NORTEL NETWORKS

Passport 7400, 15000, 20000

Configuration Guide

241-5701-600

Passport 7400, 15000, 20000

Configuration Guide

Publication: 241-5701-600
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

List of figures

List of tables

About this document

This document describes the Passport system and provides the procedures you need to configure the Passport system.

The following topics are discussed in this section:

Who should read this document and why

This guide is for anyone who performs the following tasks for configuring the Passport system:

- planning
- installing and provisioning
- operating and maintaining

What you need to know

This guide assumes that you understand the architecture and operation of Passport products. You also require basic UNIX knowledge.

You can acquire Passport product knowledge by reading 241-5701-030 *Passport 7400, 15000, 20000 Overview*.

Before you operate and maintain Passport, make sure you understand the following:

- Passport concepts
  - Passport hardware and software
  - Passport installation, commissioning, and provisioning
  - Passport-to-Passport interworking
  - Passport-to-DPN-100 interworking (applicable to Passport 7400 series only)
- UNIX
  - UNIX workstations
  - UNIX operating system, its facilities, and commands
- standard network operations and maintenance activities
- Preside Multiservice Data Manager workstation concepts

How this document is organized

This document contains the following sections:

- “Passport file system maintenance” (page 197)
- “Passport electrical interface equipment protection configuration” (page 205)
- “Passport 7400 optical interface line protection configuration” (page 211)
- “Passport 15000 or 20000 optical interface line and equipment protection configuration” (page 219)
- “Hitless services on Passport” (page 239)
- “Maintenance monitor configuration” (page 249)
- “Passport configuration concepts” (page 257)

What’s new in this document

The following features were added to this document:

- “PVG: VrAp Carrier Grade” (page 21)
- “Voice services processor 3 with optical TDM interface (2pOC3ChSmIrVsp3)” (page 22)
- “Y-Protection for FPs in a Passport 15000 or 20000” (page 22)

Other changes made to this document include the following:

- the section “Understanding CP equipment sparing” (page 258) was updated with information about performing a CP switchover.
- the section “Changing the CP equipment protection mode” (page 125) was added.
- corrected holdOffTimer(hoTime) in the figure “APS components and attributes” (page 280) to be holdOffTime(hoTime)

PVG: VrAp Carrier Grade

The following section was updated for this feature.

- “Changing the CP equipment protection mode” (page 125)

Voice services processor 3 with optical TDM interface (2pOC3ChSmIrVsp3)

The following sections were added or updated for this feature.

- “Hot standby applications and features” (page 240)

Y-Protection for FPs in a Passport 15000 or 20000

The following sections were added or updated for this feature:

- the Prerequisites and SFP type in “Configuring a port to use an SFP optical module” (page 80)
- the Prerequisites of “Configuring line and equipment protection for Passport 15000 or 20000 optical interfaces” (page 221) regarding the configuration of the use of line automatic protection switching (line APS or LAPS) in general and with a third-party interface that does not support using LAPS
- the Prerequisites of “Configuring line protection for optical interfaces on Passport 15000 or Passport 20000” (page 225) regarding the use of Y-protection with line protection
- “Configuring Y-protection for dual FPs in a Passport 15000 or 20000” (page 231) to indicate what commands to enter to enable it
- “Processor card sparing” (page 326) to acknowledge a new form of Passport 15000 or 20000 equipment protection
- the figure “LAPS components and attributes” (page 275) to add attributes for Y-protection
- “Understanding Y-protection for dual FPs” (page 348) to explain what it is and does

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.

Procedure conventions

This document uses the following procedure conventions:

- You can enter commands using full component and attribute names, or you can abbreviate them. The commands used in the procedures contain the full component and attribute names in the first instance. In the second instance, the component and attribute names are abbreviated. For more information on abbreviating component and attribute names, see 241-5701-060 *Passport 7400, 15000, 20000 Components*. All component and attribute names are formatted in italics.
- The introduction of every procedure states whether you must perform the procedure in operational mode or provisioning mode. For more information on these modes, see “Operational mode” (page 24) or “Provisioning mode” (page 24).
- When you complete a procedure, you can verify your changes and then activate them as the new node configuration. For more information on completing configuration changes and exiting provisioning mode, see “Activating configuration changes” (page 25).

Operational mode

Procedures contained within this document can either be performed in operational mode or provisioning mode. When you initially log into a Passport node, you are in operational mode. Passport uses the following command prompt when you are in operational mode:

```
#>
```

where:
is the current command number.

In operational mode, you work with operational components and attributes. In operational mode, you can do the following:

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

Provisioning mode

To change from operational mode to provisioning mode, type the following command at the operator prompt:

```
start Prov
```

Only one user can be in provisioning mode at a time. Passport uses the following command prompt whenever you are in provisioning mode:

```
PROV #>
```

where:
is the current command number.

In provisioning mode, you work with the provisionable components and attributes that contain the current and future configurations of the node. You can add and delete components, and display and set provisionable attributes. For information on completing the configuration changes, exiting provisioning mode, and returning to operational mode, see “Activating configuration changes” (page 25).

For information on operational and provisionable attributes, see 241-5701-060 *Passport 7400, 15000, 20000 Components*.

Activating configuration changes

Several procedures in this document ask that you complete the configuration changes. When you complete the configuration changes, you are activating the configuration changes, confirming that you want to activate them, and saving the changes. You are instructed to complete the configuration changes only at the end of procedures that you perform in provisioning mode.

CAUTION

Activating a provisioning view can affect service

Activating a provisioning view can result in a control processor reload or restart, causing all services on the Passport node to fail. See 241-5701-050 *Passport 7400, 15000, 20000 Commands* for more information.

Use the following procedure to activate configuration changes:

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

   ```
   check Prov
   ```

   Correct any errors and verify the provisioning changes again.

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

   ```
   save Prov
   ```

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

   ```
   activate Prov
   ```

   ```
   confirm Prov
   ```

   ```
   commit Prov
   ```

4. End the provisioning session:

   ```
   end Prov
   ```

Related documents

See the following documents for related information:

- 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*
- 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade*. This document provides detailed instructions about installing and maintaining Passport 15000 and 20000 hardware.
- 241-5701-050 *Passport 7400, 15000, 20000 Commands*. This document describes the commands you use to operate and maintain Passport.
- 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*. This document describes each Passport function processor.
- 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*. This document provides conceptual and procedural information about troubleshooting the Passport system.

How to get more help

For information on training, problem reporting, and technical support, see the "Nortel Networks support services" section in the product overview document.

Chapter 1
Basic node setup

After the StartUp utility has been run, set up the Passport node so that it can support the specific services and features of your network.

Navigation links

- "Prerequisites to basic node setup" (page 27)
- "Basic node setup flow" (page 27)
- "Task navigation" (page 28)

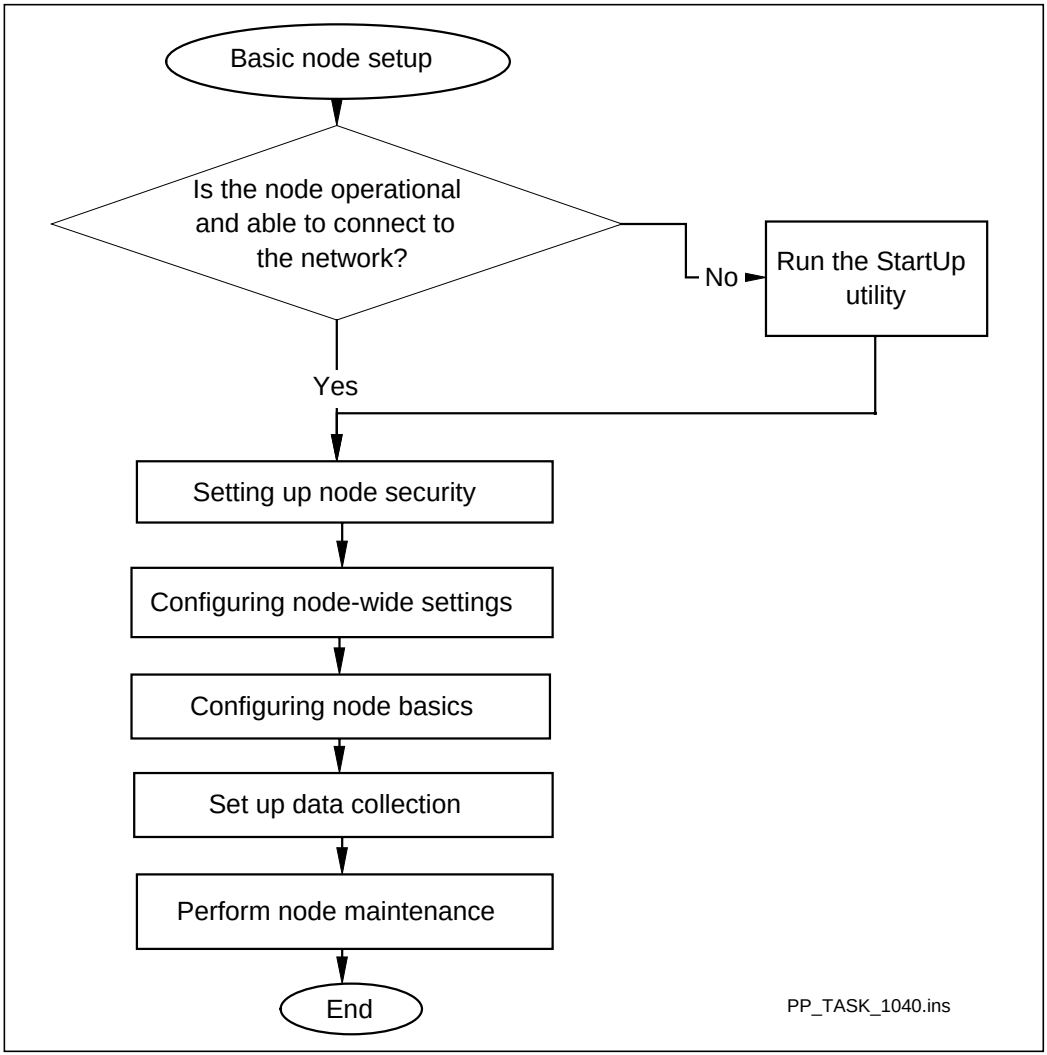
Prerequisites to basic node setup

- The node is operational and able to connect to the network as described in 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.
- If you are unfamiliar with the basic components of the Passport node, see "Passport system overview" (page 258).

Basic node setup flow

This task flow shows you the sequence of procedures you perform to set up your node. To link to any procedure, go to "Task navigation" (page 28).

Figure 1
Basic node setup task flow



Task navigation

- Run the StartUp utility. See 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.
- “Setting up node security” (page 30)

- “Configuring node identification” (page 31)
- “Configuring general service parameters” (page 34)
- “Configuring node basics” (page 35)
- Set up data collection. See 241-5701-611 *Passport 7400, 15000, 20000 Data Collection Guide*.
- “Performing node maintenance” (page 36)

Setting up node security

Configure the node security to ensure that all users have proper switch access and to prevent unauthorized control of the node.

For more information on Passport security, see NN10600-605 *Passport - MDM Network Security: Operations*.

CAUTION

Configure user IDs immediately

The first configuring task must be to configure at least one user ID with system administration impact. If you do not configure a user ID, your Passport node has no security. Anyone can access the node without a user ID and password.

Configuring node identification

Configure node identification using the *nodeName*, *nodeId*, and *regionId* attributes of the *ModuleData* component. Every Passport node must be identified on the network.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).
- The *nodeId*, *nodeName*, and *namsId* can be set using the Passport StartUp software. Before performing this procedure, verify that the node node has not already been identified. For more information, see 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.

Procedure steps

CAUTION
Node restart
Changing the node identifier, node name, or region identifier results in a node restart.

1. Set the Passport node identifier:

   ```
   set Mod nodeid <nodeid>
   ```

2. Set the Passport node name:

   ```
   set Mod nodeName <name>
   ```

3. Set the Passport region identifier:

   ```
   set Mod regionId <regionId>
   ```

4. Set the Passport network administration (nams) identifier:

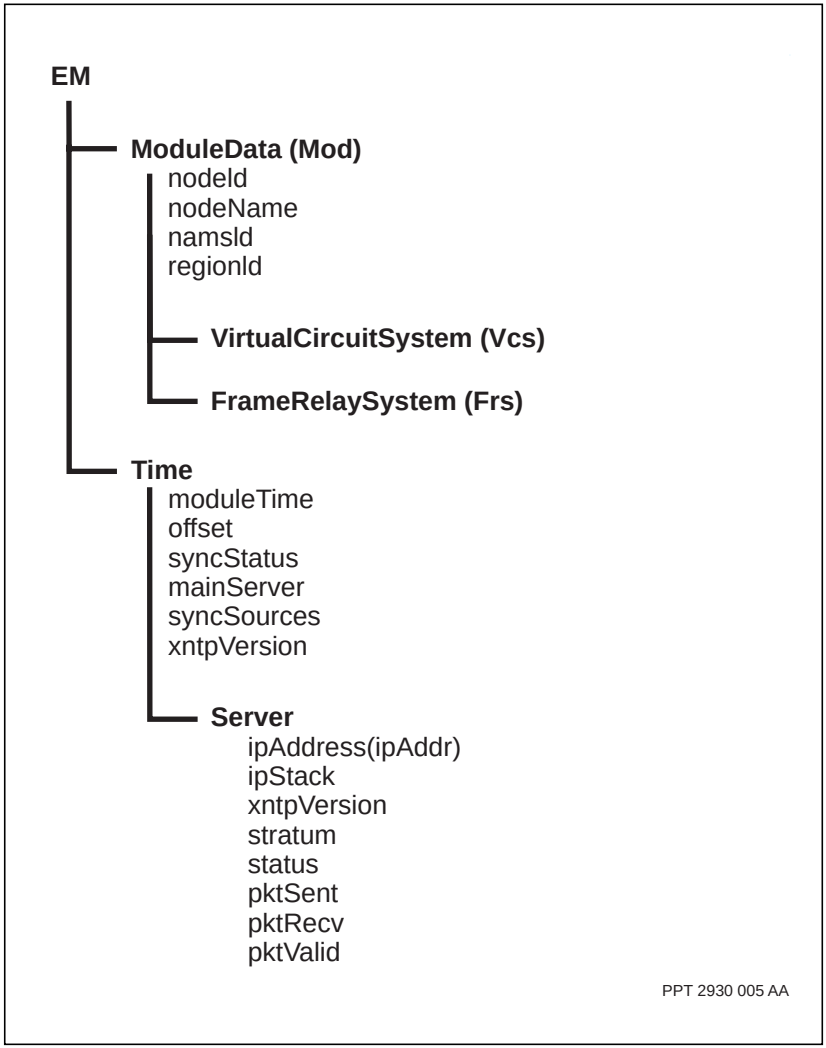
   ```
   set Mod namsId <namsId>
   ```

Variable definitions

Variable	Value
<name>	A 12-character ASCII string that is unique to every Passport node in a network. The default is *noname*. Only the following set of characters is permitted in the node name: • uppercase and lowercase alphanumeric characters • period (.) • underscore (_) For example, LA_12 is valid and LA$%12 is invalid. The *nodeName* attribute is a unique name given to each Passport node in order to distinguish the node from other nodes within the network. The *nodeName* attribute is used by the Nortel Networks' Preside Multiservice Data Manager.
<nodeid>	Any number between 1 and 4095. The node identifier must be unique for each Passport node. The *nodeId* attribute is a number that uniquely identifies the node component instance in the Passport network. Passport uses the node identifier for routing control and in some data packets sent to other Passport nodes in the network. Routing protocol packets indicate the node identifiers for all other nodes in the network.
<regionId>	Any number between 0 and 126. The *regionId* attribute identifies the nodes that belong to a topology region within a network. Neighbor nodes exchange region identifier values to determine whether or not they belong to the same topology region.
<namsId>	Any number between 256 and 49151. It must be unique across the entire network of Passport nodes supporting the transport of DPN traffic as well as all DPN resource modules (RMs) and access modules (AMs) in the network. The *namsId* attribute holds the network administration (Nams) identifier, which identifies nodes that support DPN traffic.

Procedure job aid

Figure 2
Node identification component hierarchy



Configuring general service parameters

Configure general service parameters using two components, *VirtualCircuitSystem* and *FrameRelaySystem*, to define the general characteristics of virtual circuits and the frame relay service. The figure "Node identification component hierarchy" (page 33) illustrates these components.

The Passport StartUp utility sets the attributes existing under these components with default values. You have the option to customize the attributes to suit the requirements of the network. Many of the attributes must have the same values across a Passport subnet so that the Passport nodes can communicate with each other. If you do decide to change values, do so with extreme caution. Call Nortel Networks for assistance if necessary.

CAUTION

Risk of data loss

Changing the node-wide attributes of the *VirtualCircuitSystem* and *FrameRelaySystem* components can cause the node to become isolated from other nodes in the network. This node isolation can cause data loss.

Configuring node basics

Configure node basics to specify the processor cards and their ports, the Passport trunks that connect the node to other nodes, and a network management interface.

Procedure steps

1. Configure the cards and ports. See “Common processor card procedures” (page 75).
2. Configure the Passport trunks. See 241-5701-420 *Passport 7400, 15000, 20000 Trunking Guide* for details.
3. Configure the IP interface over virtual circuit (IPIVC) or the IP interface over frame relay (IPIFR) for network management connections.

   See 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity* for details.

Performing node maintenance

Perform node maintenance regularly to maintain the performance of your Passport node. The following tables indicate when to perform the activities:

- "Regularly scheduled node activities" (page 36)
- "Regularly scheduled hardware activities" (page 37)

Table 1
Regularly scheduled node activities

Frequency of activity	Activity	Where to find procedure
Daily	Time-of-day accounting	241-5701-650 *Passport 7400, 15000, 20000 Accounting Fundamentals*
	Sending Passport accounting data to a billing host	241-5701-650 *Passport 7400, 15000, 20000 Accounting Fundamentals*
Weekly	Checking synchronization	"Synchronizing disks" (page 198)
	Checking spooling	241-5701-611 *Passport 7400, 15000, 20000 Data Collection Guide*
	Backing up service data	241-6001-023 *Preside MDM Configuration Management for Passport User Guide*
Monthly	Cleaning up software files	241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*

(Sheet 1 of 2)

Table 1 (continued)
Regularly scheduled node activities

Frequency of activity	Activity	Where to find procedure
	Cleaning up configuration files	The *tidy Prov* command in 241-5701-050 *Passport 7400, 15000, 20000 Commands*
	If you have automatic bus clock source testing disabled, perform a manual bus clock source test. ***Note:*** This activity applies to Passport 7400 only.	241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*
(Sheet 2 of 2)		

Table 2
Regularly scheduled hardware activities

Frequency of activity	Activity	Where to find procedure
Daily	No daily activities needed	
Weekly	No weekly activities needed	
Monthly	Changing the air filter	241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* or 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*
	Fabric card test ***Note:*** This activity applies to Passport 15000 and 20000 only.	"Displaying the configuration or capacity of a fabric card" (page 190)
(Sheet 1 of 2)		

Table 2 (continued)
Regularly scheduled hardware activities

Frequency of activity	Activity	Where to find procedure
	Bus test ***Note:*** This activity applies to Passport 7400 only.	"Passport 7400 bus maintenance tasks" (page 191)
	Card test	241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*
	Port test	241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*
	Disk test	241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*
(Sheet 2 of 2)		

Chapter 2
Network and node time configuration

Configure network and node time to add the network time servers, set network time, and configure a time zone offset.

Navigation links

- "Prerequisites to network and node time configuration" (page 39)
- "Network and node time configuration flow" (page 39)
- "Task navigation" (page 40)

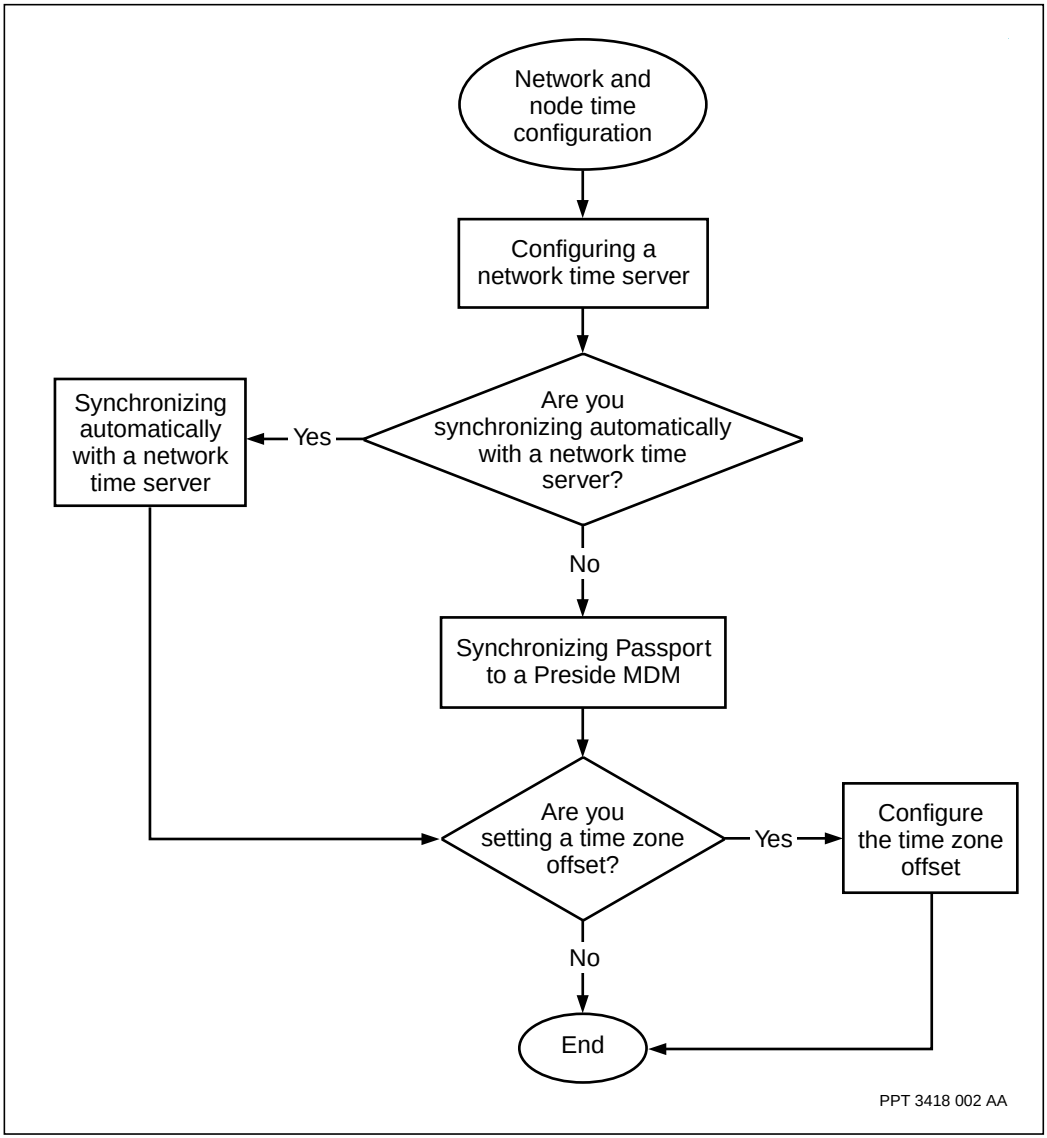
Prerequisites to network and node time configuration

- See "Understanding network time and date configuration" (page 312) for additional information about this task.
- You must have a network time protocol (NTP) server configured on a Preside MDM or third party network management device (MD). See 241-6001-303 *Preside MDM Administrator Guide* for additional information.

Network and node time configuration flow

This task flow shows you the sequence of procedures you perform to network and node time configuration. To link to any procedure, go to "Task navigation" (page 40).

Figure 3
Network and node time configuration task flow



Task navigation

- “Configuring a network time server” (page 42)

Configuring a network time server

Configure a network time server to add a time server to the Passport. You can add up to 10 servers on a Passport node.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Add a *Server* component for each network time server:

```
add Time Server/<n>
```

2 Check, activate and confirm the provisioning changes:

```
check prov
activate prov
confirm prov
```

Variable definitions

Variable	Value
<n>	The instance of the *Server* component. You can configure up to 10 *Server* components (1–10) on a Passport node.

Synchronizing automatically with a network time server

Synchronize automatically with a network time server to synchronize your Passport node with up to 10 MDs that are acting as network time servers.

Prerequisites

- See RFC 1305, *Network Time Protocol (Version 3)* for more information on public NTP.
- See “Additional information for synchronizing automatically with a network time server” (page 43) for more information about this procedure.

Procedure steps

1. Specify the IP address of the network time server:

   ```
   set Time Server/<n> ipAddress <address>
   ```

2. Select the IP routing stack for time server connectivity:

   ```
   set Time Server/<n> ipStack <type>
   ```

Variable definitions

Variable	Value
<address>	The IP address of the MD that you want to set as a time server to your node.
<type>	Either ipiFrIpiVc (for frame relay/X.25 connectivity to a time server MD) or VrIp (for IP virtual router connectivity to a time server MD).The time servers must connect to the Passport via the same connection type (for example, all using vrIP or all using ipiFrIpiVc). Mixed connections are not supported.

Additional information for synchronizing automatically with a network time server

An MD can be any workstation running either:

- Preside Multiservice Data Manager with public network time protocol (NTP)
- some other management system running public NTP.

In case a network time server is not specified, Passport automatically attempts to synchronize with a Preside MDM workstation it can reach using its IP interface over frame relay (IPIFR) or its IP interface over virtual circuit (IPIVC). If time servers are deleted when Passport is up and running, Passport does not synchronize with a Preside MDM workstation. For example, automatic synchronization works at startup if no time servers are specified.

The node gets the network time from the network management interface system (NMIS) notification of a new fast management information protocol (FMIP) session. In this case, the system decides which and how many MDs the Passport node synchronizes with. Preside Multiservice Data Manager connectivity, IPIFR, and IPIVC are explained in detail in 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.

> ***Note:*** As soon as you configure a *Server* component, the Passport software disables the automatic synchronization capability.

Synchronizing manually to a network time server

Synchronize manually to a network time server to manually synchronize your Passport node with any MD that is running public NTP software. Passport may be synchronized with up to 10 MDs. These MDs can be any workstation running either Preside MDM with NTP or some other management system running public NTP. All MDs must synchronize with a common reference time.

Prerequisites

CAUTION

Risk of confusion in the interpretation of accounting records and alarm time stamps

Nortel Networks recommends that you synchronize all nodes in a network from a reliable time reference.

When set manually, the node time is not initially precisely the same on all network nodes and also eventually drifts out of synchronization due to the different precision of the local clocks on each node.

This eventually results in alarms and accounting records not reporting an accurate time stamp.

- If there is a difference of more than 1000 seconds between the network time server MD and your Passport node, synchronization does not occur.
- Preside MDM must be synchronized to a time source before a Passport is synchronized. See 241-6001-303 *Preside MDM Administrator Guide*.
- If the node is powered off for more than 24 hours, perform the following procedure in provisioning mode. For information on working in provisioning mode, see “Provisioning mode” (page 24).
- See “Additional information for synchronizing manually with a network time server” (page 46) for more information about this procedure.

Procedure steps

1. Stop the time synchronization on Passport. Lock all the provisioned time server components for each provisioned server:

   ```
   lock Time Server/<n>
   ```

2 Ensure that the Passport module time changes to unsynchronized:

```
d Time syncStatus
```

3 On Passport, make sure that the time offset is set to 0. Configure the node time so that it is set on UTC and as close as possible to Preside MDM UTC time: (less than 1000 seconds of UTC):

```
display time moduletime

set time offset 0

set time moduleTime <yyyy-mm-dd> <hh:mm:ss>
```

4 On Passport, restart synchronization by unlocking the time server components:

```
unlock Time Server/<n>
```

5 Monitor the progress by checking the syncStatus attribute:

```
d Time syncStatus
```

Variable definitions

Variable	Value
<hh>:<mm>:<ss>	The hour, minute, and second.
<n>	The instance value of the time server.
<yyyy>-<mm>-<dd>	The year, month, and day.

Additional information for synchronizing manually with a network time server

The MD for manual synchronization can be any workstation running management software that includes NTP (such as Preside MDM or third party). Passport XNTP software allows you to choose exactly which and how many (up to 10) MDs with which to synchronize your node. This flexibility means that you can choose MDs in both the WAN and LAN.

Connectivity to MDs running public NTP can be using IPIFR/IPIVC, or IP, over link layer protocols such as frame relay, X.25, asynchronous transfer mode (ATM), Ethernet, and point-to-point protocol (PPP).

Configuring the time zone offset

Configure the time zone offset to set the manually offset the time from UTC.

Prerequisites

CAUTION
Risk of confusion in the interpretation of accounting records and alarm time stamps
Nortel Networks recommends that you set the time zone offset to the same value for every node in the same network.

If nodes in the same network have different time zone offsets and two alarms on different nodes are generated at the exact same time, they have different time stamps. This can result in difficulties when correlating time between the two Passport nodes.

- See “Additional information for configuring the time zone offset” (page 47) for more information about this procedure.

Procedure steps

1. Set the *offset* attribute of the *Time* component to the number of minutes that the node local time is before or after the network time. The Passport must be synchronized before setting the time offset.

   ```
   set Time offset <offset value>
   ```

Variable definitions

Variable	Value
<offset value>	is the value of the *offset* attribute.

Additional information for configuring the time zone offset

When your node synchronizes with an MD acting as a network time server, Passport XNTP sets the node time to the network time (reference time), which is UTC. This happens whether synchronization is done automatically or

manually. You can account for different time zones by setting the difference from UTC using the *offset* attribute. The *offset* attribute is a writable operational attribute under the *Time* component.

The time zone offset value ranges from –720 to 900 minutes, which represents a range from –12 hours to +15 hours. A time offset between 0 and 900 minutes (+15 hours) represents a time ahead of UTC (or east of the prime meridian). A time offset value between 0 and –720 minutes (–12 hours) represents a time behind UTC (or west of the prime meridian).

Verifying the time configuration on the node

Verify the time configuration on the node to ensure that you have correctly configured module and network time on your node.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1. Display the operational attributes of the *Time* component:

   ```
   display Time
   ```

   A number of attributes display, including the current module time, timezone offsets, synchronization status, and time server sources.

2. Display the provisionable attributes of the configured time servers:

   ```
   display -p Time Server/*
   ```

3. Display the operational attributes of the configured time servers:

   ```
   display Time Server/*
   ```

4. Display the operational attributes of a particular time server:

   ```
   display Time Server/<n>
   ```

5. Display the current time on the node:

   ```
   display Time moduleTime
   ```

   The current time on the node displays in the form yyyy-mm-dd hh:mm:ss.

Variable definitions

Variable	Value
<n>	The instance value of the *Server* component.

Chapter 3
Network clock synchronization configuration

Configure network clock synchronization (NCS) to provide the clock rates for connected ports so that they operate in synchronization. This prevents data loss or data retransmission for synchronous services.

Navigation links

- "Prerequisites to network clock synchronization configuration" (page 51)
- "Network clock synchronization configuration flow" (page 51)
- "Task navigation" (page 53)

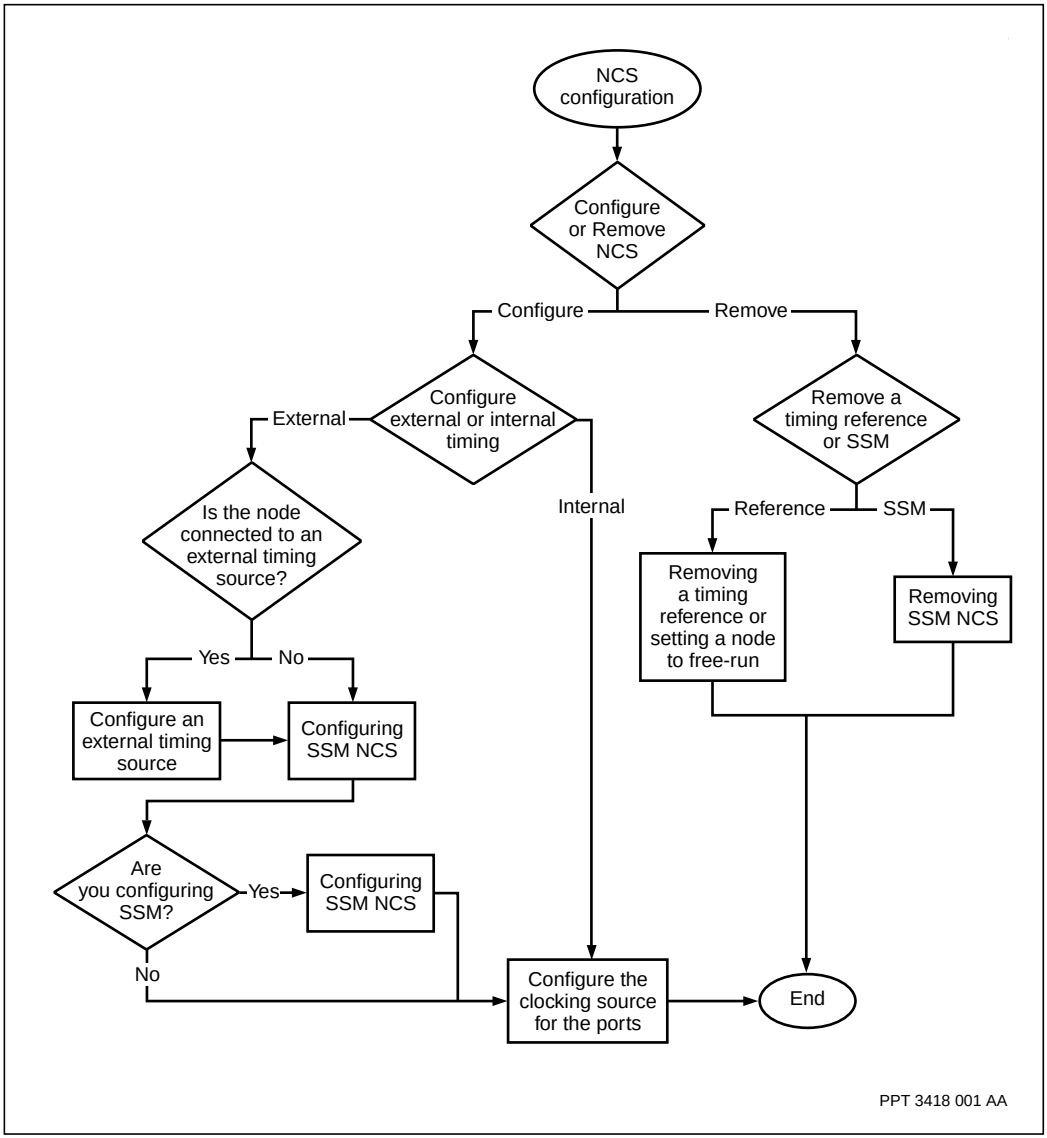
Prerequisites to network clock synchronization configuration

- See "Understanding NCS" (page 290) for additional information.

Network clock synchronization configuration flow

This task flow shows you the sequence of procedures you perform to configure network clock synchronization. To link to any procedure go to "Task navigation" (page 53).

Figure 4
Network clock synchronization configuration task flow



Task navigation

The following references are listed alphabetically:

- “Configuring an external timing source” (page 54)
- “Configuring NS” (page 56)
- “Configuring SSM NCS” (page 60)
- “Configuring the clocking source for the ports” (page 58)
- “Removing a NCS reference or setting a node to free-run” (page 63)
- “Removing SSM NCS” (page 64)

Configuring an external timing source

Configure an external timing source to enable a node to use an external clocking sources as a timing reference. Perform this procedure on nodes connected directly to an external timing source, for example, a stratum-1 clock.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).
- For information about the Passport 7400 BITS termination panel see the 241-7401-200 *Passport 7400 Hardware Description* or for information about the Passport 15000 and 20000 Alarm/BITS module in the 241-1501-200 *Passport 15000, 20000 Hardware Description*.

Procedure steps

1 Determine what kind of signal is expected:

```
display Shelf Card/0 cardType
```

For Passport 15000 and 20000 if the control processor is of type *CPeD*, the signal is from a DS1 line. If the control processor is of type *CPeE*, the signal is from an E1 line.

For Passport 7400 if the control processor is of type CP, the external timing port can be provisioned to be either E1 or DS1.

2 Add the external timing feature to the feature list (FL) of the CP:

```
set Sw Lpt/cp featureList externalTiming
```

3 Verify the configuration changes, activate the edit view, and confirm that the activation was successful:

```
check Prov
activate Prov
confirm Prov
```

4 Define one or both external timing ports to receive the signal.

If the signal is from a DS1 line, enter:

```
add lp/<x> EDS1/0
```

```
add lp/<x> EDS1/1
```

If the signal is from an E1 line, enter:

```
add lp/<x> EE1/0
```

```
add lp/<x> EE1/1
```

5 If the signal is from a DS1 line, set the configurable attributes:

```
set lp/<x> EDS1/<y> lineType/<linetype>
```

6 To enable 2MHz analog BITS termination on an EE1 port, change the default setting of RxSynchClk:

```
set lp/<x> EE1/<y> RxSynchClk squareWave
```

Variable definitions

Variable	Value
<linetype>	*d4* or *esf*
<x>	The instance of the Lp.

Configuring NS

Configure NS to add network synchronization and set clocking references.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).
- If there are no references where the node can receive a timing signal, do not configure any references. This forces the node clocking to run in free-run mode.
- The individual ports of an optical interface card configured for automatic protection switching (APS) can each serve independently as a reference source. However, the pair of them as defined by the *Aps* component instance cannot be used as a single reference source.

Procedure steps

1 Create the network synchronization component:

```
add networkSynchronization
```

2 Define up to three sources of the timing signal:

```
set networkSynchronization <reference_type> <path>
```

3 Define the criteria that a timing reference must meet for the signal to be a usable timing reference:

```
set networkSynchronization useableReferences
<useRef_value>
```

4 Set the amount of time the *NetworkSynchronization* component waits before using a port as a timing reference after it has been cleared of its degraded or disabled status:

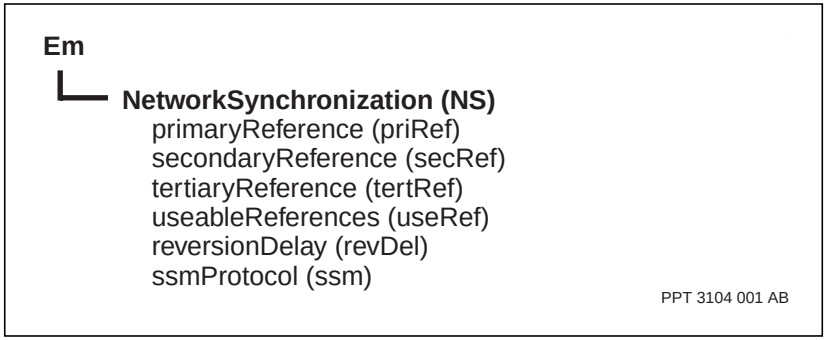
```
set networkSynchronization reversionDelay
<revDel_value>
```

Variable definitions

Variable	Value
<path>	The logical port to be used as a timing reference.
<reference_type>	The type of network synchronization reference. Up to three sources can be defined using the components *primaryReference*, *secondaryReference*, and *tertiaryReference*.
<revDel_value>	The value of the *reversionDelay* attribute. Can have the value manual or the number of minutes, between 0 and 120, can be set. The default is 0 minutes.
<useRef_value>	The value of the *useableReferences* attribute. Can have the value enabled, default value, or notDegraded.

Procedure job aid

Figure 5
NS component hierarchy



Configuring the clocking source for the ports

Configure the clocking source for the ports so that the necessary clocking source is used to synchronize the transmission of data.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).
- If you are using an external timing source, Nortel Networks recommends that the *clockingSource* for all ports be set to module.
- If you are using a V.11 or V.35 FP, see “Clocking for V.11 and V.35 FPs” (page 307) for additional information.
- See 241-5701-060 *Passport 7400, 15000, 20000 Components* for LP port types and *clockingSource* values.

Procedure steps

1. Set all ports of the LP to synchronize with the necessary timing source:

   ```
   set Lp/<x> <port_type>/<y> clockingSource
   <clockingSource_type>
   ```

2. Repeat step 1 for all ports on the LP.
3. For ports on a V.11 or V.35 FP set the *linkMode* attribute.

   ```
   set lp/<x> x21/<y> linkMode <linkMode_value>
   ```

   ```
   set lp/<x> V35/<y> linkMode <linkMode_value>
   ```

Variable definitions

Variable	Value
<clockingSource_type>	The value for the type of clocking source used for synchronizing the transmit clock.
<linkMode_value>	The value of the x21 or V35 port *linkMode.* It can be set to either dte or dce.
<port_type>	The type of port.

(Sheet 1 of 2)

Variable	Value
<x>	The instance of the Lp.
<y>	The instance of the port.
(Sheet 2 of 2)	

Configuring SSM NCS

Configuring synchronization status messages (SSM) network clock synchronization to allow the NCS system to choose the best clock signal based on the quality level of the SSM, making it available to all ports on the node that have module timing.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Set the *ssmProtocol* value to enabledMigration. This is an intermediate step to allow the S1 Bytes associated with the active timing references to be propagated to adjacent nodes in the network without invoking any SSM clock source selection functionality. This is a recommended step when migrating your NCS network to use SSM.

```
set networkSynchronization ssmProtocol
enabledMigration
```

2 Activate and confirm the provisioning changes.

```
activate prov
confirm prov
```

3 Prior to enabling SSM, display the current S1 Bytes being received and transmitted on the provisioned timing references to determine what SSM clock source selections will occur when SSM is enabled. If one or more standby timing references in the network will be selected when SSM is enabled, it is important to understand what other clock source selection changes may occur as a result. This step will help predict these changes. For example, on a SONET, the command syntax would be:

```
display -o lp/<x> sonet/<y> s1Rx
```

```
display -o lp/<x> sonet/<y> s1Tx
```

4 Optionally, set the *s1RxDefault* attribute. This attribute specifies the default S1 Bytes reported by the port when the received S1 Byte is 0 (quality unknown). The default value is applied until a non-zero S1 byte is reported.

```
set lp/<x> sonet/<y> s1RxDefault <default>
```

Note: This attribute needs to be configured only if the equipment at the remote end of the port does not support SSM transmission

5 Activate SSM functionality (setting the value of the ssmProtocol attribute to either enabledRevertive or enabledNonRevertive enables SSM functionality on the node).

```
set networkSynchronization ssmProtocol <value>
```

6 For E1 ports, set the *ssmE1SaNumber* attribute to specify the San used by the network for SSM signalling.

```
set lp/<x> e1/<e1_value> ssmE1SaNumber <san_value>
```

7 Optionally, if using E1BITS timing on a node, you can set the quality level normally assigned with the BITS timing reference as follows:

```
set lp/<x> ee1/<ee1_value> ssmRxDefault
<quality_value>
```

8 Optionally, if using DS1BITS timing on a node, you can set the quality level normally assigned with the BITS timing reference as follows:

```
set lp/<x> eds1/<eds1_value> ssmRxDefault
<quality_value>
```

Variable definitions

Variable	Value
<default>	The provisioned value of the s1RxDefault attribute. It can be set to any value from 0 to 15, or it can be set to none.
<e1_value>	The instance value of the e1 component.
<eds1_value>	The instance value of the eds1 component.
<ee1_value>	The instance value of the ee1 component.
<quality_value>	The provisioned value of the ssmRxDefault attribute. For a summary of acceptable quality level values, refer to “SONET/SDH quality level (QL) mapping table” (page 306).
<san_value>	The provisioned value of the ssmE1SaNumber attribute. The default value of none disables SSM signalling on the specified E1 port.

(Sheet 1 of 2)

Variable	Value
<value>	The provisioned value of the ssmProtocol attribute. It can be set to one of four possible values: disabled, enabledRevertive, enabledNonRevertive, enabledMigration.
<x>	The instance of the Lp.
<y>	The instance of the Sonet port.

(Sheet 2 of 2)

Removing a NCS reference or setting a node to free-run

Remove a NCS reference to remove a previously configured reference. When the attribute parameter is omitted, the reference is set to nil (no reference).

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1. Set the particular attribute without identifying a new reference.

   ```
   set NetworkSync <reference_type>
   ```

2. Repeat for all references that you would like to remove.

Variable definitions

Variable	Value
<reference_type>	One of the primaryReference, secondaryReference, or tertiaryReference attribute.

Removing SSM NCS

Remove SSM NCS to disable the SSM functionality on the port or node.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 To disable SSM functionality on a particular port, set the port Tx and Rx override attributes to 0.

```
set lp/<x> sonet/<y> s1RxOverride 0
```

```
set lp/<x> sonet/<y> s1TxOverride 0
```

2 To disable SSM functionality on an entire node, set the *ssmProtocol* attribute to disabled.

```
set networkSynchronization ssmProtocol disabled
```

Variable definitions

Variable	Value
<x>	The instance value of the LP.
<y>	The instance of the port.

Chapter 4
Software, applications, and features additions and updates

Add and configure applications or update the application version or patch list to allow the Passport node to support the services required by your network.

Navigation links

Prerequisites to software, applications, and features additions and updates

- If you are unfamiliar with Passport software concepts, see "Understanding Passport software" (page 327).

Software, applications and features additions and updates tasks

Adding and configuring applications

Add and configure the applications required by your network on the Passport node.

Note: You can add certain applications only after the associated feature has been included in the feature list of a logical processor type (LPT). See "Configuring the software features of an LPT" (page 179).

Prerequisites

- Before you can add and configure applications, you must have previously installed the Passport software by running StartUp. As part of the software installation, StartUp will add default applications and the software installer will download the release software to the node. You can then add and configure applications. For instructions on running StartUp, see 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.
- Perform the following procedure in provisioning mode. For more information, see "Provisioning mode" (page 24).

Procedure steps

1. Determine what applications have already been added to the node:

   ```
   list
   ```

2. Add a new application:

   ```
   add <application>
   ```

3. Refer to the specific service guides for additional information about configuring applications.
4. Verify that you added the application correctly:

   ```
   list
   ```

5. Complete the configuration changes. See "Activating configuration changes" (page 25).

Variable definitions

Variable	Value
<application>	The application that you want to add.

Removing and replacing specific applications and patches

Indicate which specific applications and patches that you want to remove from the application version list (AVL) or patch list. You can then specify recently downloaded applications and patches that you want added to the AVL or patch list.

Prerequisites

- Keep a copy of the committed provisioning file that was running before you updated the AVL until you confirm that the new software functions properly. To revert to the old version of the software, you need this file. See 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*.
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Display the current AVL:

```
display Software AvList
```

2 Display the current patch list:

```
display Software PatchList
```

3 Delete the unwanted software applications in the AVL:

```
set Software AvList ~<avName>
```

To list multiple applications, precede each application with a tilde (~) and separate each of them with a space.

4 Add the new software applications to the AVL:

```
set Software AvList <avName>
```

To list multiple applications, separate each of them with a space.

5 Remove unwanted patches from the patch list:

```
set Software PatchList ~<patch>
```

6 Check the configuration changes and activate the new AVL. See “Activating the AVL configuration changes” (page 72).

7 Verify the changes to the AVL:

```
display Software AvList
```

8 Verify the changes to the patch list:

```
display Software PatchList
```

Variable definitions

Variable	Value
<avName>	The application version that you want to delete.
<patch>	The name of the unwanted patch. To remove multiple patches, precede each patch name with a tilde (~) and separate each of them with a space.

Removing and replacing all applications and patches

If required, remove and replace all applications and patches.

To replace all the application versions and patches with new versions in a single command, use an exclamation mark. The exclamation mark tells the system to delete all the applications or patches in the AVL or patch list.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Display the current AVL:

```
display Software AvList
```

2 Display the current patch list:

```
display Software PatchList
```

3 Remove all the applications in the AVL and replace them with new applications:

```
set Software AvList ! <avName>
```

To list multiple application versions, separate each of them with a space.

4 Remove all the patches in the patch list and replace them with new patches:

```
set Software PatchList ! <patch>
```

To list multiple patches, separate each of them with a space.

5 Check the configuration changes and activate the new AVL. See the procedure “Activating the AVL configuration changes” (page 72).

6 Verify the changes to the AVL:

```
display Software AvList
```

7 Verify the changes to the patch list:

```
display Software PatchList
```

Variable definitions

Variable	Value
<avName>	The application version that you want to add.
<patch>	The patch that you want to add.

Activating the AVL configuration changes

Once you have updated the feature list, activate the AVL configuration changes.

Note: If you are only applying a patch to an application version, you do not have to modify the AVL, only the patch list. For more information, see “Changing the patch list” (page 74).

Prerequisites

- When you update the AVL to perform a software upgrade, you have to verify the configuration twice using the *check Prov* command. First, you must verify the configuration before you can activate it using the old software version, then after activation using the new software version. You need a second *check Prov* to ensure that the node configuration is based on the software and component model that you want to run as configuration might have changed since the first *check Prov* was done, or a view migration might have introduced new components. See 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide* for more information.
- When you update the AVL you also must ensure that the patch list is still valid. In general, a new application version incorporates the changes in the preceding patches, making them obsolete. For more information on specific application versions and patches, see the *Passport Release Report.*
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1. Perform a semantic check on the configuration changes to the AVL in the edit view:

   ```
   check Prov
   ```

   A message is displayed indicating whether or not processor reboots will occur when the new provisioning data is activated.

2. Activate the changes to the AVL:

   ```
   activate Prov
   ```

Note: If the standby CP resets during the software activation, continue the standard software activation sequence on the active CP. Allow both CPs to load the new software and perform the remaining steps on the active CP.

3 Enter provisioning mode again:

```
start Prov
```

4 Confirm that the new configuration is still valid following the reboot:

```
confirm Prov
```

5 Recheck the edit view and verify that the new configuration is valid now that the new application versions are running:

```
check Prov
```

6 After running tests on the new software to ensure that it works properly, commit and save the current view:

```
commit -file(<name>) prov
```

7 Verify that the committed view is now running:

```
display ProvisioningSystem committedFileName
```

```
display ProvisioningSystem currentViewFileName
```

Ensure that the committed file name and the current view file name are the same.

Variable definitions

Variable	Value
<name>	The name you want to give the committed view.

Changing the patch list

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.

Prerequisites

- You cannot put a patch on the patch list unless its associated application version is on the AVL. See “Application versions” (page 331). Some patches can require other patches to also be on the patch list. Certain combinations of patches do not work together. For more information on patches, see “Patches” (page 331). See the *Passport Release Report* for the restrictions on particular patches.
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1. Display the current patch list:

   ```
   display Software PatchList
   ```

2. Specify the patches that you want to enable:

   ```
   set Software PatchList <list>
   ```

3. Display the new patch list to verify that you have properly defined it:

   ```
   display Software PatchList
   ```

4. Complete the configuration changes. See “Activating configuration changes” (page 25).

Variable definitions

Variable	Value
<list>	A list of patches. The patch names in the list must be separated by a space. To remove a particular patch from the patch list, precede it with a tilde (~) character. To replace all of the patches on the list with new patches, begin the list with an exclamation mark (!) followed by a space.

Chapter 5
Common processor card procedures

Use these common processor card procedures to perform maintenance or troubleshooting activities.

Navigation links

- “Prerequisites to common processor card procedures” (page 75)
- “Common processor card tasks” (page 75)

Prerequisites to common processor card procedures

For conceptual information supporting the procedures listed in this section, see “Understanding Passport control and function processors” (page 315).

Common processor card tasks

Use the alphabetical list below to locate the processor card procedure you want to do:

- “Comparing the card type of an inserted card and its configured slot” (page 77)
- “Configuring a new processor card” (page 78)
- “Configuring a port to use an SFP optical module” (page 80)
- “Decommissioning an FP” (page 82)
- “Displaying information about daughter cards on a Passport 7400 processor card” (page 83)
- “Displaying the memory capacity of a processor card” (page 84)

- “Displaying the status of a processor card” (page 93)
- “Displaying the status of an installed SFP optical module” (page 85)
- “Locking a function processor” (page 88)
- “Locking a port” (page 89)
- “Preparing an active FP for being replaced” (page 90)
- “Re-enabling an LP” (page 94)
- “Removing from service a failed FP” (page 97)
- “Removing from service a standby electrical FP” (page 99)
- “Removing from service an optical FP configured with LAPS” (page 100)
- “Removing from service an unspared FP” (page 104)
- “Reinitializing a processor card” (page 95)
- “Returning an FP to service” (page 106)
- “Switching between active and standby processor cards” (page 110)
- “Switching SONET line protection to the mate FP” (page 111)
- “Temporarily disabling an LP” (page 113)
- “Unlocking a function processor” (page 114)
- “Unlocking a port” (page 115)

Comparing the card type of an inserted card and its configured slot

Make sure the card physically inserted in a slot matches the type of card configured for that slot in the system software.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1. Display the card type of the card inserted in a particular slot:

   ```
   display Shelf Card/<m> insertedcardType
   ```

2. Display the type of card configured for the slot.

   ```
   display Shelf Card/<m> cardType
   ```

   If the configured card type does not match the inserted card type, the processor card does not start and its status LED turns solid amber.

3. Look up the minimum software load for the card type of the product engineering code (PEC) of the inserted card in 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* to ensure that the vintage of the card is compatible with the vintage of the software. If they are not compatible, decide whether to upgrade the software for the switch (a migration) or to replace the FP with a compatible card.

Variable definitions

Variable	Value
<m>	The slot number of the processor card.

Configuring a new processor card

Configure a new processor card by specifying the type of card installed in a slot on the shelf and, if part of a one-for-n sparing configuration, where the card connects to the sparing panel.

Prerequisites

- Install all required hardware. See 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade* or 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade*. FPs do not have to be physically installed in the shelf: however, you must know the slot number where an FP is installed before you configure it.
- Configure the required LP and logical processor types (LPT). See “Logical processor, port, and channel configuration” (page 163).
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Add a new *Card* component instance to represent the processor card:

```
add Shelf Card/<m>
```

If the *Card* component instance already exists, you can skip this step.

2 Set the type of the new processor card:

```
set Shelf Card/<m> cardType <cardtype>
```

3 If you are using the processor card as part of a one-for-n sparing configuration, configure where the processor card connects to the sparing panel:

```
set Shelf Card/<m> sparingConnection <connector>
```

For more information on sparing, see “Configuring one-for-n equipment protection for Passport electrical interfaces” (page 206).

Variable definitions

Variable	Value
<cardtype>	The type of the processor card. For information on the type associated with a particular processor card, see “Processor card instances” (page 317) or 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.
<connector>	The connector on the sparing panel. The default value is *notApplicable*. If the processor card is the spare card, use the value *spare*. If the processor card is the main card on a Passport 7400 series, use one of these values: *mainA*, *mainB*, *mainC*, or *mainD*. If the processor card is the main card on a Passport 15000 or 20000 or an MSA32 card of a Passport 7400, use one of these values: *mainA*, *mainB*, *mainC*, *mainD*, *mainE*, or *mainF*. If the processor card is to be part of a one-for-one (1:1) sparing configuration using a one-for-one sparing panel, leave the attribute *sparingConnection* set to the default value notApplicable.
<m>	The slot number of the processor card. Passport numbers its slots starting at zero.

Configuring a port to use an SFP optical module

Configure a function processor (FP) port to use a small form-factor pluggable (SFP) optical transceiver module that is plugged into an optical module socket (port) on the faceplate.

Prerequisites

- When configuring the card, component *OpticalModule* is automatically added. The default is none. You must match the software port configuration to the type of inserted SFP module so that the port can operate.
- The port must be locked. For information on locking a port, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.
- The description of what an SFP module is, the listed types of available SFPs, and the specific FPs that use them are identified in the chapter on processor cards in 241-1501-200 *Passport 15000, 20000 Hardware Description*.
- When configuring an FP with cardtype 16pOC3PosAtm (NTHW44) to use Y-protection on a port, the only supported type of SFP module is *OC3SmIr*. The SFP modules with PEC NTTP02CD must be connected when this configuration is being entered. Since the NTHW44 supports more than one version of SFP module, you must ensure the appropriate ones are plugged into the ports that are to use Y-protection. The custom Y-splitter cables should already be made but not connected while the configuration occurs.
- You can display the operational status of a port by doing the procedure “Displaying the status of an installed SFP optical module” (page 85).
- Other FP configuration information is included in 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Procedure steps

1 Add the Ethernet port.

```
add lp/<m> ethernet/<p>
```

2 Set the type of SFP optical module.

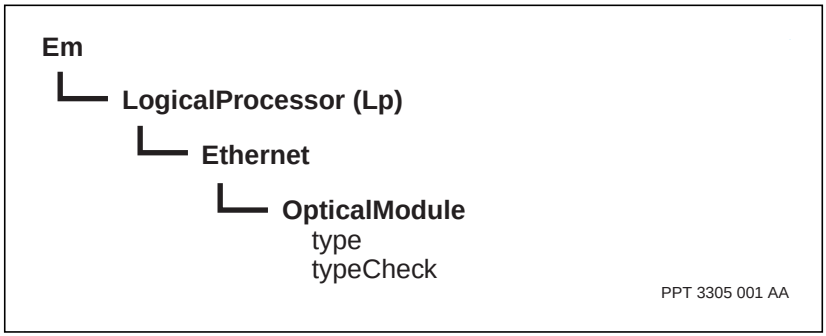
```
set lp/<m> Ethernet/<n> OpticalModule type <type>
```

Variable definitions

Variable	Value
<m>	The instance value for the logical processor (LP).
<n>	The instance value for the port.
<p>	The instance value for the Ethernet port.
<type>	One of the following types of optical module: • *OC3MmSr*, *OC3SmIr*, or *OC3SmLr* for an NTHW44 port • *OC3SmIr* for an NTHW44 port with an NTTP02CD when configuring the port for Y-protection • *LX* or *SX* for an NTHW49 port • *none* for an FP that does not have SFP module sockets (ports) on its faceplate

Procedure job aid

Figure 6
SFP optical module component hierarchy



Decommissioning an FP

Decommission an FP by removing it from a shelf slot and nullifying or changing that slot's configuration (provisioning) in preparation to install a blank processor card.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see "Provisioning mode" (page 24).
- Whether or not another card type is being deployed in the slot, nullify the existing software configuration by setting its attributes back to the defaults.

Procedure steps

1 Set the *cardtype* attribute to none.

```
set Shelf Card/<m> cardType none
```

2 If the FP was configured as a spare card, delete the spare card for the LP.

```
set Lp/<n> spareCard !
```

3 If the FP was configured as a main card, delete the LP and all associated services as described in the procedure "Deleting an LP" (page 182).

4 Activate configuration changes. See "Activating configuration changes" (page 25).

Variable definitions

Variable	Value
<m>	The slot number of the processor card you want to decommission. Passport numbers its slots starting at zero.
<n>	The number of the LP.

Displaying information about daughter cards on a Passport 7400 processor card

Display information about daughter cards on a Passport 7400 processor card to determine daughter card attributes such as type, memory size, and product equipment code.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1. List all processor cards that have daughter cards:

   ```
   list Shelf Card/* DaughterCard/*
   ```

   The system displays alist of all daughter cards on all processor cards.

2. Display information about the daughter cards on a particular processor card:

   ```
   display Shelf Card/<m> DaughterCard/*
   ```

Variable definitions

Variable	Value
<m>	The slot number of the processor card.

Displaying the memory capacity of a processor card

Display the memory capacity of a processor card to determine how much memory a processor card is using. When you set up sparing between CPs, both CPs must have the same amount of memory and disk space.

Procedure steps

1 Display the memory capacity and utilization of a processor card.

```
display Shelf Card/<m> capacity, utilization
```

Variable definitions

Variable	Value
<m>	The slot number of the processor card.

Displaying the status of an installed SFP optical module

Display the status of an installed small-form pluggable (SFP) optical transceiver module to determine whether it matches the software port configuration for it and to confirm its operational status.

Prerequisites

- You need an optical FP that is configured to use an SFP optical module.
  - The 16-port OC-3/STM-1 POS and ATM card (NTHW44) must have the component *sonet* or *sdh* configured.
  - The 4-port Gigabit Ethernet card (NTHW49) must have the component *enet* configured.
- Identify the PEC versions of all SFP modules that are available for the specific FP in 241-1501-200 *Passport 15000, 20000 Hardware Description*.
- Whenever an FP that uses SFP modules is inserted into a slot, the ports (sockets) of its SFP module must be matched to the socket by following the procedure “Configuring a port to use an SFP optical module” (page 80).
- To get any status about an SFP module, it must be plugged into the socket on the FP faceplate. When an SFP is plugged into a powered FP, it is automatically tested for its ability to operate.
- Alarm 7011 5480 is generated to indicate the installed SFP module is not operating because:
  - it fails diagnostics after insertion
  - it mismatches the software configuration of the SFP for the port
  - it is not a Nortel Networks part
- When removing an SFP module, its port must be locked in software, as described in 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*. The status of the SFP is still provided when the port is locked.
- For information about the commands used in the following procedure, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.
- Do the procedure commands in operational mode.

Procedure steps

1. Display the status of the installed version of the SFP module for a port by entering:

   `display lp/<lp> sonet/<s> OpticalModule`

   or

   `display lp/<lp> sdh/<s> OpticalModule`

2. Ensure that the *insertedType* matches the capability of the PEC version that is labelled on the SFP module.

   - *OC3MmSr*, *OC3SmIr*, or *OC3SmLr* for an NTHW44
   - *LX* or *SX* for an NTHW49
   - *none* for an FP that does not have SFP module sockets (ports) on its faceplate

   When *insertedType* indicates *none* (the default), it means the card has not been configured, or the card does not have SFP module sockets.

3. When the *insertedType* indicates *typeMismatch*, either change the software configuration to match the installed module or use an appropriate module. You can query what type of SFP module is configured for the port by entering:

   `display -provisioned lp/<lp> sonet/<s> OpticalModule`

   or

   `display -provisioned lp/<lp> sdh/<s> OpticalModule`

   The configured type is one of the SFP modules in step 2.

4. When *failureCause* indicates *internalError*, check for alarm 7011 5480. Do the remedial action of the alarm or replace the SFP module to restore signal throughput.

5. When *failureCause* indicates *absentOm*, install the SFP module so that an operational state can be indicated.

6. When *failureCause* indicates *unsupportedOm*, install an SFP module that is provided by Nortel Networks.

7. Confirm normal operation of the SFP module by observing these in the response:

- adminstate = unlocked, which applies to the component *OpticalModule*; an SFP module can be enabled but not sending signals through because the port itself is locked
- operationalState = enabled
- usageState = active or idle
- insertedType = one of the following:
  none for the default for an FP without SFP module sockets
  LX for the 1000BASE-LX for single-mode intermediate reach
  SX for the 1000BASE-SX for multimode short reach
  OC3MmSr for the multimode short reach
  OC3SmIr for the single-mode intermediate reach
  OC3SmLr for the single-mode long reach
- failureCause = noFailure

Variable definitions

Variable	Value
<lp>	The number of the logical processor for the card.
<s>	The number of the SONET or SDH port on the card. Use an asterisk (*) to display all the ports on a card.

Locking a function processor

Lock a function processor (FP) to remove it from service.

Prerequisites

- To ensure that the FP shuts down correctly, the associated LP must be unlocked when you lock the card.
- Review the information in “Considerations for locking processor cards” (page 318).
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

CAUTION
Risk of service loss
Forcing an active (in-service) FP into the locked state causes the FP to drop the traffic on the FP, depending on how equipment protection is configured for that FP. If the FP is unspared, all traffic is dropped. If the FP is a spared optical card, up to 50 milliseconds of traffic can be lost. If the FP is a spared electrical card, up to 100 milliseconds of traffic can be lost.

1 Lock the FP using one of the following commands:

```
lock Shelf Card/<m>
```

or

```
lock -force Shelf Card/<m>
```

Variable definitions

Variable	Value
<m>	The slot number of the processor card.

Locking a port

Lock a port during maintenance procedures to remove it from service. Locking a port prevents the port from running the software defined in its logical processor.

Prerequisites

- If you are unfamiliar with lock command concepts, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Lock the port using one of the following commands:

```
lock Lp/<n> <port>/<p>
```

or

```
lock -force Lp/<n> <port>/<p>
```

Variable definitions

Variable	Value
<n>	The instance number of the logical processor linked to the port.
<p>	The port number.
<port>	The port type.

Preparing an active FP for being replaced

Prepare an active FP for being replaced as part of an upgrade, downgrade, or redeployment.

Prerequisites

- If you are unfamiliar with removing and replacing FPs, see "Considerations for replacing function processors" (page 321).
- For more information on the commands that are used in the following procedure, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.
- Perform the following procedure in operational mode. For more information, see "Operational mode" (page 24).

Procedure steps

1 If the card was configured for LAPS, ensure that LAPS is not degraded. (For an electrical FP, skip this step.)

```
display laps/* osiState
```

Under *osiAvail*, determine if any LAPS has a status of *degraded*. If so, you must determine the cause of the degradation. For example, if the mate port is out of service, an active port can be degraded because it cannot be switched over to an out-of-service port. You must fix any degraded laps on either card before proceeding with this procedure.

2 Check all software alarms that are generated for the switch that houses the FP being replaced. All alarms are described in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

For a spared FP, address the remedial action of any alarm indicating that the standby or mate FP is not available to take over the traffic of the active FP.

For an unspared FP, consider the status of the far end and address the worst problem first.

3 If your site records indicate that the network was configured to back up the traffic of an unspared FP, removing the FP from service may cause the network to reroute far-end traffic away from the FP. For example, the configuration can have an intra-network card as opposed to an access card or have a node connected to two nodes to split services. PNNI links may have been set up to do this. If your site records indicate that one or more PNNI links pass through the FP, busy or lock each of those links at the far end.

4 Verify that the former standby card is now carrying traffic (is in service).

```
display Shelf Card/* sps
```

Record the slot number of the in-service LP.

5 Switch the traffic from the active card to the standby card and block the system's access to the standby card.

```
lock -force Shelf Card/<m>
```

Whenever a card is locked, the alarm 7012 0100 is generated. Whenever a standby card is locked, the alarm 7054 0105 is generated.

Note: Whether the card ports are configured as *unidirectional* or *bidirectional*, or as a *revertive* or *non-revertive* mode, the command *lock* handles all associated Passport connections at the far end. For information about these attributes, refer to "Configuring line and equipment protection for Passport 15000 or 20000 optical interfaces" (page 221).

6 Observe the status LED on the faceplate of the standby FP. When the switchover completes, its LED cycles to solid green to indicate a successful switchover.

If the LED is other than solid green, the switchover did not occur. Contact your next level of support to determine your next step.

7 Verify that the former standby card is now carrying traffic (is in service).

```
display Shelf Card/* sps
```

Record the slot number of the in-service LP.

8 Observe the traffic on the active card to ensure it is flowing. Use appropriate test equipment to monitor the cell counts.

9 If the switchover did not occur, abort this procedure and refer to 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for diagnosing FPs.

- For FP fiber optic cards, if the active and standby LEDs on the faceplates do not swap within 50 milliseconds, the switchover may not occur.
- For FP cards with electrical interfaces (such as DS3s, E3s, or E1s), if the active and standby LEDs on the faceplates do not swap within 100 milliseconds, the switchover will not occur. Ensure also that the LED on the sparing panel faceplate for the Spare card is lit to indicate active traffic.

Variable definitions

Variable	Value
<m>	The slot number of the active card. For information about the command *lock*, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Displaying the status of a processor card

Display the status of a processor card whenever you want to display operational attributes such as *failureCause*, *sparingConnectionStatus*, or *currentLP*.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Display the status of a particular processor card:

```
display Shelf Card/<m>
```

Variable definitions

Variable	Value
<m>	The slot number of the processor card.

Re-enabling an LP

Re-enable an LP by using the unlock command if you have disabled an LP using the lock command.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Unlock the LP:

```
unlock Lp/<n>
```

After you unlock an LP, the LED status display light on its main processor card quickly pulses red while the software loads. Once the software is loaded, the processor card becomes enabled.

Variable definitions

Variable	Value
<n>	The number of the LP.

Reinitializing a processor card

Reinitialize a processor card during maintenance or troubleshooting activities by resetting or restarting the card.

Prerequisites

CAUTION
Risk of data loss
When you reset or restart a processor card, it is temporarily unable to provide service. During the time that the processor card is restarting, data can be lost.

CAUTION
Risk of losing stable SVC connections
When you reset or restart a processor card, a loss of switched virtual circuit (SVC) connections may occur. Although stable SVC calls should remain active in a redundant processor configuration, exercise caution when issuing this command.

- Review the information in "Considerations for reinitializing a processor card" (page 321) if you are unfamiliar with reinitializing processor cards.
- Perform the following procedure in operational mode. For more information, see "Operational mode" (page 24).

Procedure steps

1. For a complete reinitialization, use the reset command:

   ```
   reset Shelf Card/<m>
   ```

2. For a faster reinitialization, use the restart command:

   ```
   restart Shelf Card/<m>
   ```

3. If you want to reset all the processor cards, use the resent command to reset the shelf:

   ```
   reset Shelf
   ```

Variable definitions

Variable	Value
<m>	The slot number of the processor card.

Removing from service a failed FP

Confirm a function processor (FP) has already been automatically removed from service by the system due to a failure, and lock it to prevent the software from trying to use it when a replacement FP is inserted. This applies to any FP.

Prerequisites

- If you are unfamiliar with removing FPs from service, see “Considerations for replacing function processors” (page 321).
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Confirm the card is out of service.

```
display Shelf Card/<m>
```

If the *operationalState* indicates *disabled*, the card is out-of-service.

2 Lock the out-of-service card to prevent the system from trying to use it when the replacement is inserted. Refer to “Locking a function processor” (page 88).

3 Return immediately to 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* to replace the out-of-service FP.

4 When the system automatically removes a card from service. Examine the test results to determine why the card was removed from service by the system. Query commands of FP test results are described in 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.

Variable definitions

Variable	Value
<m>	The slot number of the standby card determined in this procedure. For information about the command *lock*, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*. Whenever a card is locked, the alarm 7012 0100 is generated. Whenever a standby card is locked, the alarm 7054 0105 is generated. The alarms are described in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

Removing from service a standby electrical FP

Remove from service a standby electrical function processor (FP) such as DS1, DS3, E1, or E3 before you remove the FP from a shelf.

Prerequisites

- If you are unfamiliar with removing FPs from service, see "Considerations for replacing function processors" (page 321).
- Perform the following procedure in operational mode. For more information, see "Operational mode" (page 24).

Procedure steps

1. Identify and record the software level or PCR that is running in the switch containing the standby FP. You will need it to label the PCR onto the faceplate of the card.

   ```
   display software avl
   ```

   Note: The response indicates the configured (provisioned) software that is running through the switch, not the software that might be loaded on the inactive CP. When removing a card for re-deployment or repair, it is important to know what version of software was running on it.

2. Block the standby card and ports from being put into service.

   ```
   lock -force Shelf Card/<m>
   ```

3. If you are doing this procedure to replace an FP, return immediately to 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade*.

Variable definitions

Variable	Value
<m>	The slot number of the standby card determined in this procedure. For information about the command *lock*, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*. Whenever a card is locked, the alarm 7012 0100 is generated. Whenever a standby card is locked, the alarm 7054 0105 is generated. The alarms are described in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

Removing from service an optical FP configured with LAPS

Remove from service an optical function processor (FP) that is configured for line automatic protection switching (LAPS) in a Passport 15000 or 20000 before removing the card from the shelf.

Prerequisites

- If you are unfamiliar with removing FPs from service, see "Considerations for replacing function processors" (page 321).
- Identify from your site records whether any private network-to-network (PNNI) links pass through either of the FP pair. The procedure will indicate when to remove the PNNI links from service.
- An FP that supports only intra-card LAPS (single-FP LAPS) has port-to-port sparing on the same card. For this configuration, follow the procedure "Removing from service an unspared FP" (page 104).
- Perform the following procedure in operational mode. For more information, see "Operational mode" (page 24).

Procedure steps

1 Identify and record the software level or PCR that is running in the switch containing the FP. You will need it to label the PCR onto the faceplate of the card.

```
display software avl
```

Note: The response indicates the configured (provisioned) software that is running through the switch, not the software that might be loaded on the inactive CP. When removing a card for re-deployment or repair, it is important to know what version of software was running on it.

2 Verify that the card supports LAPS.

```
display -p laps/*
```

If the card was configured for LAPS, the response will indicate a status of the working and protection lines for the card pair you plan to work on.

3 For dual-FP LAPS, there can be ports providing service (active) on both cards so there is no card with a standby status. Identify which card was originally designated as the standby card by entering the command:

```
display Shelf Card/* sps
```

The value under *Card* in the response is the slot number. Under *osiStby*, the value *serv* means that the card is active while *hot* means that the card is the hot standby.

4 Identify which SONET lines are providing service (as opposed to being on hot standby).

```
display laps/* nearendrxactiveline
```

The lines with status *working* are providing service while the lines with *protec* are on hot standby. When *nearEndRequest* indicates

- *signalFailure* it usually means a cable has been cut
- *signalDegrade* it usually means a bit error
- *forcedSwitch* it means a manual switchover was invoked and the mate port is not available

5 Ensure that LAPS is not degraded.

```
display laps/* osiState
```

Under *osiAvail*, determine if any LAPS has a status of *degraded*. If so, you must determine the cause of the degradation and fix it on either card before proceeding with this procedure. Record all port numbers that are degraded then refer to the 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* to do the task for determining FP problems with the procedure on determining the cause of degraded LAPS. Return to this procedure when the degradations are fixed.

CAUTION
Risk of service interruption from a degraded LAPS
You must determine the cause of each degraded LAPS port because a switchover to one means it can remain out of service longer than 50 milliseconds.

6 When removing the card from service for an upgrade or a redeployment (as opposed to a failure), ensure that traffic is running on the mate FP, using step 7 through step 8. If traffic is not running on the mate before the removal, it is unlikely traffic will run on the replacement FP after the return to service.

7 Verify that the services are unlocked and enabled and that there are no unexpected alarms.

```
d <service>/*
```

8 Verify that all connections are up and passing traffic and that there are no signalling alarms.

```
d -o -c <service>/* <connection>/*
```

For example:

```
d -o -c atmif/* vcc/*
d -o -c fruni/* dlci/*
```

9 Check all software alarms that are generated for the switch that houses the FP being replaced. Address the remedial action of any alarm involving equipment or software for the FP being replaced.

10 Prepare the far-end ports for the near-end ports being removed from service. This step applies to any FP.

11 If your site records indicated that you have at least one PNNI link passing through the FP to be removed from service, you must first busy or lock the PNNI link at the far end to remove it from service. At the facility level of operation, as opposed to the service level, switch the PNNI traffic off the target FP to its mate by following the procedure “Switching SONET line protection to the mate FP” (page 111).

12 Switch any traffic from the ports on the near-end target card to the mate card and block the target card and ports from being put into service.

```
lock -force Shelf Card/<m>
```

Note: Whether the card ports are configured as *unidirectional* or *bidirectional*, or as a *revertive* or *non-revertive* mode, the command *lock* handles all associated Passport connections. For information about these attributes, refer to “Configuring line and equipment protection for Passport 15000 or 20000 optical interfaces” (page 221).

13 Observe the traffic on the active card to ensure it is flowing. Use appropriate test equipment to monitor the cell counts.

14 If the switchover did not occur, abort this procedure and refer to 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for diagnosing FPs. For FP fiber optic cards with LAPS, if the active (target) and standby (mate) LEDs on the faceplates do not swap within 50 milliseconds, the switchover may not occur.

Variable definitions

Variable	Value
<connection>	The type of connection for a particular service. For example, vcc for atm or dlci for FrUni.
<m>	The slot number of the standby card configured in this procedure. For information about the command *lock*, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*. Whenever a card is locked, the alarm 7012 0100 is generated. Whenever a standby card is locked, the alarm 7054 0105 is generated. The alarms are described in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.
<service>	The service running on a particular card. For example, atmif or FrUni.

Removing from service an unspared FP

Remove an unspared (unprotected) function processor (FP) from service before removing the FP from the shelf.

Prerequisites

- If you are unfamiliar with removing FPs from service, see "Considerations for replacing function processors" (page 321).
- Identify from your site records whether any private network-to-network (PNNI) links pass through the FP. The procedure will indicate when to remove the PNNI links from service.
- Perform the following procedure in operational mode. For more information, see "Operational mode" (page 24).

Procedure steps

1 Identify and record the software level or PCR that is running in the switch that has the standby FP.

```
display software avl
```

Note: The response indicates the configured (provisioned) software that is running through the switch, not the software that might be loaded on the inactive CP. When removing a card for re-deployment or repair, it is important to know what version of software was running on it. Label the PCR onto the faceplate.

2 Typically, when an unspared FP is removed from service, all traffic to that FP is dropped.

CAUTION
Risk of service interruption
When an unspared card is removed from service either manually or automatically by the system (for example, by the command *lock*), all traffic to the card is dropped. If you must remove an in-service card from service, ensure that you do it during a period of lowest traffic for that card, and you do not delay inserting the replacement card.

If your site records indicate that the network was configured to back up the traffic of an unspared FP, removing the FP from service may cause the

network to reroute far-end traffic away from the FP. For example, the configuration can have an intra-network card as opposed to an access card or have a node connected to two nodes to split services. PNNI links may have been set up to do this. If your site records indicate that one or more PNNI links pass through the FP, busy or lock each of those links at the far end.

3 Check all software alarms that are generated for the switch that houses the FP being replaced. Address the remedial action of any alarm indicating that the standby or mate FP is not available to take over the traffic of the active FP.

4 Prevent a shelf reset by entering the command:

```
lock -force Shelf Card/<m>
```

Whenever a card is locked, the alarm 7012 0100 is generated. Whenever a standby card is locked, the alarm 7054 0105 is generated. The alarms are described in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

Note: For a VSP3 card, do not lock the gigabit Ethernet ports.

5 If you are doing this procedure to replace an FP, return immediately to 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* to replace the out-of-service FP.

If you are doing this procedure to test an FP, return immediately to 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.

Variable definitions

Variable	Value
<m>	The slot number of the card. For information about the command *lock*, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Returning an FP to service

After inserting the replacement FP into its slot, return the FP to service.

Prerequisites

- If you are unfamiliar with removing FPs from service, see “Considerations for replacing function processors” (page 321).
- Monitor for alarms generated against the equipment that the FP connects to. While the replaced FP is returning to service, alarms generated for linked equipment can help indicate the progressive operation of the replaced FP, and the status of connected equipment. All alarms are described in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Verify that the replacement FP is appropriate for the software configuration of the slot by doing the procedure “Comparing an inserted card type to a configured card type” (page 16).

2 While the replacement FP is inserted and out of service, test each port according to the type of FP as described in 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*. This is optional.

Note: If the replacement card is a 4-port DS3, see also 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* about changing the FP configuration for a replacement card.

3 As required, return to service any equipment that is involved in the port connection up to the far-end termination. If the equipment is other than Passport equipment, it will also have to be unlocked. Since the FP is still locked, Passport and far-end alarms will still be generated.

4 After port testing passes, unlock the FP so that it can return to service.

```
unlock Shelf Card/<m>
```

Whenever a card is unlocked, the alarm 7012 0100 is generated. Whenever a standby card is unlocked, the alarm 7054 0105 is generated.

Wait until the cycling of the LEDs ends at fast flashing green. If the LED stays solid red after loading is attempted, the card is an incompatible vintage or was previously loaded with software that is incompatible with the current software running on the switch. Use a compatible card. If the

LED is other than green, see 241-1501-200 *Passport 15000, 20000 Hardware Description*, the section describing the status LEDs of an FP.

5 If the FP was re-configured, identify whether the type of FP or any of the changed services require an FP reset.

6 A switchback to make the newly replaced card the active card again is optional for optical FPs and electrical FPs in one-for-one equipment protection. A switchback is necessary for an electrical FP that is configured in one-for-n equipment protection because the FP designated as the Spare must be the standby card for all the cards in the same equipment protection group.

If the attribute *revertive* is enabled, the FP that was originally configured as the active card will automatically be made active again (unless it already is) after the minimum 5-minute timeout. A longer timeout is user-defined. Switchback behavior depends on the type of card.

Otherwise, to make the replaced Main card active again, do the procedure “Switching between active and standby processor cards” (page 110).

7 Test the card according to its type as described in 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.

Note: For a VSP3 card, if its gigabit Ethernet ports were cabled, the ports are not to be locked in software and the card can be tested only while in-service. The first Ethernet port to return to service becomes the active port if both ports were configured to spare each other.

8 Ensure that the spared services on the FP are up and running. For a spared fiber optic card, check that LAPS is not degraded.

```
display Shelf Card/* sps
```

For an unspared card, check that the status of the logical processor (LP) is working.

```
display lp/<n>
```

Verify that the services are unlocked and enabled and that there are no unexpected alarms.

```
d <service>/*
```

Verify that all connections are up and passing traffic and that there are no signalling alarms.

```
d -o -c <service>/* <connection>/*
```

For example:

```
d -o -c atmif/* vcc/*
d -o -c fruni/* dlci/*
```

9 If so configured, ensure that LAPS on the FP is operating normally.

```
display laps/*
```

10 If so configured, ensure that the SONET and SDH ports on the FP are operating normally.

```
display lp/* son/*

display lp/* sdh/*
```

Confirm that the port associated with the fixed line is operating.

11 Check for alarms indicating a problem with the newly replaced FP. If you detect unexpected alarms indicating:

- at least one disabled LAPS line
- an STS alarm on an optical card
- a port alarm on an electrical card

Contact your next level of Nortel Networks technical support to determine your course of action.

12 While the FP is returning to service, verify that:

- the Tx and Rx connections continue to increase
- there are no cell mis-insertions
- PVC connections are OK
- SVC and SPVC connections are OK

Otherwise, contact your next level of Nortel Networks technical support.

13 Monitor whether alarms have been generated for any equipment that is linked to the Passport that houses the replaced FP. Alarms for linked nodes provide more status information about the operation of the replaced.

14 Return to service any disabled non-Passport far-end equipment and verify in-service throughput. This includes unlocking or returning to service any PNNI links that were removed from service.

15 Soak the card according to your site requirements.

Variable definitions

Variable	Value
<m>	The slot number of the processor card.
<n>	The number of the LP. Note the LP number of the in-service card.

Switching between active and standby processor cards

Switch between the active and standby processor cards in a sparing configuration using the *switchover Lp* command.

Prerequisites

CAUTION
Risk of service loss
A CP switchover can result in loss of service. See “Understanding CP equipment sparing” (page 258) for more information.

If the FP is a spared optical card, up to 50 milliseconds of traffic can be lost. If the FP is a spared electrical card, up to 100 milliseconds of traffic can be lost.

- You can also schedule a switchover for a later time and cancel a scheduled switchover. You cannot schedule a switchover for the CP, that is, Lp/0.
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Immediately switch between the active and standby processor card:

```
switchover Lp/<n>
```

Note: A switchover of Lp/0 causes a temporary loss of connectivity until the other CP becomes active.

Variable definitions

Variable	Value
<n>	The number of the LP.

Switching SONET line protection to the mate FP

Switch SONET line protection to the mate FP to switch traffic on the active SONET line (working or protection) away from the FP you want to replace. You must complete this procedure before locking the SONET ports on the FP to be replaced to ensure there is no impact to services. This is a facility-level procedure as opposed to a service-level procedure.

Prerequisites

- The sparing arrangement must provide an FP card which is the mate for the FP to be replaced. These are pairs of cards in adjacent slots (that is, slots 2 and 3, slots 3 and 4) up to and including slots 14 and 15.
- Refer to the Network Specification Book to determine which SONET ports are configured on the FP to be replaced.

Procedure steps

1 Display all instances of LAPS currently operating on the switch:

```
display -p laps/*
```

Record all of the LAPS instances operating on the FP to be replaced.

2 Determine if there are active SONET lines operating on the FP to be replaced:

```
display laps/<m> nearEndRxActiveLine
```

Record the LAPS instances displayed under *neRxLine*.

3 Switch the active SONET lines from the LP to be replaced to the *hotStandby* LP.

If the active SONET line is the protection line on the FP to be replaced:

```
switch -protectionToWorking Laps/<m>
```

If the active SONET line is the protection line on the FP to be replaced:

```
switch -workingToProtection Laps/<m>
```

Variable definitions

Variable	Value
<m>	The number of the LAPS instance on the FP to be replaced.
<n>	The number of the LP associated with the FP to be replaced.
<o>	The number of the Sonet ports configured on the LP to be replaced.
<p>	The number of the SONET ports configured on the LP located on the far-end Passport.

Temporarily disabling an LP

Disable an LP using the lock command to prevent it from running the software configuration defined in its LPT. Since a locked LP cannot run its software, it is disabled.

Prerequisites

- If you are unfamiliar with the concepts relating to locking LPs, see “Locking and disabling LPs” (page 289) for information.
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Lock the LP using one of the following commands:

```
lock Lp/<n>
lock -force Lp/<n>
```

Variable definitions

Variable	Value
<n>	The number of the LP. You cannot lock Lp/0 (the CP).

Unlocking a function processor

Unlock a function processor (FP) using the *unlock* command if you have locked the card by using the *lock* command or the *lock* command with the *force* option.

After you unlock an FP in a Passport 7400 switch, it loads and starts running its logical processor (if defined). After you unlock an FP in a Passport 15000 or 20000 switch, it restarts its logical processor (if defined).

Prerequisites

Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Unlock the FP.

```
unlock Shelf Card/<m>
```

Variable definitions

Variable	Value
<m>	The slot number of the processor card.

Unlocking a port

Unlock a port after you have completed maintenance procedures to return it to service. Unlocking a port allows the port to run the software defined in its logical processor.

Prerequisites

- If you are unfamiliar with lock command concepts, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Restore service to the port:

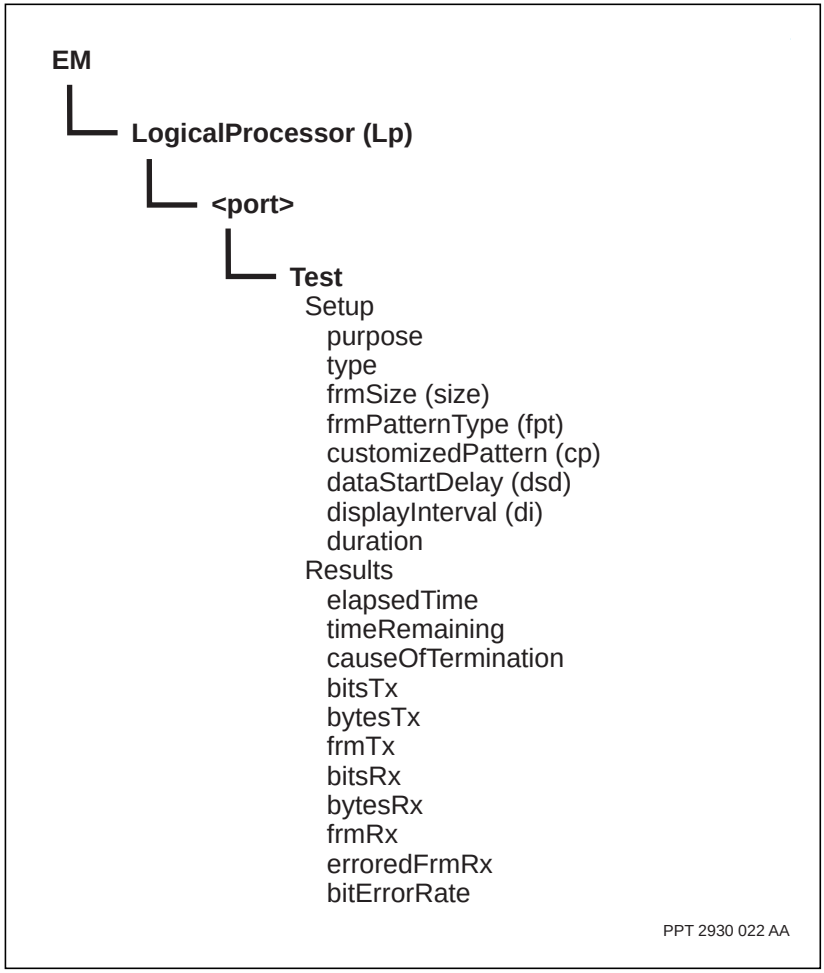
```
unlock Lp/<n> <port>/<p>
```

Variable definitions

Variable	Value
<n>	The instance number of the logical processor linked to the port.
<p>	The port number.
<port>	The port type.

Procedure job aid

Figure 7
Port test components and attributes



Chapter 6
Control processor procedures

Based on your network or nodal requirements, specific control processors configurations may be required. For procedures common to both control and function processors, see “Common processor card procedures” (page 75).

Navigation links

Prerequisites to control processor procedures

- The procedures in this section assume that the control processor are configured using the procedures in “Common processor card procedures” (page 75).

Control processor tasks

Working with Passport 7400 CPs

If you want to upgrade, downgrade, add, or replace a Passport 7400 CP, see the following task flows 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*:

- To upgrade from a CP (NTNQ01) to a CP-with-BITS (NTNQ03) to introduce external timing capability, or downgrade if you no longer want to use a BITS source as a reference for network synchronization, see "Control processor upgrade."
- To add a second CP to a Passport 7400, see "Control processor addition."
- To replace a failed CP, see "Failed control processor replacement."

Disabling and enabling hot standby for CP switchover

Use hot standby for CP switchover to allow FPs running services that support it to continue operating without interruption during a CP switchover. By default, hot standby for CP switchover is enabled. When hot standby for CP switchover is disabled, cold standby for CP switchover is still available.

Note: The standards from the Open Standards Interface (OSI) group use different terminology when referring to standby modes. When you display the *standbyStatus* attribute for the CP LP (Lp/0), it reports *notSet* for both standby modes.

Prerequisites

- Hot standby for CP switchover does not support the removal of the active CP. Removing the active CP causes unexpected behavior on the bus of a Passport 7400 switch or the fabric of a Passport 15000 and 20000 switch. It can cause all processors cards to reset.
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 If you want to enable hot standby for CP switchover, delete the noHitlessCpSwitch feature:

```
set Sw Lpt/CP featureList ~noHitlessCpSwitch
```

When the noHitlessCpSwitch feature is not on the feature list of the CP LPT, hot standby for CP switchover is enabled.

2 If you want to disable hot standby for CP switchover, add the noHitlessCpSwitch feature:

```
set Sw Lpt/CP featureList noHitlessCpSwitch
```

When the noHitlessCpSwitch feature is on the feature list of the CP LPT, hot standby for CP switchover is disabled.

Locking external timing ports

Lock external timing ports to cause the system to switch to the standby timing reference.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1. Find out which external timing ports are in use.

   ```
   display lp/0 *
   ```

2. Lock the external timing ports.

   ```
   lock lp/0 <external_port>/0
   lock lp/0 <external_port>/1
   ```

Variable values

Variable	Value
<external_port>	EDS1 (for DS1 lines) or EE1 (for E1 lines).

Unlocking external timing ports

Unlock external timing ports to enable the system to use the BITS source for network synchronization.

Prerequisites

- Replacing a BITS termination panel does not require a shelf reset. Network synchronization will return to the BITS source automatically, if it is provisioned as the reference source.
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1. Find out which external timing ports are in use.

   ```
   display lp/0 *
   ```

2. Unlock the external timing ports.

   ```
   unlock lp/0 <external_port>/0
   unlock lp/0 <external_port>/1
   ```

Variable values

Variable	Value
<external_port>	EDS1 (for DS1 lines) or EE1 (for E1 lines).

Configuring CP equipment sparing

Set up sparing between processor cards to ensure that in the event of a CP failure, a backup card is available to support node operations. Configure a spare CP manually if one was not previously configured using the StartUp utility.

Prerequisites

- In you are unfamiliar with CP sparing concepts, see “Understanding CP equipment sparing” (page 258).
- For Passport 15000 and 20000, the main CP is in slot 0, while the spare CP is in slot 1. Ensure the main CP and the spare CP are of the same type by verifying that the first 6 characters of their product engineering codes (PECs) are identical. As well, the amount of memory and disk space must be the same.

Procedure steps

1. Verify that you have a second CP in your switch.

   ```
   display Shelf Card/* insertedCardType
   ```

   If you do not have a second CP, ask the hardware installer to install one and see “Adding a spare CP to a single-CP node” (page 127) for information on how to configure it.

2. Specify the main CP.

   ```
   set LogicalProcessor/0 mainCard Shelf Card/<m>
   ```

3. Specify the spare CP.

   ```
   set LogicalProcessor/0 spareCard Shelf Card/<n>
   ```

4. Verify that you have correctly configured CP equipment sparing.

   ```
   display LogicalProcessor/0
   ```

5. Activate the configuration changes. See “Activating configuration changes” (page 25).

6. Synchronize the new standby disk with the active disk.

   ```
   synchronize FileSystem
   ```

   When the synchronization is complete, an alarm appears to indicate that the file system is now synchronized.

Variable definitions

Variable	Value
<m>	The slot number of the main card. Passport numbers its slots starting at 0. The main CP is in slot 0.
<n>	The slot number of the spare card. Passport numbers its slots starting at 0. The main CP is always in slot 0. In a Passport 15000 or 20000 switch, the spare CP is in slot 1. In a Passport 7400 switch, the spare CP is in the last slot of the shelf.

Changing the CP equipment protection mode

Change the CP equipment protection mode to enable hot CP switchover (CPSO) capabilities. When CP equipment protection is enabled (hot), CP based services can provide warm or hot CP switchover capabilities. Hot CP equipment protection also allows a CP switchover to the current view.

Prerequisites

- If you are unfamiliar with CP sparing concepts, see “Understanding CP equipment sparing” (page 258).
- If hot CP standby is enabled (hot), then the *maxNumberJournalFiles* attribute in *ProvisioningSystem* must be enabled by setting it to a value other than none. See the following note for additional information on support of CPSO and hitless software migration (HSM) by the *maxNumberJournalFiles* attribute of the *Prov* component.

  Note: The *maxNumberJournalFiles* attribute specifies the maximum number of journal files that can be saved. A value of none specifies that journaling is disabled, while any other value specifies that journaling is enabled. The *Shelf cpEquipmentProtection* attribute must be set to cold when the *maxNumberJournalFiles* attribute is set to none.
  The value of the *maxNumberJournalFiles* attribute must be greater than the value of the *Prov currentJournal* operational attribute. If it is not, the resulting impact is that journal log file saving becomes operationally disabled. A critical alarm with index 7000 0037 is also raised against the *Prov* component. A Commit Prov command would need to be entered to re-enable journaling.
  The operator may want to set the *maxNumberJournalFiles* attribute to be less than the default value of 2000 in order to force a *Commit Prov* command to be entered more frequently. If a switch reset to the committed view occurs, the *Restore Prov* command may take less time to complete in this case, since there are fewer journal log files to load and activate.

- The standby CP will restart when the *cpEquipmentProtection* attribute is changed from cold to hot and hot to cold.
- Perform this procedure in “Provisioning mode” (page 24).

Procedure steps

1. Modify the CP equipment protection mode.

   ```
   set Shelf cpEquipmentProtection
   <cpEquipmentProtection>
   ```

   Note: Setting the attribute *cpEquipmentProtection* to a value of *Hot* may require the command *commit prov* to be entered. The command *commit prov* commits the view during a hitless software migration to get the spare CP to a hot standby state. For hitless software migration procedures, see 241-5701-272 *Passport 7400, 15000, 20000 Software Upgrade*.

2. Complete the configuration changes. See “Activating configuration changes” (page 25).

Variable definitions

Variable	Value
<cpEquipmentProtection>	Hot (CP equipment protection is enabled) or cold (CP equipment protection is disabled).

Adding a spare CP to a single-CP node

You must configure a spare CP only if you are installing a second CP on a node that has only a single CP. Once you have configured the spare CP, you do not need to reconfigure it to replace the spare CP. For information on replacing a CP, see “Replacing a CP in a two-CP node” (page 142).

If you no longer want to use a spare CP, you must physically remove the spare CP, then delete its configuration. See “Removing a spare CP” (page 129) for more information.

Prerequisites

- If you are unfamiliar with CP sparing in a single-CP node, see “Considerations for adding a spare CP to a single-CP node” (page 263).
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Show which cards are currently configured.

```
display Shelf Card/*
```

2 If the card does not already exist, add it to the shelf.

```
add Shelf Card/<m>
```

3 Specify CP as the type of processor card.

```
set Shelf Card/<m> cardType <c>
```

4 Set the *spareCard* attribute.

```
set Lp/0 spareCard Shelf Card/<m>
```

5 Complete the configuration changes. See “Activating configuration changes” (page 25).

6 Insert a new CP in the spare CP slot.

Passport 15000 and 20000 designates slot 1 for the spare CP. In the case of Passport 7400 series switches, the spare CP is located in the last slot of the shelf.

See 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* or 241-7401-240 *Passport 7400 Hardware*

Installation, Maintenance and Upgrade for information on physically installing a CP.

7 After the second CP starts (its status LED is flashing green), verify that the disks on both CPs are available.

```
list Fs Disk/*
```

Two instances of the *Disk* component appear, one for each CP.

8 Synchronize the new standby disk with the active disk.

```
synchronize Fs
```

When the synchronization is complete, an alarm indicates that the file system is now synchronized.

Variable definitions

Variable	Value
<c>	The card type (*CP*, *CPeD*, or *CPeE*).
<m>	The slot number of the spare CP. Passport 15000 and 20000 designates slot 1 for the spare CP. In the case of Passport 7400 series switches, the spare CP is located in the last slot of the shelf.

Removing a spare CP

Remove a spare CP to disable CP redundancy. When you remove a spare CP to disable CP redundancy, you must also delete its configuration.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Determine which CP is currently active.

```
display Lp/0 mainCardStatus, spareCardStatus
```

If the *mainCardStatus* attribute has a value of *active*, the main CP is active. If the *spareCardStatus* attribute has a value of *active*, the spare CP is active.

2 If the spare CP is active, switch over the CPs so that the main CP is active.

```
switchover Lp/0
```

Note: A switchover of LP/0 causes a temporary loss of connectivity until the other CP becomes active.

3 Remove the spare CP.

See 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* or 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade* for information on removing a CP.

4 Enter provisioning mode.

```
start Prov
```

5 Remove the spare configuration.

```
set Lp/0 spareCard !
```

6 Remove the card configuration.

```
set Shelf Card/<m> cardType none
```

7 Complete the configuration changes. For more information see “Activating configuration changes” (page 25).

Variable definitions

Variable	Value
<m>	The slot number of the spare CP. Passport 15000 and 20000 designates slot 1 for the spare CP. In the case of Passport 7400 series switches, the spare CP is located in the last slot of the shelf.

Replacing a CP in a single-CP node

A Passport node with a single CP has no backup in the event of a failure of the CP. A CP failure interrupts all services on the node. You must replace the failed CP immediately.

Procedure steps

There are three general steps in replacing a CP in single-CP node:

1 Re-establish connection to the network (and Preside Multiservice Data Manager, if available).

The quickest way to re-establish connection to the network is to take the standby CP from a donor node. A donor node is a two-CP node within the same Passport group as defined in Preside Multiservice Data Manager. See 241-6001-023 *Preside MDM Configuration Management for Passport User Guide* for more information on Passport groups.

If a donor node is not available, you must follow the startup procedures described in 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*, to re-establish a connection to the network.

2 Reinstall the software.

If you have a Preside Multiservice Data Manager backup of the node, you can use Preside Multiservice Data Manager to reinstall the software. Preside Multiservice Data Manager also performs backups of journal log files that will enable you to restore the switch to its current view. If you do not have a backup, you must reinstall software for the node using the procedures described in 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*.

3 Reconfigure the node.

If you have a Preside Multiservice Data Manager backup of the node, you can use Preside Multiservice Data Manager to configure the node. If you do not have a backup, you must manually reconfigure the node.

How you replace the CP depends on whether or not you have a recent Preside Multiservice Data Manager backup of the node and whether or not you have a donor node available in the network. The following sections explain how to replace a CP for each of the backup and donor node combinations:

- “Replacing a CP using a donor node and backup” (page 133)
- “Replacing a CP using a donor node only” (page 137)
- “Replacing a CP using a backup only” (page 139)
- “Replacing a CP without a donor node or backup” (page 141)

Replacing a CP using a donor node and backup

Replace a CP using a donor node and a backup to quickly re-establish a connection to the network from the failed node. Do this by taking the spare CP from the donor node and inserting it into the node with the failed CP. Once connected to the network, you can restore the software and configuration using the Preside Multiservice Data Manager backup.

Prerequisites

- For information on physically replacing a CP, see either 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade* or 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade.*
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 If necessary, force the main CP on the donor node to become the active CP.

```
switchover Lp/0
```

Note: A switchover of LP/0 causes a temporary loss of connectivity until the other CP becomes active.

2 Remove the spare CP from the shelf of the donor node. You will install this CP on the failed node after you have configured a new spare CP on the donor node.

3 Insert a new CP into the spare slot of the donor node. For Passport 15000 and 20000, the spare CP resides in slot 1. For Passport 7400, the spare CP resides in the last slot of the shelf.

Nortel Networks recommends that the new spare CP have the same size disk as the main CP.

4 Synchronize the new standby disk with the active disk on the donor node.

```
synchronize Fs
```

This step can take several hours, depending on the amount of data stored on the active disk and the difference between the two disks.

5 Remove the failed CP from the shelf of the failed Passport.

6 Install the CP you removed from the donor node into the main slot (slot 0) of the failed Passport.

7 When the CP comes up (LED is lit solid green), clean up the disk. Remove any unnecessary files including unused software, unused provisioning files, and the spooling files stored in the /spooled/closed directory. For information on removing files, see the following:

- tidy Prov, tidy Sw, remove Sw Av, and remove Fs commands in 241-5701-050 *Passport 7400, 15000, 20000 Commands*
- 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*

8 Change the node name, node ID, and the addresses of the IPIVC interface, the IPIFR interface, or the OAM Ethernet port to the values of the failed node. This step allows you to restore your connection to the network and Preside Multiservice Data Manager.

For information on changing the node name and ID, see “Configuring node identification” (page 31). For information on changing the address of IPIVC or IPIFR, see 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.

9 Restore the files from the last Preside Multiservice Data Manager backup. See 241-6001-023 *Preside MDM Configuration Management for Passport User Guide* for procedures on file restore.

10 Activate the provisioning view that was running when the last backup to Preside Multiservice Data Manager was made:

```
reloadCp -file(<view>) Lp/0
```

If the provisioning view changed since the last Preside Multiservice Data Manager backup, you must manually reconfigure the changes.

Variable definitions

Variable	Value
<view>	The name of the provisioning view.

Reconfiguring a donor CP

Reconfigure a donor CP to establish network management connectivity and identify the switch as a unique node in the network.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Synchronize the new standby disk with the active disk on the donor node.

```
synchronize Fs
```

This step can take several hours, depending on the amount of data stored on the active disk and the difference between the two disks.

2 Remove the failed CP from the shelf of the failed Passport.

3 Install the CP you removed from the donor node into the main slot (slot 0) of the failed Passport.

4 When the CP comes up (LED is lit solid green), clean up the disk. Remove any unnecessary files including unused software, unused provisioning files, and the spooling files stored in the /spooled/closed directory. For information on removing files, see the following:

- tidy Prov, tidy Sw, remove Sw Av, and remove Fs commands in 241-5701-050 *Passport 7400, 15000, 20000 Commands*
- 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*

5 Change the node name, node ID, and the addresses of the IPIVC interface, the IPIFR interface, or the OAM Ethernet port to the values of the failed node. This step allows you to restore your connection to the network and Preside Multiservice Data Manager.

For information on changing the node name and ID, see “Configuring node identification” (page 31). For information on changing the address of IPIVC or IPIFR, see 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.

6 Restore the files from the last Preside Multiservice Data Manager backup. See 241-6001-023 *Preside MDM Configuration Management for Passport User Guide* for procedures on file restore.

7 Activate the provisioning view that was running when the last backup to Preside Multiservice Data Manager was made.

```
reloadCp -file(<view>) Lp/0
```

If the provisioning view changed since the last Preside Multiservice Data Manager backup, you must manually reconfigure the changes.

Variable definitions

Variable	Value
<view>	The name of the provisioning view.

Replacing a CP using a donor node only

Replace a CP using a donor node only by taking the spare CP from the donor node and inserting it into the node with the failed CP. The spare CP allows you to quickly re-establish a connection to the network on the failed node. Once connected to the network, you must manually reinstall the software and reconfigure the node.

Prerequisites

- For information on physically replacing a CP, see either 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade* or 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade.*
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 If necessary, force the main CP on the donor node to become the active CP.

```
switchover Lp/0
```

Note: A switchover of LP/0 causes a temporary loss of connectivity until the other CP becomes active.

2 Remove the spare CP from the shelf of the donor node. You will install this CP on the failed node after you have configured a new spare CP on the donor node.

3 Insert a new CP into the spare slot of the donor node. For Passport 15000 and 20000, the spare CP resides in slot 1. For Passport 7400, the spare CP resides in the last slot of the shelf.

Nortel Networks recommends that the new spare CP have the same size disk as the main CP.

4 Synchronize the new standby disk with the active disk on the donor node.

```
synchronize Fs
```

This step can take several hours, depending on the amount of data stored on the active disk and the difference between the two disks.

5 Remove the failed CP from the shelf of the failed Passport.

6 Install the CP you removed from the donor node into the main slot (slot 0) of the failed Passport.

7 When the CP comes up (LED is lit solid green), clean up the disk. Remove any unnecessary files including unused software, unused provisioning files, and the spooling files stored in the /spooled/closed directory. For information on removing files, see the following:

- tidy Prov, tidy Sw, remove Sw Av, and remove Fs commands in 241-5701-050 *Passport 7400, 15000, 20000 Commands*
- 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*

8 Change the node name, node ID, and the addresses of the IPIVC interface, the IPIFR interface or the OAM Ethernet port to the values of the failed node. This step allows you to restore your connection to the network and Preside Multiservice Data Manager.

For information on changing the node name and ID, see “Configuring node identification” (page 31). For information on changing the address of IPIVC or IPIFR, see 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.

9 Install the application versions (AVs) for the node using the procedures described in 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*.

10 Manually reconfigure the node.

Replacing a CP using a backup only

Replace a CP using a backup only by replacing the failed CP with a new CP. Then, re-establish connection to the network using the StartUp procedures. After the new CP is connected to the network, you can restore the software and configuration using the Preside Multiservice Data Manager backup.

Prerequisites

- For information on physically replacing a CP, see either 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade* or 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade.*
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1. Obtain a new CP.
2. Remove the failed CP from the shelf on the failed Passport.
3. Insert the new CP into the main slot (slot 0) of the failed Passport.
4. Re-establish the connection to the network using the startup procedures in 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.
5. Clean up the file system of the new CP. Remove any unnecessary files including unused software, unused provisioning files, and the spooling files stored in the /spooled/closed directory. For information on removing files, see the following:
   - tidy Prov, tidy Sw, remove Sw Av, and remove Fs commands in 241-5701-050 *Passport 7400, 15000, 20000 Commands*
   - 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*
6. Restore the files from the last Preside Multiservice Data Manager backup. See 241-6001-023 *Preside MDM Configuration Management for Passport User Guide* for procedures on file restore.
7. Activate the provisioning view that was running when the last backup to Preside Multiservice Data Manager was made.

   ```
   reloadCp -file(<view>) Lp/0
   ```

If the provisioning view changed since the last Preside Multiservice Data Manager backup, you must manually reconfigure the changes.

Variable definitions

Variable	Value
<view>	The name of the provisioning view.

Replacing a CP without a donor node or backup

Replace a CP without a donor node or backup by replacing the failed CP with a new CP. You must then re-establish connection to the network using the startup procedures. After the new CP is connected to the network, you must manually reinstall the software and reconfigure the node.

Prerequisites

- For information on physically replacing a CP, see either 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade* or 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade.*
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1. Obtain a new CP.
2. Remove the failed CP from the shelf on the failed Passport.
3. Insert the new CP into the main slot (slot 0) on the shelf of the failed Passport.
4. Re-establish the connection to the network using the startup procedures described in 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.
5. Clean up the file system of the new CP. Remove any unnecessary files including unused software, unused provisioning files, and the spooling files stored in the /spooled/closed directory. For information on removing files, see the following:
   - tidy Prov, tidy Sw, remove Sw Av, and remove Fs commands in 241-5701-050 *Passport 7400, 15000, 20000 Commands*
   - 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*
6. Reinstall the application versions (AVs) for the node using the procedures described in 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*.
7. Manually reconfigure the node.

Replacing a CP in a two-CP node

Replace a CP in a two-CP node to replace a failed CP or upgrade a CP without interrupting service on the node. In a two-CP node, you can remove the standby CP without interrupting service on the node, provided the appropriate software commands are entered in coordination with removing the CP from the shelf.

Prerequisites

- In the unlikely event that both CPs fail simultaneously or the inactive CP is unavailable to take over the traffic of the active CP, follow the procedures in "Replacing a CP in a single-CP node" (page 131).
- Perform the following procedure in operational mode. For more information, see "Operational mode" (page 24).

Procedure steps

1 If necessary, force the CP you want to remove to become the standby CP.

```
switchover Lp/0
```

Note: A switchover of LP/0 causes a temporary loss of connectivity until the other CP becomes active.

2 Reset the offline CP so that it can be removed without losing traffic.

```
reset shelf card /<m>
```

3 Have someone be ready at the CP to continue with the physical removal and insertion procedures as soon as the LED indicates solid red for a few seconds. See 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* or 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*, for information on removing a CP.

4 When the replacement CP is inserted into the slot, it automatically begins to boot. You can observe the boot process of the CP at the local operator terminal.

5 After the new CP starts loading software (its status LED is fast flashing green), verify that the disks on both CPs are available.

```
list Fs Disk/*
```

Two instances of the *Disk* component appear, one for each CP.

Note: If the new CP has the same volume name as the active CP, the new standby disk is automatically synchronized with the active disk. Disk synchronization can take a long time (up to an hour or more). When synchronization is complete, an alarm indicates that the file system is now synchronized.

6 If the new standby disk did not automatically synchronize with the active disk, manually synchronize the two disks:

```
synchronize Fs
```

This command can take a long time (up to an hour or more). When synchronization is complete, an alarm indicates that the file system is now synchronized.

7 Leave the inactive CP inactive. It is not necessary to restore it to active status because the system functions normally regardless which one is currently active.

Variable definitions

Variable	Value
<m>	The slot number of the new processor card.

Upgrading a CP2 to a CP3 in a single-CP node

CP3 control processors are used in Passport 15000 and 20000 nodes only.

Before upgrading a CP2 to a CP3, ensure that the node is operating with software that supports the CP3. Refer to the table on minimum CP software requirements in 241-1501-200 *Passport 15000, 20000 Hardware Description*.

The CP3 requires PowerPC applications. Before downloading the software to run on the CP3, ensure that the *processorTargets* attribute of the *Software Download* component is set to *i960 ppc*.

See Passport 7400, 15000, 20000 Release Notes to see which software vintage supports the CP3, or the table of minimum CP software vintages in 241-1501-200 *Passport 15000, 20000 Hardware Description*. See 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide* to verify the following:

- the vintage of the software that the node is currently using
- whether the application version list (AVL) of the node contains application versions that support PowerPC (ppc) applications

Also, you can reduce the time required to upgrade to a CP3 by doing the following:

- turn off data collection, to minimize file system activity
- minimize the accounting data on the disk
- keep only the minimum number of software versions on the disk

CAUTION
Upgrading a CP2 to a CP3 has the same service impact as replacing a CP2. Some new call connections may not be set up during CP switchover.

To upgrade a CP2 to a CP3, follow the same procedures as in “Replacing a CP in a single-CP node” (page 131) except that the new CP is a CP3.

Upgrading a CP2 to a CP3 in a two-CP node

Upgrade a CP2 to a CP3 to enhance your Passport 15000 or 20000 node with CP3 capabilities. In a two-CP node, you repeat the procedure twice; once for each CP in the node.

CP3 control processors are used in Passport 15000 and 20000 nodes only.

Note: A two-CP node should operate with a CP3 and a CP2 only during the upgrade procedure. Normal operation requires that a two-CP node operates with two identical CPs, either two CP3s or two CP2s.

CAUTION
Upgrading a CP2 to a CP3 has the same service impact as replacing a CP2. Some new call connections may not be set up during CP switchover.

Prerequisites

- Before upgrading a CP2 to a CP3, ensure that the node is operating with software that supports the CP3.
- The CP3 requires PowerPC applications. Before downloading the software to run on the CP3, ensure that the *processorTargets* attribute of the *Software Download* component is set to *i960 ppc*.
- You can reduce the time required to upgrade to a CP3 by turning off data collection, minimizing the accounting data on the disk, and keeping only the minimum number of software versions on the disk.
- Before migrating a Passport 15000 platform from a CP2 processor to a CP3, ensure there is enough available space on the CP2, see “Determining file system capacity” (page 200). If there is not enough available space, the CP2 may not be able to synchronize its disk with the CP3 when trying to revert to CP2 after a CP3 switchover.
- See “Timeout for a subsequent CP switchover” (page 266) for information about performing CP switchover and disconnecting the Ethernet cable on the CP.

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).
- See the *Passport 7400, 15000, 20000 Release Notes* to see which software vintage supports the CP3.
- See 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide* to verify the following:
  - — the vintage of the software that the node is currently using
  - — whether the AVL of the node contains application versions that support PowerPC (ppc) applications
  - — the current and committed provisioning views are the same

Procedure steps

1 Verify which CP is providing service.

```
display Lp/0 activeCard, spareCardStatus
```

2 If you are using OamEnet, verify the status of the active and spare CPs.

```
display Lp/0 oamenet/0 active, standby
```

3 If necessary, force the CP you want to upgrade to become the standby CP.

```
switchover Lp/0
```

4 Lock the file system.

```
lock fs
```

5 If the current standby CP is the one to be replaced then lock the card.

```
lock -force shelf card/<x>
```

6 Upgrade the CP hardware, see the task “CP upgrade” in the 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade*.

Log on to the local operator terminal if you want to observe the boot process of the new CP.

7 After the new CP3 finishes initialization, the status LED is slowly flashing red, unlock the card:

```
unlock shelf card/<x>
```

8 Unlock the file system.

```
unlock fs
```

9 Verify that the disks on both CPs are available.

```
list Fs Disk/*
```

If the new CP3 has the same volume name as the active CP, the new standby disk is automatically synchronized with the active disk. Disk synchronization can take up to an hour or more. When synchronization is complete, an alarm indicates that the file is now synchronized.

10 If the new standby disk did not automatically synchronize with the active disk, manually synchronize the two disks.

```
synchronize Fs
```

You can check on the progress of the synchronization by entering.

```
d Fs synchstatus
```

```
d Fs synchprogres
```

11 Once the file system is synchronized and the new CP3 is available, force the remaining CP2 to become the standby CP.

```
switchover Lp/0
```

Note: A switchover of Lp/0 causes a temporary loss of connectivity until the other CP becomes active.

12 Repeat step 1 to step 11 for the remaining CP2.

13 Once the file system is synchronized and the revertibleTimerCountdown attribute is zero, switch control back to the starting configuration, making CP0 the active processor.

```
display shelf
```

If the revertibleTimerCountdown is zero proceed with the switchover.

```
switchover Lp/0
```

Variable definitions

Variable	Value
<x>	The slot number of the inactive processor card, either 0 or 1.

Downgrading a CP3 to a CP2

Before downgrading a CP3 to a CP2, ensure the following:

- The node is operating with software that supports the CP2.

  The CP2 requires i960 applications. Before downloading the software to run on the CP2, ensure that the processorTargets attribute of the Software Download component is set to i960 ppc.

  See 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide* to verify whether the AVL of the node contains application versions that support i960 applications.

- The file system of the node fits on the CP2 hard disk.

  The hard disk of a CP3 has a greater capacity than that of a CP2. See “Determining file system capacity” (page 200) to ensure you have enough space to synchronize a CP3 to a CP2.

To downgrade a CP3 to a CP2, follow the same procedure in “Upgrading a CP2 to a CP3 in a single-CP node” (page 144). In this case, the node is currently using CP3s and the new CPs are CP2s.

Chapter 7
Control processor OAM Ethernet port configuration

Configure the CP OAM Ethernet port on each control processor (CP) to manage Passport nodes connected to the management network. The Passport nodes can be connected locally or remotely.

Navigation links

Prerequisites to CP OAM Ethernet port configuration

- If you are unfamiliar with CP OAM ethernet concepts, see "Understanding the control processor OAM Ethernet port" (page 332).

CP OAM Ethernet port configuration tasks

- “Changing the mode of the OAM Ethernet port on a CP3 control processor” (page 162)
- For information on configuring IP security (IPSec) for OAM traffic, see 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.

Configuring the CP OAM Ethernet port

Configure the CP OAM Ethernet port if it was not configured when the StartUp utility was run. The port is usually configured by StartUp if you select the OAM Ethernet method of Preside Multiservice Data Manager connectivity.

Note: The *DiscardRouteEntry* subcomponent of the *Static* component identifies destination networks and nodes that do not receive packets through this service. The system discards packets addressed to these destinations immediately. No notification is sent to the sending host that the Passport system has discarded the packets. There is one *DiscardRouteEntry* subcomponent for each route that you want to restrict. For more information on the *Ip Static DiscardRouteEntry* component, see 241-5701-805 *Passport 7400, 15000, 20000 Understanding IP*.

Prerequisites

- If you are unfamiliar with CP OAM Ethernet port configuration, see "Understanding the control processor OAM Ethernet port" (page 332).
- Perform the following procedure in provisioning mode. For more information, see "Provisioning mode" (page 24).

Procedure steps

1 Add the *oamEnet* and *ip* features to the feature list of the CP.

```
set Software Lpt/CP featureList oamEnet ip
```

Note: The oamEnet and ip features must be part of the software application version list (AVL). For more information on adding features to the AVL, see "Software, applications, and features additions and updates" (page 65).

2 Add the *OamEthernet* component to the logical processor for the CP.

```
add LogicalProcessor/0 oamEnet/0
```

3 If you want to gather and report extended statistics, enable the *extendedStatistics* attribute.

```
set LogicalProcessor/0 oamEnet/0 extendedStatistics
enabled
```

Note: This attribute has a default value of *disabled*.

4 Create a LAN media application. Adding this component automatically creates a *Framer* subcomponent.

```
add LanApplication/0
```

5 Associate the LAN media application with the OAM Ethernet port.

```
set LanApplication/0 Framer interfaceName
LogicalProcessor/0 oamEnet/0
```

6 Optionally, disable the *switchoverOnFailure* attribute to ensure that the OAM Ethernet port does not switch over to the port on the spare CP when the test process detects a hardware or link failure.

```
set LogicalProcessor/0 oamEnet/0 switchoverOnFailure
disabled
```

This attribute has a default value of *enabled*.

7 Add a management virtual router (attribute *Vr managementAccess* is enabled) if one doesn't already exist. By default, the first virtual router (VR) you create on a Passport node is the management VR:

```
add Vr/0
```

8 Specify where the virtual router resides.

```
set Vr/0 vrp lp/0
```

9 Enable IP on the virtual router.

```
add Vr/0 Ip
```

10 Add a protocol port to the virtual router.

```
add Vr/0 ProtocolPort/oam0
```

11 Associate the LAN media application with the protocol port.

```
set LanApplication/0 linkToProtocolPort
Vr/0 ProtocolPort/oam0
```

12 Enable IP on the protocol port.

```
add Vr/0 ProtocolPort/oam0 IpPort
```

13 Add a logical IP interface under the *IpPort* component.

```
add Vr/0 ProtocolPort/oam0 IpPort IpLogicalInterface/
<IPaddress>
```

14 Provision a network mask for the protocol port.

```
set Vr/0 ProtocolPort/oam0 IpPort IpLogicalInterface/
<IPaddress> netmask <netmaskaddress>
```

15 Provision a broadcast address for the protocol port.

```
set Vr/0 ProtocolPort/oam0 IpPort IpLogicalInterface/
<IPaddress> broadcastAddress <broadcastaddress>
```

16 Verify the configuration of the OAM Ethernet port.

```
display Software Lpt/CP featureList

display LogicalProcessor/0 oamEnet/0

display LanApplication/0 Framer interfaceName

display Vr/0 ProtocolPort/oam0 IpPort
```

17 Add a *Static* component as a subcomponent of the *Ip* component.

```
add Vr/0 Ip Static
```

18 Add static route(s), for routing to the management workstation, to the route table. The *RouteEntry* component can specify one management host or a subnetwork/network containing multiple management workstations/hosts.

```
add Vr/0 Ip Static RouteEntry/
<ipAddress2>,<destmask>,<tos>
```

19 Provision a *NextHop* component for each defined static route. The NextHop_ipAddress parameter must denote a locally attached host.

```
add Vr/0 Ip Static RouteEntry/
<ipAddress2>,<destmask>,<tos> nextHop/
<nextHop_ipAddress>
```

20 Set the metric for the route (optional).

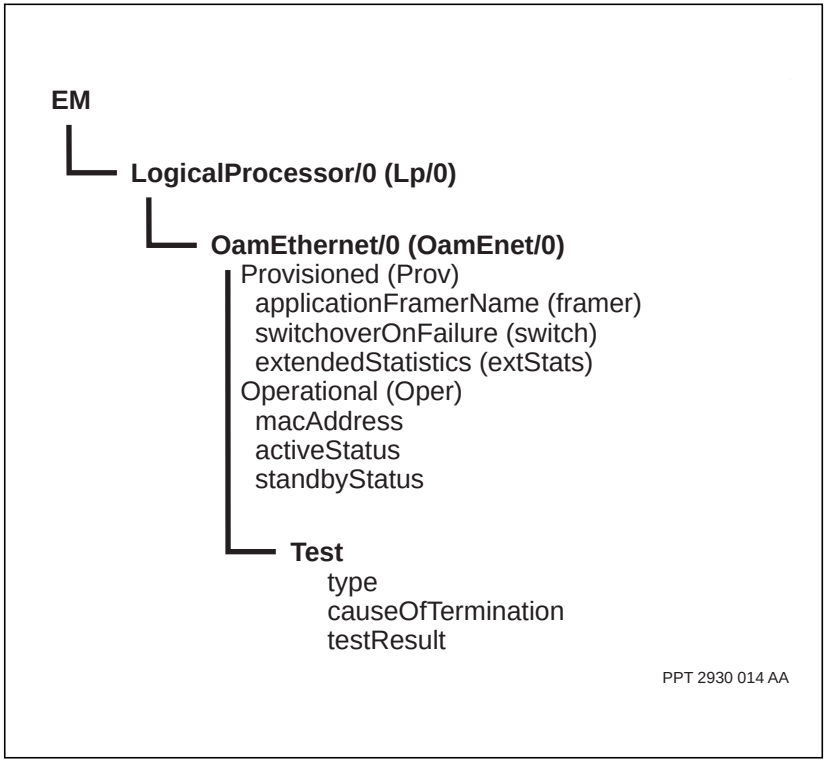
```
set Vr/0 Ip Static RouteEntry/
<ipAddress>,<destmask>,<tos>
nextHop/<nextHop_ipAddress> metric <cost>
```

Variable definitions

Variable	Value
<broadcastaddress>	The broadcast address.
<cost>	A relative metric value (ranges from –1 to +65535) assigned to the static route—the assigned cost judges route preference.
<destmask>	The subnetwork mask used with the IP address. If <ipAddress> specifies a host, provision <destmask> as 255.255.255.255. Also, provision locally attached hosts as *Arp HostEntry* components instead of a *Static* component entry. For more information on the *IP Static RouteEntry* component, see 241-5701-805 *Passport 7400, 15000, 20000 Understanding IP*.
<IPaddress>	The IP address of the OAM Ethernet port.
<ipAddress2>	The IP address of the remote management workstation (can refer either to a specific node or to a network).
<netmaskaddress>	The netmask address.
<nextHop_ipAddress>	The IP address of the next router in the path to the destination. Since this is a specific node and cannot be a network, there is no subnetwork mask.
<tos>	The type of service (currently, only the default value of 0 is supported).

Procedure job aid

Figure 8
Configuring the CP OAM Ethernet port component hierarchy



Enabling CP switchover for a CP OAM Ethernet port failure

Enable CP switchover for a CP OAM Ethernet port failure if you want the system to switch to the spare CP if it detects a port or link failure on the CP OAM Ethernet port.

Prerequisites

- If you are unfamiliar with CP OAM Ethernet port concepts, see “Understanding the control processor OAM Ethernet port” (page 332).
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Display the current switchover behavior of the port.

```
display Lp/0 oamEnet/0 switchoverOnFailure
```

2 Set the switchoverOnFailure attribute to the required value.

```
set Lp/0 oamEnet/0 switchoverOnFailure enabled
```

Disabling CP switchover for a CP OAM Ethernet port failure

Disable CP switchover for a CP OAM Ethernet port failure if you want the system to switch to the spare CP if it detects a port or link failure on the CP OAM Ethernet port.

Prerequisites

- If you are unfamiliar with CP OAM Ethernet port concepts, see “Understanding the control processor OAM Ethernet port” (page 332).
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1. Display the current switchover behavior of the port.

   ```
   display Lp/0 oamEnet/0 switchoverOnFailure
   ```

2. Disable the switchoverOnFailure attribute.

   ```
   set Lp/0 oamEnet/0 switchoverOnFailure disabled
   ```

Changing the statistics gathered from the CP OAM Ethernet port

Change the statistics gathered from the CP OAM Ethernet port by specifying whether the system gathers extended statistics.

Prerequisites

- If you are unfamiliar with CP OAM Ethernet port, see “Understanding the control processor OAM Ethernet port” (page 332).
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Set the extendedStatistics attribute to the required value.

```
set Lp/0 oamEnet/0 extendedStatistics <value>
```

Variable definitions

Variable	Value
<value>	*Enabled* or *disabled*. The default is *disabled*.

Configuring the line speed of the OAM Ethernet port on a CP3 control processor

Configure the line speed of the OAM Ethernet port on a CP3 control processor to match the requirements of the far end.

Prerequisites

- If you are unfamiliar with CP OAM Ethernet port concepts, see "Understanding the control processor OAM Ethernet port" (page 332).
- Perform the following procedure in provisioning mode. For more information, see "Provisioning mode" (page 24).

Procedure steps

1 Set the lineSpeed attribute to the required value.

```
set Lp/0 oamEnet/0 lineSpeed <value>
```

Variable definitions

Variable	Value
<value>	*AutoConfig*, *tenMeg*, or *hundredMeg*. The default is *autoConfig*. ***Note:*** When set to autoConfig, the CP3 automatically sets the line speed to match the requirements of the far-end hub. The actual line speed can be obtained from the *actualLineSpeed* attribute.

Changing the mode of the OAM Ethernet port on a CP3 control processor

Change the mode of the OAM Ethernet port on a CP3 control processor to specify whether the port operates in half or full duplex mode.

Prerequisites

- If you are unfamiliar with CP OAM Ethernet port concepts, see "Understanding the control processor OAM Ethernet port" (page 332).
- Perform the following procedure in provisioning mode. For more information, see "Provisioning mode" (page 24).

Procedure steps

1 Set the duplexMode attribute to the required value.

```
set Lp/0 oamEnet/0 duplexMode <value>
```

Variable definitions

Variable	Value
<value>	*AutoConfig*, *half*, or *full*. The default is *autoConfig*. ***Note:*** When set to autoConfig, the CP3 automatically sets the duplex mode to match the requirements of the far end hub. The actual duplex mode can be obtained from the *actualDuplexMode* attribute.

Chapter 8
Logical processor, port, and channel configuration

Define or modify the link between logical processors and the ports and channels on processors cards. The link between these entities determines how services on supported each Passport node.

Navigation links

- "Prerequisites to logical processor, port, and channel configuration" (page 163)
- "Logical processor, port, and channel configuration tasks" (page 163)

Prerequisites to logical processor, port, and channel configuration

- If you are unfamiliar with the concepts associated with logical processors (LPs), ports, and channels, see "Understanding logical processors, ports, and channels" (page 282).

Logical processor, port, and channel configuration tasks

The tasks to configure a logical processor, port, or channel are listed alphabetically.

- "Adding a channel to a port" (page 165)
- "Adding an LP and linking it to an LPT" (page 167)
- "Adding an LPT" (page 170)

Adding a channel to a port

Add channels to FPs that provide port channelization. The Passport software automatically adds channel 0 when you add a port.

> ***Note:*** This procedure does not apply to the OC-48/STM-16 ATM with APS FP. See instead the procedure "Adding an Sts component to a port with the FP is operating with a single path" (page 172) or "Adding an Sts component to a port when the FP is operating with multiple paths" (page 173).

Prerequisites

- To determine whether an FP supports channelization, see appropriate list of configuration parameters in the 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.
- Perform the following procedure in provisioning mode. For more information, see "Provisioning mode" (page 24).

Procedure steps

1. Add a *Channel* component to the port.

   ```
   add lp/<n> <port>/<p> Chan/<r>
   ```

   The Passport software automatically adds channel 0 when you add a port.

2. Assign timeslots to the *Channel* component.

   ```
   set lp/<n> <port>/<p> Chan/<r> timeslots <t>
   ```

3. If the port type requires that a data rate be assigned to timeslots, assign a rate for the timeslots within each channel.

   ```
   set lp/<n> <port>/<p> Chan/<r> timeslotDataRate <rate>
   ```

4. Repeat this procedure for each channel.
5. Verify the configuration of the channels.

   ```
   display LogicalProcessor/* <port>/* <c>/*
   ```

Variable definitions

Variable	Value
<c>	The channel type for the port.
<n>	The LP number.
<p>	The port number.
<port>	The port type.
<r>	The channel number. See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* for valid values for <r>.
<rate>	The timeslot data rate.
<t>	The list of timeslots.

Adding an LP and linking it to an LPT

Add an LP to define the software, sparing, and port configurations of processor cards. You must associate an LPT, which is a list of software features, with every LP.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1. Display existing LPTs and their features to determine if any are suitable.

   ```
   display Sw Lpt/* featureList
   ```

   If a suitable LPT does not exist, create one using the procedure “Adding an LPT” (page 170).

2. Add a *LogicalProcessor* (*Lp*) component.

   ```
   add Lp/<n>
   ```

3. Link the LP to an LPT:

   ```
   set Lp/<n> logicalProcessorType Sw Lpt/<lpt_name>
   ```

4. Set the main card for the LP.

   ```
   set Lp/<n> mainCard Shelf Card/<m>
   ```

5. If necessary, set the spare card for the LP.

   ```
   set Lp/<n> spareCard Shelf Card/<m>
   ```

6. If you are configuring a one-for-n sparing configuration, repeat step 2 to step 5 for each FP in the sparing configuration.

Variable definitions

Variable	Value
<lpt_name>	The name of the LPT you want to use.

(Sheet 1 of 2)

Variable	Value
<m>	The slot number of the main card. Passport numbers its slots starting at 0.
<n>	The number of the LP, from 1 through 15. Passport reserves 0 for the CP.
(Sheet 2 of 2)	

Additional information about LP sparing guidelines

Use the following sparing guidelines when creating a new LP:

- In a one-for-n sparing configuration for Passport 15000 and 20000, you can configure up to six LPs with the same spare card. For Passport 7400, you can configure up to four LPs with the same spare card. To support this configuration, you must connect the processor cards to a sparing panel. You must also configure the sparing connection. For information on the hardware requirements of one-for-n sparing, see 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* or 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*. For information on configuring the sparing connection, see “Configuring one-for-n equipment protection for Passport electrical interfaces” (page 206).
- With Passport 15000 and 20000, CPs on *Lp/0* can only reference the cards in slots 0 and 1. The card in slot 0 must be configured as the main card. The card in slot 1 must be configured as the spare card.
- With the Passport 7400 series switches, CPs on *Lp/0* can only reference the cards in the first and last slots of the switch. The card in the first slot must be configured as the main card. The card in the last slot must be configured as the spare card. For example in a 16-slot switch, the main card must be *Card/0* and the spare must be *Card/15*.
- *Lp/0* must be spared to ensure redundancy of Preside Multiservice Data Manager connectivity when Preside Multiservice Data Manager is connected through the Ethernet port of the CP.
- No two LPs can reference the same processor card as main.
- The main and spare processor cards of an LP must be of identical card types.

- Before setting up sparing between processor cards, check the PECs of the active and spare cards. For CPs, all eight digits of the PECs must match. For FPs, the first six digits (four letters and two numbers) must match.

  Note: Some Passport 7400 processor cards have equivalent PECs. See 241-7401-200 *Passport 7400 Hardware Description* for a list of equivalent PECs. Except where noted, processor cards with equivalent PECs can be used as spares for each other.

- For MSA32 FP sparing, electrical interfaces are protected inter-card (electrical sparing protection) while optical interfaces are protected intra-card (APS line protection). Regardless of either PEC or card type:

  — DS1 FPs can only spare other DS1 FPs and only for electrical interfaces

  — E1 FPs can only spare other E1 FPs and only for electrical interfaces

For information on creating an LPT, see “Adding an LPT” (page 170). For more information on sparing, see “Understanding equipment protection for Passport electrical interfaces” (page 270).

Once you have the software and sparing configured, you can configure the ports on the processor card by adding port subcomponents to the *LogicalProcessor* component. For information on configuring ports, see “Configuring ports on an LP” (page 177).

Adding an LPT

Add an LPT to define a group of software features you can assign to an LP. You can only use features that are part of a software application version (AV) currently available on the node. You can assign more than one feature to an LPT.

Prerequisites

CAUTION
Risk of processor memory fragmentation
Processor memory can become fragmented as software features are added and deleted through configuration and activation cycles. To ensure optimal use of FP memory, always specify the features in order of priority, with the first feature being the feature that you want the best performance. Otherwise, once a certain level of fragmentation has occurred, it might not be possible to load new software. In the worst case, FPs may reset.

- Exactly which combinations of features you can use depends on the type of the processor card you intend to associate with the LPT (through the LP). For a list of supported feature combinations, see *Passport 15000 Engineering Notes and Guidelines*.
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Add a new *LogicalProcessorType* (*Lpt*) component.

```
add Sw Lpt/<lpt_name>
```

2 Define the feature list.

```
set Sw Lpt/<lpt_name> featureList <features>
```

You can display all features available on your node using the following command:

```
list Sw Av/* Feature/*
```

The feature names are the instance values of the *Feature* component.

Variable definitions

Variable	Value
<lpt_name>	A name for the LPT. The name can contain up to 25 alphanumeric characters. Passport converts the name to all uppercase letters.
<features>	A list of the features of the LPT, separated by spaces. Make sure you specify the features in order of priority. Make the first feature on the list the one for which you want the best performance.

Adding an Sts component to a port with the FP is operating with a single path

Add an *Sts* component to a channelized optical FP. When you have configured the whole port to operate with a single path, only one *Sts* component is allowed. This procedure concatenates all the available bandwidth of the port into one path.

Prerequisites

- See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* for the appropriate values for the Sts component and the concatenation level.

Procedure steps

1. Add the *Sts* component.

   ```
   add Lp/<n> <port>/<p> <path>/0
   ```

2. Set the concatenation level.

   ```
   set Lp/<n> <port>/<p> <path>/0 concatNumber <c>
   ```

Variable definitions

Variable	Value
<c>	The concatenation level.
<n>	The LP number.
<p>	The port number.
<path>	The path type.
<port>	The port type.

Adding an Sts component to a port when the FP is operating with multiple paths

When you configure a port to operate with multiple paths, each *Sts* component represents a bundle of STS timeslots. You need to assign these timeslots in contiguous groups.

For example, for the OC-48/STM-16 ATM FP with APS, you need to add the first *Sts* component with a value 0 and set its concatenation level. Then you add the second *Sts* component with a value of 12 and set its concatenation level.

Prerequisites

- See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* for the maximum number of *Sts* components you can define.You do not need to define all the available *Sts* components on a port if they are not all needed.
- See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* for the appropriate values for the Sts component and for the concatenation level.

  Note: If you use incorrect *concatNumber* values or *Sts* component instances, your provisioning view is rejected with errors when you try to activate it.

Procedure steps

1. Add an *Sts* component:

   ```
   add Lp/<n> <port>/<p> <path>/<r>
   ```

2. Set the concatenation level:

   ```
   set Lp/<n> <port>/<p> <path>/<r> concatNumber <c>
   ```

3. For each *Sts* component you want to add, perform the preceding two steps.
4. If desired, define the ATM interface application components associated with the *Sts* components you have just defined.

Variable definitions

Variable	Value
<c>	The concatenation level.
<n>	The LP number.
<r>	The *Sts* component instance.
<p>	The port number.
<path>	The path type.
<port>	The port type.

Canceling a scheduled switch between active and standby function processors

Cancel a scheduled switch between active and standby function processors (FPs) if you no longer need to have the system perform the switch at a designated time.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1. To cancel a scheduled switchover, use the switchover Lp command with the cancel option:

   ```
   switchover -cancel Lp/<n>
   ```

Variable definitions

Variable	Value
<n>	The number of the LP.

Changing the LPT used by an LP

Change the software running on an LP by changing its LPT. The LPT defines the software features of the LP. For more information, see “Configuring the software features of an LPT” (page 179).

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1. Display existing LPTs and their features to determine if any are suitable.

   ```
   display Sw Lpt/* featureList
   ```

   If a suitable LPT does not exist, create one using the procedure “Adding an LPT” (page 170).

2. Set the LPT for the LP.

   ```
   set Lp/<n> logicalProcessorType Sw Lpt/<lpt_name>
   ```

Variable definitions

Variable	Value
<lpt_name>	The name of the LPT you want to use.
<n>	The number of the LP.

Configuring ports on an LP

For each LP, you must configure the ports that exist on the processor card. The 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* specifies the type and number of ports, including tributary ports, that can be configured.

> ***Note:*** You can spare four ports or less on an 8-port DS1/E1 IMA card using a single termination panel. The configured ports must be in the range of 0 to 3 or 4 to 7. If you do not connect a sparing panel when a port has been configured, the FP poll for the missing connection and causes a "click" in the panel serving the other bank of ports.

Sts and*Vc4* components are not automatically created when you add a port, so you need to add them separately. See the procedure "Adding an Sts component to a port with the FP is operating with a single path" (page 172) or "Adding an Sts component to a port when the FP is operating with multiple paths" (page 173).

If this is a channelized FP that supports more than one channel, add additional channels using the procedure "Adding a channel to a port" (page 165).

If it is not a channelized FP, set provisionable attributes using the procedure "Customizing port attributes" (page 181).

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see "Provisioning mode" (page 24).
- See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* for valid values for the procedure variables.

Procedure steps

1 Review the possible port types for the FP.

```
help Lp
```

The listed subcomponents are the possible port types.

2 Add a port that is appropriate for the type of interface required.

```
add Lp/<n> <port>/<p>
```

3 If the FP supports tributary ports beneath the port you added in step 2, add a tributary port.

```
add Lp/<n> <port>/<p> <trib_port>/<q>
```

4 Repeat this procedure for each port.

Variable definitions

Variable	Value
<n>	The LP number.
<p>	The port number.
<port>	The port type.
<q>	The tributary port number.
<trib_port>	The tributary port type.

Configuring the software features of an LPT

Add or delete software features from an LPT by changing its *featureList* attribute.

Prerequisites

CAUTION

Deleting a feature from an in-use LPT

If you delete a feature from an in-use LPT (referenced by an LP), the active processor card and the standby processor card reset. If no other in-use LPT contains the feature, the whole node can reset.

- With Passport 15000 and 20000, applications and features fall into three categories: hot standby, warm standby, and cold standby. See “Hitless services on Passport” (page 239) for definitions. Do not create an LPT that mixes cold standby applications or features with hot standby or a warm standby applications or features. A single cold standby application or feature in an LPT changes all other applications and features into cold standby.
- When changing the *featureList* attribute, make sure you specify the features in order of priority. Make the first feature listed the feature that you want the best performance.
- For more information on removing features, see the section “Deleting an LP” (page 182).
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Add or delete features from the feature list of the LPT.

```
set Sw Lpt/<lpt_name> featureList <featurechanges>
```

Make sure your modified feature list specifies the features in order of priority. Make the first feature on the list the one for which you want the best performance.

To delete a feature, put a tilde (~) before the feature name. For example, to delete the atmTrunks feature, use the following in <featurechanges>:

```
~atmTrunks
```

To add a feature, include the feature name on the list. To add the atmTrunks feature, use the following in <featurechanges>:

```
atmTrunks
```

To clear the feature list and replace it with a new list, use an exclamation point (!) as the first element in the list. For example, to clear the current feature list and replace it with the atmTrunks feature, use the following list of changes:

```
! atmTrunks
```

2 Verify that the changes are successful.

```
display Sw Lpt/<lpt_name> featureList
```

Variable definitions

Variable	Value
<featurechanges>	A list of feature changes separated by spaces.
<lpt_name>	The name of the LPT for which you are changing the features.

Customizing port attributes

If required, you can customize any of the attributes associated with a port.

Prerequisites

- For more information on attribute values, use the help command for the port type or refer to 241-5701-060 *Passport 7400, 15000, 20000 Components*.
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Set the value of the port attribute.

```
set LogicalProcessor/<n> <port>/<p> [<subcomponents>]
<attribute> <attributevalue>
```

Variable definitions

Variable	Value
<attribute>	The name of the attribute.
<attributevalue>	The value for the attribute.
<n>	The LP number.
<p>	The port number.
<port>	The port type.
<subcomponents>	Represents any subcomponents (such as tributary ports or channels) that have provisionable attributes. This is an optional parameter.

Deleting an LP

Delete an LP by deleting its *LogicalProcessor* (*Lp*) component. When you delete an *Lp* component, you also delete all its subcomponents.

Prerequisites

- You must also delete services that were associated with the deleted *Lp* component. To delete all associated services simultaneously, use the clear -rf prov command. Alternatively, you can delete every associated service individually using the delete command.
- If you delete an LP and are left with a processor card with no LP assigned to it, that processor card does not load when you activate your configuration changes.
- If you delete the last LP running a particular software feature, the CP resets when you activate your configuration changes. This situation occurs when the deleted LP uses an LPT that is not used by any other LP and contains a feature not contained by any other currently used LP:
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).
- If you have deleted the LP of an active card, the semantic check indicates that the card will reset when you activate the configuration changes. If you have deleted the last LP running a particular software feature, the semantic check also indicates that the CP will reset when you activate the configuration.

Procedure steps

1 Delete the LP component and all of its subcomponents.

```
delete Lp/<n>
```

The number of components deleted appears.

Variable definitions

Variable	Value
<n>	The number of the LP you want to delete.

Deleting BITS ports on Passport 7400

Delete a BITS port on Passport 7400 if you will no longer use a BITS source as a reference for network synchronization or if you are removing a CP-with-BITS and replacing it with a regular CP.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Delete the BITS ports.

```
delete lp/0 <BITS_port>EE1/<port>
```

This command deletes the external timing component and all its subcomponents. The number of components deleted appears.

2 Complete the configuration changes. See “Activating configuration changes” (page 25).

Variable definitions

Variable	Value
<BITS_port>	EDS1 (for DS1 lines) or EE1 (for E1 lines).
<port>	*0* or *1*.

Scheduling a switch between active and standby function processors

Schedule a switch between the active and standby function processors (FPs) in a sparing configuration if you want to switch traffic to the standby FP at a designated time. You cannot schedule a switchover for the CP, that is, *Lp/0*.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Schedule a switchover for a specific time.

```
switchover -time(<yyyy>-<mm>-<dd> <hh>:<mn>) Lp/<n>
```

Variable definitions

Variable	Value
<dd>	The two-digit day.
<hh>	The two-digit hour.
<mm>	The two-digit month.
<mn>	The two-digit minute.
<n>	The number of the LP.
<yyyy>	The four-digit year.

Chapter 9
Passport 15000 or 20000 fabric card configuration

Configure or display the attributes associated with Passport 15000 or Passport 20000 fabric cards as part of installing or maintaining these elements of system hardware.

Navigation links

- "Prerequisites to Passport 15000 or Passport 20000 fabric card configuration" (page 185)
- "Passport 15000 or Passport 20000 fabric card configuration tasks" (page 185)

Prerequisites to Passport 15000 or Passport 20000 fabric card configuration

- If you are unfamiliar with the concepts associated with Passport fabric cards, see "Understanding the fabric card" (page 336)

Passport 15000 or Passport 20000 fabric card configuration tasks

- "Locking a fabric card" (page 186)
- "Unlocking a fabric card" (page 187)
- "Displaying the operating mode of fabrics" (page 188)
- "Displaying the status of a fabric card" (page 189)
- "Displaying the configuration or capacity of a fabric card" (page 190)

Locking a fabric card

Lock a fabric card to deflect new traffic or transfer existing traffic from the fabric to its mate. The system removes the fabric from service without locking it when a fabric fault is detected.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Check the status of the fabric cards to ensure that the mate can accommodate taking over all traffic on the node. You cannot lock a fabric unless its mates is unlocked and enabled with LED status solid green.

```
display Shelf fabricCard/*
```

2 Lock the fabric card.

```
lock Shelf fabricCard/<n>
```

When the fabric is locked, alarm 0000 1000 is generated. Record whether the upper or the lower fabric was locked.

When locking the fabric fails, alarm 7002 0013 is generated with a reason for the failure.

Variable definitions

Variable	Value
<n>	x (for the fabric in the upper position of the shelf) or y (for the fabric in the lower position of the same shelf).

Unlocking a fabric card

Unlock a fabric to enable the card to be returned to service. Load-balancing between the fabrics recurs by having the formerly transferred traffic in progress transferred back to the newly-in-service mate fabric.

The unlocking works on the card in the fabric slot regardless whether the fabric is the same one at the time of the locking.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Unlock the fabric card.

```
unlock Shelf fabricCard/<n>
```

Variable definitions

Variable	Value
<n>	x or y.

Displaying the operating mode of fabrics

Display the operating mode of the fabrics to determine whether both fabric cards are in service (dual-fabric mode) or only one fabric card is in service (single-fabric mode).

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Determine which fabric cards are in service.

```
display Shelf backplaneOperatingMode
```

The *backplaneOperatingMode* attribute appears with one of the following values:

- dualFabric—both fabric cards are in service and their LEDs are solid green
- dualFabricDegraded—both fabric cards are in service but have at least one disabled *fabricPort* on an FP; both LEDs are solid green
- singleFabricX—fabric card x is in service, but fabric card y is out of service and its LED is red
- singleFabricY—fabric card y is in service, but fabric card x is out of service and its LED is red

The reasons for a fabric or fabric port being out of service are indicated in the 7002 series of alarms.

Note: If the reset button under the handle of a Passport 20000 fabric is not fully engaged, the fabric stays out of service and shows a solid red LED.

Displaying the status of a fabric card

Use the attributes of the *FabricCard* component to view information on the status of a fabric card.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Display the status of a particular fabric card.

```
display Shelf fabricCard/<n>
```

A list of operational attributes of the *FabricCard* component appears. See the figure “Fabric components and attributes” (page 337).

Variable definitions

Variable	Value
<n>	x or y.

Displaying the configuration or capacity of a fabric card

Use the attribute *slotConfiguration* of the *Shelf* component to view the configuration or capacity of the fabric card after it is installed, powered up, and loaded. The configuration identifies the type of switch as a Passport 15000 or 20000.

Note: For the initial release of Passport 20000, the fabric is the 70 G version with PEC NTPN02, but the shelf backplane is designed to accommodate other capacities.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Display the slot configuration of a particular fabric card.

```
display Shelf slotConfiguration
```

One of the following configurations is displayed:

- *40G* for a Passport 15000
- *70G* for a Passport 20000

Chapter 10
Passport 7400 bus maintenance

Maintain the two 800 Mbit/s buses to enable proper communication between the processor cards on each Passport 7400 shelf.

Navigation links

Prerequisites to Passport 7400 bus maintenance

- If you are unfamiliar with the concepts relating to the Passport 7400 bus, see "Understanding the Passport 7400 bus" (page 341).

Passport 7400 bus maintenance tasks

Locking and unlocking a bus

Lock a bus to temporarily prevent it from carrying data. When you perform bus tests you must lock the bus. After testing, you must unlock the bus.

Prerequisites

- For information on testing a bus, see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.
- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).
- Ensure the other bus is unlocked and enabled. You can lock a bus only if the other bus is unlocked and enabled.

Procedure steps

CAUTION
Risk of data loss
To reduce the risk of data loss, do not lock a bus during peak periods of traffic. Bus system capacity is reduced by half when a bus is locked, potentially causing minimal data loss due to congestion. If problems occur on the enabled bus, card crashes can also occur.

1. Lock the bus.

   ```
   lock Shelf Bus/<n>
   ```

2. While the bus is locked, perform any necessary testing.
3. Unlock the bus.

   ```
   unlock Shelf Bus/<n>
   ```

Variable definitions

Variable	Value
<n>	x or y.

Enabling and disabling automatic bus clock testing

The automatic bus clock source test can cause minor data loss. You can enable and disable the automatic testing. By default, automatic bus clock source testing is disabled.

Prerequisites

- If you disable automatic testing, you should manually test the bus clock source at least once a month. See 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1. To enable automatic testing, set the *automaticBusClockTest* attribute to enabled.

   ```
   set Shelf Test automaticBusClockTest enabled
   ```

2. To disable automatic testing, set the *automaticBusClockTest* attribute to disabled.

   ```
   set shelf test automaticBusClockTest disabled
   ```

Interpreting the bus clock source status

When Passport 7400 is performing automatic bus clock source testing, you can determine the status of the bus clock source by displaying the *clockSourceStatus* attribute. This attribute also shows the status of the bus clock source after a manual test.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Display the status of the bus clock source.

```
display Shelf Bus/* clockSourceStatus
```

2 Use the table “Interpreting bus clock source status” (page 195) to interpret the value of the attribute.

Procedure job aid

Table 3
Interpreting bus clock source status

Test result	Explanation
ok	All operational cards can receive signals from the clock source. No remedial action is necessary.
failed	At least one operational card is unable to receive signals from the clock source. This condition causes an alarm. Replace the hardware item that is most likely to have failed (see below) and rerun the bus test. Repeat until you correct the problem. The following are the most likely points of failure, in order, if a clock source fails for only one card: • card that failed test • card containing the clock source • backplane The following are the most likely points of failure, in order, if a clock source fails for multiple cards: • card containing the clock source • cards that failed test • backplane The card at the opposite end of the shelf from the active CP provides the alternate clock source. If the slot is empty, no alternate clock source is available.
unknown	The status of the clock source is not known. This is the normal clock source status when the automatic bus clock source testing is disabled. To determine the status of the clock source, manually run the bus clock source test. See 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.

(Sheet 1 of 2)

Table 3 (continued)
Interpreting bus clock source status

Test result	Explanation
testInProgress	The clock source is currently being tested. The new test runs after the current test is complete.
notApplicable	The LP associated with the alternate clock source is down or not configured.
(Sheet 2 of 2)	

Verifying which buses are in service

To determine which buses are in service, view the operating mode of the backplane by typing the following command in operational mode. For information on working in operational mode, see “Operational mode” (page 24).

```
display Shelf backplaneOperatingMode
```

The backplaneOperatingMode attribute is displayed with one of the following values:

- dualBus—both buses are in service
- singleBusX—bus X is in service but bus Y is out of service
- singleBusY—bus Y is in service but bus X is out of service

Chapter 11
Passport file system maintenance

Maintain the Passport file system so that software, configuration files, and data generated by the node are stored properly.

Navigation links

Prerequisites to Passport file system maintenance

- If you are unfamiliar with Passport file system concepts, see "Understanding the Passport file system" (page 343)

Passport file system maintenance tasks

Synchronizing disks

Synchronize disks so that both the active and standby CPs in a node have identical content.

Depending on the amount of stored data on the active disk and the difference between the two disks, the synchronization can take several hours.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Synchronize the disks.

```
synchronize Fs
```

Displaying information about the file system

Display operational attributes for the file system to determine the status, usage, and available space of the file system as a whole and on individual disks.

Displayed information about the file system includes the volume name, synchronization status, capacity, free space, and usage percentage.

Displayed information about the disks of the file system includes the volume name, capacity, and free space on the disk. The instance number of the *Disk* component corresponds to the slot number of the CP that holds the disk.

Note: If there are different numbers of bad blocks on the disks in a dual-disk system, the reported free space can differ on the two disks.

Prerequisites

- Perform the following procedure in operational mode. For information on working in operational mode, see “Operational mode” (page 24).

Procedure steps

1 Display information about the file system.

```
display Fs
```

2 Display information about the disks of the file system.

```
display Fs Disk/*
```

Determining file system capacity

Determine file system capacity to ensure that a CP3 to CP2 synchronization can occur without failure.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Display information about the file system on the CP2 and CP3 using the procedure “Displaying information about the file system” (page 199).

2 Subtract the amount of free space from the capacity to determine the amount of space available on the CP3 disk:

```
freeSpace - capacity = <amount_of_data>
```

If the <amount_of_data> exceeds the value of the *capacity* attribute for the CP2, the synchronization from CP3 to CP2 will fail.

Variable definitions

Variable	Value
<amount_of_data>	The amount of space available on a CP.

Changing the volume name of a disk

Change the volume name of a disk by setting its *volumeName* attribute. The disks on the active and standby CPs must have the same volume name for Passport to automatically synchronize them.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 If you are changing the volume name of the active CP’s disk, lock the file system.

```
lock Fs
```

CAUTION

Locking the file system

Minimize the time you spend in lock Fs. Locking the file system results in a condition where configuration activity can fail, downloading can fail, and spooling can stop if you stay in this state too long.

2 Lock the disk whose volume name you want to change.

```
lock Fs Disk/<n>
```

3 Set the volume names on the disk.

```
set Fs Disk/<n> volumeName <volumename>
```

4 Unlock the disk.

```
unlock Fs Disk/<n>
```

5 If you previously locked the file system, unlock it.

```
unlock Fs
```

Variable definitions

Variable	Value
<n>	The number of the disk. The disk number corresponds to the slot number of the CP that holds the disk.
<volumename>	The new volume name of the disk (up to 11 characters).

Formatting a disk

Format a disk to erase all files and directories and reset the volume name of the disk. To support synchronization between different-sized disks, Passport can format a disk to a size smaller than its physical capacity.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

CAUTION

Never format the disk on the active CP. Loss of important files can result from using the format command.

If your node has only one CP, do not format its disk. Only format a disk if you have two CPs and one of them is in standby mode.

If you need to format the disk on the active CP and you have a two-CP node, first use the switchover command to make the active CP the standby. Once it has become the standby CP, you can format its disk.

1. Lock the disk on the standby CP.

   ```
   lock Fs Disk/<n>
   ```

2. Format the disk on the standby CP to its maximum size.

   ```
   format -volumename(<volumename>) Fs Disk/<n>
   ```

   If you want to format the disk to a smaller size to maintain backward compatibility with older equipment, use the -backward option.

   ```
   format -volumename(<volumename>) -backward Fs Disk/<n>
   ```

3. Do a disk read test to exclude all bad disk media in the file system. Due to the above format, the bad disk medium information is lost and needs to be re-established.

4. Set test type.

   ```
   set Fs disk/<n> test type diskRead
   ```

5 Start the test.

```
start Fs disk/<n> test
```

6 Wait for its completion.

7 Fix the file system due to the possible bad media found.

```
set Fs disk/<n> test type filesystemCheck
```

```
start fs disk/<n> test
```

8 Wait for its completion.

9 Unlock the disk.

```
unlock Fs Disk/<n>
```

10 Synchronize the file system.

```
synchronize Fs
```

The synchronization can take several hours depending on the amount of data on the active disk.

Variable definitions

Variable	Value
<n>	The slot number of the standby CP.
<volumename>	The volume name of the disk. If you do not specify a volume name, Passport uses the first 11 characters of the node name.

Chapter 12
Passport electrical interface equipment protection configuration

Configure electrical function processor (FP) equipment sparing so that the spare card can take over in case the main card fails. This type of equipment sparing uses a single LP to define both the main and spare FP.

Navigation links

- "Prerequisites to Passport electrical interface equipment protection configuration" (page 205)
- "Configuring one-for-n equipment protection for Passport electrical interfaces" (page 206)

Prerequisites to Passport electrical interface equipment protection configuration

- If you are unfamiliar with the concepts associated with electrical equipment sparing on Passport, see "Understanding equipment protection for Passport electrical interfaces" (page 270).

Configuring one-for-n equipment protection for Passport electrical interfaces

Configure one-for-n equipment protection for Passport electrical interfaces. The configuration settings for equipment protection are different for electrical interfaces that are one-for-one (1:1) or one-for-n (1:n) where n is not 1.

Procedure steps

1 Configure the sparing panel connection to specify the main card.

```
set Shelf Card/<m> sparingConnection <connector>
```

2 Configure the sparing panel connection to specify the spare card. For a one-for-one configuration:

```
set Shelf Card/<n> sparingConnection notApplicable
```

For a one-for-n configuration:

```
set Shelf Card/<n> sparingConnection spare
```

3 For the LP to be spared, set the attribute *spareCard* to point to the spare FP.

```
set LogicalProcessor/<x> spareCard Shelf Card/<n>
```

4 Verify that you have correctly configured the equipment sparing.

```
display Shelf Card/* sparingConnection
```

5 Confirm that the status of *sparingConnection* is appropriate for your one-for-one (1:1) or one-for-n (1:n) configuration as described in 241-5701-060 *Passport 7400, 15000, 20000 Components*.

```
display LogicalProcessor/* mainCard
```

```
display LogicalProcessor/* spareCard
```

6 To configure the sparing behavior so that an immediate switchover will occur if the main FP fails, set the attribute *oneForNSparingBehavior* to *immediateSwitchOver*.

```
set Lp/n oneForNSparingBehavior immediateSwitchOver
```

Note: This step is optional. The default setting for the attribute is *delayedSwitchOver*.

7 Complete the configuration changes. See “Activating configuration changes” (page 25).

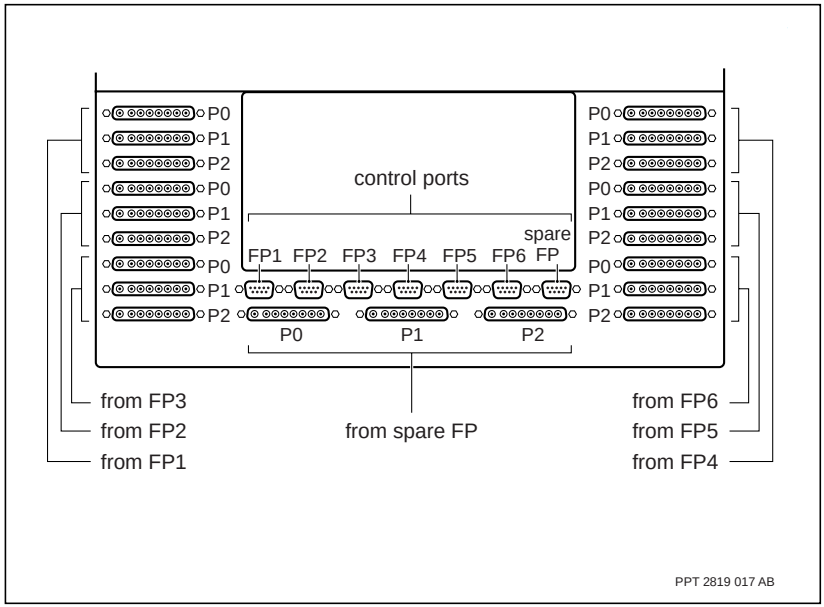
Variable definitions

Variable	Value
<connector>	is the connector on the sparing panel. The default value is *notApplicable*. If the processor card is the spare card, use the value *spare*. If the processor card is the main card on a Passport 7400 series, use one of these values: *mainA*, *mainB*, *mainC*, or *mainD*. If the processor card is the main card on a Passport 15000 or 20000 or an MSA32 card of a Passport 7400, use one of these values: *mainA*, *mainB*, *mainC*, *mainD*, *mainE*, or *mainF*. ***Note:*** If the processor card is to be part of a one-for-one (1:1) sparing configuration, using a one-for-one sparing panel, leave the attribute *sparingConnection* set to the default value *notApplicable*.
<m>	is the slot number of the main card, or a new processor card that you intend to use as a main card.
<n>	is the slot number of the spare card.
<x>	is the instance value of the LP.

Procedure job aid

With a Passport 15000 or 20000, use the figure “FP cable connections on a one-for-six sparing panel” (page 208) and the table “Locations on the sparing panel and corresponding connector values” (page 208) to determine the value of <connector> that corresponds to the physical location of the connector on the sparing panel. For example, the connector in the upper right-hand corner of the sparing panel, as shown in the figure “FP cable connections on a one-for-six sparing panel” (page 208), is labeled FP4 and as such corresponds to a value of mainD in the table “Locations on the sparing panel and corresponding connector values” (page 208).

Figure 9
FP cable connections on a one-for-six sparing panel



In the table “Locations on the sparing panel and corresponding connector values” (page 208), FPn corresponds to the location of FP connectors as shown in “FP cable connections on a one-for-six sparing panel” (page 208). Determine the value of `<connector>` by mapping the corresponding location on the sparing panel.

Table 4
Locations on the sparing panel and corresponding connector values

Sparing panel connector	<connector> value
FP1	mainA
FP2	mainB
FP3	mainC
FP4	mainD
(Sheet 1 of 2)	

Table 4 (continued)
Locations on the sparing panel and corresponding connector values

Sparing panel connector	<connector> value
FP5	mainE (only Passport 15000 or 20000, Passport 7400 MSA32)
FP6	mainF (only Passport 15000 or 20000, Passport 7400 MSA32)
(Sheet 2 of 2)	

Chapter 13
Passport 7400 optical interface line protection configuration

Set up line automatic protection switching (line APS) to enable a form of SONET line sparing on optical FPs. Under line APS, two lines are defined: working and protection. While both lines carry the user payload, only one is deemed active at any time. The active line is the line where the receiving end takes its data.

Navigation links

- "Prerequisites to Passport 7400 optical interface line protection configuration" (page 211)
- "Passport 7400 optical interface line protection configuration tasks" (page 211)

Prerequisites to Passport 7400 optical interface line protection configuration

- If you are unfamiliar with line protection for Passport 7400, see "Understanding line protection for Passport 7400 optical interfaces" (page 279)

Passport 7400 optical interface line protection configuration tasks

- "Configuring line protection for Passport 7400 optical interfaces" (page 213)
- "Locking the protection line on Passport 7400" (page 215)

- “Switching between the working and protection lines on Passport 7400” (page 216)
- “Clearing a switch request on Passport 7400” (page 217)

Configuring line protection for Passport 7400 optical interfaces

Configure line automatic protection switching (Line APS) to protect SONET or SDH ports on Passport 7400 optical cards.

Note: You cannot connect an optical interface on a Passport 7400 that uses the *Aps* component to an optical interface on another Passport 7400 that does not use the *Aps* component.

Prerequisites

- The logical processor type (LPT) associated with these ports must have Line APS in its feature list.
- See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* for information on port numbers for APS protection pairs.

Procedure steps

1 Configure the line APS feature.

```
set sw lpt/aps featurelist aps
```

2 Link the logical processor (LP) to the line APS application.

```
set sw lp/<n> lpt sw lpt/aps
```

3 Add the *AutomaticProtectionSwitching* component.

```
add aps/<a>
```

4 Link the *AutomaticProtectionSwitching* component to the ports on the LP.

```
set aps/<a> workingLine lp/<n> <port>/<p> Path/0
```

```
set aps/<a> protectionLine lp/<n> <port>/<q> Path/0
```

5 If the line terminating equipment at both the near and far ends should determine the receiving interface, change the protection mode to bidirectional.

```
set aps/<a> mode bidirectional
```

Bidirectional mode must be configured at both ends. The default setting is unidirectional. This means that the line terminating equipment at each end determines which interface it receives traffic on.

6 If you want Line APS to revert automatically from the protection to the working line once a failure has cleared, change the scheme to revertive.

```
set aps/<a> revertive yes
```

The default setting is non-revertive. This means that after a failure has cleared, the protection line stays active until the operator issues a switchover command.

7 Verify your configuration of the *AutomaticProtectionSwitching* component.

```
display aps/<a>
```

8 Complete the configuration changes. See “Activating configuration changes” (page 25).

Variable definitions

Variable	Value
<a>	The instance number of the *AutomaticProtectionSwitching* component. For Passport 7400-series FPs, the *AutomaticProtectionSwitching* instance can be any value between 0 and 255.
<n>	The instance of the LP linked to the line APS application. At this point, lp/<n> is configured as the main card.
<p>	The port number on the working LP.
<port>	Either *Sonet* or *Sdh*.
<q>	The port number on the protecting LP.

Locking the protection line on Passport 7400

Lock the protection line on Passport 7400 to prevent the APS system from using the protection line as the active line.

There are several commands the operator can use to set the active line. The *protectionLockout* verb prevents the protection line from being used as the active channel. If the protection line is active when *protectionLockout* is issued, the working line becomes active.

Procedure steps

1 Lock out the protection line.

```
protectionLockout Aps/<n>
```

Variable definitions

Variable	Value
<n>	The instance of the *Aps* component.

Switching between the working and protection lines on Passport 7400

Switch between the working and protection lines on Passport 7400 to manually override the APS system and specify which line the system uses as the active line.

You can issue the switch command when the *Aps* component is locked or unlocked.

Prerequisites

- The *switch* verb is used to effect a switch of the active line. The *-force* option is used to invoke the changeover with the higher priority *nearEndRequest* value of *forcedSwitch*. When *-force* is not used as an option, the *nearEndRequest* value is the lower priority *manualSwitch*.
- The working and protection lines should be synchronized with the same timing source to make sure there is no service impact during equipment or line switchovers.

Procedure steps

1 Enter one of the following commands to switch between the working and protection lines.

```
switch [-force] -protectionToWorking Aps/<n>
switch [-force] -workingToProtection Aps/<n>
```

Variable definitions

Variable	Value
<n>	The instance of the *Aps* component.

Clearing a switch request on Passport 7400

Clear a switch request on Passport 7400 to allow the APS system to automatically select the active line. Using the *clear* command clears the following *nearEndRequest* values:

- lockoutOfProtection
- forcedSwitch
- manualSwitch

Procedure steps

1 Clear a switch request.

```
clear Aps/<n>
```

Variable definitions

Variable	Value
<n>	The instance of the *Aps* component.

Chapter 14
Passport 15000 or 20000 optical interface line and equipment protection configuration

Configure or modify line automatic protection switching (line APS or LAPS) on a Passport 15000 or 20000 node to extend the line APS functionality available from Passport 7400 series nodes.

Navigation links

- "Prerequisites to Passport 15000 or Passport 20000 optical interface line and equipment protection configuration" (page 219)
- "Passport 15000 or Passport 20000 optical interface line and equipment protection configuration tasks" (page 220)

Prerequisites to Passport 15000 or Passport 20000 optical interface line and equipment protection configuration

- If you are unfamiliar with the concepts associated with line and equipment protection for Passport 15000 or Passport 20000 optical interfaces, see "Understanding line and equipment protection for Passport 15000 or 20000 optical interfaces" (page 274).

Passport 15000 or Passport 20000 optical interface line and equipment protection configuration tasks

Configuring line and equipment protection for Passport 15000 or 20000 optical interfaces

Configure line automatic protection switching (line APS or LAPS) to protect against line failures on Passport 15000 or 20000 optical cards. By configuring the working and protection ports of line APS on different LPs, equipment protection is also enabled in addition to line protection.

Prerequisites

- Your switch must meet the requirements listed in “Switch requirements for configuring line and equipment protection for Passport 15000 or 20000 optical interfaces” (page 276)
- You cannot connect an optical interface on a Passport 15000 or 20000 that uses the *Laps* component to an optical interface on another Passport 15000 or 20000 that does not use the *Laps* component or to any third party optical interface that does not support line APS.
- When the dual-FP configuration involves the 16-port OC-3/STM-1 POS and ATM cards (16pOC3PosAtm or NTHW44), the Y-protection capability supports LAPS for dual FPs at the near end while LAPS is unsupported at the far end interface (Passport or non-Passport). Refer to the procedure “Configuring Y-protection for dual FPs in a Passport 15000 or 20000” (page 231).
- You can use the *LineAutomaticProtectionSwitching* component in an equipment sparing configuration to provide both line and equipment protection at the same time.
- See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* at each description of a card type for limitations about choosing slots and port numbers for LAPS protection pairs.
- The logical processor type (LPT) associated with these ports must have APS in its feature list.
- The software logical processor type (SW LPT) of the logical processor (LP) must be the same for the working line and the protection line attributes.
- The attributes for the working and the protection lines:
  - cannot be empty

  - must have the same card types
  - for FPs that use small-form pluggable (SFP) optical modules, must have the same type and vintage of optical module

- When linked to the LAPS component, SDH or SONET components must have the same instance and cannot have provisioned subcomponents.
- Only a single *vc4* or *sts* component may be provisioned under the LAPS component. See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* at the configuration considerations of each card type for the way LAPS handles this per type of optical FP.

CAUTION

Risk of loss of service by interface attribute mismatch

Special care should be taken when connecting an optical interface on one Passport 15000 or 20000 that uses the *Laps* component for equipment protection to another optical interface on a different Passport 15000 or 20000 that does not use the *Laps* component. You can make such a connection when both Passport 15000 or 20000 switches are connected through an optical transport device, such as a Nortel Networks OC-48 TransportNode or a third party device.

A mismatch can occur between the interface attributes set through the *Laps* component of the first Passport 15000 or 20000 and the equivalent interface attribute set through the port components of the LP of the second Passport 15000 or 20000. In particular, the default value of the *alarmActDelay* attribute is 2000 when set through a *Laps* component, but only 500 when set through a port component. This can cause loss of service between both nodes when an equipment protection switchover occurs on the Passport 15000 or 20000 with the *Laps* component.

To avoid loss of service, ensure the interface attributes set through the port component match the equivalent interface attributes set through the *Laps* component. For example, the *alarmActDelay* attribute of each switch should be set to 2000.

Procedure steps

1. Add the *Laps* component.

   ```
   add Laps/<a>
   ```

2. Add the path component, either *Sts* for Sonet or *Vc4* for Sdh.

   ```
   add Laps/<a> <path>/<o>
   ```

3. Add the *AtmIf* component.

   ```
   Add AtmIf/<c>
   ```

4. Link the *Laps* component to the ports on the LP.

   ```
   set AtmIf/<c> interfacename Laps/<a> <path>/<o>

   set Laps/<a> workingLine Lp/<m> <port>/<p>

   set Laps/<a> protectionLine Lp/<n> <port>/<p>
   ```

5. If both near and far end line terminating equipment must negotiate to determine the line to receive the payload from, change the *mode* attribute to bidirectional.

   ```
   set Laps/<a> mode bidirectional
   ```

   Bidirectional mode must be configured at both ends. The default setting is unidirectional. This means that the line terminating equipment at each end determines independently where to receive the payload.

6. If you want line APS to revert automatically from the protection to the working line once a failure has cleared, set revertive to yes.

   ```
   set Laps/<a> revertive yes
   ```

   The default setting is nonrevertive. This means that after a failure has cleared, the protection line stays active until the operator issues a switchover command.

7. Verify your configuration of the LAPS component.

   ```
   display Laps/<a>
   ```

8. Complete the configuration changes. See “Activating configuration changes” (page 25).

Variable definitions

Variable	Value
<a>	The instance number of the *Laps* component. The *Laps* instance must be between 0 and 15999.
<c>	The instance number of the *AtmIf* component. The *AtmIf* instance must be between 1 and 4095.
<m>	The LP number of the working line.
<n>	The LP number of the protection line.
<o>	The path number.
<p>	The port number on the LP. It must be the same on both the working line and the protection line.
<path>	*Sts* or *Vc4*.
<port>	*Sonet* or *Sdh*.

Configuring line protection for optical interfaces on Passport 15000 or Passport 20000

Line automatic protection switching (line APS) is configured to protect against line (port) failures on Passport 15000 or 20000 optical cards.

Prerequisites

- Your switch must meet the requirements listed in “Switch requirements for configuring line and equipment protection for Passport 15000 or 20000 optical interfaces” (page 276).
- When you are configuring the *LineAutomaticProtectionSwitching* component, ensure that the FPs use module timing to synchronize with the CP. If the clocking source is not set to module timing, cell loss and corruption could result in some configurations. Refer to “Network clock synchronization configuration” (page 51) for more information on clock configuration.
- You can use the *LineAutomaticProtectionSwitching* component in an equipment sparing configuration to provide both line and equipment protection at the same time. For more information on equipment sparing and line sparing, see “Understanding line and equipment protection for Passport 15000 or 20000 optical interfaces” (page 274).
- The logical processor type (LPT) associated with these ports must have LAPS in its feature list.
- Y-protection provides equipment protection (EP) and hitless software migration (HSM) that can co-exist with standard LAPS on the same port pairs. Refer to “Configuring Y-protection for dual FPs in a Passport 15000 or 20000” (page 231).
- See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* at each description of a card type for limitations about choosing slots and port numbers for LAPS protection pairs.

Procedure steps

1. Add the *LineAutomaticProtectionSwitching* component.

   ```
   add LineAutomaticProtectionSwitching/<a>
   ```

2. Link the *LineAutomaticProtectionSwitching* component to the ports on the logical processor.

```
set LineAutomaticProtectionSwitching/<a> workingLine
LogicalProcessor/<n> <port>/<p> <path>/<o>

set LineAutomaticProtectionSwitching/<a>
protectionLine LogicalProcessor/<n> <port>/<q>
<path>/<o>
```

3 If the line terminating equipment at both the near and far ends should determine the receiving interface, change the protection mode to bidirectional.

```
set LineAutomaticProtectionSwitching mode
bidirectional
```

Bidirectional mode must be provisioned at both ends. The default setting is unidirectional, which means that the line terminating equipment at each end determines which interface it receives traffic on.

4 If you want LAPS to revert automatically from the protection to the working line once a failure has cleared, change the revertive attribute to yes.

```
set LineAutomaticProtectionSwitching revertive yes
```

The default setting is no, which means that after a failure has cleared, the protection line stays active until the operator uses a switchover command.

5 Verify your configuration of the *LineAutomaticProtectionSwitching* component.

```
display LineAutomaticProtectionSwitching
```

6 Complete the configuration changes. See “Activating configuration changes” (page 25).

Variable definitions

Variable	Value
<a>	The instance number of the *LineAutomaticProtectionSwitching* component. For Passport 15000 or 20000 FPs, the *LineAutomaticProtectionSwitching* instance can be any value between 0 and 15999.
<n>	The logical processor number. It must be the same for both the working line and the protection line.
<p>	The working port number on the logical processor.
<path>	*Sts* or *Vc4*.

(Sheet 1 of 2)

Variable	Value
<port>	*Sonet* or *Sdh*.
<q>	The protecting port number on the logical processor.
<o>	The path number.

(Sheet 2 of 2)

Converting from a non-protected FP to a protected FP with LAPS on Passport 15000 or Passport 20000

Convert a SONET single FP to a protected FP in a dual-FP line APS (LAPS) configuration.

Prerequisites

- The configuration of your node must match the requirements listed in "Nodal requirements for converting line and equipment protection" (page 277)
- If you have configured the *LineAutomaticProtectionSwitching* component, ensure that the FPs use module timing to synchronize with the CP. If the clocking source is not set to module timing, cell loss and corruption could result in some configurations. Refer to "Network clock synchronization configuration" (page 51) for more information on clock configuration.
- See the FP-specific sections in this guide for information on port numbers for line APS protection pairs.

CAUTION
Risk of loss of service by installing line APS protection
Converting from a non-protected single-FP to a protected dual-FP with line APS causes a traffic outage.

Procedure steps

1. Configure the spare FP. See "Configuring a new processor card" (page 78).
2. Add the ports to the LP. See "Configuring ports on an LP" (page 177).
3. Add the *Laps* component.

   ```
   add Laps/<a>7
   ```

4. Add the path component, either *Sts* for Sonet or *Vc4* for Sdh.

   ```
   add Laps/<a> <path>/<o>
   ```

5. Add the atmcell component.

   ```
   add Laps/<a> <path>/<o> atmcell
   ```

6 Link the *Laps* component to the ports on the LP.

```
set atmif/<c> interfacename Laps/<a> <path>/<o>
```

7 Delete the path from the port.

```
Delete Lp/<n> <port>/<p> <path>/0
```

8 Link the *Laps* component to the ports on the LP.

```
set Laps/<a> workingLine Lp/<n> <port>/<p>
```

```
set Laps/<a> protectionLine Lp/<n> <port>/<q>
```

Note: The working line and protection line ports are configured in pairs (for example, port 0 and port 1) and are located on different LPs.

Variable definitions

Variable	Value
<a>	The instance number of the *Laps* component.
<c>	The *atminterface* instance. The *atmif* instance must be between 1 and 4095.
<n>	The LP number. It must be the same for the working and protection lines.
<o>	The path number
<p>	The port number on the working LP; the working line and protection line ports are configured in pairs (for example, port 0 and port 1).
<path>	*Sts* or *Vc4*
<port>	*Sonet* or *Sdh*.
<q>	The port number on the protection LP.

Converting from single-FP to dual-FP protection

Convert a SONET single-FP line APS to a dual-FP line APS configuration.

Prerequisites

- The configuration of your node must match the requirements listed in "Nodal requirements for converting line and equipment protection" (page 277)
- Converting from single-FP line APS to dual-FP line APS causes both FPs to reset.
- See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* for information on port numbers for line APS protection pairs.

Procedure steps

1. Remove the line APS link from one port.

   `Remove Laps/<a> protectionLine Lp/<n> <port>/<q> <path>/0`

2. Replace the line APS link with a link to the other port.

   `Set Laps/<a> protectionLine Lp/<m> <port>/<p> <path>/0`

3. Complete the configuration. See "Activating configuration changes" (page 25).

Variable definitions

Variable	Value
<a>	The instance number of the *Laps* component.
<m>	The LP number of the working line.
<n>	The LP number of the protection line.
<p>	The port number on the working LP; the working line and protection line ports are configured in pairs (for example, port 0 and port 1).
<path>	*Sts* or *Vc4*
<port>	*Sonet* or *Sdh*
<q>	The port number on the protection LP; the working line and protection line ports are configured in pairs (for example, port 0 and port 1).

Configuring Y-protection for dual FPs in a Passport 15000 or 20000

Configure Y-protection for some or all ports of dual FPs in a Passport 15000 or 20000 to spare each other or their port pairs when the far-end interface does not support line automatic protection switching (line APS or LAPS).

Prerequisites

- The cards that are to be configured for Y-protection must be 16-port OC-3/STM-1 POS and ATM FPs with PEC NTHW44 and software name 16pOC3PosAtm. The cards must be installed in adjacent slots with the left one in an even-numbered slot in the range 2 to 14.
- You must configure LAPS for the dual FPs as the start of configuring Y-protection. The SFP modules with PEC NTTP02CD must be installed and the Y-splitter cables must be disconnected before you begin the configuration.
- Decide which port pairs will be configured for LAPS with Y-protection. You must first configure the port pair for LAPS, then alter the configuration to include Y-protection. The procedure includes the steps for the NTHW44 FPs.
- The table “The changes to a LAPS configuration when configuring Y-protection” (page 233) indicates how components of LAPS are the same or different when Y-protection is configured.
- Ensure that you are familiar with the interactions and operational behavior described in “Understanding Y-protection for dual FPs” (page 348).

Procedure

1. Start provisioning.

   ```
   start prov
   ```

2. Add a logical processor type (LPT) and add the *aps* feature to the LPT.

   ```
   add sw lpt/laps fl aps
   ```

3. Set the card type of the two NTHW44 FPs.

   ```
   set shelf card/<n> cardtype 16pOC3PosAtm
   ```

   ```
   set shelf card/<n+1> cardtype 16pOC3PosAtm
   ```

4 Add a logical processor (LP) for each card, and set the main card and LPT.

```
add -s lp/<p> main shelf card/<n>, lpt sw lpt/aps

add -s lp/<q> main shelf card/<n+1>, lpt sw lpt/aps
```

5 Add the SDH components.

```
add lp/<p> sdh/<s>

add lp/<q> sdh/<s>
```

6 Add a small-form pluggable (SFP) optical module for the NTHW44 cards only if it has not already been done for the cards.

```
add lp/<p> sdh/<s> OpticalModule

add lp/<q> sdh/<s> OpticalModule
```

7 Set the type of SFP optical module (om) for each port on both cards.

```
set lp/<p> sdh/<s> om type OC3SmIr
```

Repeat for all 31 ports. Use *OC3SmIr* for each port that is to be configured with Y-protection. Use the other types available to the card as described in “Configuring a port to use an SFP optical module” (page 80).

8 Add the *Laps* component and set the working and protection lines.

```
add laps/<a> working lp/<p> sdh/<s>, protection lp/<q>
sdh/<s>
```

9 Add a *vc4* component.

```
add laps/<a> vc4/<v>
```

10 Set the attribute *protocol* to enable Y-protection. The other attributes will be set automatically to default values that should not be changed by you.

```
set laps/<a> protocol yProtection
```

11 Check, activate, confirm, and save the provisioning (configuring).

```
check prov
activate prov
confirm prov
save -f(fileName) prov
end prov
```

12 Add services to the FPs as required.

Variable definitions

Variable	Value
<a>	The LAPS identifying number.
<fileName>	The user-defined file name to capture the provisioning entries.
<n>	The slot number of the left FP of the dual FP configuration.
<n+1>	The slot number of the right FP of the dual FP configuration.
<p>	The LP number of the main card.
<q>	The LP number of the standby card.
<s>	The SDH identifying number.
<v>	The number of the vc4 component.

Procedure job aid

Table 5
The changes to a LAPS configuration when configuring Y-protection

	LAPS attribute	Description of difference with Y-protection
instance	a pair of spared ports	0 to 15999
provisional attribute	workingLine	links to an SDH or SONET component. It acts as a label of the component to allow switching software to uniquely identify a physical line.
	protectionLine	links to the same SDH or SONET component as attribute *workingLine*. It acts as a label of the component to allow switching software to uniquely identify a physical line.
	Mode	is set to *notApplicable* by the system.
	Revertive	is set to *notApplicable* by the system.
	MimicAps	is set to *notApplicable* by the system.
	holdOffTime	is set to *infinite* by the system because it does not apply to this feature.
	waitToRestorePeriod	is set to *infinite* by the system because it does not apply to this feature.

(Sheet 1 of 3)

Table 5 (continued)
The changes to a LAPS configuration when configuring Y-protection

	LAPS attribute	Description of difference with Y-protection
	signalDegradeRatio	is set to *notApplicable*.
	protocol	can have the following values: • *g841AnnexB* to indicate that optimized one-plus-one bidirectional switching is used as described by ITU-T's G.841 (AnnexB) • *standard* to indicate that one-plus-one line APS is used as described by Telcordia's GR-253 and ITU-T's G.841. • *yProtection* to indicate that LAPS is used only for equipment protection and hitless software migration
	primarySectionMismatch Time	is set to *infinite* by the system because it does not apply to this feature.
operational attribute	nearEndRequest farEndRequest	does not appear when *yProtection* is selected for attribute *protocol*.
	nearEndRequestChannel farEndRequestChannel	does not appear when *yProtection* is selected for attribute *protocol*.
	sdOnLines	does not appear when *yProtection* is selected for attribute *protocol*.
	timeUntilRestore	does not appear when *yProtection* is selected for attribute *protocol*.
	protocolFailureAlarm	does not appear when *yProtection* is selected for attribute *protocol*.
	modeMismatchAlarm	does not appear when *yProtection* is selected for attribute *protocol*.
	nearEndRxActiveLine	indicates which near-end line is actively receiving data from the far end.
	switchovers	applies to *g841AnnexB* and does not appear when *yProtection* is selected for attribute *protocol*.

(Sheet 2 of 3)

Table 5 (continued)
The changes to a LAPS configuration when configuring Y-protection

	LAPS attribute	Description of difference with Y-protection
	primarySection	does not appear when *yProtection* or *standard* is selected for attribute *protocol*.
	primarySectionMismatch Alarm	does not appear when *yProtection* or *standard* is selected for attribute *protocol*.
operational verbs	protectionLockout	does apply when *yProtection* is selected for attribute *protocol*.
	switch	does apply when *yProtection* is selected for attribute *protocol*.

(Sheet 3 of 3)

Locking the protection line on Passport 15000 or Passport 20000

Lock the protection line to prevent the protection line from being used as the active channel. If the protection line is active when *protectionLockout* is issued, the working line becomes active.

Prerequisites

- The verb *protectionLockout* is not supported for Y-protection.

Procedure steps

1 Lock the protection line.

```
protectionLockout Laps/<n>
```

Variable definitions

Variable	Value
<n>	The instance of the *Laps* component.

Switching between the working and protection line on Passport 15000 or Passport 20000

Use the verb *switch* to cause the service active line to switch activity with its standby mate in a working and protection line pair. Use the option *-force* to invoke the changeover with the higher priority *nearEndRequest* value of *forcedSwitch*. When *-force* is not used, the *nearEndRequest* value is the lower priority *manualSwitch*.

Prerequisites

- You can issue the command *switch* when the *Laps* component is locked or unlocked.
- You must use the option *-force* when the provisioned *protocol* is g841AnnexB. The ITU-T G.841 Annex B standard does not support the manual command. This protocol is currently supported only on 16pOc3SmIrAtm (with PEC NTHW24).
- The verb *switch* is not supported for Y-protection.

Procedure steps

1 Switch between the working and protection lines.

```
switch [-force] -protectionToWorking Laps/<n>
```

Variable definitions

Variable	Value
<n>	The instance of the *Laps* component.

Clearing switch requests on Passport 15000 or Passport 20000

Clear the following *nearEndRequest* values: lockoutOfProtection, forcedSwitch, or manualSwitch.

Prerequisites

- The verb *clear* is not supported for Y-protection.

Procedure steps

1 Use the command *clear* to clear switch requests.

```
clear Laps/<n>
```

Variable definitions

Variable	Value
<n>	The instance of the *Laps* component.

Chapter 15
Hitless services on Passport

A service is hitless when the software that provides the service can run uninterrupted, even when the hardware providing the service fails. This is done by having a standby instance of the software running synchronized with the active instance of the software.

This section describes the following topics about hitless services:

Types of services

With Passport, applications and features fall into three categories with respect to equipment protection:

- hot standby
- warm standby
- cold standby

Hot standby applications operate with the standby instance synchronized with the active instance of the software. Hot standby applications and features use equipment protection for electrical function processors (FP) and line and equipment protection for optical FPs to offer hitless services. During an equipment switchover, hot standby applications incur a minimal traffic interruption and established connections stay up. For electrical FPs, a service

is considered hitless if the traffic interruption is less than 100 milliseconds. For optical FPs, a service is considered hitless if the traffic interruption is less than 50 milliseconds.

Warm standby applications operate with the standby instance provisioned but not synchronized with the active instance of the software. During an equipment switchover, warm standby applications incur a longer outage of service than hot standby applications, but not as long as cold standby applications. As well, all connections must be re-established.

Cold standby applications operate with a standby instance that is not synchronized with the active instance of the software. During an equipment switchover, cold standby applications incur longer outages than hot standby and warm standby applications and all connections must be reestablished. By definition, cold standby applications cannot offer hitless services.

Warm standby applications can co-exist with hot standby applications and instances on a logical processor (LP). Although you can create a logical processor type (LPT) that mixes cold standby features with hot standby or warm standby features, Nortel Networks does not recommend this action. A single cold standby application or feature in an LP changes all other applications and features to cold standby.

See “Hot standby applications and features” (page 240) and “Warm standby applications and features” (page 242) for a list of hot and warm standby applications and features as they apply to hitless services. Any application or feature that is not listed in “Hot standby applications and features” (page 240) or “Warm standby applications and features” (page 242) is a cold standby application or feature.

Table 6
Hot standby applications and features

Application	Feature
atmBearerService	atmBearerService
(Sheet 1 of 2)	

Table 6 (continued)
Hot standby applications and features

Application	Feature
base	aal1Ces for the 4-port OC-3/STM-1Ch TDM/ CES FP (NTHW70) aps atmCore
atmNetworking	atmIisp atmPnni atmUni
aal1Ces	aal1Ces
pvg	vgsAtm vgsAtmDc vgsAtmG729 vgsIp vgsIpG729
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. The HEP and HSM are only supported for voice services processor 2 (VSP2) (NTHW87), voice services processor 3 (VSP3) (NTHW84), or voice services processor 3 with optical TDM interface (VSP3-o) (NTHW77) FP cards, and 4-port OC-3/STM-1Ch TDM/CES FP cards. The 1 + 1 sparing configuration of VSP3-o FP cards requires the VSP3-o FP cards to be in adjacent slots where the lower slot number is an even number. Application pvg is only hitless when used in conjunction with application aal1Ces (but not vice versa).	
(Sheet 2 of 2)	

Table 7
Warm standby applications and features

Application	Feature
base	aal1Ces for the 4-port DS3Ch AAL1 CES and the 2-port STM-1e channelized CES/ATM/IMA FPs (NTHR91 & NTNQ91)
	imaAtmForum for the 2-port STM-1e channelized CES/ATM/IMA FP (NTNQ91)
Note: LAN applications are considered warm standby.	
atmNetworking	atmApi dprsMcsEp dprsMcsEpIntercept porsApi routingGateway
callRedirection	callRedirection
frameRelay	frameRelayAtm frameRelayAtmNiwf frameRelayAtmIsdn frameRelayDte frameRelayNni frameRelayUni frameRelayUniPvcSvc frf5EndPoint frsVirtualFramer frUniIpOptimized ppp
huntGroupSystem	huntGroupSystem
ip	ip
(Sheet 1 of 2)	

Table 7 (continued)
Warm standby applications and features

Application	Feature
networking	callServer dpnRouting ipiFr
ServiceTrace	frameRelayNniTrace frameRelayUniTrace atmUniTrace atmIispTrace atmPnniTrace atmAiniTrace frTraceRcvr x25TraceRcvr frAtmTraceRcvr atmTraceRcvr
trunks	atmTrunks porsTrunks
WanDte	LocalMedia AtmMpe
(Sheet 2 of 2)	

Hitless services minimize the interruption of cell forwarding only. During an FP switchover, all applications that were running on the FP can lose administrative data even if it is a hot standby or a warm standby application. Specifically, the following types of data are lost:

- unspooled statistics that resided on the failed FP, such as cell counts
- partial accounting records and any accounting records that reside in the memory of the FP before the FP switchover
- the OSI state (A service that is locked before the FP switchover becomes unlocked after the switchover.)

As well, hitless services do not guarantee that there are no service outages. See “Critical components and attributes” (page 244) for details.

Critical components and attributes

Service outages can occur when you change the value of some critical attributes. Depending on the component and the critical attribute, the service outage can affect an entire shelf, a pair of FPs, a single ATM interface, a single ATM PVC or non-stable calls (calls in the process of being set up).

See the following tables for a list of critical components and attributes:

- “Shelf critical components and attributes” (page 244)
- “FP Pair critical components and attributes” (page 245)
- “ATM interface critical components and attributes” (page 246)
- “ATM PVC critical components and attributes” (page 247)
- “Non-stable call critical components and attributes” (page 247)

Table 8
Shelf critical components and attributes

Component	attribute
Software (Sw)	avList (see Note)
LogicalProcessorType (Lpt)	featureList (see Note)
Card	cardType (see Note)
Module (Mod)	all attributes except for regionID
(Sheet 1 of 2)	

Table 8 (continued)
Shelf critical components and attributes

Component	attribute
Routing DpnAddressPlan (Rtg Dpn)	logicalNetworkNumber
	routingId
	moduleId
	porsTrunks
	unackTrunks
Note: These attributes cause a service outage for the entire shelf if the software configuration of the control processor is changed such that the system cannot incrementally load new software.	
(Sheet 2 of 2)	

Table 9
FP Pair critical components and attributes

Component	attribute
Software (Sw)	avList (see Note)
LogicalProcessorType (Lpt)	featureList (see Note)
Card	cardType (see Note)
Lp Eng Arc Ov	all attributes
Lp Eng Arc Cqc Ov	all attributes
Lp Eng Arc Apc Ov	all attributes
Lp Eng Arc Aqm Ov	all attributes
Lp Eng Arc Fcrc Ov	all attributes
Lp Eng Arc Fcrc Pqc Ov	all attributes
Lp Eng Fcrc Pqc Ov	ipRoutesPoolCapacity
Note: These attributes cause a service outage for the entire shelf if the LP's software configuration is changed such that the system cannot incrementally load new software.	

Table 10
ATM interface critical components and attributes

Component	attribute
Lp Sonet	ifIndex
Lp Sonet Sts	concatNumber
	ifIndex
Laps	workingLine
	protectionLine
	mimicAps
Laps Sts	concatNumber
	ifIndex
AtmInterface (AtmIf)	interfaceName
	oamSegmentBoundary
	maxVpiBits
	minimumBandwidthGuarantee
	txCellMemory
AtmIf Ca	all attributes except for bandwidthPool
AtmIf Ca Ubr	all attributes except for maxVpcs, maxVpts, maxVccs, maxCtd, and cdv
AtmIf Ca Cbr	all attributes except maxCtd and cdv
AtmIf Ca RtVbr	all attributes except maxCtd and cdv
AtmIf Ca NrtVbr	all attributes except maxCtd and cdv
AtmIf ConnMap Ov	all attributes
AtmIf Uni	version
	side
	interfaceType
(Sheet 1 of 2)	

Table 10 (continued)
ATM interface critical components and attributes

Component	attribute
AtmIf Uni Ilmi	vci
	operatingMode
AtmIf Uni Sig	vci
AtmIf Uni Sig Vcd	all attributes
AtmIf Pnni Sig	vci
AtmIf Pnni Rcc	vci
	helloHoldDown
	helloInterval
	helloInactivityFactor
AtmIf Ep	minimumBandwidthGuarentee
AtmIf Vpt Ca Ubr	all attributes except for maxVccs
(Sheet 2 of 2)	

Table 11
ATM PVC critical components and attributes

Component	attribute
AtmIf Vcc Nrp	all attributes
AtmIf Vcc Vcd	mCastConnectionType
AtmIf Vcc Vcd Tm	all attributes

Table 12
Non-stable call critical components and attributes

Component	attribute
Artg Pnni	nodeAddressPrefix
	domain
(Sheet 1 of 2)	

Table 12 (continued)
Non-stable call critical components and attributes

Component	attribute
Artg Pnni CfgNode	nodeId
	peerGroupId
	restrictTransit
(Sheet 2 of 2)	

Chapter 16
Maintenance monitor configuration

Configure maintenance monitor software so that you can add a non-intrusive monitor to the ingress and egress data flow of a single channel on a port on a 32-port MSA FP. Once configured, you can activate the system remotely.

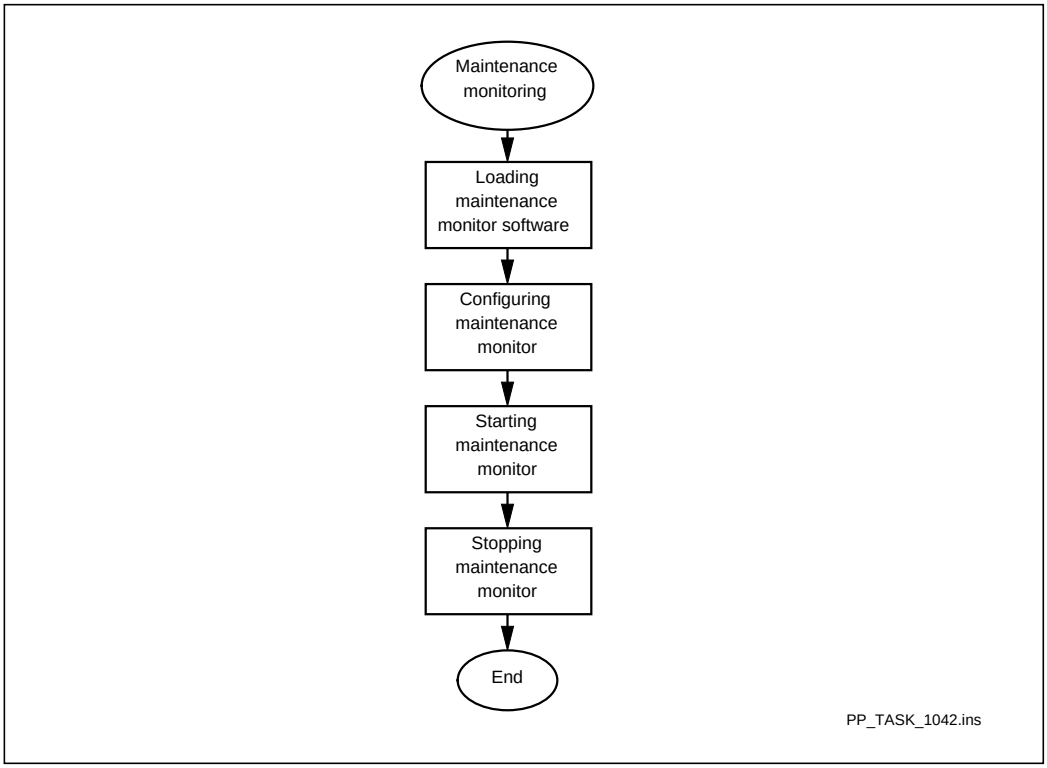
Navigation links

- “Maintenance monitor configuration task flow” (page 249)
- “Maintenance monitor configuration supporting information” (page 256)

Maintenance monitor configuration task flow

This task flow shows you the sequence of procedures you perform to configure and activate maintenance monitor software. To link to any procedure, go to “Task navigation” (page 250).

Figure 10
Maintenance monitor configuration task flow



Task navigation

- “Loading maintenance monitor software” (page 251)
- “Configuring maintenance monitor” (page 252)
- “Starting maintenance monitor” (page 254)
- “Stopping maintenance monitor” (page 255)

Loading maintenance monitor software

Load maintenance monitor software onto a node to enable an operator to configure the software.

Prerequisites

- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Activate the software package.

```
set sw avl aa11ces_<version>
```

```
set sw avl atmNetworking_<version>
```

2 Define the feature list.

```
set sw lpt/<lpt_name> featureList maintMon
```

3 Activate and confirm the provisioning changes.

```
activate prov
confirm prov
```

Variable definitions

Variable	Value
<lpt_name>	The name of the logical processor type.
<version>	The version number of the software being loaded.

Configuring maintenance monitor

Configure maintenance monitor software to enable the system to monitor a specific channel on a 32-port MSA FP.

Prerequisites

- Ensure that the channel you want to monitor is provisioned and operating with either an ATM, AAL1 CES or frame relay service.
- Set up an ATM virtual channel connection with a nailed-up end point on the port where the remote receiver is connected.
- Perform the following procedure in provisioning mode. For more information, see “Provisioning mode” (page 24).

Procedure steps

1 Add a *MaintenanceMonitorTx* component.

```
add Mmtx/<n>
```

2 Link the *MaintenanceMonitorTx* component to the LP containing the channel to be monitored.

```
set Mmtx/<n> lpName Lp/<lp>
```

A separate instance of the *MaintenanceMonitorTx* component is required for each monitored channel. Only one instance of the *MaintenanceMonitorTx* component can be linked to a particular LP.

3 Specify the traffic flow of the channel to be monitored.

```
set Mmtx/<n> direction <dir>
```

4 Add a *NailedUpAdaptationPoint* subcomponent to the *MaintenanceMonitorTx* component.

```
add Mmtx/<n> Nap
```

5 Link the *NailedUpAdaptationPoint* subcomponent to the ATM virtual channel connection to the port where the remote receiver is connected.

```
add Mmtx/<n> Nap atmConnection AtmIf/<m> Vcc/
<vpi>.<vci> Nep
```

6 Activate and confirm the provisioning changes.

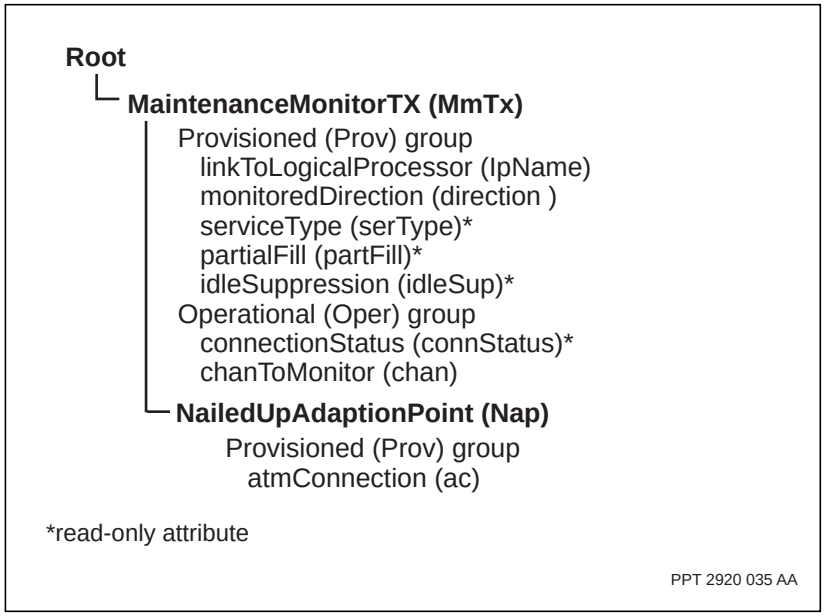
```
activate prov
confirm prov
```

Variable definitions

Variable	Value
<dir>	*ingress* or *egress*. With ingress, the traffic going into the channel is monitored. With egress, the traffic going out of the channel is monitored.
<lp>	The LP containing the channel you want to monitor.
<m>	The ATM interface with the port where the remote receiver is connected.
<n>	The instance number of the MaintenanceMonitorTX component.
<vpi.vci>	Identifies the virtual channel connection to the port where the remote receiver is connected.

Procedure job aid

Figure 11
Maintenance monitor component hierarchy



Starting maintenance monitor

Start the maintenance monitor whenever you want to start monitoring the data on a specific channel.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Use the *chanToMonitor* attribute of the maintenance monitor to specify which LP, port and channel to monitor.

```
set Mmtx/<n> chan Lp/<lp> DS1/<x> Chan/<y>
```

Variable definitions

Variable	Value
<lp>	The LP containing the channel you want to monitor. The value must be the same as the one specified in “Configuring maintenance monitor” (page 252). The specified channel must be linked by provisioning to an ATM interface, a frame relay interface, or a structured AAL1 CES interface.
<n>	The instance number of the *MaintenanceMonitorTX* component.
<x>	The instance number of the port containing the channel you want to monitor.
<y>	The instance number of the channel you want to monitor.

Stopping maintenance monitor

Stop maintenance monitor after you have gathered sufficient data from the channel.

Prerequisites

- Perform the following procedure in operational mode. For more information, see “Operational mode” (page 24).

Procedure steps

1 Clear the *chanToMonitor* attribute of the maintenance monitor.

```
set Mmtx/<n> chan !
```

Variable definitions

Variable	Value
<n>	The instance number of the *MaintenanceMonitorTX* component.

Maintenance monitor configuration supporting information

The maintenance monitor can monitor the following types of channels:

- ATM
- frame relay
- basic structured AAL1 CES

The maintenance monitor software directs the data flow as a basic structured ATM adaptation layer 1 (AAL1) circuit emulation service (CES) by means of an ATM PVC. The output AAL1 CES data stream can be directed to a local port, or to a remote port. The remote port can be located anywhere in the network that supports CES.

The following limitations apply:

- Each FP allows you to monitor only one ingress and one egress channel. The FPs that support monitoring have monitor ports labeled on their faceplates, as shown in the FP and sparing panel descriptions in 241-1501-200 *Passport 15000, 20000 Hardware Description*.
- The maintenance monitor does not carry DS1 and E1 framing or channel associated signaling (CAS) information.
- Multiport ATM IMA services cannot be monitored.

The figure “Maintenance monitor component hierarchy” (page 253) shows the maintenance monitor components and attributes that you can provision.

Chapter 17
Passport configuration concepts

This section contains reference information that supports the procedures in this guide. The following topics are included:

Passport system overview

Passport is capable of running a number of different communication services. For these services to run properly, you must configure and maintain the basic system.

Every Passport node has a shelf, a fabric card or a bus, and a number of processor cards (*Shelf*, *FabricCard* or *Bus*, and *Card* components). The shelf holds the processor cards and the fabric card or bus. The bus or fabric card allows the processor cards to communicate with the other processor cards on the shelf.

Passport has two types of processor cards: control processors (CP) and function processors (FP). A CP manages the FPs and provides basic system capabilities. An FP provides communication connections and services.

Logical processors (*LogicalProcessor* component) represent the software on a processor card that delivers one or more Passport services or capabilities. A logical processor also represents the ports and the channels of the processor card. Logical processors allow you to map software to processor cards. Logical processors also support the configuration of a spare processor card to take over in case of the failure of the main processor card.

Software and configuration files are stored on the Passport file system (*FileSystem* component). The file system consists of up to two disks (*Disk* component): one on the main CP and another on the spare CP.

The data collection system (*Collector* component) collects the data generated for troubleshooting, performance tuning, and billing. In most cases, this data is transferred to an external network management system for analysis.

Understanding CP equipment sparing

Before setting up sparing between processor cards, check the product equipment codes (PECs) of the active and spare cards. For CPs, the first six digits must match and the cards must have the same amount of memory and disk space.

The StartUp utility configures the main CP when you initially set up the node. You can also configure a spare CP using the StartUp utility. For more information, see 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*. You can also manually configure CP equipment sparing by configuring a spare CP.

> ***Note:*** When you connect both the Ethernet ports on a two-CP node through a hub or IP router, your Preside Multiservice Data Manager connectivity is also spared. In order to quickly resume the OAM Ethernet connectivity after the spare CP becomes active, direct hub or IP router sparing is required for both the active and standby CP OAM Ethernet ports.

The CP currently running the node is the active CP. The other CP is the standby CP. At any given time, either the main or the spare CP can be the active CP.

A CP switchover occurs when the active CP gives control of the node to the standby CP and the standby CP becomes the newly active CP.

There are two types of CP switchovers: automatic and manual. An automatic CP switchover occurs when the active CP resets or restarts, either due to a hardware problem or an inappropriate operator command. A manual CP switchover occurs as a result of the *switchover lp/0* command. A manual CP switchover allows the active CP to gracefully transfer control of the node to the standby CP.

> ***Note:*** After an automatic CP switchover, if the former active CP recovers, the system does not automatically switch back to the original active CP. You can cause the system to switch back to the original active CP by doing a manual CP switchover with the *switchover lp/0* command.

For information on the *switchover* command, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

There are two modes of CP equipment sparing: cold standby and hot standby. In cold standby, all function processors (FP) must restart when the CP switchover occurs. In hot standby, FPs that support this mode of operation continue running uninterrupted when the CP switchover occurs.

Note: OSI standards use different terminology when referring to CP standby modes. When you display the *standbyStatus* attribute for the CP logical processor (Lp/0), it reports *providingService* for the active CP and *coldStandby* for the standby CP. In this context, the term *coldStandby* refers to Passport 15000 or 20000 hitless services and not to CP equipment sparing. The term *coldStandby* appears independently of whether CP equipment sparing is in cold standby mode or hot standby mode. See “Hitless services on Passport” (page 239) for more details.

CAUTION
Risk of damage to the CP
Do not remove the active CP from the shelf as a way of simulating active CP failure.

To test the behavior of hot standby CP redundancy under CP failure conditions, use the *restart lp/0* command or the *reset lp/0* command.

For information on CP sparing, see the following sections:

CP standby states

There are three CP standby states when CP equipment protection is enabled (hot): steady-state, synchronizing, and manual synchronization.

In steady state, all standby applications have been created, have had their provisioning data delivered, and are ready to take over should a control processor switchover (CPSO) occur. If a CPSO occurs, then the following events will occur:

- Standby applications on this CP will become active.
- CP applications that are cold will have their provisioning data delivered after all standby applications have been notified to switchover.

  Note: Activating a configuration change will cause the standby CP to go from steady state to synchronizing state. In addition, applications can also cause the system to go from this state to synchronizing state.

There are four main windows in the synchronizing state:

- Provisioning data being delivered to the standby CP applications: If a CPSO occurs in this window, then the standby CP resets and reloads with the committed view. All FPs in the shelf are reset and the CPSO is disabled. Note, that this window is only entered if provisioning data is delivered to the standby CP applications. The length of this window is dependant on amount of configuration changes.
- Hot/warm standby CP applications journaling operational state from active CP: Once the activation finishes on the active CP, then any changed warm or hot standby CP applications need to journal their state between the two CPs. If a single application is not ready for switchover, then a CPSO is degraded. Only those applications that are not synchronized are impacted by the CPSO.
- Loading of configuration delta pending confirm: The standby CP is temporarily unsynchronized until the user issues the confirm prov command. This command will trigger the standby CP to load the configuration delta (next state) and the CPSO is degraded.
- Standby CP provisioning system loading configuration delta.: In order to synchronize to the current view configuration, the standby CP provisioning system loads the current view configuration as represented by the committed view and the journal logs. If a CPSO occurs in this window (and all hot applications are ready for switchover), then there is

no impact to hot or warm applications. The CPSO is degraded, however, since cold CP applications will not have their provisioning data delivered until after loading has finished.

Note: Note that the above windows can overlap, but will typically be quite small, since only the delta configuration needs to be activated, journaled, and loaded.

If the active CP fails after the activation has finished but before the user has confirmed the activation, then the standby CP switches to the just activated view, with the following steps:

- Hot and warm standby CP applications are told to become active.
- The delta configuration (of the last activation) is loaded on the standby CP.
- Cold standby applications are activated.
- The confirm timer is restarted (20 minutes). If the operator does not issue confirm prov within 20 minutes, then the shelf resets to the committed view.

The manual synchronization state is entered if the standby CP is unable to synchronize to the active CP. There are two cases when this occurs:

- The provisioning system was unable to save a journal log file. In order to synchronize the standby CP to the active CP's current view, the delta between the current and edit view is automatically saved by the provisioning system during the activate prov command. If this save fails, then the activation will still proceed, but the standby CP will be unable to resynchronize itself to the new current view. In such a case the standby CP enters an unsynchronized state, and will switch to its last synchronized view if a CPSO occurs.

  If the provisioned configuration of a warm or hot standby CP application is changed while in this state, then a CPSO will result in a switch reset. In addition, any FPs that are not running this last journaled view will also be reset on a CPSO.

- The standby CP becomes active after a software migration or a reload activation to a non committed view occurs, but before the first commit is done. These journal logs are based on the committed view, and therefore require the committed view to be initially equal to the current view. In this case, a CPSO causes a shelf outage.

Considerations for adding a spare CP to a single-CP node

- With Passport 15000 and 20000, the spare CP belongs in slot 1.
- With Passport 7400 series switches, the spare CP always goes in the last slot of the shelf. For example, if you have a 16-slot Passport switch, you must insert the new spare CP in slot 15.
- For all Passport switches, the slot that normally houses the spare CP can house an FP. In this case, the node has only a single CP operating without a spare.
- When you add a spare CP, make sure all eight digits of the PECs for both CPs match. This ensures that the spare CP has the same amount of memory and disk space as the main CP.
- To add a spare CP to a single-CP node, you must configure the spare CP, insert it on the shelf, and synchronize its disk to the active CP.

  Note: A spare CP can provide Preside Multiservice Data Manager connectivity redundancy when Preside Multiservice Data Manager is connected through the OAM Ethernet port of the CPs. For information on configuring the Ethernet port, see "Configuring the CP OAM Ethernet port" (page 153). For information on cabling the Ethernet port, see 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* or 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*.

Automatic CP switchover in cold standby mode

In cold standby mode, all FPs restart when a CP switchover occurs. During the restart, all service connections on all FPs terminate. When the restart is complete, the FPs re-establish the following connections:

- Routing: PNNI, DPRS, and PORS
- Traffic: PVC and SPVC

Requirements for a CP switchover in cold standby mode

All the following requirements must be met for a CP switchover to occur in cold standby mode:

- The standby CP is fault-free.
- The file system is synchronized.

Automatic CP switchover in hot standby mode

When a CP switchover occurs, those FPs configured exclusively with features that support hot standby for CP switchover continue running uninterrupted. If you configure an FP with one or more features that do not support hot standby for CP switchover, it restarts as if it is in cold standby mode.

The table "Applications and features that support hot standby for CP switchover" (page 264) identifies the features that support hot standby. If an application or feature is not listed in this table, then it does not support hot standby mode.

Table 13
Applications and features that support hot standby for CP switchover

Application	Feature
base	aps
	atmCore
atmNetworking	atmAini
	atmEbr
	atmIisp
	atmPnni
	atmUni
aal1Ces	aal1Ces
atmBearerService	atmBearerService
(Sheet 1 of 3)	

Table 13 (continued)
Applications and features that support hot standby for CP switchover

Application	Feature
frameRelay	frameRelayNni
	frameRelayUni
	frameRelayUniPvcSvc
	mpaNetworkLink
ip	ip (see Note 2)
mpls	mplsCrldp (see Note 3)
networking	dpnRouting
trunks	atmTrunks
	dpnTrunks (see Note 1)
	frDpnTrunks
	porsTrunks
	unackTrunks
vtds	bitTransparent
	echoCancellor
	hdlcTransparent
	silenceSuppressor
	vtds
	voice
	voiceCompressor

(Sheet 2 of 3)

Table 13 (continued)
Applications and features that support hot standby for CP switchover

Application	Feature
wanDte	atmMpe (see Note 2)
	frameRelayDte (see Note 2)
Note 1: The dpnTrunks feature on an FP does not cause that FP to restart on CP switchover, but all DPN trunks restage if a CP switchover occurs. The network routes traffic destined for DPN nodes around this node while DPN trunks restage. ***Note 2:*** During a CP switchover, ILS FPs configured with these features reset. The WAN FPs do not reset. However, ILS services on the WAN FPs do reset. ***Note 3:*** MPLS service on the FP are interrupted during a CP switchover, but other services on the FP that support hot standby mode are not interrupted.	
(Sheet 3 of 3)	

There is an internal CP timer that can affect an automatic CP switchover. Refer to “Timeout for a subsequent CP switchover” (page 266).

Timeout for a subsequent CP switchover

After a CP switchover, Passport considers that a second CP switchover within 10 minutes to be an indication of a more serious fault. It attempts to recover from this second CP switchover by a shelf reset, which has more impact on service than a CP switchover. Before executing the *switchover Lp* command, the value of the *revertibleTimerCountdown* attribute, under the Shelf component, must be zero. If you cause a second CP switchover within a 10-minute period, or remove the Ethernet cable from the faceplate of the active CP, the next manual or automatic switchover occurs in cold standby mode (all FPs on the node restart). This behavior prevents Passport from continually switching from the active to the standby CP because of complications from an automatic CP switchover.

> ***Note:*** Passport does not allow you to remove the active CP without first preparing the system. Removing the active CP without due preparation causes unexpected behavior on the bus or fabric and can cause a full shelf reset.

Requirements for a CP switchover in hot standby mode

All the following requirements must be met for a CP switchover to occur in hot standby mode:

- The standby CP is fault-free and has loaded the committed provisioning view.
- The software for hot-standby mode is enabled.
- A software upgrade is not in progress.
- More than 10 minutes has elapsed since the completion of the last CP switchover. You can initiate a manual CP switchover with the switchover lp/0 command within this 10-minute limit. However, after the manual CP switchover, if an automatic CP switchover occurs within 10 minutes, the switchover occurs in cold standby mode (all FPs on the node restart). Refer to “CP switchover operator commands” (page 269).
- The file system is synchronized.

If one or more of these requirements are not met, the CP switchover occurs in cold standby mode; that is, all FPs restart.

Even if all the above requirements are satisfied, individual FPs may not continue providing service during a CP switchover in hot standby node. An FP continues to provide service if all the following requirements are met:

- All features configured on the FP support hot standby mode for CP switchover.
- The configured data loaded on the FP matches that of the newly active CP. For example, if the FP is running uncommitted data and you issue a switchover -force lp/0 command, an FP restart occurs.
- The newly active CP resynchronizes with the FP within approximately 60 seconds. This is required to ensure routing tables are updated correctly and that routing loops do not occur for more than 60 seconds. If the newly active CP cannot resynchronize with the FP within approximately 60 seconds, the FP resets.

If one or more of these requirements are not met, the FP may restart during a CP switchover in hot standby mode.

Effects of a CP switchover

For all CP switchovers (in either cold or hot standby mode), the following common effects occur:

- Network management sessions such as telnet, FTP, and FMIP, terminate, dropping all connections to the active CP. A local network management session on the standby CP does not terminate. However, it is suspended until the CP becomes active.
- Information stored in the edit view is lost unless it was saved on disk.
- Some components that were in the locked state move to the unlocked state. The fabricCard or bus component remains locked if it was locked prior to the switchover.
- The operational attributes of CP-resident components revert to default values.
- All Preside Multiservice Data Manager activities such as provisioning, backup/restore, software download, the FTP connection between MDM and Passport, and performance viewer sessions terminate.
- If you have connected Preside Multiservice Data Manager through the OAM Ethernet port of the CPs, connectivity is lost until the standby CP becomes active.
- New ATM connections cannot be established in FPs until the ATM routing system is available after the switchover. The time to wait highly depends on the network topology, but the wait should not exceed 30 seconds in most cases.
- After the CP switchover, new DPRS forwarding tables must be received by the FPs from the active CP within 3 minutes. Otherwise, DPRS-based frame relay (FR) connections will be cleared.

In addition to the previous common effects, for a CP switchover in cold standby the following occurs:

- All traffic is interrupted until the network routes around the failed node.
- All connections established by the Path Oriented Routing System (PORS) involving this node must be rerouted.
- All existing calls that originate or terminate on the node are interrupted.

- No new calls that originate or terminate on the node are possible until the node recovers.

In addition to the previous common effects, for a CP switchover in hot standby the following occurs:

- There are no network disruptions for most CP switchovers in hot standby mode.
- The existing connections will stay up for most CP switchovers in hot standby mode on FPs that fully support hot standby mode. On Passport 7400 some minor cell loss may occur.
- Call setup is interrupted for less than 30 seconds for most CP switchovers in hot standby mode.

CP switchover operator commands

Entering the *switchover lp/0* command causes a manual CP switchover. This is the only operator command that causes a CP switchover without interrupting calls in progress.

> ***Note:*** An automatic CP switchover cannot occur for 10 minutes after a manual CP switchover. Refer to "Timeout for a subsequent CP switchover" (page 266).

Entering any of the following commands causes an automatic CP switchover:

- reset Shelf Card/<activeCP>
- reset Lp/0
- restart Shelf Card/<activeCP>
- restart Lp/0
- activate Prov (during a software upgrade)
- reload Cp Lp/0 (during a software upgrade)

> ***Note:*** An automatic CP switchover can affect calls that are in progress by causing the shelf to reset.

For more information on these commands, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Understanding equipment protection for Passport electrical interfaces

You can configure electrical function processor (FP) equipment sparing by configuring a spare card and wiring the interfaces of the main and spare card through a sparing panel. The spare card can take over in case the main card fails. This type of equipment sparing uses a single LP to define both the main and spare FP.

The card currently providing service is the active card. The other card is the standby card. At any given time, either the main or the spare card can be the active card. If the active card fails, the standby automatically takes over. The change from the active to standby card is called a switchover. The activity of detecting the failure and performing the switchover temporarily disrupts traffic through the switch. The degree of disruption depends on the level of standby support provided by the services running on the cards, for example hot, warm, and cold. See “Hitless services on Passport” (page 239).

Different types of FPs support different types of equipment sparing. Some FPs support one-for-one sparing, and some FPs support both one-for-one and one-for-*n* sparing. Some FPs do not support any type of equipment sparing. For information about the sparing capabilities of a specific FP, see 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Before setting up sparing between processor cards, check the product equipment codes (PECs) of the active and spare cards. For FPs, the first six digits (four letters and two numbers) must match.

For MSA32 FP sparing, electrical interfaces are protected intercard (electrical sparing protection) while optical interfaces are protected intracard (APS line protection). Regardless of either PEC or card type:

- DS1 FPs can only spare other DS1 FPs and only for electrical interfaces
- E1 FPs can only spare other E1 FPs and only for electrical interfaces

Note: Some Passport 7400 processor cards have equivalent PECs. See 241-7401-200 *Passport 7400 Hardware Description* for a list of equivalent PECs. Except where noted, processor cards with equivalent PECs can be used as spares for each other.

For information on installing and connecting FPs, termination panels, and sparing panels, see 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* or 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*.

See these sections about the different types of FP equipment sparing:

- "One-for-one equipment sparing" (page 271)
- "One-for-n equipment sparing" (page 271)
- "Switching from the spare FP back to the main FP" (page 273)

One-for-one equipment sparing

In one-for-one sparing, a single spare FP acts as a backup for a single main FP. Some FPs on the Passport 7400 series switch support one-for-one equipment sparing using a one-for-one sparing panel to terminate the cable connections of two FPs. One FP is active while the second FP of the same type operates as a standby in case of failure. Some FPs support one-for-one sparing without using a sparing panel, for example, lan-based cards.

When an active (main) FP connected to a one-for-one sparing panel fails, all traffic is switched to the standby (spare) FP. When the main FP recovers, it comes up as the new standby. Traffic reverts from the spare FP back to the main FP if the active (spare) FP fails or you issue the switchover command and the recovered (main) FP is running as standby.

In a one-for-one sparing configuration, hot standby services are hitless.

To configure one-for-one electrical interface FP sparing for Passport 7400, see "Configuring a new processor card" (page 78).

One-for-n equipment sparing

One-for-n equipment sparing enables you to protect multiple main FPs with a single spare FP. All FPs must be of the same type and vintage.

In one-for-n sparing on a Passport 7400 series switch, a single FP acts as a backup for up to four main FPs. In one-for-n sparing on a Passport 15000 or 20000 switch, a single FP acts as a backup for up to six main FPs. In a one-for-n sparing configuration, you must configure *n* logical processors (LP) to point to the same spare FP. The includes the FPs connected to any 32-port

multi-service access (MSA32) sparing panel. For information about configuring LPs, see “Logical processor, port, and channel configuration tasks” (page 163).

In a one-for-n sparing configuration, hot standby services are not hitless.

One-for-n equipment sparing requires the use of a separate one-for-n sparing panel. For information about the termination or sparing panels supported by a specific FP, see 241-1501-200 *Passport 15000, 20000 Hardware Description* or 241-7401-200 *Passport 7400 Hardware Description*. For information about installing a sparing panel, see 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* or 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*.

When a main FP connected to a one-for-n sparing panel fails, the control processor (CP) identifies which main FP has failed. The CP then instructs the failed FP to restart and starts a sparing timer. If the main FP does not restart by the time the sparing timer expires, traffic switches to the spare FP.

If the main FP restarts before the sparing timer expires, traffic does not switch to the spare. However, if the FP fails again within a specified stability period, traffic immediately switches to the spare FP. The CP then instructs the main FP to come up in standby mode.

If the main FP fails to come up in standby mode after three restarts, the CP places the failed FP into a rejected state. You need to replace the FPs that are in a rejected state.

When the spare FP is in use, all the other main FPs are not protected. If a spare FP fails and recovers while there are many main FP failures, the spare always carries the traffic of the FP with the lowest LP number.

To configure electrical interface FP sparing for Passport, see “Passport electrical interface equipment protection configuration” (page 205).

Immediate switchover to spare for one-for-n sparing

By default, the system delays a switchover to the spare FP when an active main FP fails. By changing the setting for the *oneForNSparingBehavior* attribute, you can configure the system to allow an immediate switchover to occur. To configure this behavior see "Passport electrical interface equipment protection configuration" (page 205).

Switching from the spare FP back to the main FP

You can use the *switchover Lp* command to switch traffic back to a main FP if you have replaced a failed main FP and a failed main FP has restarted and is in standby mode.

If you have scheduled a switchover from a spare FP back to a main FP and another main FP fails, the CP forces the switchover and spares the failed FP.

For information on performing a switchover, see "Switching between active and standby processor cards" (page 110). For information on the *switchover* command, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Manual FP switchover

Entering any of the following commands causes a manual switchover:

- switchover Lp/<activeFP>
- reset Shelf Card/<activeFP>
- reset Lp/<activeFP>
- restart Shelf Card/<activeFP>
- restart Lp/<activeFP>
- lock -force Lp/<activeFP>
- lock -force Shelf Card/<activeFP>

CAUTION
Data loss may occur
When you reset or restart a processor it is temporarily unable to provide service. During the time the processor is restarting, data can be lost.

CAUTION

Loss of stable SVC connections may occur

When you reset or restart a processor card, a loss of SVC connections may occur. Although stable SVC calls should remain active in a redundant processor configuration, exercise caution when issuing this command.

For more information on these commands, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

You cannot perform a manual switchover if

- there is no standby control processor (CP) or the standby CP is not operational
- a software upgrade is in progress

Understanding line and equipment protection for Passport 15000 or 20000 optical interfaces

Line automatic protection switching (line APS or LAPS) on a Passport 15000 or 20000 node extends the line APS functionality available from Passport 7400 series nodes.

Both single-FP APS and dual-FP APS on a Passport 15000 and 20000 node offer:

- revertive and non-revertive switching schemes
- unidirectional and bidirectional operating modes

The defaults are the same as for Passport 7400 series nodes. See “Understanding line protection for Passport 7400 optical interfaces” (page 279).

Line APS on a Passport 15000 and 20000 node uses:

- a logical processor (LP) to define the main port where a service runs
- a second LP to define a spare port where the service runs if the FP containing the main port fails.

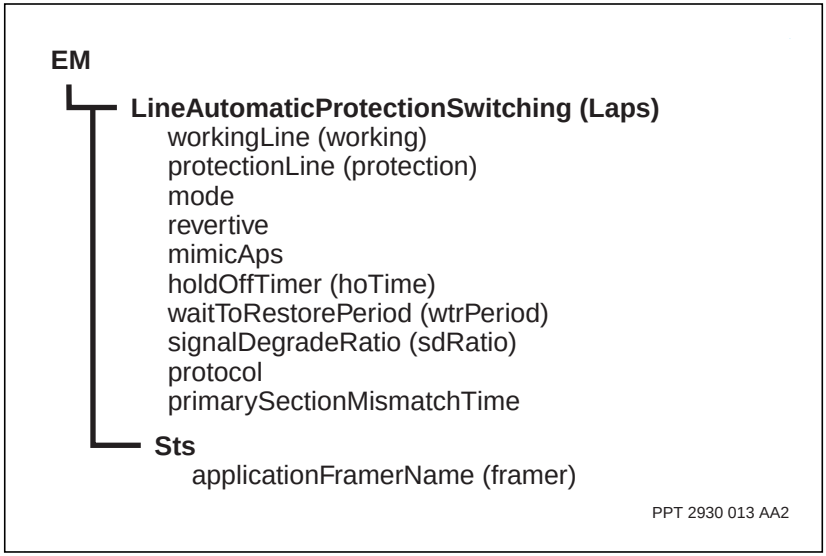
- SONET line automatic protection switching (line APS) to link the ports from both LPs

For Passport 15000 and 20000 switches, line APS:

- is implemented using the *LineAutomaticProtectionSwitching (Laps)* component
- applies to predetermined pairs of ports on a single FP to provide the same level of functionality as with Passport 7400 series nodes. This is called single-FP APS
- can also apply to predetermined pairs of ports on a pair of FPs. This is called dual-FP APS. This configuration specifies both line and equipment protection

The figure "LAPS components and attributes" (page 275) illustrates the components and attributes of the *Laps* component.

Figure 12
LAPS components and attributes



The following sections contain information about line APS for Passport 15000 and 20000 optical interfaces:

Switch requirements for configuring line and equipment protection for Passport 15000 or 20000 optical interfaces

Ensure the following prerequisites exist for line APS and equipment sparing on optical FPs on Passport 15000 or 20000 switches:

- The main port that runs the service must have a spare port on a separate FP.
- Both FPs must be in adjacent card slots. One FP must be located in an even-numbered card slot, other than slot 0. The other FPFP must be located in the next higher odd-numbered card slot. For example, if the one FP is in card slot 4, the other FP must be in card slot 5.
- A port is always paired with its matching port on the other FP. For example, FP4 port 0 is paired with FP5 port 0, while FP4 port 1 is paired with FP5 port 1.
- FPs with spared port-pairs can run other services on their other ports. The other services can be spared, or unspared. The other services can be hitless or not.
- Ensure the first LP of the port on the working line is set up.

- The working and protection lines should be synchronized with the same timing source to make sure there is no service impact during equipment or line switchovers.
- Ensure the second LP of the port on the protection line is set up.

  Note: Some services are no longer hitless when combined with other services on the same FP. See “Hitless services on Passport” (page 239) for details.

CAUTION
Risk of loss of service by improper timing source
Ports configured for equipment protection/dual FP APS should use the same timing source to make sure there is no service impact during equipment or line switchovers. This can be accomplished by using the module clock as the port’s clocking source.

For more information about choosing the location of FPs in a Passport 15000 or 20000 switch, see 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade*.

Nodal requirements for converting line and equipment protection

When converting line and equipment protection, the following assumptions about the configuration of the node exist:

- An interface, for example, AtmIf is already implemented and uses single FP.
- The main port that runs the service must have a spare port on a separate FP.
- Both FPs must be in adjacent card slots. One FP must be located in an even-numbered card slot, other than slot 0. The other FP must be located in the next higher odd-numbered card slot. For example, if the one FP is in card slot 4, the other FP must be in card slot 5.
- A port is always paired with its matching port on the other FP. For example, FP4 port 0 is paired with FP5 port 0, while FP4 port 1 is paired with FP5 port 1.

- FPs with spared port-pairs can run other services on their other ports. The other services can be spared, or unspared. The other services can be hitless or not.
- The bidirectional mode applies and can be configured. See "Passport 15000 or 20000 optical interface line and equipment protection configuration" (page 219).
- The revertive mode applies and can be configured. See "Passport 15000 or 20000 optical interface line and equipment protection configuration" (page 219).

For more information about choosing the location of FPs in a Passport 15000 or 20000 switch, see 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade*.

Working line on Passport 15000 or 20000 optical interfaces

The *workingLine* attribute of the *Laps* component specifies which line of an APS pair does not carry overhead signals that specify which line passes traffic to the Passport 15000 or 20000 fabric. In single-FP and dual-FP line APS, the working line can be the active line, or the standby line.

For information on how to configure the *workingLine* attribute, see 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Protection line on Passport 15000 or 20000 optical interfaces

The *protectionLine* attribute of the *Laps* component specifies which line of an APS pair carries overhead signals that specify which line passes traffic to the Passport 15000 or 20000 fabric. In single-FP and dual-FP line APS, the protection line can be the active line, or the standby line.

For information on how to configure the *protectionLine* attribute, see 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Revertive and non-revertive switching on Passport 15000 or 20000 optical interfaces

The *revertive* attribute of the *Laps* component is similar to the *revertive* attribute of the *Aps* component used by Passport 7400 series nodes. See "Revertive and non-revertive switching on Passport 7400 optical interfaces" (page 281) for details.

For information on how to configure the *revertive* attribute, see 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Unidirectional and bidirectional mode on Passport 15000 or 20000 optical interfaces

The *mode* attribute of the *Laps* component is similar to the *mode* attribute of the *Aps* component used by Passport 7400 series nodes. See “Unidirectional and bidirectional mode on Passport 7400 optical interfaces” (page 281) for details.

For information on how to configure the *mode* attribute, see 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Understanding line protection for Passport 7400 optical interfaces

Line automatic protection switching (line APS) is a standards-defined feature enabling a form of SONET line sparing on optical FPs. Under line APS, two lines are defined: working and protection. While both lines carry the user payload, only one is deemed active at any time. The active line is the line where the receiving end takes its data.

When the working line is active, the protection line operates as a backup. Line failure, signal degradation or an operator command can cause the active line to switch from working to protection.

Line APS standards define two switching schemes: revertive and non-revertive. Revertive switching causes the active channel to revert to the designated working line when the condition causing the switchover is cleared. Non-revertive switching allows the protection line to remain active until the criteria for a switchover are met and an operator issues a manual switchover. The non-revertive scheme is the default for optical FPs.

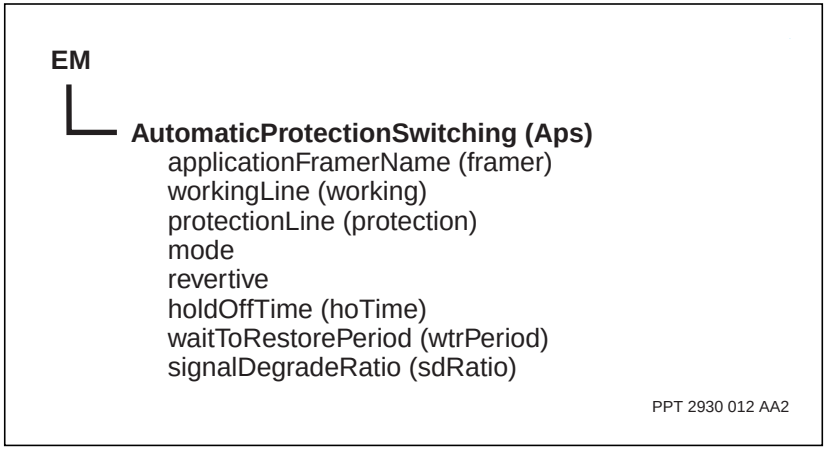
A line APS system can operate in either unidirectional mode or bidirectional mode. In unidirectional mode, each end decides independently the line it receives data from. In bidirectional mode, the two ends negotiate to determine the active line. Unidirectional mode is the default.

For Passport 7400 series switches, line APS:

- is implemented using the AutomaticProtectionSwitching (Aps) component
- applies to predetermined pairs of ports on a single FP. This is called single-FP APS.

The figure “APS components and attributes” (page 280) illustrates the components and attributes of the *Aps* component.

Figure 13
APS components and attributes



See the following sections for a description of Line APS for Passport 7400 optical interfaces:

- “Working line on Passport 7400 optical interfaces” (page 281)
- “Protection line on Passport 7400 optical interfaces” (page 281)
- “Revertive and non-revertive switching on Passport 7400 optical interfaces” (page 281)
- “Unidirectional and bidirectional mode on Passport 7400 optical interfaces” (page 281)

Working line on Passport 7400 optical interfaces

The *workingLine* attribute is used to designate one line as the working line. Like the protection line, the working line always carries a full user payload. The working line can be active, or it can operate as a backup to the protection line.

For information on how to configure the working line, see 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Protection line on Passport 7400 optical interfaces

The *protectionLine* attribute is used to designate one line as the protection line. Like the working line, the protection line always carries a full user payload. The protection line can be active, or it can operate as a backup to the working line.

For information on how to configure the protection line, see 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Revertive and non-revertive switching on Passport 7400 optical interfaces

The *revertive* attribute defines the switching scheme in use for line APS. There are two switching schemes: revertive and non-revertive. Under revertive switching, the working line resumes being the active line once any condition causing a switchover is cleared, and the time configured in the *waitToRestore* attribute expires. Under non-revertive switching, the protection line remains active until conditions warrant a switchover back to the working line. The default scheme is non-revertive.

For information on how to configure the *revertive* attribute, see 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Unidirectional and bidirectional mode on Passport 7400 optical interfaces

The *mode* attribute sets the conditions for each end of a connection to determine where it receives the user payload. In unidirectional mode, each end unilaterally decides the line it receives data from. In bidirectional mode,

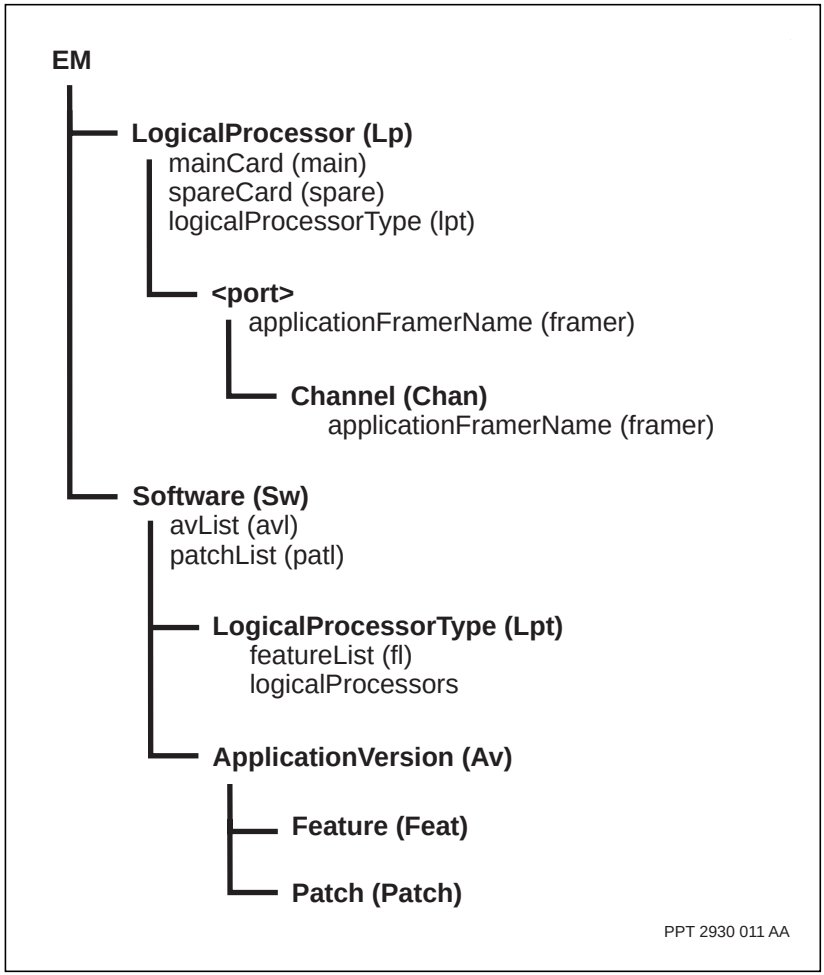
each end confers with the other in to decide the line it receives data from. Bidirectional mode must be configured at both ends to be operational. Unidirectional mode is the default.

For information on how to configure the *mode* attribute, see 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Understanding logical processors, ports, and channels

An LP represents the software on a processor card that delivers one or more Passport services or capabilities. An LP also represents the ports and the channels of the processor card. Because the LP is a logical entity, you can map it to any processor card to suit the Passport configuration. The figure "LP components and attributes" (page 283) illustrates the components and attributes that define an LP.

Figure 14
LP components and attributes



Function processor and control processor sparing uses LPs to define the processor software and configuration regardless of whether the main or spare processor is currently active.

For more information on LPs, see the following sections:

- “Ports and channels” (page 284)

Ports and channels

For each LP, you must configure the ports that exist on the processor card. Subcomponents of the *LogicalProcessor* (Lp) component represent the ports and have a name that corresponds to the port type. For example, *DS1* components represent DS1 ports. The number of ports you define (instances of the port component) must correspond to the actual number of ports on the processor card.

For example, if you create an LP for a V.35 processor card, you add eight *V35* subcomponents (numbered 0 to 7) to the *Lp* component to represent each of the eight ports on the processor card.

Some processor cards can also have channels on their ports. If you are configuring an LP for a channelized port, you have to add *Channel* subcomponents to the *port* component. For example, on a DS1C card you can add between 1 and 24 *Channel* components (numbered 0 to 23) under each of its four DS1 *port* components (numbered 0 to 4).

After you define the ports and channels of an LP, you can link them to the service that you want to run on that port or channel. You create the link by setting the *applicationFramerName* (*framer*) attribute of the port or channel to the *Framer* component for the service.

For example, if you want to run an unacknowledged Passport trunk (instance number 4) on a V35 port, you set the *applicationFramerName* attribute of the port as follows:

```
Trunk/4 UnAcked Framer
```

Applications and features on LPs

Passport software is divided into applications. Each application contains the software necessary to provide a particular type of service. The trunks application, for example, contains the software for all the variations of trunks you can run on Passport.

Each application has a version number appended to its name. For example, if the trunks application is version AA01, its application version is trunks_AA001. The *ApplicationVersion* (*Av*) component, which is a subcomponent of *Software* (*Sw*), indicates each application version that is currently available on the node.

Applications are further divided into features. Features contain the software necessary to provide a particular service. For example, the trunks application has a number of features, one for each type of Passport trunk:

- dpnTrunks
- unackTrunks
- porsTrunks
- frDpnTrunks
- atmTrunks

The *Feature* (*Feat*) component, which is a subcomponent of each *ApplicationVersion* component, indicates the features that are available in each application version.

Mixing spared and unspared applications and features on Passport 15000 and 20000 LPs

Line and equipment protection offers the flexibility of defining an LP with some applications and features that are spared and other applications and features that are unspared. For example, you can configure an LP to define four optical ports, as follows:

- the first port is the working line of a spared interface that uses dual-FP line automatic protection switching (line APS). Its protection line is defined through another LP.
- the second port is an unspared interface

- the third port is the working line of an spared SONET interface that uses single-FP line APS. Its protection line is defined as the fourth port of this LP.

In the preceding example, the four SONET ports are used by three different application instances. One application instance uses the first SONET port (and a second port defined through another LP). A second application instance uses the second SONET port. A third application instance uses the third and fourth SONET ports. Of the three application instances, two are spared and one is unspared.

The equipment protection sparing status of a port depends on the service applications and features that are linked to the LP and are using that port. Applications and features fall into three categories: hot standby, warm standby, and cold standby. See “Hitless services on Passport” (page 239) for details.

Logical processor types

When you define an LP, you specify a set of features to run on the processor card using a logical processor type (LPT). An LPT is a group of features that you can assign to one or more LPs. Since more than one LP can be running the same software, you can assign a single LPT to many LPs.

You create a new LPT by adding a *LogicalProcessorType* (*Lpt*) subcomponent to the *Software* (*Sw*) component. You then set the *featureList* (*fl*) attribute to contain a list of the features in the LPT.

To assign an LPT to a particular LP, you must set the *logicalProcessorType* (*lpt*) attribute of the *Lp* component to the name of the LPT. For example, to assign the LPT named CP to Lp/0, you set its *lpt* attribute as follows:

```
Software Lpt/CP
```

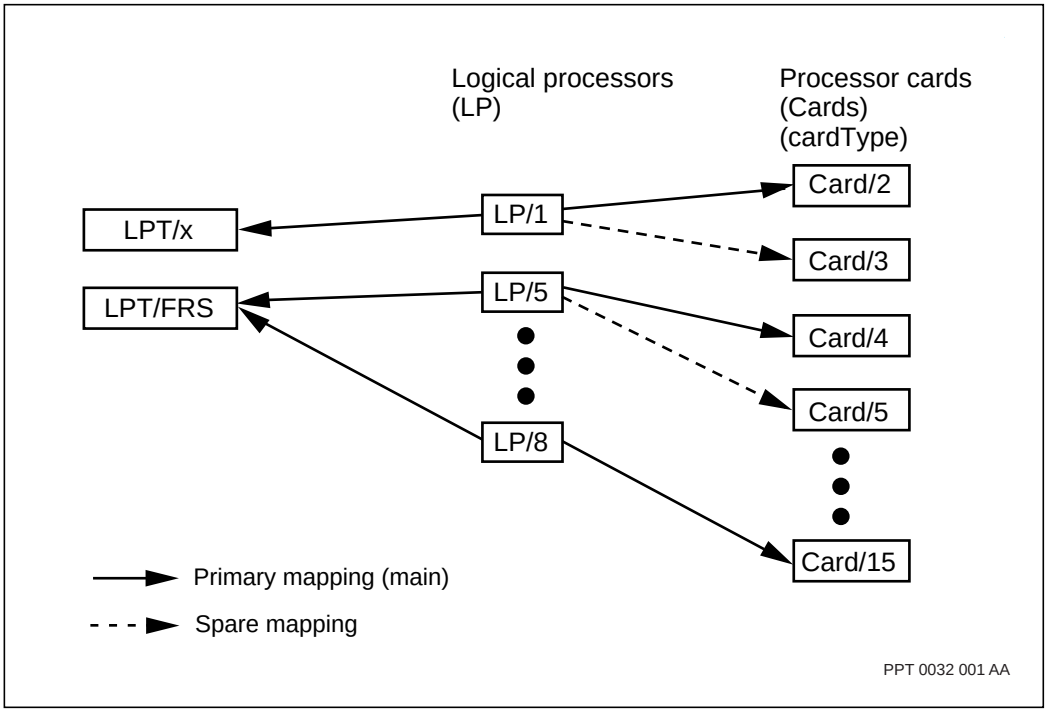
The read-only *logicalProcessors* attribute of the *Lpt* component shows which LPs are using the LPT.

Note: Do not define LPTs that mix cold standby applications or features with hot standby or a warm standby applications or features. A single cold standby application or feature in an LPT changes all other

applications and features into cold standby. See “Hitless services on Passport” (page 239) for details. Warm standby applications and features can co-exist with hot standby applications and instances in an LPT.

The figure “Relationship between LPTs, LPs, and processor cards in a Passport 15000 or 20000 switch” (page 287) illustrates the relationship between LPTs, LPs, and processor cards.

Figure 15
Relationship between LPTs, LPs, and processor cards in a Passport 15000 or 20000 switch



In the example, Lpt/FRS contains the software features required to run the frame relay service. Since this LPT maps to both Lp/5 and Lp/8, these two LPs can provide frame relay services. Processor cards 4 and 15 are main cards for LPs 5 and 8, respectively. Processor card 5 is a spare card for Lp/5 and runs the software and services defined for Lp/5 if processor card 4 fails.

A Passport 15000 or 20000 processor card has two types of memory for storing software features: normal and shared. Normal memory is used for processor code and data. Shared memory is used for data traffic. When you define the feature list of an LPT, you do not need to list the features in any particular order.

Logical processor configuration

Passport software does not link to a processor card directly. Rather, it links to a logical entity called an LP. Each LP represents the software that delivers Passport services or capabilities. You can associate an LP with one or more processor cards.

When you associate an LP with more than one processor card, you have processor card sparing. In a sparing configuration, one processor card is the main and the other is the spare. Typically, the main processor card is active and provides the services and capabilities of the LP. The spare card is in standby mode, waiting to take over in case the main card fails.

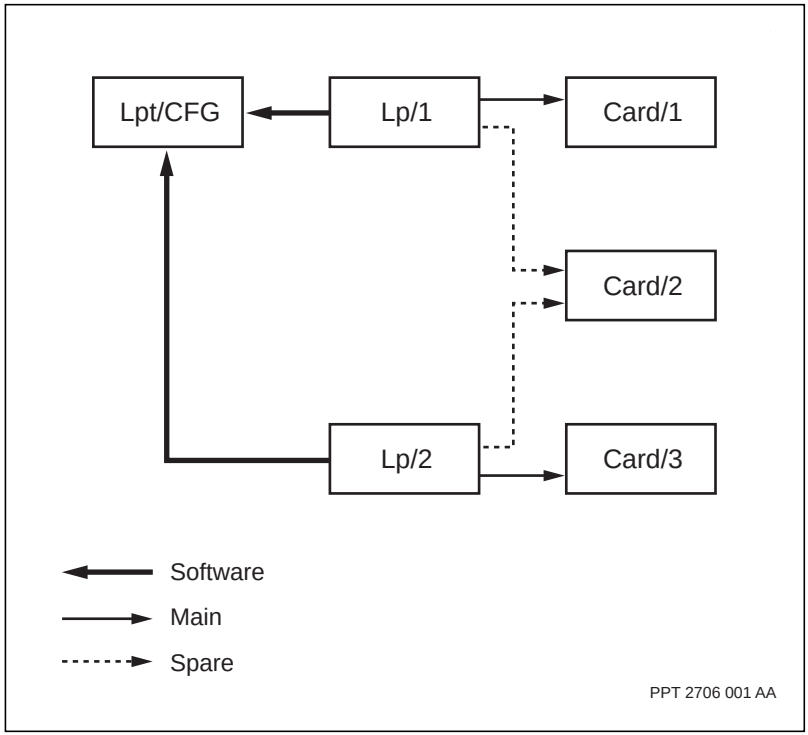
If the main card fails, Passport performs an automatic switchover. During a switchover, the standby processor card becomes active and the active processor card comes up as standby. You can manually switch the active and standby processor cards using the switchover command.

Passport supports one-for-one sparing, where one processor card serves as a standby for a single processor card. Passport also supports one-for-n sparing. For one-for-n sparing for Passport 7400, one processor card acts as a standby for up to four processor cards. For one-for-n sparing for Passport 15000 and 20000, one processor card acts as a standby for up to six processor cards. Both types of sparing require specific hardware configurations. For information on the hardware requirements of sparing, see 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade* or 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*.

An LPT defines the software associated with an LP. An LPT is a group of software features that you can assign to many LPs.

The figure “Sample relationship between LPTs, LPs, and processor cards” (page 289) illustrates a one-for-n sparing configuration of LPTs, LPs, and processor cards.

Figure 16
Sample relationship between LPTs, LPs, and processor cards



The LPs 1 and 2 both share the same LPT. LP 1 has processor card 1 as its main card and processor card 2 as its spare card. LP 2 has processor card 3 as its main card and processor card 2 as it spare card. If either card 1 or 3 fails, card 2 takes over. For this configuration to work, you must correctly connect the processor cards to a sparing panel and configure the sparing connection. For information on configuring the sparing connection, see “Configuring a new processor card” (page 78).

Locking and disabling LPs

When you lock a running LP, the LP moves into the shutting down state. The LP stays in the shutting down state until some condition causes it to stop running (an operator command or an error). Once the LP stops running, it moves to the locked state.

You can immediately disable (skipping the shutting down state) an LP using the force option of the lock command. When you use the force option, the LP immediately restarts and the LP moves into the locked state. If you are unfamiliar with lock command concepts, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

When an LP is locked, the LED status display on its main processor card is slow-pulsing red.

Understanding NCS

Network clock synchronization (NCS) provides the clock rates for connected ports so that they operate in synchronization. NCS prevents data loss or data retransmission for synchronous services.

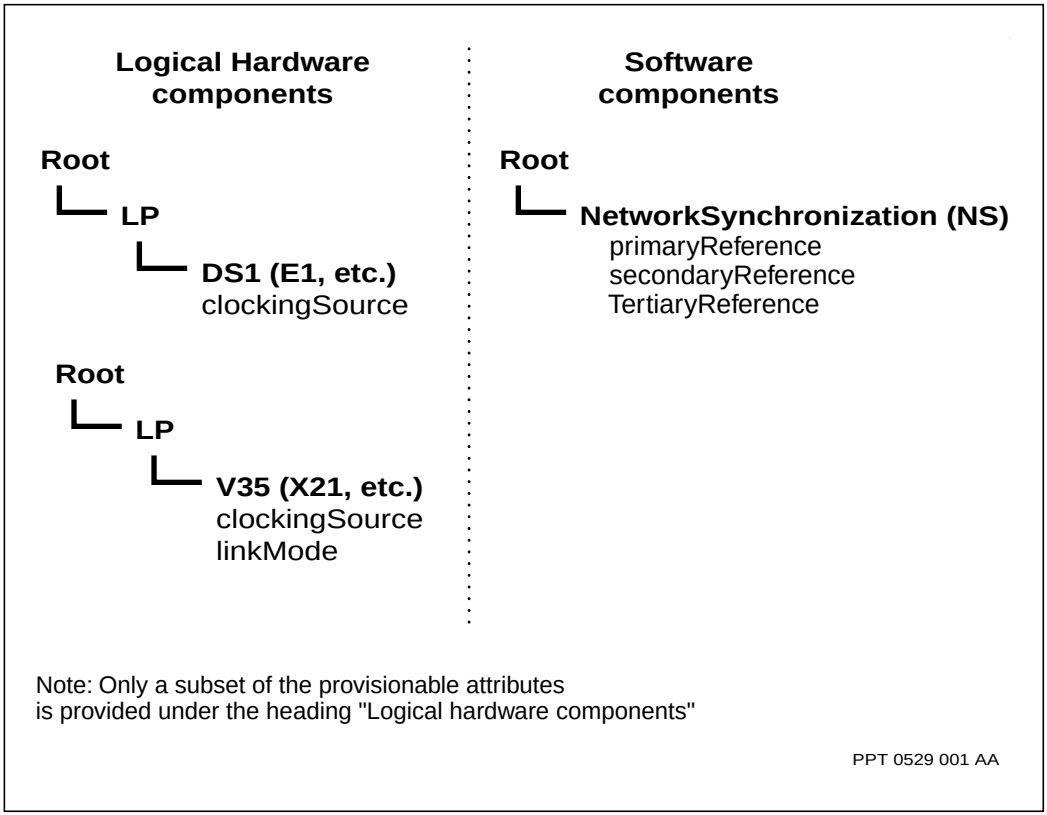
A node can be made a slave by configuring a choice of physical ports where the stratum-3 can derive its clock. If no references are configured in the *NS* component, the node runs as a master (with the stratum-3 free-running at its centre frequency).

> ***Note:*** If all of the configured references of the *NS* component in the slave node are out of service, the stratum-3 is free-running in hold-over mode.

The physical ports can be made to synchronize with a clocking source (using the port attribute *clockingSource*). For example, the *clockingSource* can be set to *module, local,* or *line*. The value *module* means that the stratum-3 clock of the CP generates the port's transmit clock. The value *local* means the FP uses its own crystal oscillator as a reference. The value *line* means the clock signal received from the port generates the transmit clock. For more information on clocking, see "Understanding basic clocking" (page 291).

The figure "Components and attributes used for NCS" (page 291) shows the configurable software and logical hardware components and attributes for NCS. The term *reference* indicates a reference for the CP. The reference receives the network clock signal from another node and passes it to the CP (to use as a reference).

Figure 17
Components and attributes used for NCS



Understanding basic clocking

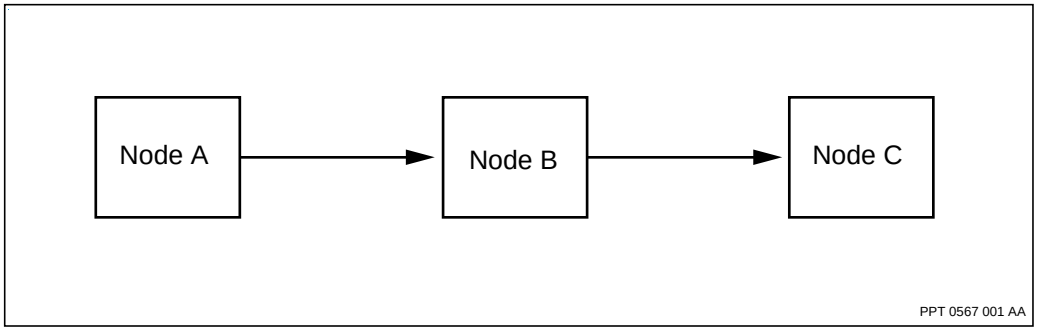
The figure “Data flow in a network” (page 292) shows the flow of data from node A to node B, then to node C. If the transmit clock at node A is faster than the one at node B, node B receives data faster than it can send it. Eventually, the buffer at node B overflows.

Similarly, if the transmit clock at node A is slower than the one at node B, the buffer at node B underruns. This is because the transmission rate of node B is greater than the rate it receives data.

Buffer overflow and underrun result in either data loss or data retransmission. In the case of overflow, data is lost. In the case of underrun, the last transmitted data is usually repeated. Therefore, providing a synchronized network is critical for synchronous services.

Note: NCS errors are not the only cause of underruns and overflows. Traffic congestion can cause the same result.

Figure 18
Data flow in a network



Understanding synchronization

The figure “Hierarchical clock synchronization network” (page 294) shows an example of a hierarchical clock synchronization network. In the hierarchical synchronization method, a frequency reference is transmitted from one node to another node. Nodal clocks supply a synchronization reference to specific nodes, each of which can in turn supply a reference to other nodes.

For added reliability, the synchronization network usually consists of primary and secondary (backup) reference facilities. When primary reference fails (for instance, when a port is disabled or a Passport trunk connection fails), a node can switch to its secondary reference. A tertiary reference can also be configured on Passport.

The synchronization network is divided into levels called *stratum*. Nodes in each stratum are characterized by a standard level of clock accuracy and stability. See the figure “ANSI (T1.101) stratum levels” (page 295) for a

partial list of stratum level characteristics. Stratum 1 provides the highest level of clock accuracy and stability and is typically implemented using a cesium (atomic) clock.

When an external stratum 1 or 2 clocking source is used, the CP oscillator will vibrate at that level of accuracy and distribute the clock to the ports of the FPs. When no external clocking source is configured, Passport modules conform to the stratum 3 standard which has an accuracy of 4.6×10^{-6}, for a DS1. This translates to 1.544 Mhz +/-7 Hz). In addition, stratum 2 and 3 nodes (which includes Passport nodes) must be equipped with a stable internal clock that can bridge reference interruptions (holdover). See the table "ANSI (T1.101) stratum levels" (page 295) for additional information about stratum levels.

Additional information about free-run frequencies and free-run accuracies for Passport FPs, see "Free-run frequency and accuracy of FPs" (page 295).

Figure 19
Hierarchical clock synchronization network

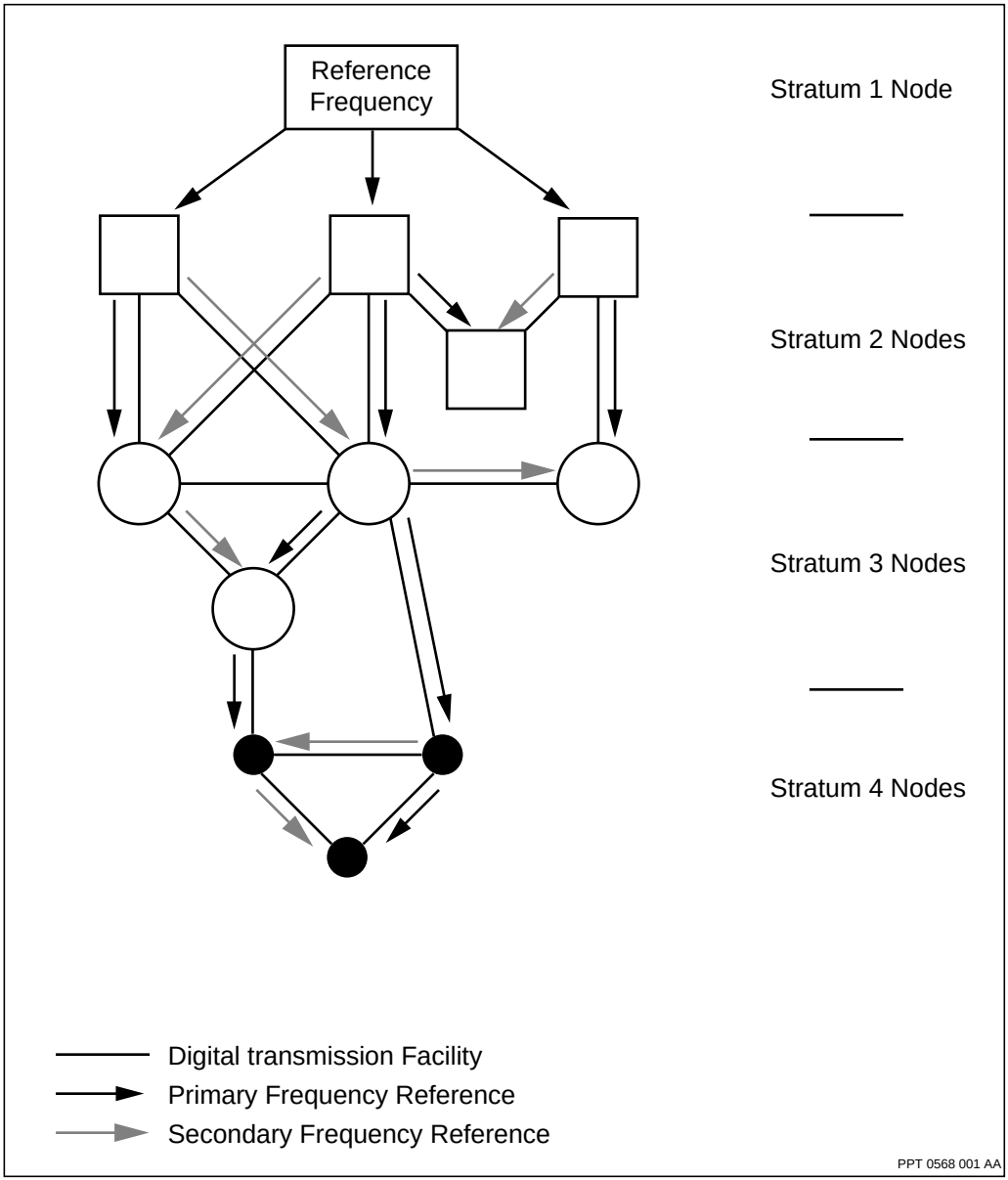


Table 14
ANSI (T1.101) stratum levels

Specification	Stratum 1	Stratum 2	Stratum 3	Stratum 4
Accuracy	1.0 x 10^{-11}	1.6 x 10^{-8}	4.6 x 10^{-6}	3.2 x 10^{-5}
Holdover stability	N/A	1 x 10^{-10} per day	must be less than or equal to 255 DS1 slips in first 24 hours of holdover	Not required

Table 15
Free-run frequency and accuracy of FPs

FP or FP type	Free-run frequency	Free-run accuracy
OC-12/STM-4	622 MHz	+/- 20 ppm
DS3	44.736 MHz	+/-20 ppm
E3	34.368 MHz	+/- 20 ppm
OC-3/STM-1	155.52 MHz	+/-20 ppm
16-port OC-3/STM-1	155.52 MHz	+/- 50 ppm
DS1 MSA with OC-3 ports	155.52 MHz	+/-20 ppm
E1 MSA with STM-1 ports	155.52 MHz	+/- 20 ppm
OC-48/STM-16	2.488 GHz	+/-4.3 ppm

Understanding NCS for Passport

NCS needs to be running on the Passport network nodes to ensure the nodes are operating at a synchronized clock rate. NCS synchronizes the clocking of nodes to a single master clock signal. NCS provides an identical clock to interfaces across the network such that the clock rate of data entering and leaving is the same. For this reason, a Passport module can join a stratum synchronized network.

Synchronization minimizes frame slips and data loss for bit-transparent data applications. The figures “Network synchronization component and provisionable attribute” (page 296) and “Network synchronization component and operational attributes” (page 296) show the provisionable and operational attributes for the network synchronization component.

Passport provides the necessary hardware and software to allow a synchronized network to support synchronous services.

Figure 20
Network synchronization component and provisionable attribute

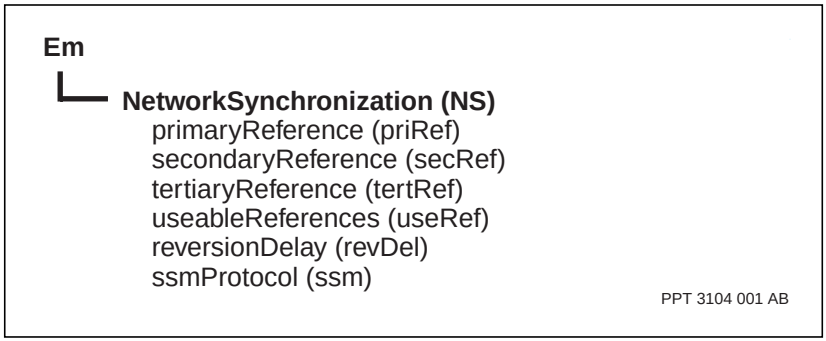
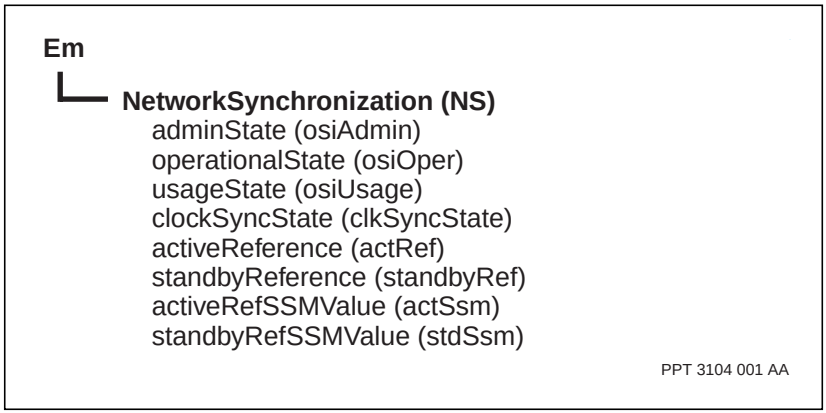


Figure 21
Network synchronization component and operational attributes



For more information on NCS for Passport, see the following sections:

Clock distribution

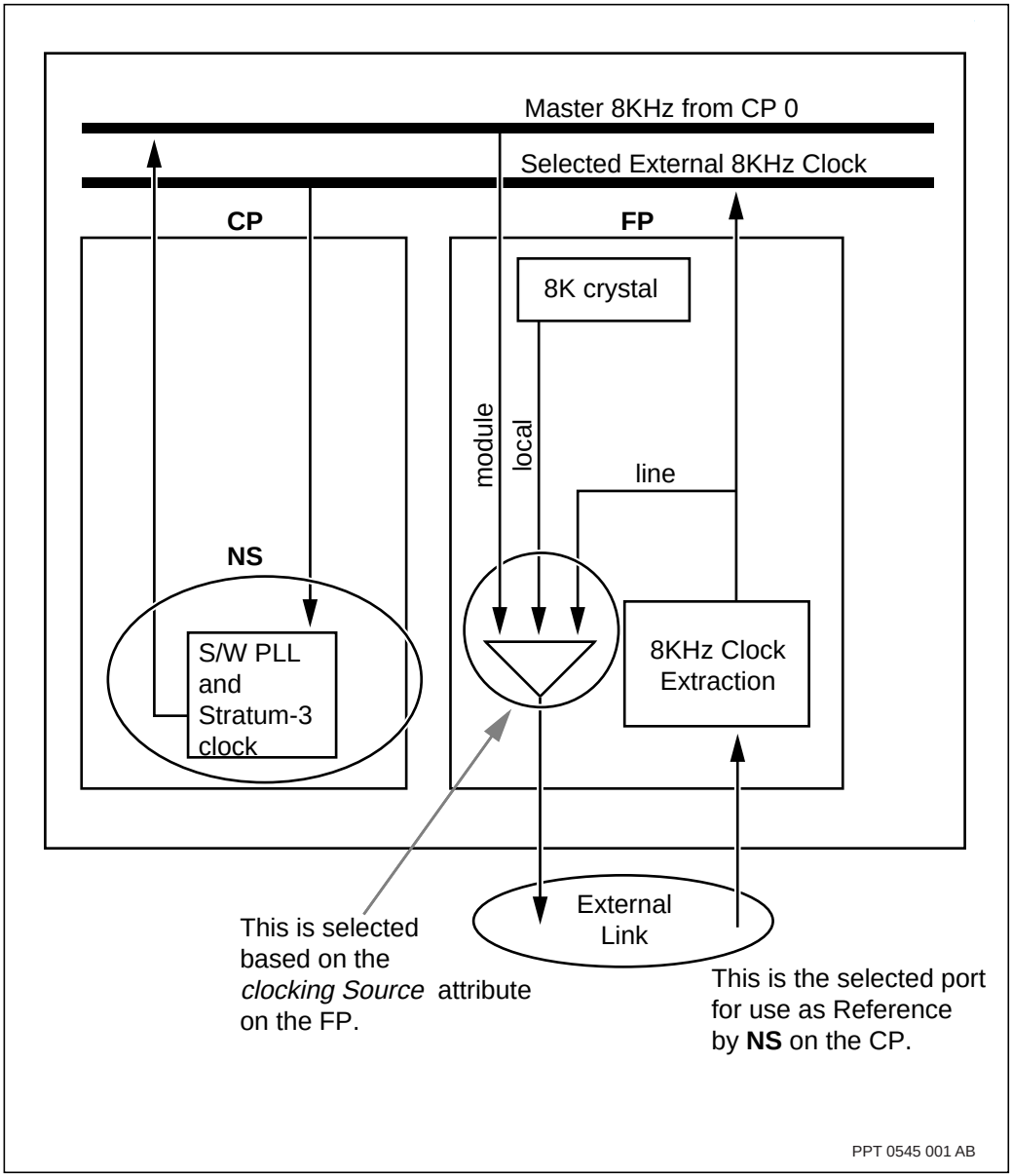
The figure “Passport module 8 kHz clock distribution” (page 298) represents a simplified view of the distribution of clocks on a Passport node. Each FP provides a means of extracting an 8 kHz reference clock from its connected external link. The control processors (CP) can choose an extracted clock from a port to be used as a reference for this node. The chosen reference clock signal is relayed across the backplane to the CP.

Passport provides a provisionable *NetworkSynchronization* (*NS*) component for selecting the port or ports to be used as reference sources. Up to 3 ports can be configured as reference sources (primaryReference, secondaryReference, and tertiaryReference).

If the clocking source for networking synchronization comes from line timing, set the clocking source for all ports, including the port used as the reference, to module. As the figure “Passport module 8 kHz clock distribution” (page 298) shows, the *clockingSource* attribute selects an outgoing clock source unrelated to the incoming clock.

For more information on timing reference signals, see “Timing reference signals” (page 299).

Figure 22
Passport module 8 kHz clock distribution



Timing reference signals

Passport can obtain its clock signal from the following sources:

- line timing, where the reference signal is extracted from an incoming traffic-carrying signal. The clock signal can come from a node on the Passport network that you designate as *master*. Alternatively, you can use a clocking signal from another source (for example, a source outside the Passport network). Any external source used must be at least as accurate as a stratum-3 clock.
- external timing, where the reference signal is provided by a non-traffic carrying link that uses an E1 or DS1 signal. The source of the link is a highly accurate and very reliable building-integrated timing supply/synchronization supply unit (BITS/SSU). The BITS/SSU derives its timing from a stratum-1 source, for example an atomic clock or global positioning system (GPS) receiver.
- internal timing, where the internal oscillator of the CP provides the signal

  Note: Passport supports a combination of timing modes (internal and external).

Network clock tree

You configure NCS in a Passport network by creating a network clock synchronization hierarchy, also known as a network clock tree. The object of configuring your network with NCS is to force a number of nodes to use a clocking signal that conforms to one master clock. When you create a clock synchronization hierarchy, one clock is designated as master. Adjoining nodes in the network synchronize with the clock signal from that master node. Nodes farther from the master synchronize to the signal of the nearest configured node.

For networks not carrying time-sensitive traffic, it is possible to have one core Passport running in free-run and all other Passports in the network synchronized to it. In this situation, the Stratum-3 clock is the synchronization source, but the same clock is used everywhere in the networks. In this configuration, the core Passport is acting as the master clock source.

To create a network clock tree, do the following:

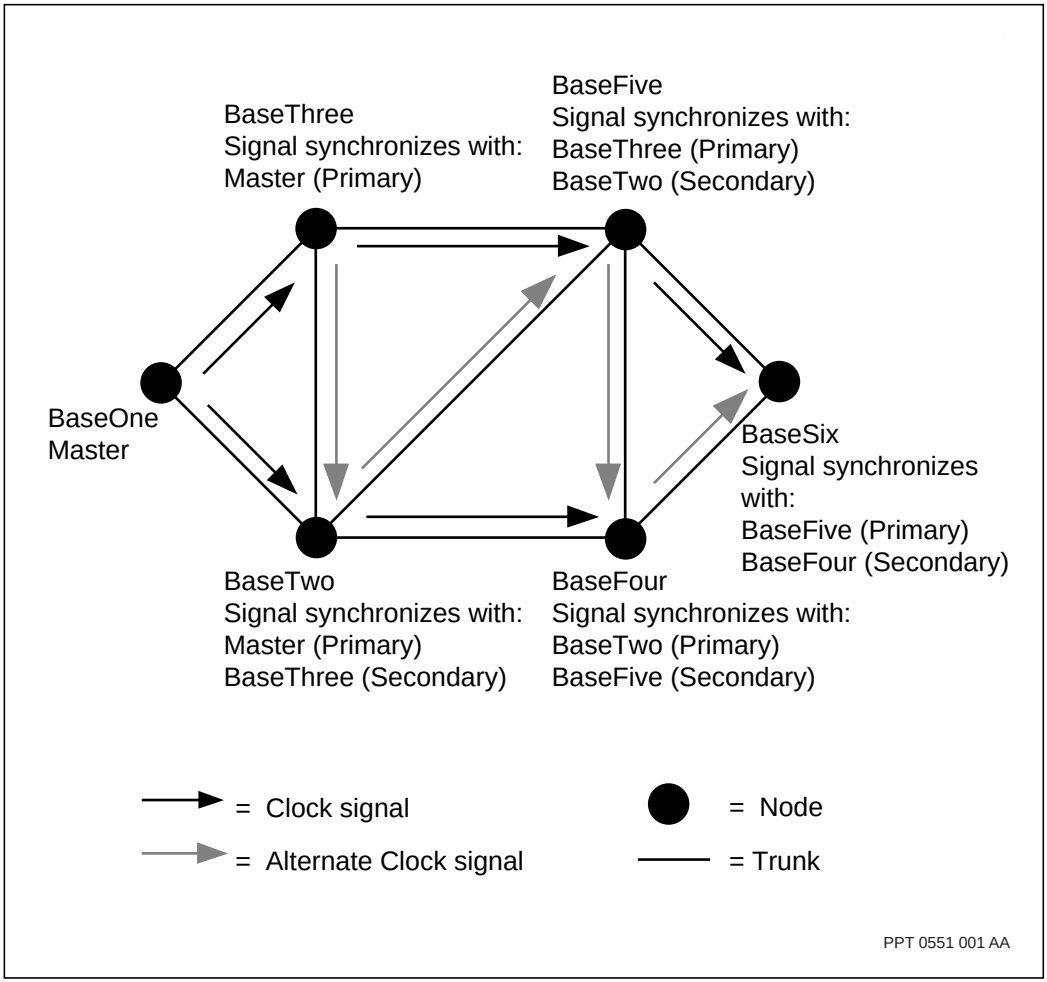
- configure the clocking signal from one node port as the master signal to which all other node ports conform. Alternatively, configure the node to receive a clocking signal from an external source. For example, a stratum-1, stratum-2, or stratum-3 signal outside the Passport network can be the external source.
- configure the nodes neighboring the master to synchronize with the clocking signal from the master node
- configure each node in the network to synchronize with the NCS clocking signal of the nearest NCS-configured node.

The figure “Network using NCS” (page 301) shows a network using NCS. The master signal is taken from a BaseOne port. Each successive node synchronizes with the signal of the last, from BaseSix node in turn back to the master. For example, BaseSix synchronizes with BaseFive, which in turn synchronizes with BaseThree, which synchronizes with the master, BaseOne.

BaseTwo is configured to obtain an alternate clock signal from BaseThree. If BaseOne fails, BaseThree reverts to free-running status and generates the master clock signal for the network.

Similarly, if both BaseOne and BaseThree fail, BaseTwo assumes free-running status and supplies the master signal for the network.

Figure 23
Network using NCS



Redundancy in case of failure

You can specify up to three sources for a clocking signal. These sources are referred to as primary, secondary, and tertiary, and are used as first, second, and third choices, respectively, for the clocking signal.

The clocking signal source is altered under any of the following conditions:

- the *activeReference* port (supplying the reference clock to the module) determines that its connection to the network or external source is bad. For example, there can be a loss of signal or loss of frame.
- the *activeReference* port goes to the locked state as a result of operator commands
- a DS1 or E1 *activeReference* port on the FP is configured to have a local clock source
- the configured *primaryReference* becomes enabled or a new *primaryReference* is configured
- the logical processor (LP) that the *activeReference* port is on becomes disabled

When a clocking signal becomes degraded, the source will continue to be used if the *useableReferences* attribute is set to enabled, the default value. If the *useableReferences* attribute is set to notDegraded, either a failure or signal degradation will result in an automatic clock source switchover.

When a clocking source is cleared from a disabled or degraded state the *NetworkSynchronization* component will revert to that source based on the value of the *reversionDelay* attribute. Before reverting, the *NetworkSynchronization* component will either wait a configured amount of time or a revert command must be issued if the attribute is set to manual. The revert command can be issued with the -force option.

> ***Note:*** The reversion enhancement functionality based on useableReferences and reversionDelay attributes is not supported on every functional processor that supports network clock synchronization. See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* to determine which card is supported.

NCS requirements and limitations

When engineering NCS, consider the following items:

- a node must synchronize to a reference of equal or better quality (a stratum-3 or better clock source)

- a node must synchronize to the highest quality clock supplied by a directly-connected node
- choose references so that a synchronization loop is never formed (nodes synchronizing to each other with no reference to the master signal)
- choose references with the greatest availability. Factors that contribute to availability include:
  - historical record (stability)
  - present activity
  - facility length
  - physical medium (twisted pair, coaxial cable, radio, or satellite link)
  - number of repeaters
- choose a minimum of active and standby references within the same physical medium. (For example on the V.35 FP of Passport 7400 switches, four ports are cabled into one physical high-density cable. Select no more than one reference in this cable.)
- individual ports of an optical interface card configured for APS can each serve independently as a reference source. However, pairs of ports cannot be used as a single reference source. Pairs of ports for APS are defined by the *Aps* component instance for Passport 7400 series switches or the *Laps* component instance for Passport 15000 and 20000 switches.
- DS1, E1, V.35, X.21, E3, and DS3 are valid port components
- when configuring NCS through a V.35 FP on a Passport 7400 switch, the data circuit terminating equipment (DCE) end must be the reference source that provides the clocking signal to the remote data terminal equipment (DTE) end

Note: APS does not support the local source clocking.

NCS operating states

The *NetworkSynchronization* (NS) component has the following three operating states:

- free run: when the NS component is in the free run state, either no reference was configured or none of the configured references are valid. If no reference was configured for NCS, the clock runs at its center

frequency (as a master clock). If however, one or more references were configured, but none of the configured references are valid, the clock free runs in hold-over mode. Hold-over mode means that the stratum-3 clock on the CP continues to operate at its last adjusted frequency and does not update its frequency.

- synchronizing: When the NS component is in the synchronizing state, the stratum-3 clock on the CP is trying to synchronize its frequency to a valid configured reference. This state lasts approximately 1 to 2 minutes, provided the reference is stable and of good quality. If the configured reference is not stable, the *NS* component can remain in the synchronizing state for more than 2 minutes. If the *NS* component remains in the synchronizing state for more than fifteen minutes, the node generates an alarm. The alarm indicates that the quality of the configured reference is questionable. When the configured reference is not stable or of good quality, the stratum-3 clock on the CP operates in hold-over mode.

  The *NS* component can also be in the synchronizing state when a port becomes disabled or a Passport trunk goes down. Under these circumstances, the *NS* component automatically initiates a change from the primary reference to the secondary or tertiary reference.

- synchronized: when the *NS* component is in the synchronized state, the clock is phase-locked to the configured reference. This is the normal mode of operation. As long as the *NS* component remains in this state, a net phase deviation of no more than 50 microseconds (with respect to the reference) is ensured. If a reference is lost when the *NS* component is in the synchronized state and no other reference was configured, the stratum-3 clock on the CP runs in hold-over mode. The clock runs at the last adjusted frequency made before the failure.

Building-integrated timing supply

An external synchronization interface requires a timing reference signal that ultimately has its origin outside the Passport network. This means that at least one node is connected to a timing source, such as BITS.

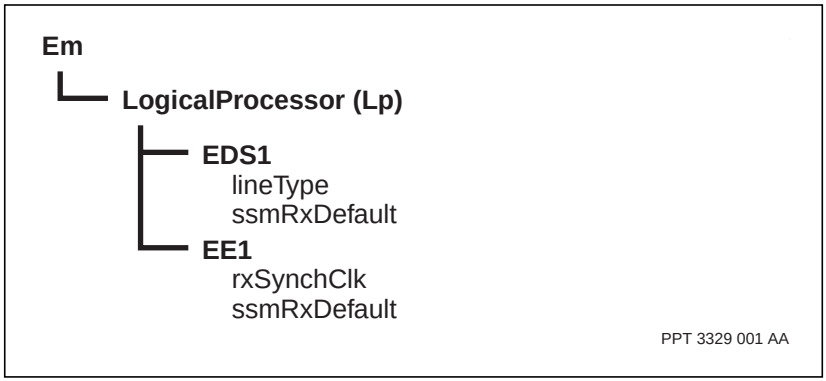
The BITS concept stipulates that all digital equipment in a physical structure must receive timing from the same master clock. This master clock produces a stratum-3 or better reference signal.

The implementation of BITS has the following advantages:

- the designation of a master timing supply for each structure simplifies and enhances the reliability of the timing distribution. The BITS concept minimizes the number of synchronization links entering a building, since each piece of equipment no longer has its own external timing source.
- since BITS provides a large number of signals for distribution, a single high-quality reference timing source can be shared among many services within an office
- the BITS is location-dependent, not service-dependent. This makes record keeping for provisioning and maintenance purposes easy when new digital services are introduced.

The figure “BITS components and attributes” (page 305) illustrates the components and attributes of external timing ports. Even though the ports are physically located on the alarm/BITS card (for Passport 15000 and 20000) and on the CP (optional for Passport 7400), the ports are logically configured as a subcomponent of the LP.

Figure 24
BITS components and attributes



SSM network clock synchronization

Synchronization status messages (SSM), defined as S1 Bytes in the SONET, SDH, DS1, and E1 overhead with the NCS system, provide an automatic method of choosing the best clock source in a network. The provisionable attribute *ssmProtocol* under the *NS* component determines if SSM functionality is enabled. When SSM is enabled, the NCS system chooses the

best clock signal based on the quality level of the SSM, making it available to all ports on all nodes configured with module timing. The use of SSM helps prevent timing loops and improves reliability of timing distribution.

Note: SSM are not transmitted on the BITS interface.

Since the SONET and SDH S1 byte definitions have different values for the equivalent clock quality level, a mapping table assists in determining the best clocking source available. The *NS* component makes switching decisions based on the Quality Level (QL), as seen in the table "SONET/SDH quality level (QL) mapping table" (page 306). In cases where the quality level on a port is not provided, a value of "Quality Unknown" is used.

Table 16
SONET/SDH quality level (QL) mapping table

Rx S1 Mapping to QL						**QL Mapping to Tx S1**					
SONET/ DS1 acronym	S1 Byte (binary / decimal)		SDH/E1 acronym	S1 Byte (binary / decimal)		QL	SONET/ DS1 acronym	S1 Byte (binary / decimal)		SDH/E1 acronym	S1 Byte (binary / decimal)	
			STU	0000	0	0	STU	0000	0	STU	0000	0
PRS or ST1	0001	1	PRC	0010	2	1	PRS or ST1	0001	1	PRC	0010	2
STU	0000	0				2	STU	0000	0	STU	0000	0
ST2	0111	7	SSUT	0100	4	3	ST2	0111	7	SSUT	0100	4
TNC	0100	4				4	TNC	0100	4	SSUL	1000	8
ST3E	1101	13				5	ST3E	1101	13	SSUL	1000	8
ST3	1010	10	SSUL	1000	8	6	ST3	1010	10	SSUL	1000	8
SMC	1100	12	SEC	1011	11	7	SMC	1100	12	SEC	1011	11
ST4	N/A					8	ST4/SMC	1100	12	SEC	1011	11
PNO or RES	1110	14		1110	14	15	DNU	1111	15	DUS	1111	15

(Sheet 1 of 2)

Table 16 (continued)
SONET/SDH quality level (QL) mapping table

Rx S1 Mapping to QL							QL Mapping to Tx S1						
DUS	1111	15	DNU	1111	15	15	DNU	1111	15	DUS	1111	15
Note: A QL of 1 is the highest quality level and a QL of 0 or 15 is the lowest level.													
(Sheet 2 of 2)													

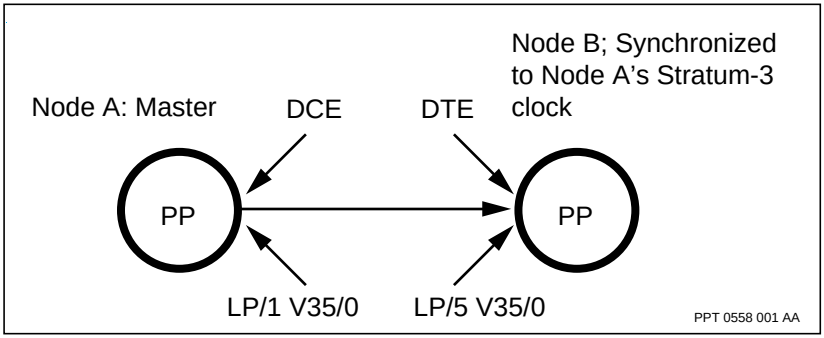
Refer to “Configuring SSM NCS” (page 60) for details on configuring SSM functionality.

Clocking for V.11 and V.35 FPs

You must be careful when setting the *clockingSource* and *linkmode* attributes for nodes that contain V11/V35 FPs. The figure “Example of a V11/V35 two-node network” (page 307) shows a V11/V35 two-node network that contains Node A and Node B. If you want to set up Node A as the master clock source with the clock signal of Node B synchronized to the clock signal of Node A, the following points must be addressed.

- to designate Node A as the master end, set the *linkmode* attribute for Node A to *dce*
- to designate Node B as the slave end, set the *linkmode* attribute for Node B to *dte*

Figure 25
Example of a V11/V35 two-node network



Because the *clockingSource* attribute is used to select an outgoing clock source and is not related to the incoming clock, set the *clockingSource* attribute for Node A to *module*. Because Node B is not used for external clocking, its *clockingSource* attribute does not have to be set.

> ***Note:*** When setting the *linkmode* attribute, you must be aware of the physical termination of the individual V11/V35 FP on the node. If there is a mismatch between the type of hardware connection and the *linkmode* setting, the hardware connection overrides the *linkmode* setting. As a result, the configured setting for the *linkmode* attribute is not recognized. To avoid this problem, ensure that the configured setting for the *linkmode* attribute matches the physical termination of the FP.

The output ports of an individual V11/V35 FP are grouped into two separate connections. Ports 0 through 3 represent one connection and ports 4 through 7 represent another connection. Each of these connections can be set to either *dte* or *dce* depending on its physical connection. For connections that are physically connected as *dce* and have ports with *linkmode* set as *dce*, you must set the *clockingsource* attribute to the same value for all ports of that connection. This can be *module*, *local*, or *line*. For example, if the first connection (ports 0 through 3) is connected as *dce* and the *linkmode* attributes for these ports are set to *dce*, the value set for the *clockingsource* attribute for ports 0 through 3 must all be the same. This is not applicable if the connection is set to dte.

Set the *linkMode* attribute to *dte*. The link mode is set when you configure your hardware. The hardware setup is shown by the operational attribute, *actualLinkMode*. Setting the *linkmode* attribute does not override the hardware configuration.

The incoming clock must be a multiple of 56 kbit/s or 64 kbit/s ranging from 56 kbit/s to 2048 kbit/s.

The *linkMode* attribute must be set to *dce*. The actual link mode is set when you configure your hardware. The hardware setup is shown by the *actualLinkMode* attribute (operational attribute).

> ***Note:*** If one port is selected with a *clockingSource* of module, all other dce ports on that LP must select module for their *clockingSource*.

Example of external clock source configuration

In this example, the objective is to set up the stratum-3 clock on Node A to synchronize with an external clock source. The external clock source must be stratum-3 or higher. Node A becomes the clock source for the rest of the Passport network. Node B synchronizes to the clock on Node A, as shown in figure “Example of a two-node network” (page 311).

Procedure steps

Configure Node A:

1. Enter prov mode on Node A:

   `start Prov`

2. Add the *NetworkSync* component:

   `add NetworkSync`

   The NetworkSync component does not need an instance value.

3. Display the attributes of the *NetworkSync* component:

   `d ns`

   The system displays:

   ```
   NS
     primaryReference =
     secondaryReference =
     tertiaryReference =
   ```

   Note: If there is not an external reference for Passport to slave off of, do not configure any references. This forces the Passport clocking to free run.

4. Select the source for the reference clock for the module. Typically the *secondaryReference* and the *tertiaryReference* attributes are also set at this point:

   `set NetworkSync primaryReference lp/2 ds1/0`

5. Set the transmit clock port lp/2 ds1/0 (logical processor instance 2, ds1 port instance 0) to synchronize with the Node A stratum-3 clock. To do this, use the module value for the *clockingSource* attribute:

   `set lp/2 ds1/0 clockingSource module`

   Note: This *clockingSource* attribute can be set to *line*, but it is good practice to always set it to *module*.

The clocking source for this module and the rest of the Passport network slaving off of this module are now synchronized to the external equipment.

6 Set port lp/1 ds1/0 (this is the Passport trunk to Node B) to synchronize with the Node A stratum-3 clock:

```
set lp/1 ds1/0 clockingSource module
```

Note: The *clockingSource* attribute of this port must be set to *module*. If it is set to *line* or *local*, Node B clocking is isolated from Node A.

The clocking used by this port is now synchronized with the Node A stratum-3 clock. See the figure “Example: results of Node A commands” (page 311).

7 Verify the configuration changes, activate the edit view, confirm that the activation was successful, and commit the provisioning changes:

```
check Prov
activate Prov
confirm Prov
commit Prov
```

Configure Node B:

1 Enter the prov mode on Node B:

```
start Prov
```

2 Add the *NS* component. It does not need an instance value:

```
add NetworkSync
```

At this point you can use the *display* command to display the component.

3 Set the *NS* component to reference lp/5 ds1/0 (logical processor instance 5, ds1 port instance 0):

```
set NetworkSync primaryReference lp/5 ds1/0
```

If this is a larger network you set secondary and perhaps tertiary references at this point. These back up the primary reference in case of network problems.

4 Though the *clockingSource* attribute does not have to be changed from its default, it is good practice to always set it to module:

```
set lp/5 ds1/0 clockingSource module
```

See the figure “Example: results of Node B command” (page 312).

5 Verify the configuration changes, activate the edit view, confirm that the activation was successful, and commit the provisioning changes:

```
check Prov
activate Prov
confirm Prov
commit Prov
```

Procedure job aid

Figure 26
Example of a two-node network

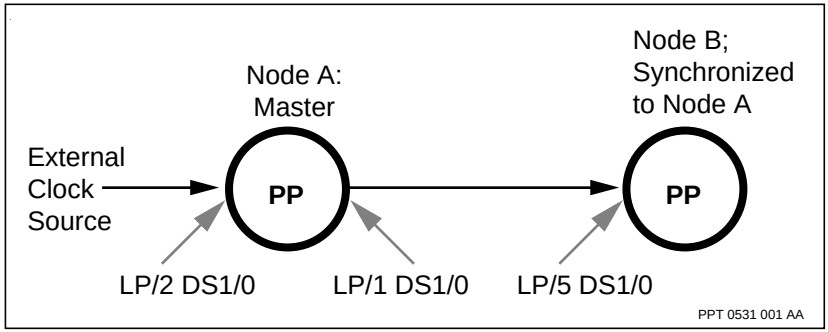


Figure 27
Example: results of Node A commands

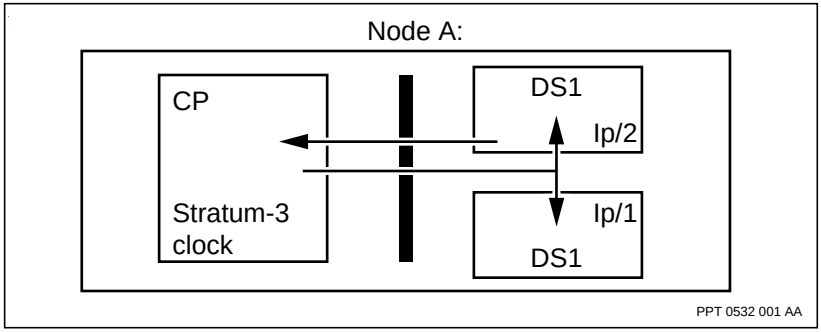
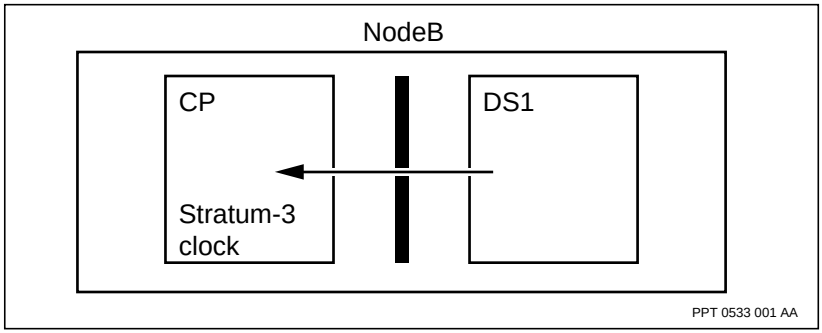


Figure 28
Example: results of Node B command



Understanding network time and date configuration

The *Time* and *Server* components provide access to management devices (MD) acting as network time servers. Passport XNTP is the software feature on Passport switches that controls network time synchronization. The XNTP protocol relays time server data between Passport nodes and MD time servers using the user datagram protocol (UDP) over IP. These MDs can reside in the LAN or WAN environments, or both.

There are three types of time to consider when configuring the time on a Passport node:

- reference time
- network time
- module time

The reference time is the date and time that is the official reference around the world. The universally accepted reference time is Coordinated Universal Time (UTC) which, in general, is equivalent to Greenwich Mean Time (GMT).

The network time is the date and time that is common across the whole network. This is the date and time to which all nodes in the network synchronize internally. Nortel Networks recommends that you use UTC for the network time. The network time is controlled by one or more time servers.

The module time is the time on a particular Passport node. In most cases, you synchronize the module time on a node to the network time on a time server. You then adjust for time zone differences using a time zone offset. Passport uses the module time for time stamps in alarms, accounting records, and other time-stamped data.

CAUTION

Risk of confusion in the interpretation of alarm and accounting record time stamps

Nortel Networks recommends that your network be synchronized to a reliable time server running reference time. Failure to do so can result in difficulties when correlating time between multiple Passport nodes.

The following sections contain conceptual information about managing date and time of day in a Passport network. As well, the following sections contain procedures for configuring date and time on a Passport node. There are three main approaches to configuring time in a Passport network:

- “Operating the whole network using reference time” (page 313)
- “Operating the whole network in a single time zone” (page 314)
- “Operating each node in its own time zone” (page 314)

Operating the whole network using reference time

This approach is recommended by Nortel Networks. It guarantees there is no confusion with the date and time presented in alarms, accounting records, and other time-stamped data. All such data generated by the network has the same, consistent time stamp based on UTC.

With this approach, a time offset of zero is configured on each node in the Passport network. As well, the whole network is synchronized to a common time reference. When the whole network is on reference time, the reference time is used as network time as well as module time.

Operating the whole network in a single time zone

This approach can be used by networks where all nodes are within the same time zone. This approach can also be used by networks that are operated as if all nodes are in the same time zone. All alarm, accounting records, and other time-stamped data has the same, consistent time stamp based on a single time zone.

With this approach, a non-zero time offset representing a specific time zone is selected to be used for the whole network. The selected time offset is configured on each node in the Passport network.

As well, the whole network is synchronized to a common time reference. When the whole network is offset to a single time zone, the offset time is used as network time as well as module time.

Although the reference time (UTC) is used to synchronize all Passports in the network, each node displays time using the selected, common time offset. In this manner, the date and time reported by all nodes in the network is the same.

Operating each node in its own time zone

This approach can be used by networks that require that each node in the network display the time based on the time zone where the node resides. All alarm, accounting record, and other time-stamped data has a time stamp that corresponds to the time on the node it is coming from.

With this approach, a different time offset is configured on each node in the Passport network. However, the whole network is still synchronized to a common time reference.

Although the reference time (UTC) is used to synchronize all Passports in the network, each node displays time using its own time offset, based on the time zone where the node resides. In this manner, the date and time reported by all nodes in the network can be different.

CAUTION

Risk of confusion in the interpretation of alarm and accounting record time stamps

Nortel Networks recommends that nodes not be operated each with its own time offset as there is a risk of confusion in the time stamp of alarms and accounting records.

For example, two nodes in different time zones generate a different time stamp for accounting records produced on both nodes at the exact same time.

Understanding Passport control and function processors

The following section explain the basic concepts of configuring control and function processors:

- "Passport processor overview" (page 315)
- "Processor card instances" (page 317)
- "Considerations for locking processor cards" (page 318)
- "Considerations for reinitializing a processor card" (page 321)
- "Considerations for replacing function processors" (page 321)
- "Understanding processor card configuration" (page 318)
- "Daughter cards on Passport 7400 processor cards" (page 326)
- "Processor card sparing" (page 326)
- "Hot standby for CP switchover" (page 327)

Passport processor overview

Passport has two types of processor cards: control processors (CP) and function processors (FP). CPs manage the FPs in the shelf and provide basic system capabilities.

CPs control the timing for:

- the fabric card or bus
- file storage

- data collection
- command processing
- interfaces for management devices

Passport 15000 and 20000 switches have two types of CPs: CP2 and CP3. CP2 offers a lower-cost option, while CP3 offers increased processing power and connection space.

Passport 7400 switches support two types of CPs: the base model CP and CP with building integrated timing supply (BITS). The CP with BITS has a port on the faceplate for direct input of two external timing sources.

For information about the CP Operation, Administration and Maintenance (OAM) Ethernet port, see “Control processor OAM Ethernet port configuration” (page 151).

Because a CP is critical to the whole node, you often use two CPs to provide redundancy. If the active CP fails, Passport automatically switches over to the standby CP. If you enable this feature, FPs with applications that support hot standby for CP switchover continue running uninterrupted during the switchover from active to standby CP. For more information see “Understanding CP equipment sparing” (page 258).

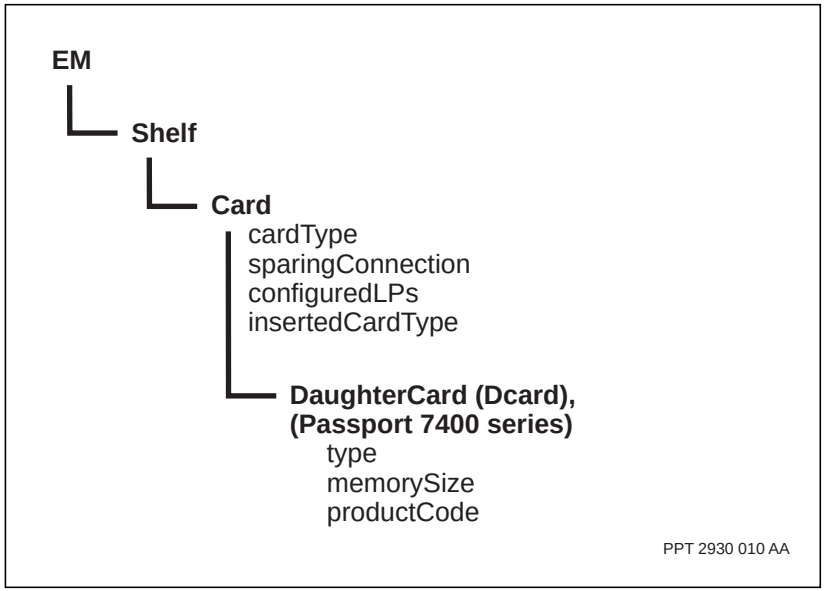
FPs provide communication connections and services. FPs support:

- physical interface connections to subscriber lines and network trunks
- software that performs real-time functions associated with the forwarding and routing of frames

Passport switches support a number of FPs that can run a variety of different communication services, including frame relay, Asynchronous Transfer Mode (ATM), Ethernet, and voice services, depending on the type of Passport switch you have.

The figure “Processor card components and attributes” (page 317) shows the components and attributes for a processor card. For more information on the types of processor cards, see “Processor card instances” (page 317).

Figure 29
Processor card components and attributes



Processor card instances

An instance of the *Card* component represents each processor card. The instance number corresponds to the slot where the card is inserted. Slots are numbered from left to right, starting at 0. For example, Card/2 represents an FP inserted in the third slot from the left.

You must configure the type of the card you are inserting in the slot by setting the *cardType* attribute. A CP on a Passport 7400 node has a card type of *CP*. A CP on a Passport 15000 or 20000 node has a card type of *CPeD* or *CPeE*, depending on whether it supports DS1 or E1 Building-Integrated Timing Supply (BITS) timing. FPs can be of various types depending on the function of the card. If the card that is actually inserted in the slot (as indicated by the *insertedCardType* attribute) does not match the configured card type, the processor card does not start and its status LED turns solid amber.

Some FPs on the Passport 7400 series switches contain daughter cards, which are specialized cards attached to the FP. If an FP has daughter cards, *DaughterCard* subcomponents appear under the *Card* component for the FP.

The instance number, that is automatically set by Passport, indicates the location of the daughter card. The attributes of the component give information about the type, memory size, and product equipment code (PEC) of the daughter card.

Understanding processor card configuration

Instances of the *Card* component (a subcomponent of *Shelf*) represent each processor card. The instance number corresponds to the number of the slot where the card is inserted. Slot numbers start at 0. Passport reserves slot 0 for the main CP. Passport 15000 and 20000 designates slot 1 for the spare CP. The Passport 7400 designates the last slot of the shelf for the spare CP.

> ***Note:*** Some Passport 7400 processor cards are dual slot. The procedure for configuring a dual-slot processor is the same as configuring a single-slot processor.

Logical processors (LP) represent the software configuration that runs on processor cards. When you spare processor cards, more than one processor card can run the software configuration defined in the LP. There are two ways you can use LPs to implement processor card equipment sparing. The first method uses a single LP. For example, see “Passport electrical interface equipment protection configuration” (page 205). The second method uses two LPs. For example, see “Passport 7400 optical interface line protection configuration” (page 211).

Considerations for locking processor cards

Processor cards are locked during a number of maintenance activities. Since locking a card will have an effect on the traffic normally carried on that card, the following considerations should be followed:

- Before locking an FP in software, ensure that you are aware of the consequences to the far end of the connection.
- Before locking the target FP of a protected (spared) pair, determine the status of its mate card using the appropriate procedure in “Common processor card procedures” (page 75).
  - — If the status of the card is other than in-service, see “Status LEDs of a CP or FP” for the meaning of the possible LEDs and see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and*

Testing for suggested procedures for placing the FP in the appropriate state.

- In a dual-FP inter-card LAPS configuration, manually forcing a switchover causes the mate port to keep the traffic. If the mate port is out of service and the switchover is forced, any traffic on the active port is lost. To prevent loss of traffic from a card replacement that is not due to card failure, you may first have to replace the card that has the most failed ports. When the statuses of a dual-FP LAPS configuration are queried in software, that is the time to decide which card of the pair is to be replaced first.
- If you are locking a Passport 15000 or 20000 FP to prepare it for removal, the procedures in "Common processor card procedures" (page 75) indicate when to use the command in order to minimize the impacts that locking or force locking has on services.

All function processors (FPs) should be locked in software prior to removing it from a slot, especially an FP that is configured for equipment protection. Locking an FP

- removes it from service and prevents the switch from establishing new connections on that card
- prevents it from running the software configuration defined in its logical processor (LP)

If the FP is currently running an LP, locking the FP puts the card into the shutting down state. The FP stays in the shutting down state until the LP stops running. An LP stops running when you lock it or when some condition causes it to restart (an operator command or an error). After the LP stops running, the FP moves to the locked state.

If you are running certain configured services on the FP, the LP will never stop running, in which case you need to use the *-force* option to lock the card. The *-force* option bypasses intermediate states and immediately moves the FP to the locked state. For spared optical FPs, the *-force* option can cause up to 50 ms of traffic to be dropped. For spared electrical FPs, the *-force* option can cause up to 100 ms or more of traffic to be dropped depending on the type of sparing panel. The amount of dropped traffic also depends on what the card is, what it is configured for, and how much traffic is in progress.

The person who will replace the card and the software operator who locks the card must coordinate their efforts to ensure that the FP is locked in software before physically removing the card. If you remove a standby FP before it is locked, the active FP can try to switch its traffic over to it, but will not be able to. All traffic on the active FP can be lost.

You can move an FP immediately into the locked state (skipping the shutting down state) using the *force* option of the *lock* command.

For Passport 7400, when you lock an FP using the *force* option, the LP immediately restarts and the card moves into the locked state. For Passport 15000 and 20000, when you lock an FP using the *force* option, the card moves immediately into the locked state. The LP restarts only when you restart the Passport 15000 or 20000 card.

If you lock an FP that has a defined spare card (is configured for equipment protection), the LP switches over to the standby card. For Passport 7400, when an FP is locked, its LED status light is slow-pulsing green. For Passport 15000 and 20000, when an FP is locked, its LED status light is solid red.

> ***Note:*** With line automatic protection switching (LAPS), the status LEDs on the faceplates of paired FPs do not indicate which one is active or standby. For example, both can have solid green LEDs. Before replacing a card that has been configured for LAPS, the standby card must be identified by software commands. The software query must occur very close to the actual time of card removal to minimize allowing the system to automatically switch over the cards. For information about configuring line equipment protection and manually switching over FPs configured for LAPS, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*.

When an FP is configured for equipment protection, locking the standby FP means preventing the standby FP from receiving traffic or being used as a backup. Locking is usually done to the standby FP. When you wish to replace an active FP, for example, for an upgrade or re-deployment, you must consider forcing a manual switchover in software so that the standby FP takes

over the active FP's traffic and the two FPs switch activity. Switching activity means the standby becomes the active FP, and the active FP becomes the standby.

The maximum switchover time is 50 milliseconds in the case of optical interfaces and 100 milliseconds for electrical interfaces. After a switchover completes, an in-service standby FP shows a fast-flashing green status LED on its faceplate and it can be locked.

Unlocking an FP causes it to restart, that is, triggers software activities to return the FP to service.

Considerations for reinitializing a processor card

Passport provides two methods for reinitializing a processor card: resetting and restarting. When you reset a processor card:

1 its hardware resets

2 it runs self tests

3 it reloads the software defined in its LP

When you restart a processor card, its hardware resets but it does not clear the loaded software out of memory. The processor card reinitializes the software in memory, but it does not reload the software from the file system. This behavior generally makes restarting a processor card faster than resetting the card.

If you reset or restart a spared processor card, a switchover to the standby processor card occurs. When you reset a CP, it loads the committed view. You can only restart a CP if it is currently running the committed view.

Considerations for replacing function processors

You must remove an FP from service before you can remove the card from the shelf.

Locking an FP is the prescribed method of removing it from service because it prevents the switch from establishing new connections on that card. You must ensure that an FP is locked before you physically remove it from the shelf. If you remove an FP before it is locked, all services and connections

supported by that FP are lost and system alarms are generated. Removing the card from service without locking it means some services will not automatically return to service with the card.

If the FP is spared, traffic is diverted to the spare FP when the active FP is locked. Before locking an FP, you should visually inspect the spare FP to verify that the LED is showing a fast flashing green signal, indicating that it is in standby mode and ready to be put into service. If any other signal is displayed, the FP is not in standby mode and the switchover will fail. If other LED patterns are displayed, see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing* for an explanation of these LED patterns and suggested procedures for placing the FP in the appropriate state.

Before removing an FP from service, the following points should be considered:

- When an FP has been removed from service by the system, an unspared FP is not providing service and a standby FP is not available for a backup. Minimize the impact of an out-of-service FP by doing the procedure as soon as possible. An out-of-service FP shows a solid red LED and alarm 7012 100 is generated.
- Check for other alarms to determine if other equipment is causing the FP to be out-of-service. Address the remedial action when the system allows it. All alarms are described in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.
- When you were upgrading, downgrading, or redeploying an FP when the failed FP was discovered, you must fix the failed FP first. Otherwise follow one of the other procedures in “Common processor card procedures” (page 75).
- Identify from your site records whether any private network-to-network (PNNI) links pass through the failed FP. These links may not automatically return to service when the FP is replaced, and may need to be reconfigured or manually unlocked.
- When a standby FP is removed from service by you or the system, the system cannot use it as a backup, that is, the system cannot automatically drop traffic by switching from an active card to an unavailable card. Unless the FP has already been removed from service by the system,

minimize the risk of not having a backup by doing the procedure during the period of lowest traffic for that FP. An out-of-service FP shows a solid red LED.

- During the removal from service, monitor alarms generated for equipment that is involved in the connection paths of the FP being replaced. Address the remedial action when the system allows it. All alarms are described in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

When removing an optical FP configured with LAPS:

- Dual-FP LAPS is also referred to as inter-card LAPS. Single-FP LAPS is also referred to as intra-card LAPS.
- When you are upgrading, downgrading, or redeploying a card that is configured for paired card protection through LAPS, always plan to switch the traffic from one FP (the target) to its mate. Then removing the target FP from service minimizes the affects on traffic.
- Once a port or FP is removed from service by you or the system, an attempted switchover causes the traffic to be lost because the port or card is not available. To prevent the loss, the port must be manually locked in the software. If the active card or port fails while the mate is out of service, traffic on the active card or port is lost.
- Unless the FP has already been removed from service by the system, minimize the risk of not having a backup by doing the procedure during the period of lowest traffic for that FP. An out-of-service FP shows a solid red LED.
- Identify from your site records whether the optical card to be removed from service has been configured for line automatic protection switching (LAPS). Only some optical Passport 15000 or 20000 FPs support LAPS. The 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* identifies whether an FP supports LAPS, but does not indicate whether it was actually configured to use the capability.
- Each FP of a protected pair that supports inter-card LAPS (dual-FP LAPS) can have ports providing service (the equivalent of active) or on hot standby (the equivalent of inactive or standby). The LED status of both cards is solid green, indicating both are active even if all ports on

one card are on hot standby. In this case, the following procedure temporarily removes one of the cards from service by switching traffic to its mate.

- During the removal from service, monitor alarms generated for equipment that is involved in the connection paths of the FP being replaced. Address the remedial action when the system allows it.

When removing an unspared FP:

- Check for alarms generated against the equipment the FP connects to. At the time you are about to remove the unspared FP from service, use the alarm data to determine which equipment should be fixed first in order to minimize the extent of removing the unspared card from service. The alarms are described in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.
- When an unspared FP is removed from service by you or the system, the traffic on the card is dropped. Unless the FP has already been removed from service by the system, minimize the out-of-service impact by doing the procedure during the period of lowest traffic for that FP. An out-of-service FP shows a solid red LED.
- Before removing an unspared FP from service, decide how to minimize the impact on traffic at the far end of the FP. If the unspared FP is in service or partially in service (its LED is solid green), locking it before removal causes an impact on traffic from the far end connection. The extent of traffic loss for traffic in progress and for subsequent incoming traffic depends on how much traffic is occurring and is likely to occur for the duration of the replacement and how the far-end equipment and software is set up for redundancy at your network level of system engineering. If the far end is a Passport, the system takes care of the connections according to the way the cards are configured.
- Identify from your site records whether the optical card to be removed from service has been configured for line automatic protection switching (LAPS) between pairs of ports on the same card. Only some optical Passport 15000 or 20000 FPs support intra-LAPS. The 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* identifies whether an FP supports LAPS, but does not indicate whether it was

actually configured to use the capability. When an unspared card with intra-LAPS is removed from service, the traffic on the port pair is dropped.

- Plan how to replace an unspared FP quickly and safely to minimize how long the FP's traffic links will be out of service.
- Although an unspared FP can have been removed from service by the system, you must always ensure that the card has been removed from service and lock it in software before physically removing it from the shelf. Otherwise, the replacement card may not fully return to service, or inserting the card can cause the shelf to reset.

When preparing an active card for replacement:

- In a dual-FP LAPS configuration, the mate card must be prepared for being replaced if it is part of an FP upgrade (rather than a failure). The sooner the mate card is prepared for being replaced (becomes the target card), the fewer active connections will be established on that card.
- With electrical FPs, preparing a spared active FP for being replaced means ensuring that the standby FP is ready to accommodate the traffic of the active FP with minimal impact on traffic. When the standby card has already undergone a replacement and has been confirmed to be in-service, this is an opportune time to replace the active mate. Before physically replacing an active mate, its traffic must be switched over to its standby mate so that the mate becomes the active and the active becomes the standby.
- If the FP is unspared, removing it from service drops traffic. The only preparation for an active unspared FP is to choose a period of lowest traffic before removing it from service. If your network was configured to back up the traffic of an unspared FP, removing the FP from service may cause the network to reroute far-end traffic away from the FP. For example, the configuration can have an intra-network card as opposed to an access card, have a node connected to two nodes to split services, or have PNNI links. Your site records should indicate whatever setup the network has.

Daughter cards on Passport 7400 processor cards

Some processor cards supported by Passport 7400 switches have daughter cards that provide specialized functions. The *DaughterCard* subcomponent of the *Card* component represents the daughter cards present on a processor card. The instance value, which is automatically set by Passport, indicates the location of the daughter card. The attributes of the component indicate the type, memory size, and product equipment code of the daughter card.

Processor card sparing

Before setting up sparing between processor cards, you must check the product PECs of the active and spare cards. For CPs, all eight digits of the PECs must match. For FPs, generally, the first six digits (four letters and two numbers) must match.

For MSA32 FP sparing, electrical interfaces are protected using inter-card sparing (electrical sparing protection) while optical interfaces are protected using intra-card sparing (APS line protection). Regardless of either PEC or card type:

- DS1 FPs can only spare other DS1 FPs and only for electrical interfaces
- E1 FPs can only spare other E1 FPs and only for electrical interfaces

Note: Some Passport 7400 processor cards have equivalent PECs. See 241-7401-200 *Passport 7400 Hardware Description* for a list of equivalent PECs. Except where noted, processor cards with equivalent PECs can be used as spares for each other.

For FPs, protection switching is available in case the card or signal fails. For more information, see the following sections:

- “Passport electrical interface equipment protection configuration” (page 205)
- “Passport 7400 optical interface line protection configuration” (page 211)
- “Passport 15000 or 20000 optical interface line and equipment protection configuration” (page 219)

Y-protection is a method of providing equipment protection (EP) and hitless software migration (HSM) that enables paired 16-port OC-3/STM-1 POS and ATM FPs (16pOC3PosAtm or NTHW44) to spare each other when the far-end interface does not support line automatic protection switching (line APS or LAPS). For the description of what Y-protection is and what it does for equipment protection, see "Understanding Y-protection for dual FPs" (page 348).

Hot standby for CP switchover

Hot standby for CP switchover allows FPs running services that support it to continue operating without interruption during a CP switchover.

By default, hot standby for CP switchover is enabled. You can disable it by including the *noHitlessCpSwitch* feature in the feature list of the CP LPT. When hot standby for CP switchover is disabled, cold standby for CP switchover is still available.

See also "Effects of a CP switchover" (page 268).

Understanding Passport software

The software load called the Passport Carrier Release (PCR) operates these members of the Passport family of switches:

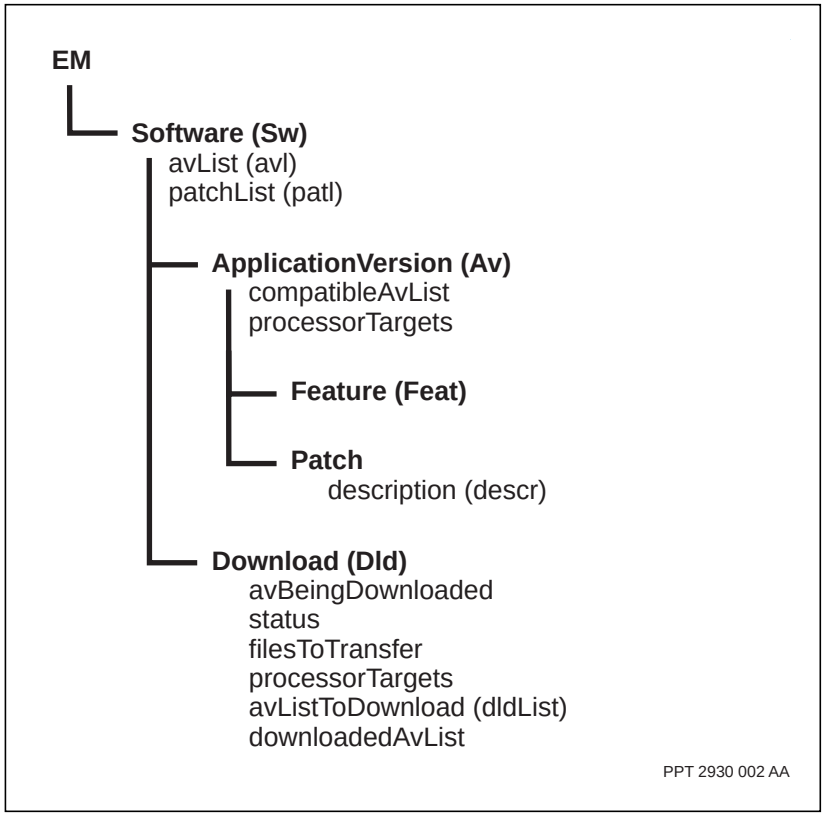
- the Passport 7000 series
- Passport 15000
- Passport 15000-VSS
- Passport 20000

The same load supports each of these switches to provide functionality and services. Each switch uses the portion of software that applies to it, and supports most of the available functionality and services. The new or changed functionality or services is directly associated with a version of the PCR, 4.1 for example.

Passport software consists of applications. Each application provides certain types of software functionality called features. An application can also have one or more patches that enhance or correct some of its functionality. Passport

software is managed using components and attributes. The figure "Software components and attributes" (page 328) illustrates the components and attributes for managing Passport software.

Figure 30
Software components and attributes



Instances of the *ApplicationVersion* component represent the software applications currently available on your node (stored on its file system). Instances of the *Feature* component represent the functionality of these applications. You can download new software applications to your node from a software distribution site (SDS) using the *Download* component of your Passport. For more information about downloading software applications from an SDS, see 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*.

Even though you can have many applications available on your node, Passport only uses the one you specify on the application version list (AVL). The AVL is represented by the *avList* attribute of the *Software* component. This capability allows you to store new applications or new versions of existing applications on the node for future use. This same capability applies to patches on an application version (AV), which you specify using the *patchList* attribute of the *Software* component.

For more information on Passport software, see the following:

- "Software structure" (page 329)
- "Components" (page 330)
- "Application versions" (page 331)
- "Patches" (page 331)

For instructions on downloading software applications from an SDS and setting the application version list, see 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*.

In most cases, Passport software is backward compatible. New software can load provisioning files and interpret provisioning views created using a previous version of the software. Consult the *Passport Release Report* for exceptions. For information on views and upgraded software, see 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*.

Software structure

Passport software has four major classes:

- base
- trunking
- networking
- access services

The figure "Passport software structure" (page 330) illustrates these four software classes and their relationship to one another.

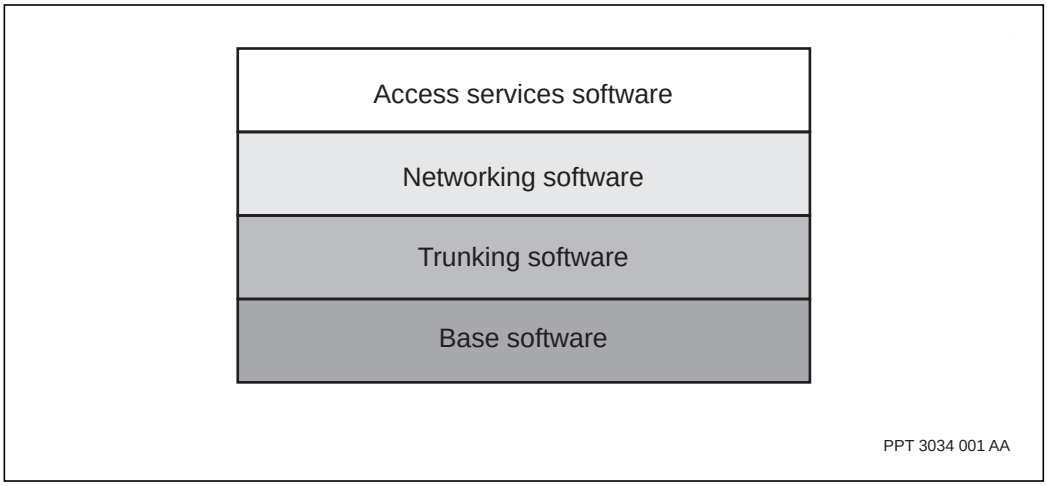
The base system provides the functions that support the access services. Its functions include software management, command processing, provisioning, shelf management, port management, file storage, data collection, and network management interfaces.

Trunking software provides the capabilities for interconnecting Passport nodes. It also allows for the interconnection of Passport and DPN-100 nodes.

Networking software provides capabilities for forwarding a packet of information from its source to its destination. Networking software includes routing and traffic management functions.

The access services run on the base system and provide the telecommunication capabilities of Passport. In general, Passport access services include frame relay, asynchronous transfer mode (ATM), Internet protocol (IP), and voice.

Figure 31
Passport software structure



Components

The main interface to Passport is by way of components. Components represent the hardware, software, and services on a Passport node. If you want to modify the configuration of the node, you change the attribute values of its

components. You can do this directly by typing commands in the text interface, or indirectly using a graphical network management tool. In either case, you are manipulating Passport components.

For detailed information on components, see 241-5701-060 *Passport 7400, 15000, 20000 Components*. For information on using commands to manipulate components, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Application versions

A particular version of an application is called an application version (AV). An application version number identifies each AV. The version number consists of two letters followed by two numbers. The most recent version of an application has the highest letter pair (with AA being the lowest) and the highest number pair (with 00 being the lowest). For example, AV numbers for a specific application can be: AA01, AA02, and AB01, where AA01 is the oldest version and AB01 is the newest.

The application version list (AVL) specifies the selected version for each application to run on a Passport node. You set the AVL using the *avList* attribute of the *Software* component.

A processor card can have one of two types of processors: i960 or PowerPC. A particular AV can support one or both of these processor types. When you define your AVL, make sure that your AV supports the processor types on your node. The *processorTarget* attribute of the *ApplicationVersion* component indicates which processors an AV supports. If the AV does not support the processor types on your node, you can download the AV, specifying the appropriate processor types.

> ***Note:*** The PowerPC (ppc) processor type is not supported on nodes with a 256-Mbyte disk on their control processors (CP).

Patches

A patch is a temporary enhancement or correction to the functionality of an application version. Patches allow for a number of small changes to be made to an application until the next version of the application is available. In general, a new application version incorporates all the changes in functionality made in the preceding patches.

Each patch has a unique name. The patch name starts with the application name, followed by a four-digit patch number (that starts at 0000). The patch name ends with a single letter (starting at A) that indicates the version of the patch. A patch is always associated with an application version. The number and version of a patch start at 0000 and A for each application version.

For example, you have a patch named base0000B, that is associated with application version base_AQ0123A. The patch modifies the behavior of the base application provided by the base_AQ0123A application version. It is the first patch (0000) released for that application version, but is the second version (B) of that patch.

You can determine the enhancement or correction provided by a particular patch by displaying the *description* attribute of the *Patch* component. This attribute provides a short description of the patch. For more information on a particular patch, see *Passport Release Notes*.

The patch list allows you to specify which patches you want to run on your Passport node. You specify the patches using the *patchList* attribute of the *Software* component.

Understanding the control processor OAM Ethernet port

The OAM Ethernet port on each control processor (CP) allows you to manage Passport nodes connected to the management network. The Passport nodes can be connected locally or remotely.

When Passport nodes are directly connected to the management network, they use local network management connectivity. Local connectivity can be achieved by connecting the Ethernet port on the management device as follows:

- directly to the physical Ethernet port on the CP
- indirectly through an Ethernet LAN to the physical Ethernet port on the CP
- indirectly through an Ethernet LAN and any number of Internet Protocol (IP) routers, one of which is connected to the physical Ethernet port on the CP

You can use local network management connectivity to manage Passport nodes.

Remote network management connectivity uses the capability of a Passport node to route IP traffic to extend the reach of the management network. In remote connectivity, a Passport node that is locally connected to the management network routes management traffic to other Passport nodes. In this scenario, many Passport nodes are controlled by the management network, but only one has local connectivity.

In remote connectivity, the management traffic can be routed over any WAN or LAN media that connect the nodes, including the following:

- Ethernet
- Asynchronous Transfer Mode multi-protocol encapsulation (ATM-MPE)
- frame relay data terminal equipment (DTE)

Note: The Passport 15000 or 20000 CP3 Ethernet Port only supports remote connectivity using ATM-MPE media.

For more information on the CP OAM Ethernet port, see the following sections:

- “OAM Ethernet port sparing” (page 334)
- “OAM Ethernet port tests” (page 335)
- “OAM Ethernet port statistics” (page 335)

For procedures on configuring and maintaining the OAM Ethernet port, see “Control processor OAM Ethernet port configuration” (page 151).

For information on IP security (IPSec) for OAM traffic, see 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.

OAM Ethernet port sparing

Note: A spare CP provides Ethernet redundancy only if both active and standby CP OAM Ethernet ports are connected to a hub or an IP router. In order to quickly resume the OAM Ethernet connectivity after the spare CP becomes active, direct hub or IP router sparing is required for both the active and standby CP OAM Ethernet ports.

The Ethernet ports on the main and spare CPs are spared at the media access control (MAC) and IP addressing level. When both these Ethernet ports are connected to a hub or an IP router, only the Ethernet port of the main CP is visible to the hub. The connection to the port on the spare CP appears to have nothing at the end of it.

When the main CP fails or a CP switchover is initiated, the OAM port of the main CP is disabled. This results in a loss of connectivity until the spare CP becomes active. Once the spare becomes active, its OAM port becomes enabled. All connection-oriented management applications must re-establish their connections.

There are two conditions related to the failure of the OAM Ethernet port that cause a CP switchover:

- a port test fails during the initialization of the hardware device when the CP first starts up
- a time domain reflectometry test fails following an absence of traffic on the link for a period of at least 25 seconds

If either of these two error conditions occurs, a CP switchover should occur. However in order to avoid impacting the service-providing applications on the FP, there are some scenarios where such port failures do not cause a CP switchover. The operational attributes of the *oamEnet* component allow the CP to correctly decide when a switchover is appropriate and when it is not.

The exception scenarios are

- an unsynchronized file system
- an unloaded provisioning database (i.e., CIT) on the standby CP
- a failed oamEnet port on the standby CP

- an FP running an uncommitted provisioning view
- a software upgrade in progress

As soon as the exception scenario clears and if the oamEnet port failure still exists, then the CP switchover occurs.

OAM Ethernet port tests

There are two categories of OAM port tests:

- port device tests that verify the controller device and its driver configuration
- link tests that verify the physical link between the CP Ethernet port and the Ethernet management network

The port device tests are initiated automatically prior to enabling the OAM port functionality. You can also initiate them manually through the *Test* subcomponent. The tests report a pass or fail.

Note: The OAM Ethernet port tests are not supported on CP3 on the Passport 15000 and 20000.

OAM Ethernet port statistics

The OAM Ethernet port supports two modes of statistics gathering:

- the primary statistics are reported to all management interfaces and cannot be turned off. They include:
  - alignment errors
  - frameTooShort
  - fcsErrors
  - numberOfRxCollisions
  - ackOfResourcesDiscards
  - overrunErrors

  These statistics require little software or storage to gather and display.

- the extended statistics can be turned on or off. They include

— singleCollisionFrames

— multipleCollisionFrames

— deferredTransmissions

— lateCollisions

— excessiveCollisions

— carrierSenseErrors

— clearToSendSignalLoss

These statistics require some software processing to gather and display. Doing so can have an adverse effect on the performance of the switch.

Understanding the fabric card

Each Passport 15000 or 20000 has two redundant fabric cards which are the switching matrix that enables communication between the processor cards on the shelf. Each fabric card is connected to 16 processor cards in the shelf through 16 card ports. The fabric cards also provide:

- the capability to reset a processor card (CPs and FPs) or a fabric card
- processor card availability functionality
- clocking to the two secondary control buses (SCB) on the backplane where they connect both fabric cards to all the processor cards

Either fabric card can handle the communication requirements of a fully provisioned switch. At start-up, the node shares the communication load across both operational fabric cards. In the event of a fabric card removal from service by the system for a fault or manually for a replacement or an upgrade, there is no degradation of performance or throughput as one fabric card takes over all traffic in progress. Connection switching between fabric cards is performed by each individual function processor (FP) and control processor (CP). That is, the decision to switch traffic from a card port to one fabric over to a port on the mate fabric is decided by the FP and CP, not the fabrics.

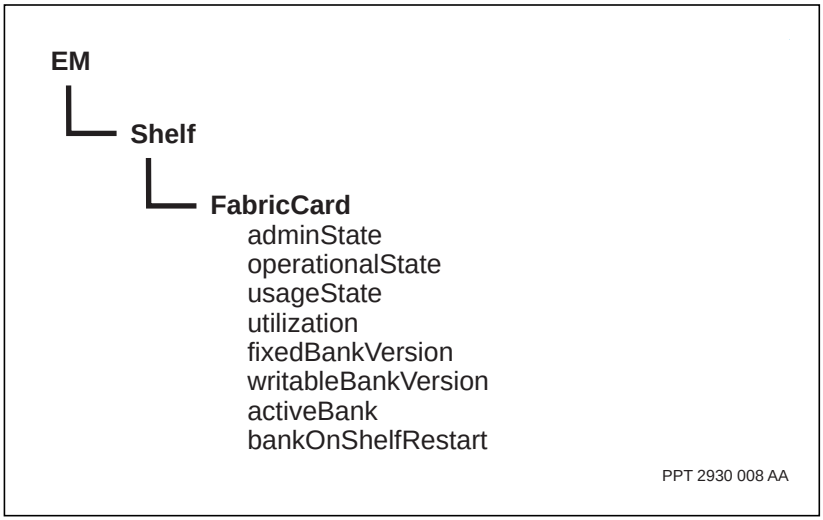
Two instances of the *FabricCard* component, x and y, represent the fabric cards. The x is the fabric in the upper physical position in a shelf while y is the lower mate. The figure “Fabric components and attributes” (page 337) illustrates the components and attributes of the fabric cards.

For more information on the fabric cards, see the following sections:

- “Single- and dual-fabric mode” (page 338)
- “Fabric ports” (page 338)
- “Fabric card firmware” (page 338)
- “Fabric card operation on Passport 15000 or 20000” (page 339)
- “Fabric card configuration” (page 340)
- “Configuring the fabric card component” (page 341)

For procedures on controlling the fabric cards and determining their status, see “Fabric card configuration” (page 340).

Figure 32
Fabric components and attributes



Single- and dual-fabric mode

When both fabric cards are operational (unlocked, in-service, with LED status solid green, the shelf is in dual-fabric mode (*backplaneOperatingMode* attribute is dualFabric). The fabrics balance and load-share the transport of processor card cells, giving a shelf bandwidth of 40 Gbit/s for a Passport 15000 or 70 Gbit/s for a Passport 20000.

> ***Note:*** In cases when both fabric cards may be operational, but at least one fabric port on an FP is disabled, the *backplaneOperatingMode* attribute is dualFabricDegraded rather than dualFabric.

When one fabric card is handling the traffic of the entire node, the node is in single-fabric mode (*backplaneOperatingMode* attribute is singleFabricX or singleFabricY) and all processor card cells run on that enabled fabric card. The single fabric card still provides a shelf bandwidth of 40 Gbit/s for a Passport 15000 or 70 Gbit/s for a Passport 20000. These Passports automatically switch between single- and dual-fabric mode depending on the state of the individual fabric cards.

> ***Note:*** If both fabric cards are out of service, the node enters fabric-less mode. In this mode, all cards in the shelf are disabled. The shelf automatically resets itself.

Fabric ports

Each fabric has 16 ports that interface with the processor cards. Each processor card has two fabric ports that interface with the fabrics. Each card component has two *fabricPort* subcomponents, one for each fabric port.

The *OsiState* attribute of the *fabricPort* component indicates the status of the user-specified fabric port on a processor card.

Fabric card firmware

A fabric card has two areas in memory to store firmware. The first area is called the fixed bank and stores a fixed version of firmware installed at the factory. The second area is called the writable bank and can store another version of firmware.

When a fabric card is initially powered up or hot-swapped, the system compares the version of firmware that is on the fabric with the version of firmware that is in the active bank of the running software. A fabric always has firmware already present either from the factory or from a previous software load. Whenever a fabric does not operate due to a mismatch of firmware versions, the system generates alarm 7002 0005 (described in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*). To enable the fabric to operate, you must manually load the indicated version of firmware.

Different versions of fabric card firmware are stored as an application version (AV) at the software distribution site (SDS). An operator can download a new version of firmware into a fabric card's writable bank.

Note: Do not include the fabric card firmware AV in the software AV list.

Fabric card firmware upgrades are not normally needed when the Passport CP and FP's software is upgraded. All Passport software is compatible with all fabric card firmware. However, some versions of fabric card firmware contain enhancements and new functionality to increase switch efficiency.

For the commands to handle fabric firmware, see 241-5701-272 *Passport 7400, 15000, 20000 Software Upgrade*, the chapter on installing new firmware on a fabric card.

Fabric card operation on Passport 15000 or 20000

The system automatically verifies that the fabric is correctly configured and functioning properly. The system uses the following components.

- *Shelf FabricCard/<n> cardPort/<p>*

  This component represents a physical port on a fabric card. The fabric card number *n* is *x* for the upper fabric card in the physical shelf or y for the lower fabric card. The card port number *p* is 0 to 15 for the ports on the FP or CP. This port sends and receives cells to and from the processor cards. Each fabric card has 16 of these subcomponents, one for each processor card in the shelf.

- *Shelf Card/<m> fabricPort/<q>*

  This component represents a physical port on a processor card. The card number *m* is 0 to 15 for the CP or FP. The fabric port *q* is x or y. The fabric port sends and receives cells to and from the fabric cards. Each processor card has two of these subcomponents, one for each fabric.

These components are added and automatically configured when the fabric cards and processor cards are physically installed and booted up.

Fabric card configuration

The Passport 15000 has a fixed fabric capacity while the Passport 20000 has configurable fabric capacities. Configuring the fabric capacity depends on the fabric that is installed in the switch. (For the initial release of Passport 20000, the fabric is the 70 Gbits/s version with PEC NTPN02, but the shelf backplane is designed to accommodate other capacities.)

The fabric card enables the processor cards on a Passport 15000 or 20000 to communicate with each other. There are two fabric cards, each represented by an instance of the *FabricCard* component (x and y). The x denotes the fabric in the upper physical position of a shelf, while the y denotes the lower mate. When both fabric cards are operational, the node is in dual-fabric mode. When in dual-mode with at least one fabric port disabled, the node is in dual-fabric degraded mode. When one fabric card is disabled, the node is in single-fabric mode.

When Passport 15000 or 20000 detects unrecoverable errors on a fabric card, or all ports on the fabric fail, it automatically removes that fabric card from service by

- deflecting incoming traffic to the other fabric
- transferring traffic in progress to the other fabric
- when all traffic is transferred, gets removed from service

You can manually remove a fabric card from service using the *lock* command.You can lock a fabric card if both fabric cards are unlocked and enabled, or when the card has been removed from its slot. The fabric card

remains locked until you unlock it using the *unlock* command. For example, when a fabric is replaced or upgraded by another card, the new card is still locked until unlocked.

If a CP switchover occurs while a fabric is locked, the fabric card remains locked after the switchover. However, if the node restarts, a locked fabric card becomes unlocked.

Configuring the fabric card component

Two fabric card instances, *Shelf FabricCard/x* and *Shelf FabricCard/y* are automatically added to the *Shelf* component hierarchy during system initialization. Therefore, manual configuration is not required.

Understanding the Passport 7400 bus

A Passport 7400 node has two 800 Mbit/s buses that enable communication between the processor cards on the shelf. The processor cards receive and send cells to each other through the buses.

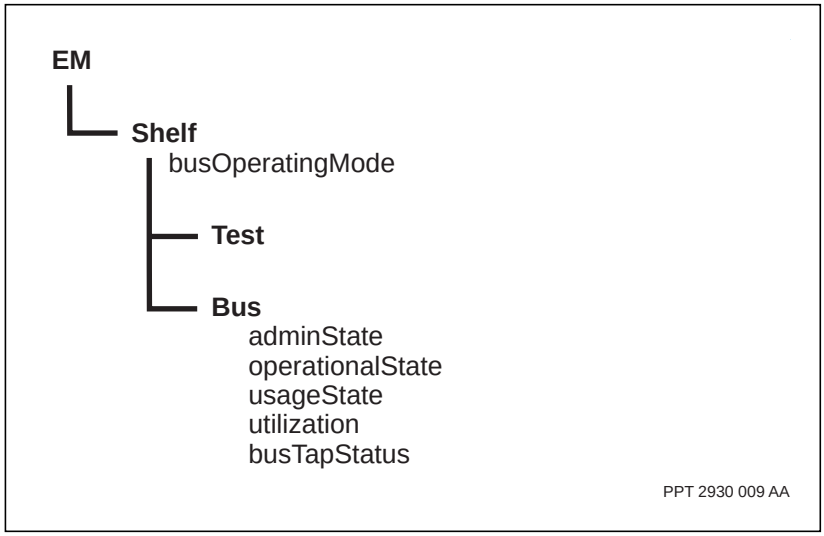
There are two buses, each represented by an instance of the *Bus* component (x and y). The figure “Bus components and attributes” (page 342) illustrates the components and attributes of the buses.When both buses are operational, the node is in dual-bus mode. When one bus is disabled, the node is in single-bus mode.

When Passport 7400 detects errors on a bus, it automatically disables that bus.

You prevent a bus from carrying data using the lock command. The bus remains locked until you unlock it using the unlock command. You can only lock a bus if both buses are unlocked and enabled. If a control processor (CP) switchover occurs, a locked bus remains locked. However if the node restarts, a locked bus becomes unlocked.

Passport 7400 provides automatic testing of the bus clock source. Since the bus clock source test can cause minor data loss, you can disable the automatic testing. If you have disabled the automatic testing, it is a good idea to manually test the bus clock source at least once a month.

Figure 33
Bus components and attributes



For more information on the buses, see the following sections:

- “Single- and dual-bus mode” (page 342)
- “Bus taps” (page 343)
- “Clock source” (page 343)

Single- and dual-bus mode

When both buses are operational, the node is in dual-bus mode (*busOperatingMode* attribute is dualBus). The buses share the transport of processor card cells, giving a bandwidth of 1.6 Gbits/s. The *utilization* attribute indicates how much of the bus bandwidth is currently in use.

When one bus is disabled, the node is in single-bus mode (*busOperatingMode* attribute is singleBusX or singleBusY) and all processor card cells run on the enabled bus. Passport automatically switches between single- and dual-bus mode depending on the state of the individual buses.

Bus taps

Each processor card has two bus taps, that provide an interface to the buses. Each card component has two *BusTap* subcomponents, one for each bus tap.

The *busTapStatus* attribute of the *Bus* component indicates the status of each bus tap.

Clock source

To properly function, the bus needs a clock signal. In most cases, the active CP provides the clock signal for the bus. The alternate clock source is the processor card (either an FP or a CP) at the opposite end of the shelf from the active CP. If that slot is empty, no alternate clock source is available. If present, the standby CP is always the alternate clock source.

The alternate clock source only provides the clock signal for the bus if a hardware failure makes it impossible for the active CP to do so. The *clockSource* attribute indicates the current clock source. The *busClockSourceStatus* attribute indicates the status of both the active and alternate clock sources. If the *busClockSourceStatus* attribute has a value of *unknown*, you should run a manual bus clock source test.

The manual bus clock source test is controlled by the *Test* subcomponent of the *Shelf* component. You perform the test using the run Shelf Test command. For a procedure on running the test, see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*. For information on the run Shelf Test command, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Understanding the Passport file system

The Passport file system stores the software and configuration files for running the node and the data generated by the node. The file system consists of up to two disks (represented by instances of the *Disk* component), one located on each of the CPs. When you have installed and configured a main and spare CP, the disks on the CPs work together to provide file system redundancy. The figure “File system components and attributes” (page 344) illustrates the components and attributes that represent the file system.

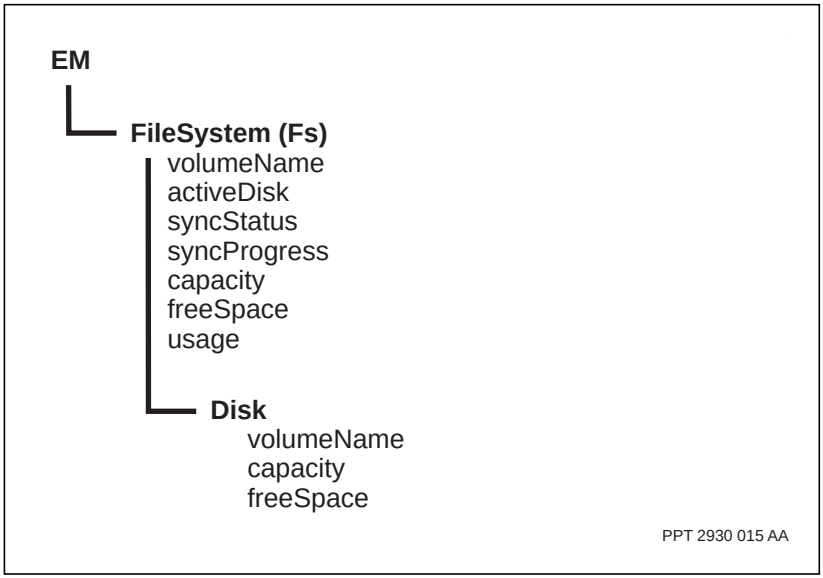
When the two disks are synchronized, Passport dynamically copies the information on the active CP's disk to the standby CP's disk. If the active CP fails and an automatic switchover to the standby CP occurs, information stored on the file system is preserved.

For more information on the file system, see the following sections:

- "File system information" (page 345)
- "Disk synchronization" (page 345)
- "Different-sized disks" (page 346)
- "File system restrictions" (page 346)
- "Disk full conditions" (page 347)

For procedures on maintaining the file system, see "Passport file system maintenance tasks" (page 197).

Figure 34
File system components and attributes



File system information

The operational attributes of the *FileSystem* (*Fs*) and *Disk* components provide information about the status, usage, and available disk space of the file system as a whole and on its individual disks.

The *activeDisk* attribute of the *FileSystem* (*Fs*) component indicates the component name of the disk on the active CP. The instance number of the *Disk* component corresponds to the slot number of the CP containing the disk. For example, the *Disk/0* component represents the disk on the CP in slot 0.

Along with a component instance, each disk also has a name. The *volumeName* attribute of the *Disk* component indicates the name of the individual disk. The *volumeName* attribute of the *FileSystem* component indicates the name of the active disk.

The *capacity* attribute indicates the maximum number of bytes of information that the disk or file system can store. The *freeSpace* attribute indicates the number of bytes currently available. When two different-sized disks are synchronized, the *capacity* and *freeSpace* attributes of the *FileSystem* component report the size of the smaller of the two disks. The *FileSystem* component has a *usage* attribute that indicates the percentage of the file system that is currently in use.

Disk synchronization

Before Passport begins copying modifications made on the active disk to the standby disk, the two disks must be synchronized. The disks are synchronized when they have identical content.

Passport automatically attempts to synchronize the disks in the following situations:

- when you insert a standby CP that has an identical disk volume name to that of the active CP
- when you power up a shelf that contains two CPs with the same disk volume name

If the disks do not have the same volume name, you can manually synchronize the disks. During the synchronization, Passport copies the contents of the active disk to the standby disk. If the two disks are completely

different and the active disk contains a lot of information, the synchronization process can take several hours. When the synchronization is complete, both disks have the same volume name. The system takes the volume name from the disk on the active CP.

The *syncStatus* attribute indicates whether the disks are synchronized, not synchronized, or in the process of synchronizing. If they are in the process of synchronizing, the *syncProgress* attribute indicates the percent completed.

You can manually initiate the synchronization process using the *synchronize Fs* command. For information on performing a manual synchronization, see "Synchronizing disks" (page 198). For information on the synchronize Fs command, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Different-sized disks

The disks on the main and spare CP can be of different sizes. The file system operates as if the two disks are the size of the smaller disk until the smaller disk is full.

If the smaller disk is full and it is the standby disk, Passport can no longer copy changes on the active disk to the standby disk. In this case, Passport disables file system redundancy and operates as if the active disk is the only available disk. If the smaller disk is the active disk, then Passport cannot write information to the file system because the active disk is full. You must take immediate action to prevent loss of information.

Although you can operate your node with differently sized disks on the main and spare CP, Nortel Networks recommends that the two disks be of the same size whenever possible. If you must operate with different-sized disks, ensure the active disk is always the smaller disk to avoid losing file system redundancy.

File system restrictions

To perform file system procedures, your user ID must have a minimum impact level of configuration.

The following restrictions apply when working with directories and files:

- The only characters that can appear in a file name are letters, numbers, the dot (.) character, and the underscore (_) character.

- File names and directory names are case-sensitive.
- If a file or directory name contains a slash (/), it must be enclosed in quotation marks (" ").
- File and directory names cannot be longer than 40 characters.
- File names with their full path cannot be longer than 128 characters.

  Note: Slashes (/) count as characters, but quotation marks (" ") do not.

- Directory names with their full path cannot exceed 125 characters.
- You can have a maximum of 10 directory levels.
- The root directory can have a maximum of 110 items (directories and files).
- When you copy a protected file, the new file is not protected.

CAUTION

Risk of damaging configuration data

The Passport provisioning system looks for saved views according to specific file name formats and file relationships. If you move or rename directories and files using the Passport file system commands (or using a non-Passport utility or application), you can destroy the integrity of the saved-view database. Affected saved views cannot be recovered unless you have backed them up. Only use the tidy prov command to remove saved views.

Disk full conditions

When a disk is 85% full, Passport generates a set alarm as a warning. The alarm clears when the disk is at 75% full (or below). When you encounter disk full conditions, spooling of data records stops and the disks on a two-CP node become unsynchronized.

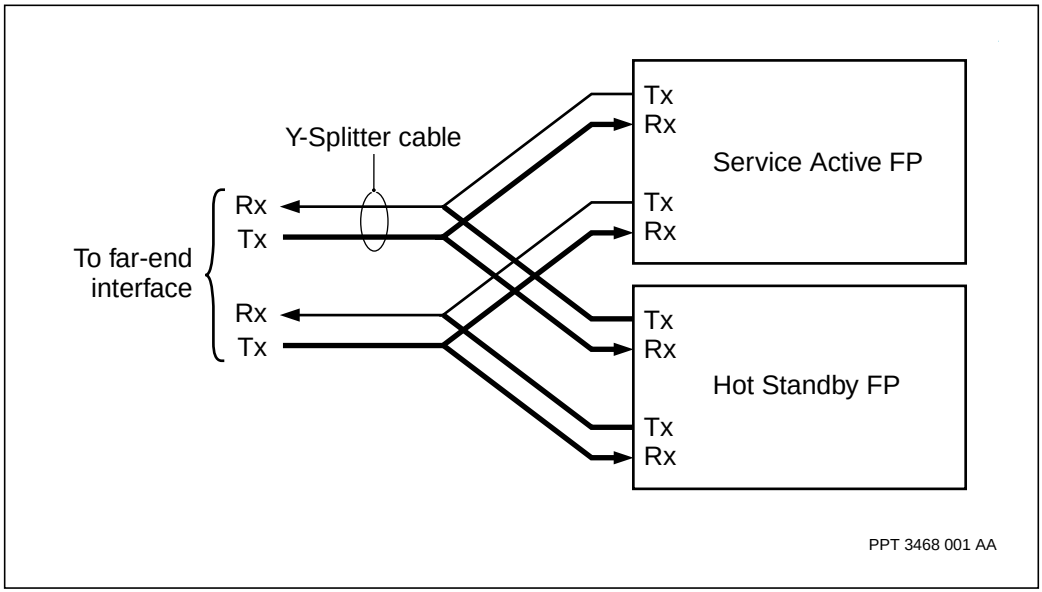
To fix a full disk problem, you must remove any unused software and provisioning files. For information on removing software files, see 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*. For information on removing provisioning files, see the tidy Prov command in

241-5701-050 *Passport 7400, 15000, 20000 Commands*. After removing unused files, you must manually synchronize the disks on a two-CP node using the synchronize command. For more information, see “Synchronizing disks” (page 198). Spooling of data records restarts automatically when disk goes below 90% full.

Understanding Y-protection for dual FPs

Y-protection is a method of line protection that enables paired 16-port OC-3/STM-1 POS and ATM FPs (16pOC3PosAtm or NTHW44) to spare each other when the far-end interface does not support line automatic protection switching (line APS or LAPS). By using fiber optical Y-splitter cables between some or all pairs of ports in a dual-FP configuration of NTHW44s and the far-end, traffic from the FPs is spared (backed up) while traffic from the far end is not. Refer to the figure “Y-protection connection between dual FPs and the far end” (page 348).

Figure 35
Y-protection connection between dual FPs and the far end



The operation of Y-protection

The operation of Y-protection between the dual NTHW44 FPs can be with or without LAPS being configured for each split pair of ports. The combinations of protected ports that you can configure on the dual FPs is

- some or all port pairs configured for LAPS
- some or all port pairs configured for either LAPS and Y-protection (LAPS and Y-protection are mutually exclusive for the same port)
- some ports not configured for any protection

Y-protection is configured as an optional extension of configuring LAPS. It depends on LAPS to operate. Like LAPS in a dual-FP configuration, Y-protection provides card-to-card protection. Unlike standard LAPS, the cards are not both active. Dual FPs with Y-protection have a designated service active FP and a hot standby FP. This means the standby line is always on the hot standby FP and its laser is switched off. The active line is always on the active FP and it does not react to k-byte changes. This accommodates the inherent problems of splitting an optical signal in this configuration.

The FP software controls the lasers of each transmit and receive port such that only the laser of an active port is on. This control ensures that the far end does not get confused by receiving signals from two different sources on the same line. This control also ensures that the laser is not turned on too soon for a reset card that is still waiting for software to be loaded.

Abnormal operation of a Y-protection connection triggers one or more of the following alarms:

- 7011 5279 for detection of a failure condition (for example, loss of signal on the active line due to a cut cable or a failed card)
- 7011 5278 for detection of a degraded condition (for example, a standby line or card is unavailable)
- 7011 5280 for detection of a failure at the far end (for example, the far end receive portion detects a SONET or SDH failure and sends an RDI to the near end)

Equipment protection for dual FPs with Y-protection

Equipment protection for dual NTHW44 FPs that are configured for Y-protection is normal, that is, includes protection from a card failure or a reset. If the far end is a Passport, then the protection of the connection behaves as it normally would for a LAPS or a non-LAPS configuration.

When a port with Y-protection fails or is locked on the service active FP, the traffic is lost because there is no line switchover. Otherwise, locking or unlocking a card, laps, logical processor (lp), or port is not affected by Y-protection being configured on it. The impact of locking or unlocking is determined by whatever else is configured.

The impact on traffic according to specific manual or system-triggered maintenance actions is described in the table of LAPS component state changes with Y-protection in 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.

Software migration between dual FPs with Y-protection

Hitless software migration can occur for the dual NTHW44 FPs while some or all of the ports are configured for Y-protection. There is still up to 50 milliseconds of traffic loss during the migration. The significant difference between normal migration and migration while Y-protection is enabled is

1 having all of the service active ports already on one card, especially if LAPS is configured for the cards

2 controlling the sequence of turning on and off the lasers to facilitate loading software onto the standby card

3 switching traffic from the service active card over to the hot standby card

4 controlling the lasers to facilitate loading software onto the remaining standby card

Card configuration for Y-protection

The rules to configure Y-protection on a pair of NTHW44 FPs are the same as configuring inter-card LAPS for the FPs, that is, adjacent slots, the first card in an even slot, and port pairs having the same numbers. To configure the software of Y-protection for a pair of FPs, see “Configuring Y-protection for dual FPs in a Passport 15000 or 20000” (page 231).

Hardware specifications of the Y-splitter cables

For the Y-splitter cable specifications, see the description of the 16-port OC-3/STM-1 POS and ATM FP in 241-1501-200 *Passport 15000, 20000 Hardware Description*.

Passport 7400, 15000, 20000
Configuration Guide

Release 5.2

Publication: 241-5701-600
Document status: Standard
Document version: 5.2S3
Document date: March 2004
Printed in Canada

NORTEL NETWORKS