spaced bold type represents words that you should type or that you should select on the screen.

- *italics*

  Statements that appear in italics in a procedure explain the results of a particular step and appear immediately following the step.

  Words that appear in italics in text are for naming.

- [optional_parameter]

  Words in square brackets represent optional parameters. The command can be entered with or without the words in the square brackets.

- <general_term>

  Words in angle brackets represent variables which are to be replaced with specific values.

- UPPERCASE, lowercase

  Passport commands are not case-sensitive and do not have to match commands and parameters exactly as shown in this document, with the exception of string options values (for example, file and directory names) and string attribute values.

- |

  This symbol separates items from which you may select one; for example, ON|OFF indicates that you may specify ON or OFF. If you do not make a choice, a default ON is assumed.

- ...

  Three dots in a command indicate that the parameter may be repeated more than once in succession.

The term absolute pathname refers to the full specification of a path starting from the root directory. Absolute pathnames always begin with the slash (/) symbol. A relative pathname takes the current directory as its starting point, and starts with any alphanumeric character (other than /).

Related documents

You may need to refer to the following documents while performing your Passport upgrade:

- 241-5701-050 *Passport 7400, 15000, 20000 Commands*
- 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*
- 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*

- 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*
- Passport Release Notes

How to get more help

For information on training, problem reporting, and technical support, see the "Nortel Networks support services" section in the *241-5701-030 Passport 7400, 15000, 20000 Overview*.

Chapter 1
Software upgrade

Upgrade software to add new functionality and reliability to your Passport by activating a new version of software.

Navigation links

- “Prerequisites to software upgrade” (page 17)
- “Software upgrade work flow” (page 17)

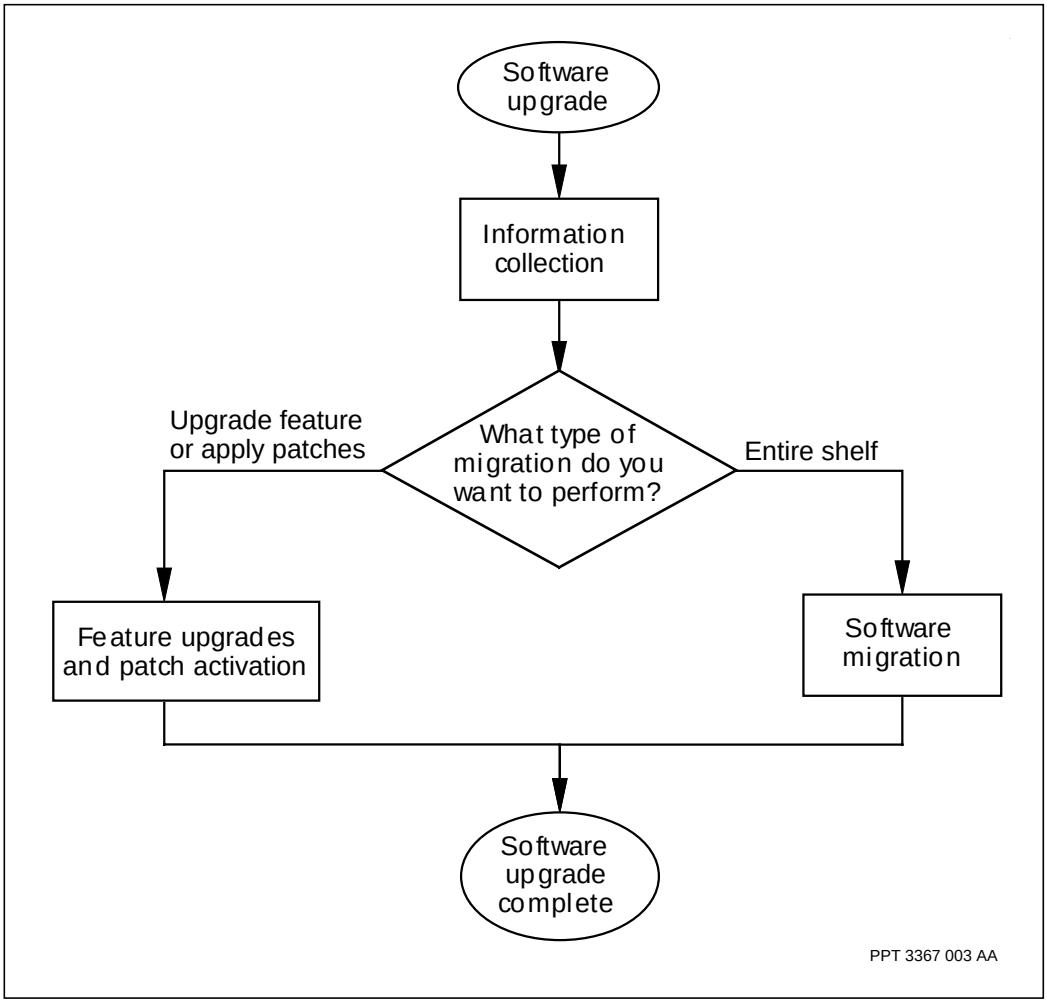
Prerequisites to software upgrade

- There is new software available and a requirement for that new software has been determined.
- Determine the correct version of software or fabric firmware you are migrating to and download it from the Passport software distribution site. Refer to 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide* for more information on downloading Passport software.

Software upgrade work flow

This work flow shows you the sequence of procedures you perform to upgrade software on your Passport. To link to any procedure, go to “Work flow navigation” (page 18).

Figure 1
Software upgrade work flow



Work flow navigation

- “Information collection” (page 19)
- “Software migration” (page 29)
- “Feature upgrades and patch activation” (page 71)

Chapter 2
Information collection

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

Navigation links

- “Prerequisites to information collection” (page 19)
- “Information collection flow” (page 19)

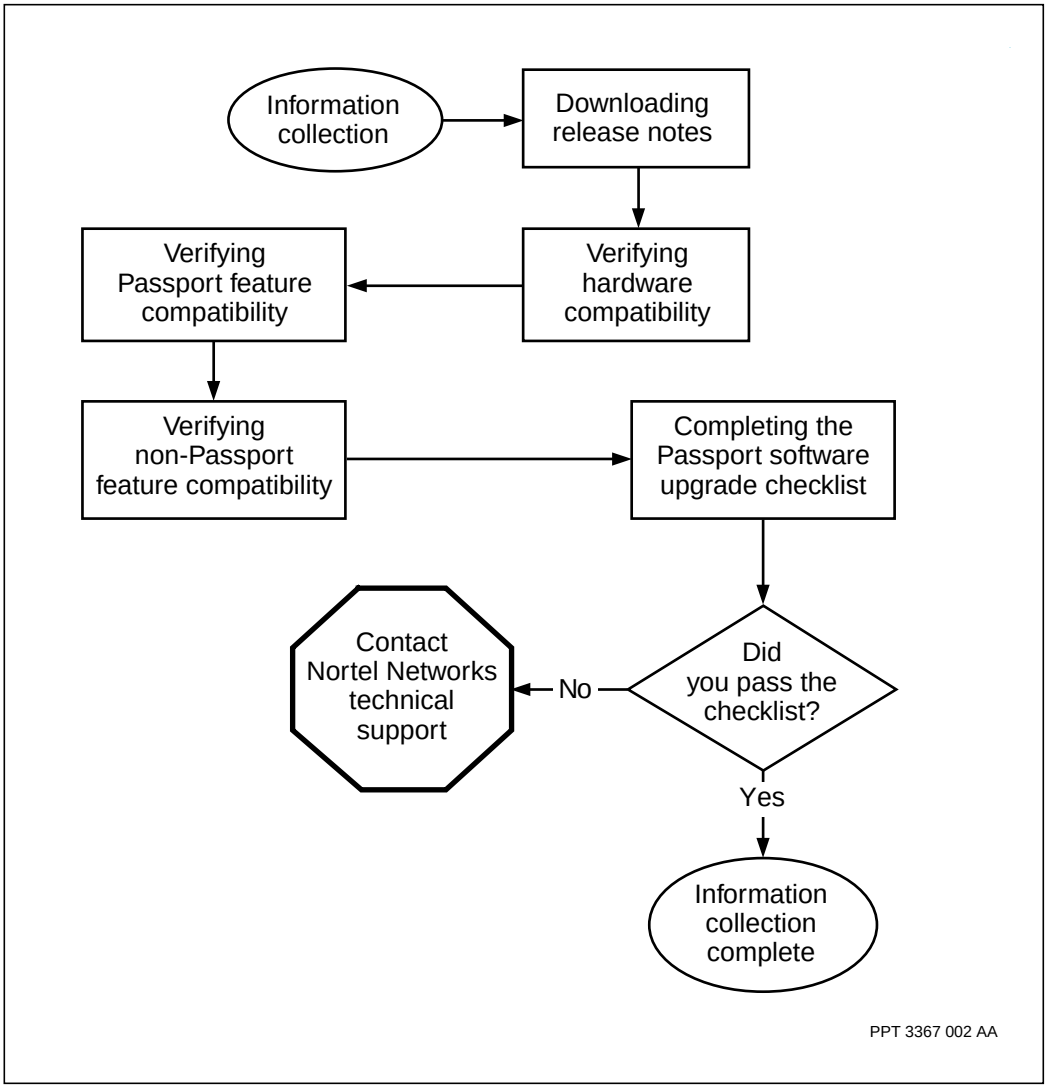
Prerequisites to information collection

- You have confirmed which release of software is active on the Passport.
- You have determined an upgrade path to identify which release you are migrating to and the releases you must migrate through to reach the intended release.
- Your Passport is operating without errors or failures.

Information collection flow

This task flow shows you the sequence of procedures you perform to collect information about the upgrade. To link to any procedure, go to “Task navigation” (page 20).

Figure 2
Information collection task flow



Task navigation

- “Downloading release notes” (page 22)
- “Verifying hardware compatibility” (page 23)

- “Verify Passport feature compatibility” (page 24)
- “Verifying non-Passport application compatibility” (page 25)
- “Completing the Passport software upgrade checklist” (page 26)
- For information about the next task, see “Software upgrade work flow” (page 18)

Downloading release notes

Download release notes to collect specific information affecting hardware and services for each of the Passport software releases (PCRs) involved in the migration.

Procedure steps

1. Got to the Nortel Networks public website.

   http://www.nortelnetworks.com/

2. In the section titled “Support” click on Technical Documentation.
3. Click on “Passport” in the list of products.
4. Click on the “documentation” link for the specific Passport product you are upgrading.
5. Select and download all the documentation you require.

   Some documentation may require you to register and login using your userid and password.

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

1. Note the product engineering codes (PECs) of all the processor cards used in your Passport.

   ```
   d shelf card/<card_no> *
   ```

2. Review the hardware compatibility section of the 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 the Release Notes of each release in the migration path.

Variable definitions

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

Verify Passport feature compatibility

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

Procedure steps

1. Create a list of all the Passport applications loaded on your Passport.
2. Refer to the Passport Release Notes of 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.

Verifying non-Passport application compatibility

Verify non-Passport application compatibility to confirm that any 3rd party software being used will not interfere with the software migration.

Procedure steps

1. List all the non-Passport applications you are using with your Passport.
2. Refer to the technical documentation of the non-Passport software you are using for any known compatibility issues with the PCR versions in your migration path.
3. Refer to the Passport Release Notes of each PCR in your migration path to confirm there are no known compatibility issues.
4. Contact your Nortel Networks Service Representative and inform them of your specific scenario to ensure there are no known compatibility issues.

Completing the Passport software upgrade checklist

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

Procedure steps

1. Complete the checklist by referring to the information discovered while performing the “Information collection task flow” (page 20).

Procedure job aid

Table 1
Passport software upgrade checklist

Task	Complete		Date and comments
	Yes	No	
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 Passport applications, features, and software.			
Migration operator has complete knowledge of migrating software versions.			
The Release Notes of 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)			
Passport hardware is compatible with all releases in the migration path.			

(Sheet 1 of 2)

Table 1 (continued)
Passport software upgrade checklist

Task	Complete		Date and comments
	Yes	No	
Passport software is compatible with all releases in the migration path.			
Non-Passport applications are compatible with all releases in the migration path.			
All provisioning files have been saved (backed up).			
Network configuration changes are prohibited.			
The software version you are migrating to has been downloaded and installed on the Passport.			
The software patches you are applying have been downloaded and installed on the Passport.			
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 Passport 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 Passport.			
(Sheet 2 of 2)			

Chapter 3
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.

Navigation links

- “Prerequisites for software migration” (page 29)
- “Software migration flow” (page 29)

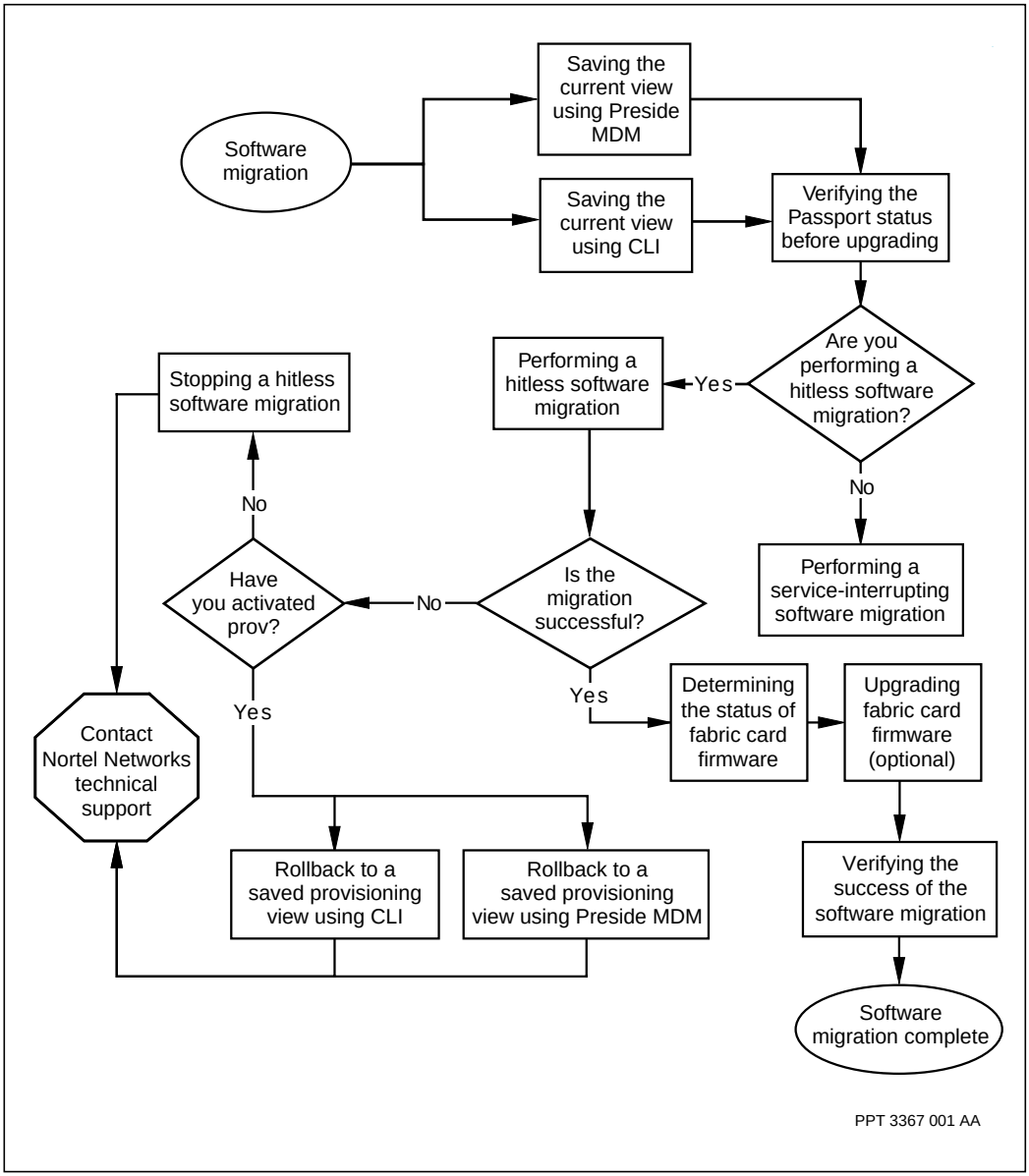
Prerequisites for software migration

- The committed view, the current view, the edit view, and the last used view must be identical. If these views are not the same, refer to the 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide* for information on making them the same.

Software migration flow

This task flow shows you the sequence of procedures you perform to migrate software. To link to any procedure, go to “Task navigation” (page 31).

Figure 3
Software migration task flow



Task navigation

- “Saving a copy of the current view with Preside MDM” (page 32)
- “Saving a copy of the current view with CLI” (page 35)
- “Verifying the Passport status before upgrading” (page 38)
- “Performing a hitless software migration” (page 43)
- “Performing a service-interrupting software migration” (page 52)
- “Stopping a hitless software migration” (page 60)
- “Rollback to a saved provisioning view using Preside MDM” (page 61)
- “Rollback to a saved provisioning view using CLI” (page 65)
- “Determining the status of fabric card firmware” (page 67)
- “Upgrading Passport 15000 or 20000 fabric card firmware” (page 68)
- “Verifying the success of the software migration” (page 70)
- For information about the next task, see “Software upgrade work flow” (page 18)

Saving a copy of the current view with Preside MDM

Save a copy of the current view with Preside MDM 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 Passport software, when the Passport switch restarts, it restarts in the operational state it was in when you saved that view.
- The backup site can be the Preside MDM server or another Passport. It can also be a Software Distribution Site (SDS) configured to store backed-up Passport service data.
- Verify that the backup site has enough space to accommodate the backup.
- Use the Passport/SNMP Devices Backup and Restore tool for saving a copy of the current view.
- The Passport/SNMP Devices Backup and Restore tool uses the */tmp* directory to perform some of its file processing (for example, archive, compress, and uncompress). Your local disk needs to have twice the amount of space as the actual size of the files you are transferring for back up. You need to clean up the local disk if errors are raised (for example, *"No space left on device")*. In this case, you can mount the */tmp* directory from a lower-usage disk on a selected file server.
- The Passport/SNMP Devices Backup and Restore tool backs up only the Passport configuration data. It does not back up the base Passport software.
- The Backup server, the Restore server, the PP Backup provider, and the PP restore provider must all be running on the Preside MDM server for the Passport/SNMP Devices Backup and Restore tool to function properly. Using the Server Administration tool from the Preside MDM toolset, verify that these four servers are running. If they are not or if you need more information, refer to 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

- The Preside MDM server may be configured to regularly back up the provisioning files from the Passport. By creating a backup of the committed file before beginning the upgrade, you ensure that you have the most current committed file you can have before beginning the migration.

Procedure steps

1. Open a Preside MDM window:

   ```
   /opt/MagellanNMS/bin/nmstool &
   ```

   The copyright dialog and the Preside MDM window open.

2. Click *OK* to close the copyright dialog.

3. From the MDM window, select Configuration > Passport Devices > Administration > Passport/SNMP Service Data Backup/Restore.

   The Passport/SNMP Devices Backup and Restore window opens.

4. From the File menu, select Open.

   The Open File dialog opens.

5. Select a device information file by entering a path and file name in the File name text box. You can also select a device using the Look in drop-down list box and clicking on the file in the display panel.

6. Click *Open* to load the selected device information file and close the dialog.

7. In the Passport/SNMP Devices Backup and Restore window, click *Backup*.

   The Passport/SNMP Devices Backup window opens.

8. In the Backup to text box, adjust where you want the Preside MDM server to put the back up file as required.

9. Select the Passport that you want to back up from the Backup Information area of the window.

   The selected devices have a check mark in the Bck column. All other devices have no entry in the Bck column.

10. In the Backup Mode Selection area, click *full*.

11. 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.

12 When the back up is finished, click *Exit* to close the window.

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 Passport software, when the Passport switch 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 Passport switch.
- You must understand UNIX and FTP.
- You must save and restore all views in binary format.

Procedure steps

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 Passport.

4. If needed, create a directory on the Preside MDM server to save the view:

   ```
   mkdir <prov_dir>.<type>.<num>
   ```

5. On the Preside MDM server, change to the directory you wish to save the provisioning files in:

```
cd <prov_dir>.<type>.<num>
```

6 From the Preside MDM server, FTP to the Passport switch:

```
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 Passport type.

13 Quit your FTP session:

```
ftp> quit
```

Variable definitions

Variable	Value
<filename>	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>	The name of the Passport switch.
<num>	The number of the file that contains the provisioning data. This number must be a 3 digit sequence.

(Sheet 1 of 2)

Variable	Value
<prov_dir>	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>	The names of the provisioning files.
<type>	The type of the file, either full or part, that contains the provisioning data.

(Sheet 2 of 2)

Verifying the Passport status before upgrading

Verify the status of the Passport before upgrading to ensure that the Passport does not have any alarms raised on it and that it has been configured correctly. In addition, by recording the current switch 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 the Preside MDM 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 the Preside MDM 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 Passport you are upgrading and all of the switches connected to it must be free of alarms.

Procedure steps

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
```

11 For a Passport 15000 or 20000 upgrade 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.

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.

12 For a Passport 15000 or 20000 display the *Laps* components:

```
display Laps/*
```

13 For each *Laps* component of a Passport 15000 or 20000, 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.

14 For a Passport 15000 or 20000 verify that the *lop, ais, rfi, slm, txAis* and *txRdi* attributes of the *Laps* components have a value of *off*:

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

15 For a Passport 15000 or 20000 verify that the *Laps* components are enabled and without alarms:

```
display Laps/* osistate
```

16 Display and record the virtual router instance values:

```
list VirtualRouter/*
```

17 Display and record the virtual router protocol port instance values:

```
list VirtualRouter/0 ProtocolPort/*
```

18 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.

19 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/*
```

20 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:

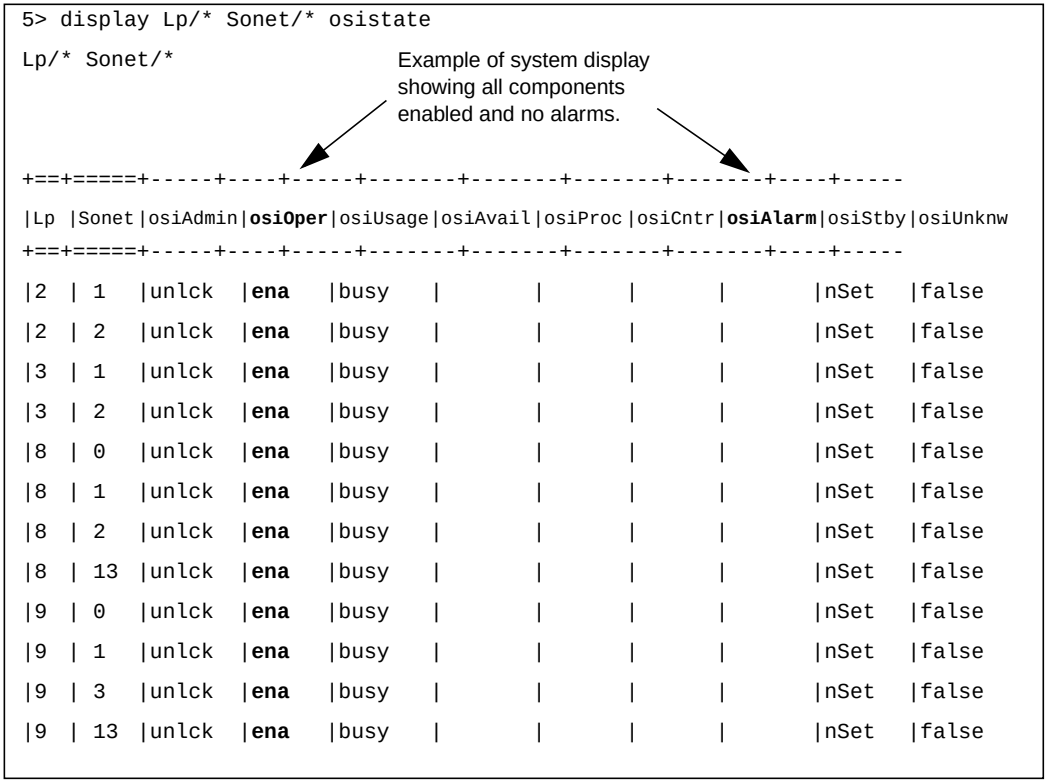
```
display –nt VirtualRouter/<vr_inst> Ip Static Route/*
Nh/*
```

Variable definitions

Variable	Value
<enet_port>	The port number of the OAM ethernet port on the control processors.
<laps_inst>	The instance value of the *Laps* component whose manual overrides you want to remove. This instance value is an integer between 0 and 15999.
<vr_inst>	The instance value of the *VirtualRouter* component.
<pp_num>	The instance value of the *ProtocolPort* component.

Procedure job aid

Figure 4
Example of osistate display



Performing a hitless software migration

Perform a hitless software migration to change the software version the Passport 15000 or 20000 is using to allow for new or improved functionality without causing a loss of service.

Prerequisites

CAUTION

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.

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 shelf 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

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 Passport.
- Do not load the software applications for the fabric. Refer to "Upgrading Passport 15000 or 20000 fabric card firmware" (page 68) for more information about upgrading the fabric firmware.
- It is recommended that you perform this upgrade using the Command Console tool on the Preside MDM server rather than a telnet session. By using the Command Console, you ensure that you will remain connected to the switch and can monitor the CP switchover. For more information on opening the Command Console, see 241-6001-303 *Preside MDM Administrator Guide*.
- The Passport switch must contain two control processors (CP). One CP must be active and the other CP must be in standby mode.
- 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.
- Refer to the description of each FP card type in 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* to understand any FP-specific migration considerations that may affect how the migration occurs.
- 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.
- You must have an advanced knowledge of Unix, the Passport software, and your network architecture.

Procedure steps

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

```
start -force prov
```

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

2 Copy the current view into the edit view to ensure that they are identical:

```
copy prov
```

Note: If you were 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.

3 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 your switch.

4 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 Passport 15000 or 20000 fabric card firmware" (page 68) for more information about upgrading the fabric firmware.

5 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 3:

```
display Software avList
```

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

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

7 Verify the patches that are going to be applied:

```
display Software patchlist
```

8 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

Potential to interrupt all calls in progress

The software upgrade for the Passport shelf 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 switch 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 and than perform the procedure "Verifying the Passport status before upgrading" (page 38) again.

9 Perform a semantic check:

```
check prov
```

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

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

WARNING

Proceeding with a non-hitless software migration

The switch will go through a normal software migration that is not hitless and all calls on the switch 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 60).

10 Save the edit view with portable formats:

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

11 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.

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 60).

Note: 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 60). To continue with the migration, type *continue prov*.

12 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 switch 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 switch. 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 switch (see step 13). If you are using the Preside MDM Command Console, the connection to the switch is automatically re-established, but you will need to get back into provisioning mode. For more information, see step 1.

13 If using telnet, when prompted, login to the Passport 15000 switch with the appropriate permissions.

14 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
```

15 Enter provisioning mode:

```
start -force prov
```

16 Perform a semantic check on the changes:

```
check prov
```

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

17 If the semantic check passes, save the view:

```
save prov
```

18 If the semantic check passes, commit the final version of the view:

```
commit prov
```

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

19 Verify that the edit view and the current view are the same:

```
display -o prov
```

20 Exit provisioning mode once the migration is complete:

```
end prov
```

Variable definitions

Variable	Value
<filename>	The name of the file to which you are saving the view. You should make this file name easily identifiable.
<new_applications>	A space-separated, case-sensitive list of application versions. The release is indicated by the version number after the underscore.
<patches>	A space-separated, case-sensitive list of patches.

Procedure job aid

Table 2
Impact of an error condition on a Passport 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.

(Sheet 1 of 3)

Table 2 (continued)
Impact of an error condition on a Passport hitless software migration

Phase	Error condition	Result and action
	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.
	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.

(Sheet 2 of 3)

Table 2 (continued)
Impact of an error condition on a Passport hitless software migration

Phase	Error condition	Result and action
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.
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.

(Sheet 3 of 3)

Performing a service-interrupting software migration

Perform a service-interrupting software migration to change the software version the Passport 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.

WARNING

Calls in progress are dropped

This 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.

- Limit the impact of the service interruption by temporarily redirecting traffic to other Passports or nodes in your network.
- The migration will take between 15 minutes and 3.5 hours of time depending on the number of calls and components that have been provisioned on the Passport.
- Do not load the software applications for the fabric. Refer to “Upgrading Passport 15000 or 20000 fabric card firmware” (page 68) for more information about upgrading the fabric firmware.
- It is recommended that you perform this upgrade using the Command Console tool on the Preside MDM server rather than a telnet session. By using the Command Console, you ensure that you will remain connected to the switch and can monitor the CP switchover. For more information on opening the Command Console, see 241-6001-303 *Preside MDM Administrator Guide*.

- Loss of service will be minimized if the Passport contains two control processors (CP). One CP must be active and the other CP must be in standby mode.
- 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.
- Refer to the description of each FP card type in 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* to understand any FP-specific migration considerations that may affect how the migration occurs.
- You must have an advanced knowledge of the Passport software.

Procedure steps

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

```
start -force prov
```

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

2 Copy the current view into the edit view to ensure that they are identical:

```
copy prov
```

Note: If you were 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.

3 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 your switch.

4 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 Passport 15000 or 20000 fabric card firmware" (page 68) for more information about upgrading the fabric firmware.

5 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 3:

```
display Software avList
```

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

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

7 Verify the patches that are going to be applied:

```
display Software patchlist
```

8 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
```

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

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

10 Save the edit view with portable formats:

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

11 Apply the changes and start the migration:

```
activate prov
```

12 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 switch 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 switch. 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 switch (see step 13). If you are using the Preside MDM Command Console, the connection to the switch is automatically re-established, but you will need to get back into provisioning mode. For more information, see step 1.

13 If using telnet, when prompted, login to the Passport 15000 switch with the appropriate permissions.

14 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
```

15 Enter provisioning mode:

```
start -force prov
```

16 Perform a semantic check on the changes:

```
check prov
```

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

17 If the semantic check passes, save the view:

```
save prov
```

18 If the semantic check passes, commit the final version of the view:

```
commit prov
```

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

19 Verify that the edit view and the current view are the same:

```
display -o prov
```

20 Exit provisioning mode once the migration is complete:

```
end prov
```

Variable definitions

Variable	Value
<filename>	The name of the file to which you are saving the view. You should make this file name easily identifiable.
<new_applications>	A space-separated, case-sensitive list of application versions. The release is indicated by the version number after the underscore.
<patches>	A space-separated, case-sensitive list of patches.

Procedure job aid

Table 3
Impact of an error condition on a Passport 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.
(Sheet 1 of 4)		

Table 3 (continued)
Impact of an error condition on a Passport hitless software migration

Phase	Error condition	Result and action
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.
	Former migrating FP cannot become active.	FP outage. The new provisioning view is maintained. Respond to alarms generated by the system.

(Sheet 2 of 4)

Table 3 (continued)
Impact of an error condition on a Passport hitless software migration

Phase	Error condition	Result and action
	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.

(Sheet 3 of 4)

Table 3 (continued)
Impact of an error condition on a Passport hitless software migration

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.

(Sheet 4 of 4)

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.

- Refer to the description of each FP card type in 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* to understand any FP-specific migration considerations that may affect how the migration occurs.

Procedure steps

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 43)

Rollback to a saved provisioning view using Preside MDM

Rollback to a saved provisioning view using Preside MDM to abort an upgrade and revert to a previous working provisioning file on the Passport 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 Passport 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.
- You must refer to the Release Notes of the PCR you are reverting to and identify any hardware or software considerations.
- The Passport restarts in the operational state it was in when you saved the current view if you revert to a saved view of an older version of Passport software.

- The Backup server, the Restore server, the PP Backup provider, and the PP restore provider must all be running on the Preside MDM server for the Passport/SNMP Devices Backup and Restore tool to function properly.

Procedure steps

1 Open a Preside MDM window:

```
/opt/MagellanNMS/bin/nmstool &
```

The copyright dialog and the Preside MDM window open.

2 Click *OK* to close the copyright dialog.

3 From the MDM window, select Configuration > Passport Devices > Administration > Passport/SNMP Service Data Backup/Restore.

The Passport/SNMP Devices Backup and Restore window opens.

4 From the File menu, select Open.

The Open File dialog opens.

5 Select a device information file by entering a path and file name in the File name text box. You can also select a device using the Look in drop-down list box and clicking on the file in the display panel.

6 Click *Open* to load the selected device information file and close the dialog.

7 In the Passport/SNMP Devices Backup and Restore window, click *Restore*.

The Passport/SNMP Devices Restore window opens.

8 In the Restore from text box, adjust where you want the Preside MDM server to restore from as required.

9 In the Restore Information area of the main window, select the device or devices whose service data you need to restore.

The selected devices have a check mark in the Rst column. All other devices have no entry in the Rst column.

10 In the Restore Mode Selection area, click *full*.

11 Click *Restore*.

When the restore completes successfully, a message is displayed in the Message area. If the restore is unsuccessful, an error dialog 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.

12 Log back into the Passport.

13 Download to the Passport any required application software missing from the Passport disk.

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

```
start prov
```

15 Activate the previously saved view:

```
activate -file(<filename>) -force prov
```

Network connectivity is lost and the switch 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.

16 Reconnect to the switch.

17 Confirm the provisioning changes:

```
confirm prov
```

18 Save the view:

```
save prov
```

19 Commit the provisioning changes:

```
commit prov
```

20 Exit provisioning mode once the migration is complete:

```
end prov
```

Variable definitions

Variable	Value
<filename>	The name of the previously saved view.
<IPAddress>	The IP address of the switch 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 Passport 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 Passport 15000 switch 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 Passport software, when the Passport restarts, it restarts in the operational state it was in when you saved the current view.

Procedure steps

1. Login to the Passport with the appropriate permissions.
2. Enter provisioning mode so that you can issue the appropriate commands:

   ```
   start prov
   ```

3 Activate the previously saved view:

```
activate -file(<filename>) -force prov
```

Network connectivity is lost and the switch 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 switch.

5 Confirm the provisioning changes:

```
confirm prov
```

6 Save the view:

```
save prov
```

7 Commit the provisioning changes:

```
commit prov
```

8 Exit provisioning mode once the migration is complete:

```
end prov
```

Variable definitions

Variable	Value
<filename>	The name of the previously saved view.
<IPAddress>	The IP address of the switch 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 fabrics must be installed and in service.

Procedure steps

1. Display the attributes of the fabric banks:

   ```
   Display -n shelf 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.

Upgrading Passport 15000 or 20000 fabric card firmware

Upgrade Passport 15000 or 20000 fabric card firmware to take advantage of enhancements and new functionality and to improve the Passport 15000 or 20000 operating efficiency.

Prerequisites

- For Passport 20000, the fabric firmware must be fabric driver 7.9 to complete your software migration or fabric replacement successfully. For Passport 7400 and Passport 15000, firmware replacement is encouraged, but is not necessary to complete your software migration or fabric replacement successfully.
- To upgrade the firmware on one fabric, both fabrics on the Passport 15000 or 20000 node must be installed and operational.
- The fabric that is receiving the new firmware version must be locked.
- The fabric that is not receiving the new firmware version must be unlocked and enabled.

Procedure steps

1 Display the fabric driver version currently installed:

```
d 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:

```
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 operates correctly with the new firmware:

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

The test results show whether the fabric is operating correctly. The 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* can assist you in understanding the test results.

6 If there are problems with the upgraded fabric, 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 corrupt, the fabric might not come up. If the writable bank is corrupt, it must be replaced. Contact your Nortel Networks representative.

7 Unlock the fabric to return it to service:

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

Variable definitions

Variable	Value
<fabcard_inst>	The instance of the fabric card, *X* for a fabric in the upper cage, or *Y* for a fabric in the lower cage.
<load>	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 Passport 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

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 Passport 15000 or 20000 equipment protection.

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

Chapter 4
Feature upgrades and patch activation

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

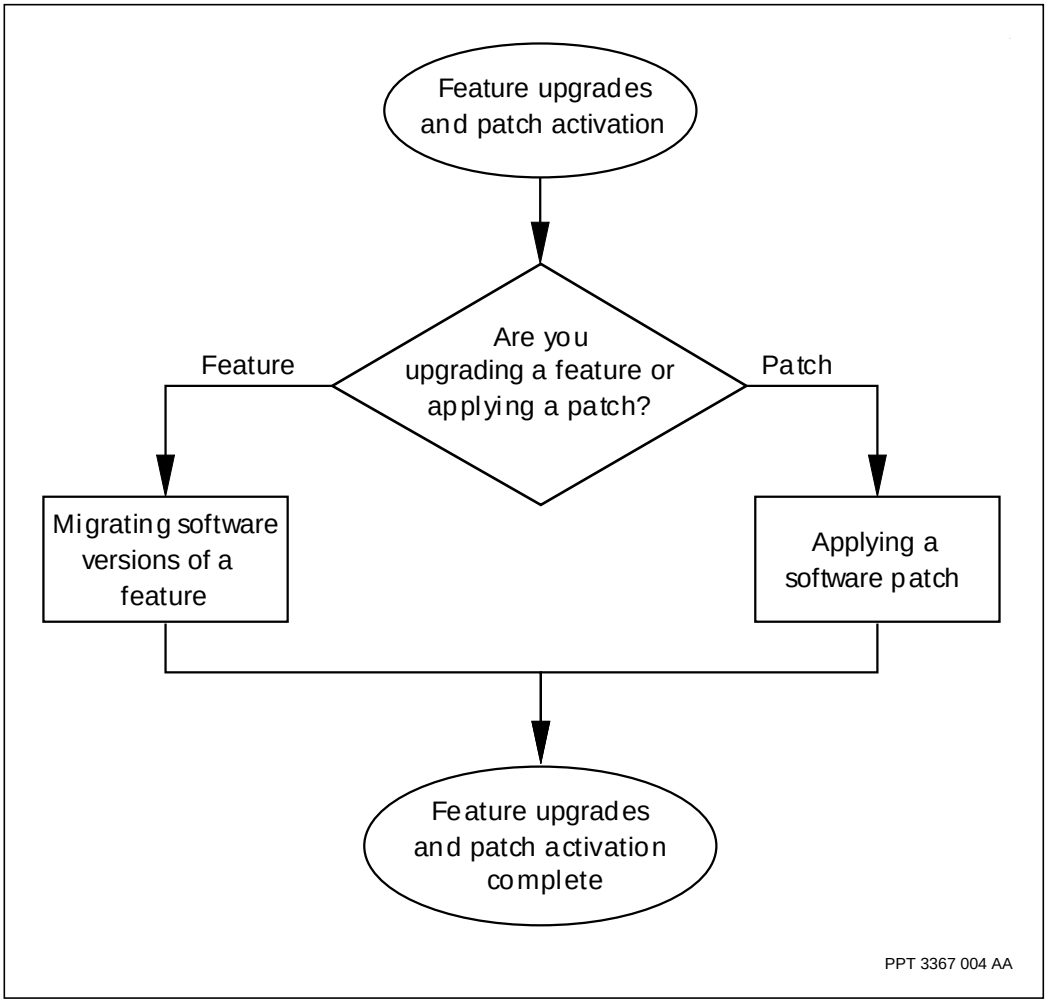
Navigation links

- “Feature upgrades and patch activation flow” (page 71)
- “Task navigation” (page 72)

Feature upgrades and patch activation flow

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 “Task navigation” (page 72).

Figure 5
Feature upgrades and patch activation task flow



Task navigation

- “Applying a software patch” (page 73)
- “Migrating software versions for a feature” (page 75)

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 shelf 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.

- The Passport switch must contain two control processors (CP). One CP must be active and the other CP must be in standby mode.
- 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.
- You must have an advanced knowledge of Unix, the Passport software, and the Succession portfolio architecture.

Procedure steps

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

   ```
   start -force prov
   ```

2. Display the current software patchlist:

   ```
   display -c Software patchList
   ```

3. Apply the Passport patches needed to the patchlist:

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

4. Verify the patches that are going to be applied:

   ```
   display Software patchlist
   ```

5. Perform a semantic check:

   ```
   check prov
   ```

6. Apply the changes and start the migration:

   ```
   activate prov
   ```

7. If the semantic check passes, commit the final version of the view:

   ```
   commit prov
   ```

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

8. Save the edit view with portable formats:

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

9. Exit provisioning mode once the migration is complete:

   ```
   end prov
   ```

Variable definitions

Variable	Value
<filename>	The name of the file to which you are saving the view. You should make this file name easily identifiable.
<patches>	A space-separated, case-sensitive list of patches.

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. 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 Passport to be upgraded must be physically installed, operational, and running Passport software.
- All affected function processors should 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 Passport 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 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* to verify minimum software requirements of function processors. Refer to 241-1501-200 *Passport 15000, 20000 Hardware Description* and 241-7401-200 *Passport 7400 Hardware Description* to verify minimum software requirements for control processors.
- The current provisioning view must be the committed view.
- Plan the software migration for an appropriate time. The software migration may take between 3 to 12 hours to complete depending on the number of function processors affected.
- There is no command to stop the software migration once it has started. Refer to “Procedure job aid” (page 78) for more information on handling errors during the feature software migration.

Procedure steps

ATTENTION	There is no command to stop the software migration once it has started.

1 Start the provisioning view.

```
start prov
```

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
```

6 Verify the provisioning changes are correct.

```
check prov
```

7 Save the edit view with portable formats.

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

8 Activate the provisioning and start the migration.

```
act prov
```

9 Immediately confirm the provisioning to prevent rollback to the previous view. Do not wait for the migration to complete before confirming the provisioning view.

```
conf prov
```

10 Monitor the generated alarms to verify the migration progress and completion.

11 Commit the provisioning view.

```
commit prov
```

CAUTION

Loss of service

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

Variable definitions

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

Procedure job aid

Figure 6
Passport alarm sequence during a feature software migration

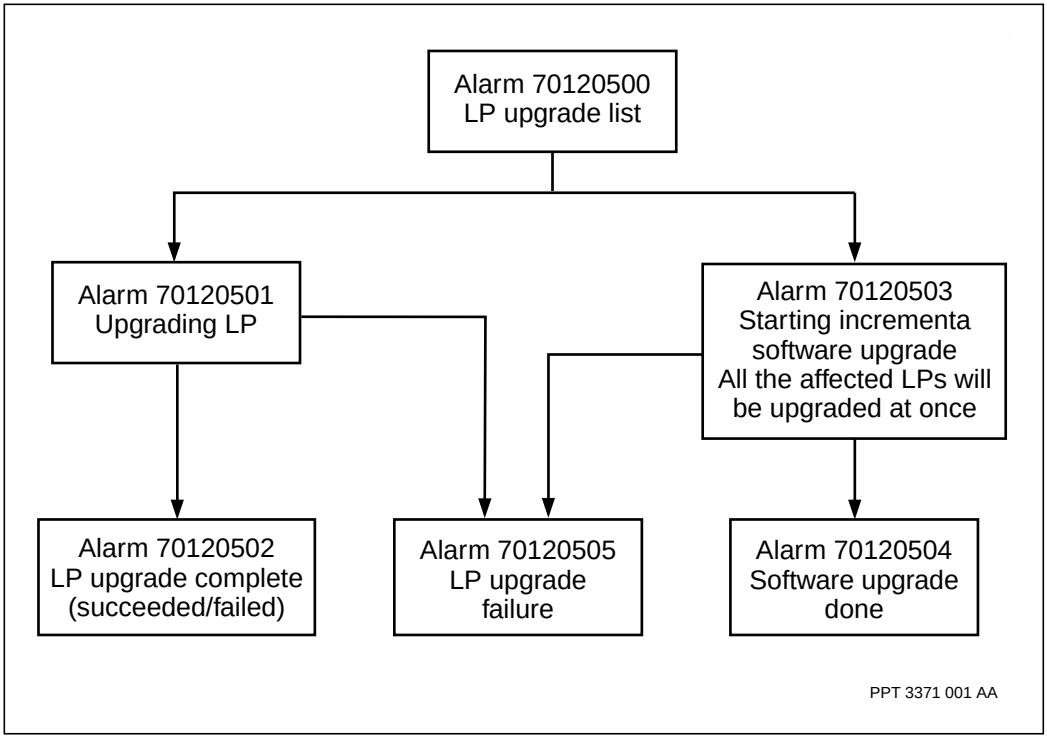


Table 4
Impact of an error condition on a feature software migration

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.
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 75) 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 75) 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.

Chapter 5
Software migration overview

Passport provides the capability of upgrading software three different ways, depending on your configuration. You may perform a complete migration that temporarily removes your Passport from service or you may choose to perform a hitless software migration that has the potential to not interrupt services. Passport also offers a migration that upgrades the software for a specific feature without upgrading the software for the entire Passport. This section describes the types of software migration and their associated processes. It covers the following topics:

- "Service-interrupting software migration for Passport" (page 81)
- "Hitless software migration for Passport 15000 and 20000" (page 83)
- "Software patches" (page 92)
- "Feature software migration" (page 93)
- "Fabric firmware upgrade" (page 93)
- "View migration during a software migration" (page 94)

Service-interrupting software migration for Passport

A service-interrupting software migration causes the whole Passport 7400, Passport 15000, or Passport 20000 and all of its applications to go out of service during the migration. To reduce the time that the Passport 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.

Table 5
Phases of a service-interrupting software migration activation on Passport

Phase	Activity
1) Active CP pre-work	The edit view is saved in a temporary file.
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.
Note: 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 Passport 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 Passport 15000 and 20000

Hitless software migration for Passport 15000 and 20000 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 83)
- "Hitless software migration equipment protection and sparing" (page 87)
- "Operator control during a hitless software migration" (page 91)

What happens during a hitless software migration?

During a hitless software migration, the Passport 15000 or 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 84)
- "Phase 2 — CP migration" (page 84)
- "Phase 3 — FP migration" (page 86)
- "Phase 4 — Migration switchover" (page 86)
- "Phase 5 — Post-migration" (page 87)

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.

Note: 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.

Note: 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.

Passport 15000 and 20000 software applications and features fall into three behavior categories during hitless software migration:

- hot standby. For a definition and description of hot standby, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*.

- warm standby. For a definition of warm standby, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*.
- cold standby. For a definition of cold standby, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*.

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 88) for a list of hot standby applications and features as they apply to hitless software migration. See "Warm standby applications and features" (page 89) 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 88) or "Warm standby applications and features" (page 89) either does not apply to Passport 15000 and 20000 or is a cold standby application or feature.

Table 6
Hot standby applications and features

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

Table 6 (continued)
Hot standby applications and features

Application	Feature
pvg	vgsAtmDc vgsAtmG729 vgslpG729 vgsAtm vgsIp
Note: Applications aal1Ces and PVG support hot equipment protection (HEP) and hitless software migration (HSM) for a 1 + 1 sparing configuration on the Passport 15000 Packet Voice Gateway (PVG) shelf. 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 Passport 15000 PVG shelf 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.	
(Sheet 2 of 2)	

Table 7
Warm standby applications and features

Application	Feature
base	aal1Ces imaAtmForum
Note: LAN applications are considered warm standby.	
(Sheet 1 of 3)	

Table 7 (continued)
Warm standby applications and features

Application	Feature
atmNetworking	atmApi dprsMcsAgent dprsMcsEp dprsMcsEpIntercept porsApi routingGateway
callRedirection	callRedirection
frameRelay	frameRelayAtm frameRelayAtmNiwf frameRelayAtmIsdn frameRelayDte frameRelayNni frameRelayUni frameRelayUniPvcSvc frf5EndPoint frsVirtualFramer ppp
huntGroupSystem	huntGroupSystem
ip	ip
networking	callServer dpnRouting ipiFr

(Sheet 2 of 3)

Table 7 (continued)
Warm standby applications and features

Application	Feature
serviceTrace	frameRelayNniTrace frameRelayUniTrace frTraceRcvr x25TraceRcvr
trunks	atmTrunks porsTrunks
WanDte	LocalMedia AtmMpe
(Sheet 3 of 3)	

Operator control during a hitless software migration

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

```
display -o prov
```

During a hitless software migration on a Passport 15000 or 20000 node, 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 a Passport 15000 or 20000 node 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

Passport software patches may be used to fix a known software problem or as a diagnosis tool.

There are 4 patch categories:

- non-disruptive patch
- disruptive patch
- cross-application patch
- combination patch

Disruptive patches impact service on affected cards and may even require a shelf restart while non-disruptive patches do not interrupt service and are loaded dynamically so all cards stay in service.

Combination patches consist of both disruptive and non-disruptive elements while a cross-application patch modifies code in more than one application.

After you download a new patch to an application version, you must enable it by adding it to the patch list. Passport does not use a patch until it is on the patch list of the current view. You cannot put a patch on the patch list unless

its associated application version is on the application version list. Some patches may require other patches to also be on the patch list. Certain combinations of patches may not work together.

For more information on patches, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*. See the *Passport Release Report* for the restrictions on particular patches.

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 Passport.

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 firmware to ensure the version in the control processors (CPs) matches or is compatible with the firmware in a replaced or upgraded fabric. A fabric 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 firmware when an update is available.

All software running on Passport 15000 or 20000 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 firmware allows you to take advantage of enhancements and new functionality and to improve the Passport 15000 or 20000 operating efficiency.

The alarms also indicate which firmware to install on the fabric card. For more information on Passport 15000 and 20000 alarms, see 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*. You can install new fabric card firmware at any time during normal switch 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.

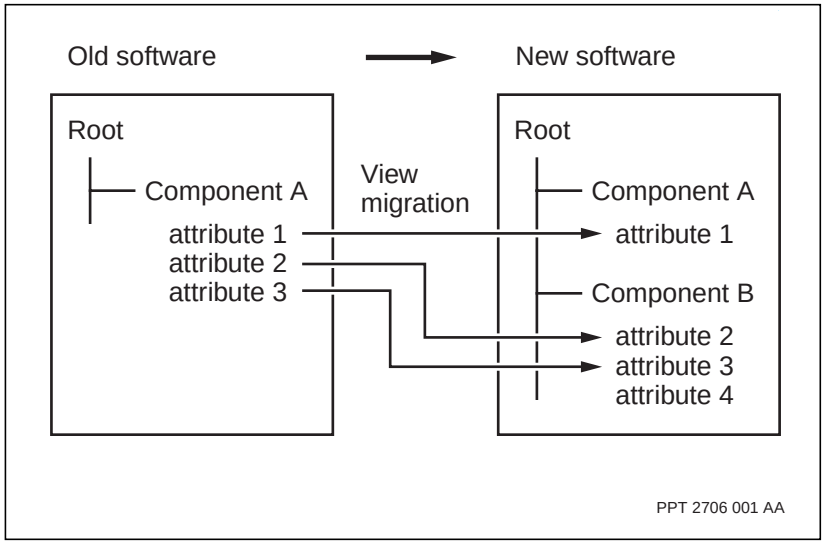
The current view and the edit view store their provisioned data using the component model of the currently running software. When you update the application version list of the edit view and activate it, you change the currently running software and move from one component model to another.

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.

> ***Note:*** 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 95) 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.

Figure 7
View migration during a software migration



Passport 7400, 15000, 20000
Software Upgrade

Release 5.2

Publication: 241-5701-272
Document status: Standard
Document version: 5.2S3
Document date: March 2004
Printed in Canada

NORTEL NETWORKS