NORTEL NETWORKS

Passport 7400, 15000, 20000

Trunking Guide

241-5701-420

Passport 7400, 15000, 20000

Trunking Guide

Publication: 241-5701-420
Document status: Standard
Document version: 5.2S1
Document date: November 2003

Publication history

March 2003

5.2S1 Standard
General availability. Contains information on Passport 7400, Passport 15000, and Passport 20000 for the PCR5.2 GA release.

Contents

List of figures

List of tables

About this document

This guide provides detailed information on using Passport trunks. Passport trunks consist of frame-cell trunks and Passport trunks over ATM (formerly known as ATM logical trunks). After reading this document, you will have a solid understanding of trunking.

Who should read this document and why

Use this guide if you perform one or more of the following tasks:

- planning a new network or upgrading an existing network
- establishing or testing connections
- reviewing trunking statistics
- technical support for trunking

What you need to know

To understand Passport trunks and Passport trunks over ATM it is helpful to know about:

- Passport software architecture

- Passport port management
- Passport processor cards (control processors and function processors)
- open systems interconnection (OSI) model
- background knowledge in networking: trunking, routing, traffic management
- ATM fundamentals (particularly virtual channel connections as described in 241-5701-702 *Passport 7400, 15000, 20000 ATM Routing and Signaling Fundamentals*)

How this document is organized

The 241-5701-420 *Passport 7400, 15000, 20000 Trunking Guide*, has the following sections:

- "Understanding Passport trunking" (page 97) describes the architecture, mechanisms, and features available for Passport trunking.
- "Passport frame-cell trunks" (page 121) concentrates on HDLC and interrupting mode mechanisms.
- "Passport trunks over ATM" (page 135) concentrates on trunking for ATM-only mechanisms.
- "Passport routing over ATM" (page 157) describes how the Passport routing systems work on Passport trunks over ATM to carry Passport non-ATM services.
- "Provisioning frame-cell trunks" (page 23) provides provisioning procedures to establish the connections.
- "Testing Passport trunks" (page 63) provides testing procedures for the network, Passport trunk connectivity, and hardware.
- "Monitoring Passport trunks" (page 69) provides operational procedures to monitor the condition of the Passport trunks.
- "Troubleshooting Passport trunks" (page 85) details debugging options.

What's new in this document

There were no new features added to this document.

Text conventions

This document uses the following text conventions:

- `nonproportional spaced plain type`

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

- **nonproportional spaced bold type**

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

- *italics*

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

  Words that appear in italics in text are for naming.

- `[optional_parameter]`

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

- `<general_term>`

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

- UPPERCASE, lowercase

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

- |

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

- ...

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

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

Related documents

This document features Passport trunking. Introductory and other relevant Passport trunking descriptions are in the following documents:

- 241-5701-400 *Passport 7400, 15000, 20000 Networking Overview*
- 241-5701-702 *Passport 7400, 15000, 20000 ATM Routing and Signaling Fundamentals*
- 241-5701-730 *Passport 7400, 15000, 20000 Inverse Multiplexing for ATM Guide*
- 241-5701-060 *Passport 7400, 15000, 20000 Components*
- 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*

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
Provisioning and maintaining trunking overview

Use the tasks listed in this section to provision and maintain trunking services on Passport 7400, Passport 15000, and Passport 20000 switches.

- "Prerequisites to provisioning and maintaining trunking" (page 19)
- "Provisioning and maintaining trunking task flow" (page 19)

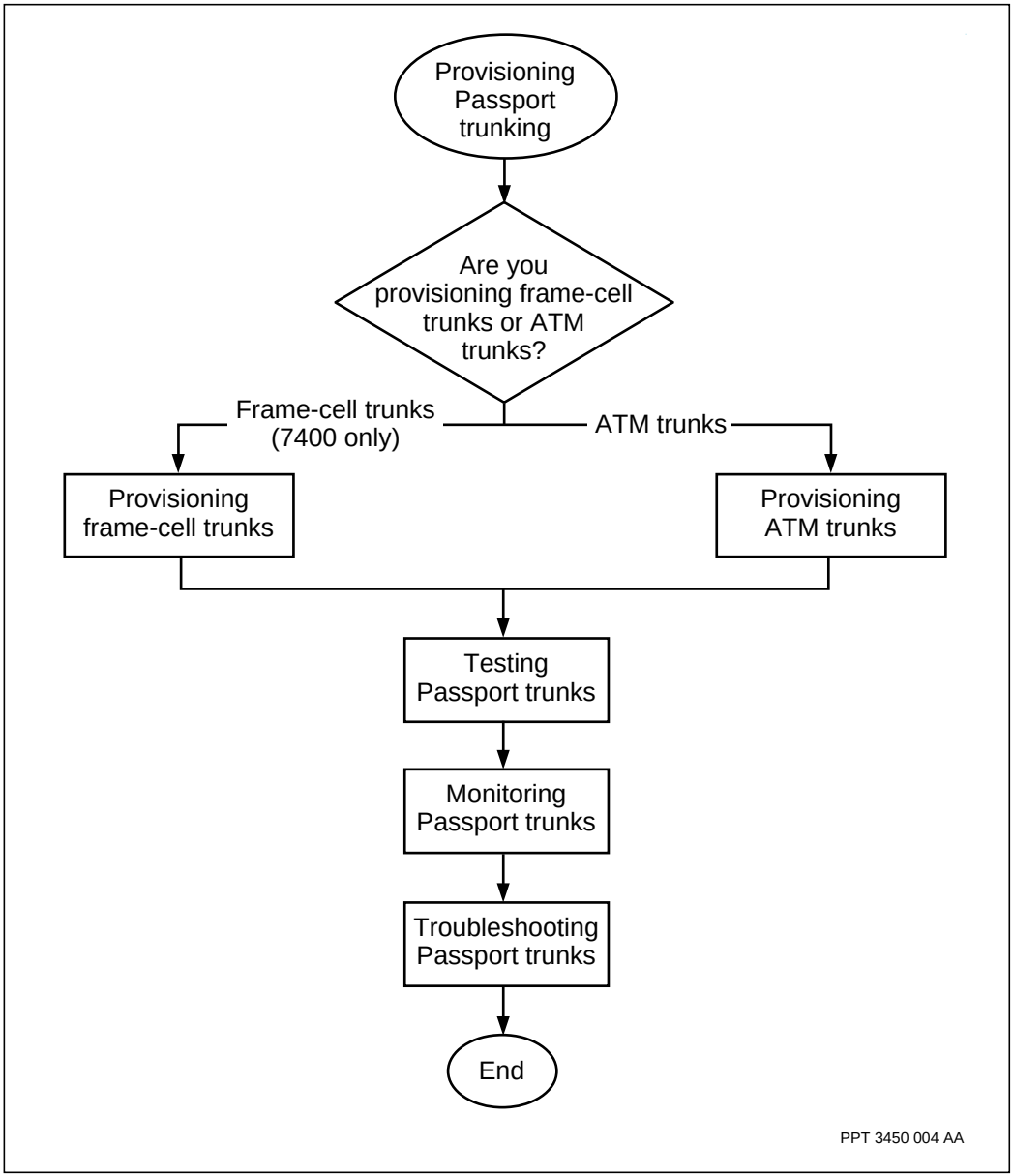
Prerequisites to provisioning and maintaining trunking

- If you are unfamiliar with Passport trunking concepts, see "Understanding Passport trunking" (page 97)

Provisioning and maintaining trunking task flow

This task flow shows you the tasks involved in provisioning and maintaining trunking. To link to any procedure, go to "Task flow navigation" (page 21).

Figure 1
Provisioning and maintaining trunking task flow



Task flow navigation

- “Provisioning frame-cell trunks” (page 23)
- “Provisioning ATM trunks” (page 41)
- “Testing Passport trunks” (page 63)
- “Monitoring Passport trunks” (page 69)
- “Troubleshooting Passport trunks” (page 85)

Chapter 2
Provisioning frame-cell trunks

Use these tasks to provision frame-cell trunking and any associated features.

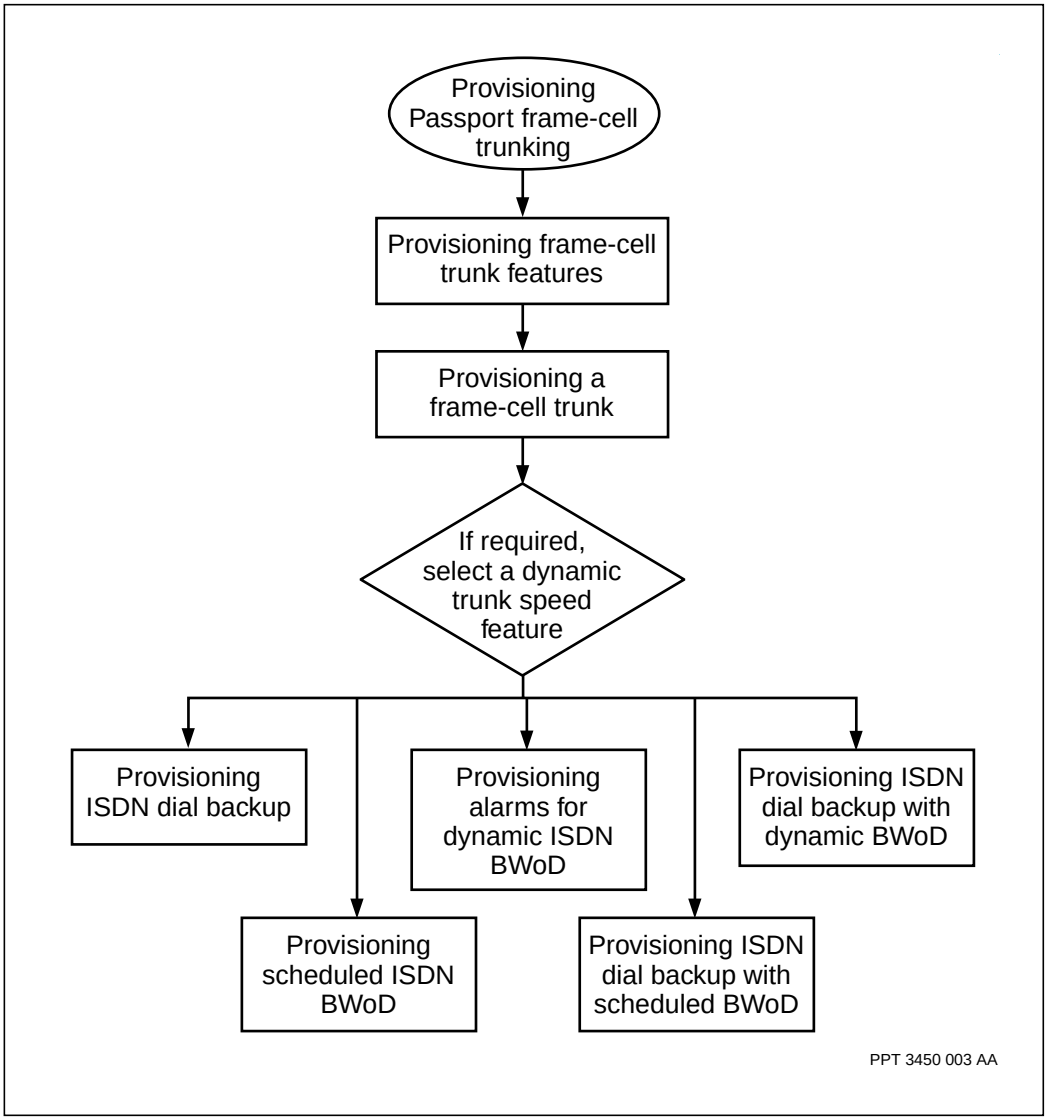
Prerequisites to provisioning frame-cell trunks

- If you are unfamiliar with frame-cell trunking or any other aspect of Passport trunking, see "Understanding Passport trunking" (page 97) and "Passport frame-cell trunks" (page 121)
- Use the "Provisioning worksheet for frame-cell trunks on a Passport 7400 series switch" (page 39) to assist in determining appropriate configuration values.

Provisioning frame-cell trunking task flow

This task flow shows you the sequence of procedures you perform to provision frame-cell trunking. To link to any procedure, go to "Task flow navigation" (page 24).

Figure 2
Provisioning frame-cell trunks task flow



Task flow navigation

- “Provisioning frame-cell trunk features” (page 26)

Provisioning frame-cell trunk features

Specify the frame-cell trunk features in the logical processor types feature list:

Prerequisites

- Download the appropriate software from the Software Distribution Site (SDS) (base, trunks, and networking) as described in 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*.
- Provision the logical processors (LPs), function processors (FPs), and ports to be used by the frame-cell trunk feature. For provisioning the hardware components, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide* and 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.
- Ensure the network administrator has supplied all of the appropriate provisioning information. This information includes such things as *Trunk* component instance values, and the type of routing used (DPRS or PORS).

  Note: Be aware that when a Passport trunk on a PQC-based FP is connected to another Passport trunk that is on a CQC-based FP, then the entire PQC-based FP reverts to software forwarding for dynamic packet routing system (DPRS). This results in a significant performance degradation.

Procedure steps

1 Start provisioning mode.

2 Add the *unackTrunks* component to the application software.

```
add sw lpt/unackTrunk
```

3 Use the set command to specify the required features in the logical processor's feature list.

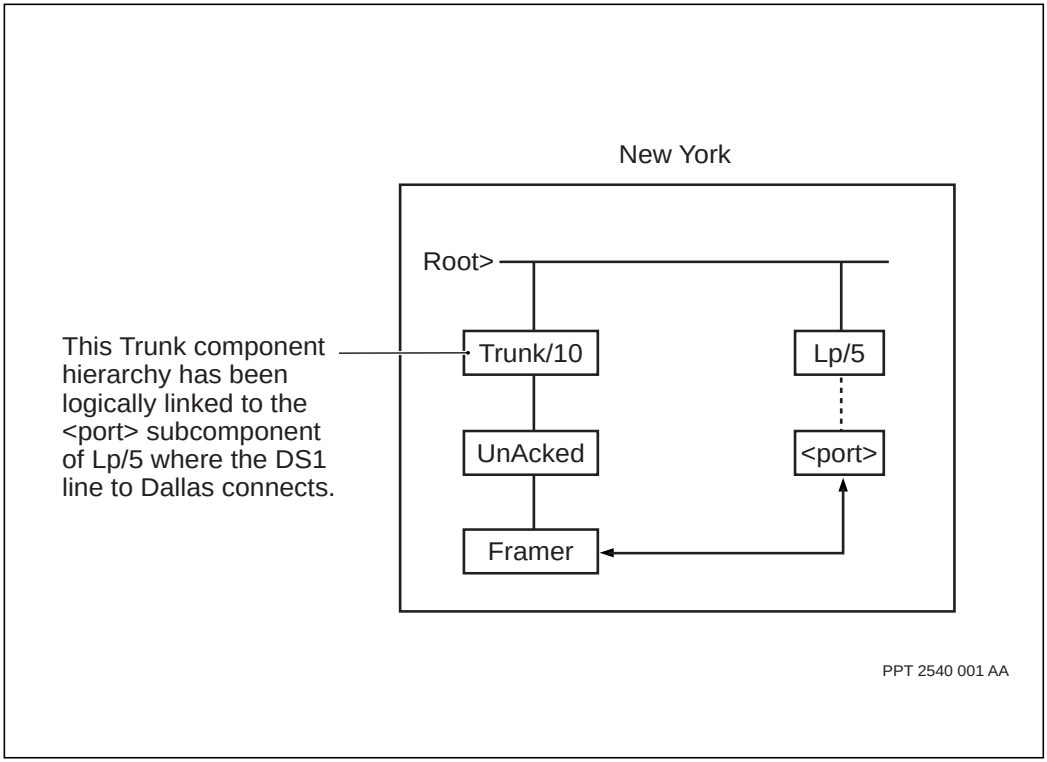
```
set sw lpt/unackTrunk featureList ! unackTrunks
porsTrunks
```

Note: You only need to add PORS trunks to the feature list if voice, video, or other connection-oriented traffic will be transferred over frame-cell trunks.

4 End provisioning mode.

Procedure job aid

Figure 3
Frame-cell trunk component hierarchy



Provisioning a frame-cell trunk

Provision a frame-cell trunk using values provided by your network administrator.

Prerequisites

- For information on which FPs support Passport trunks, refer to 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Procedure steps

1 Start provisioning mode.

2 Add a *Trunk* component.

```
add trunk/<n>
```

Note: The *Trunk* component provides the node-to-node connection. You must provision this component on both ends of the connection (on both Passport 7400, 15000 nodes).

3 Add an *UnAcked* component.

```
add trunk/<n> unack
```

The *UnAcked* component provides a Layer 2 protocol that adds the minimum amount of overhead to data on the link. The system automatically adds the *Framer* component to the selected link protocol component.

Note: Ensure the *Framer* component has the value of the *framingType* attribute set to *interrupting* if a *PathAdmin* (*Pa*) component is provisioned.

4 If you are going to use PORS routing then define the *Pa* component.

```
add trunk/<n> pa
```

The *Pa* allows the *Trunk* component to support PORS traffic.

5 Link the *Framer* component to the required Port or *Channel* component, depending on the type of FP used.

```
set trunk/<n> unack framer interfaceName lp/<p>
<port>/<m> channel/<c>
```

6 Set the framing type.

```
set trunk/<n> unack framer framingType <type>
```

7 If you need notification of Passport trunk utilization over a provisioned bandwidth threshold, set the Passport trunk utilization alarm threshold mechanism. Provision utilization thresholds for each *Trunk UnAcked* component.

```
set trunk/<n> unack framer linkUtilAlarmStatus
<status>
```

```
set trunk/<n> unack framer minorLinkUtilAlarmThreshold
<value1>
```

```
set trunk/<n> unack framer majorLinkUtilAlarmThreshold
<value2>
```

```
set trunk/<n> unack framer
criticalLinkUtilAlarmThreshold <value3>
```

Note 1: The Passport trunk utilization alarm mechanism is *disabled* by default.

Note 2: An alarm threshold of 100% disables that threshold.

8 End provisioning mode.

Variable definitions

Variable	Value
<c>	is the channel instance
<m>	is the port number
<n>	is the instance value of the *Trunk* component between 0 and 65535
<p>	is the logical processor number
<port>	is the FP type
<status>	linkUtilAlarmStatus is enabled or disabled
<type>	is interrupting if the trunk is for a PORS service or DPRS multimedia service, and hdlc for any other type of service
<value1>	specifies the minor alarm threshold percentage (0% to 100%)
<value2>	specifies the major alarm threshold percentage (0% to 100%)
<value3>	specifies the critical alarm threshold percentage (0% to 100%)

Provisioning ISDN dial backup

Enable the Passport trunk speed change reporting mechanism for ISDN dial backup applications. The Passport trunk propagates speed variations to the routing systems.

Prerequisites

- If you are unfamiliar with the dynamic speed change feature for Passport trunks, see “Dynamic Passport trunk speed change for frame-cell trunks” (page 126)

Procedure steps

1. Start provisioning mode.
2. Provision the trunk according to “Provisioning a frame-cell trunk” (page 28).
3. Select a threshold for reporting a speed change.

   `set trunk/<n> speedReportingThresholds <expected-speed-of-backup-lines, expected-speed-of-leased-line>`

   Set the period for delaying the speed change report. The default value is 30 seconds.

   `set trunk/<n> speedReportingHoldOff <seconds>`
4. If required, you can set the speed change alarms to indicate when the third-party device is in backup mode.

   `set trunk/<n> lowSpeedAlarmThreshold <expected-speed-of-leased-line>`

   If the measured speed decreases below the leased line speed, the low-speed alarm is set. The alarm indicates that the leased line failure has occurred and the third-party device is either in backup mode, or it is dialing up the backup lines. The alarm clears when the measured speed returns to the expected leased line speed.

   `set trunk/<n> highSpeedAlarmThreshold <threshold>`

   Note: No high-speed alarm is set due to a speed increase.

Variable definitions

Variable	Value
<n>	is the instance value of the *Trunk* component between 0 and 65535
<seconds>	is the period of time
<threshold>	specifies the maximum value of normal speeds for the trunk. See 241-5701-060 *Passport 7400, 15000, 20000 Components* for the default value.

Provisioning scheduled ISDN BWoD

Enable the Passport trunk speed change reporting mechanism to provision the scheduled ISDN BWoD application (Passport 7400 only). The Passport trunk propagates speed variations to the routing systems.

Prerequisites

- If you are unfamiliar with the dynamic speed change feature for Passport trunks, see "Dynamic Passport trunk speed change for frame-cell trunks" (page 126)

Procedure steps

1 Start provisioning mode.

2 Provision the Passport trunk according to "Provisioning a frame-cell trunk" (page 28).

3 Select a threshold for reporting a speed change.

```
set trunk/<n> speedReportingThresholds
<expected-speed-of-leased-line,
expected-peak-speed>
```

Set the period for delaying the speed change report. The default value is 30 seconds.

```
set trunk/<n> speedReportingHoldOff <seconds>
```

4 If required, you can set the speed change alarms to indicate when the third-party device is using the BWoD mode of operation.

```
set trunk/<n> highSpeedAlarmThreshold
<expected-speed-of-leased-line>
```

If the measured speed increases above the leased line speed, the high-speed alarm is set indicating that the third-party device is using extra bandwidth. The alarm clears when the measured speed returns to the expected leased line speed.

```
set trunk/<n> lowSpeedAlarmThreshold <threshold>
```

Note: No alarm is set due to a speed decrease.

Variable definitions

Variable	Value
<n>	is the instance value of the *Trunk* component between 0 and 65535
<seconds>	is the period of time
<threshold>	is the default value of zero.

Provisioning alarms for dynamic ISDN BWoD

In the dynamic ISDN BWoD application, the Passport trunk speed change reporting mechanism is disabled. Passport trunk speed variations do not propagate to the routing systems. The speed change alarms are necessary to indicate when the third-party device is in the BWoD mode. The feature applies to Passport 7400 series switches only).

Prerequisites

- If you are unfamiliar with the dynamic speed change feature for Passport trunks, see "Dynamic Passport trunk speed change for frame-cell trunks" (page 126)

Procedure steps

1. Start provisioning mode.
2. Provision the Passport trunk according to "Provisioning a frame-cell trunk" (page 28).
3. If required, you can set the speed change alarms to indicate when the third-party device is using the BWoD mode of operation.

   `set trunk/<n> highSpeedAlarmThreshold <expected-speed-of-leased-line>`

   If the measured speed increases above the leased line speed, the high-speed alarm indicates that the third-party device is using extra bandwidth. The alarm clears when the measured speed returns to the expected leased line speed.

   `set trunk/<n> lowSpeedAlarmThreshold <threshold>`

   Note: No alarm is set due to a speed decrease.

Variable definitions

Variable	Value
<n>	is the instance value of the *Trunk* component between 0 and 65535
<threshold>	is the default value of zero.

Provisioning ISDN dial backup with scheduled BWoD

Enable the Passport trunk speed change reporting mechanism to provision ISDN dial backup with scheduled BWoD. The Passport trunk propagates speed variations to the routing systems. This feature is available on Passport 7400 series switches only.

Prerequisites

- If you are unfamiliar with the dynamic speed change feature for Passport trunks, see "Dynamic Passport trunk speed change for frame-cell trunks" (page 126)

Procedure steps

1. Start provisioning mode.
2. Provision the Passport trunk according to "Provisioning a frame-cell trunk" (page 28).
3. Select a threshold for reporting a speed change.

   ```
   set trunk/<n> speedReportingThresholds
   <expected-backup-speed,
   expected-speed-of-leased-line, expected-peak-speed>
   ```

   Set the period for delaying the speed change report. The default value is 30 seconds.

   ```
   set trunk/<n> speedReportingHoldOff <seconds>
   ```

4. If required, you can set the speed change alarms to indicate when the third-party device is using either the backup or the scheduled BWoD mode of operation.

   ```
   set trunk/<n> lowSpeedAlarmThreshold
   <expected-speed-of-leased-line>
   ```

   ```
   set trunk/<n> highSpeedAlarmThreshold
   <expected-speed-of-leased-line>
   ```

   If the measured speed decreases below the leased line speed, the Passport trunking system sets the low decrease series trunking system sets the low decrease alarm. The alarm indicates that a leased line failure has occurred and the third-party device is either in backup mode or it is dialing up the backup lines. The alarm clears when the measured speed returns to the expected leased line speed.

If the measured speed increases above the leased line speed, the Passport trunking system sets the high-speed alarm. The alarm indicates that the third party device is using extra scheduled bandwidth. The alarm clears when the measured speed returns to the expected leased line speed.

Variable definitions

Variable	Value
<n>	is the instance value of the *Trunk* component between 0 and 65535
<seconds>	is the period of time

Provisioning ISDN dial backup with dynamic BWoD

In the dial backup application, the Passport trunk speed change reporting mechanism is enabled. The trunk propagates speed variations to the routing systems. In the dynamic BWoD application, the trunk speed change reporting mechanism is disabled. Passport trunk speed variations do not propagate to the routing systems. This feature is available on Passport 7400 switches only.

Prerequisites

- If you are unfamiliar with the dynamic speed change feature for Passport trunks, see “Dynamic Passport trunk speed change for frame-cell trunks” (page 126)

Procedure steps

1. Start provisioning mode.
2. Provision the Passport trunk according to “Provisioning a frame-cell trunk” (page 28).
3. Select a threshold for reporting a speed change.

   ```
   set trunk/<n> speedReportingThresholds
   <expected-backup-speed,
   expected-speed-of-leased-line>
   ```

4. Set the period for delaying the speed change report. The default value is 30 seconds.

   ```
   set trunk/<n> speedReportingHoldOff <seconds>
   ```

5. If required, you can set the speed change alarms to indicate when the third-party device is using either the backup or the dynamic BWoD mode of operation.

   ```
   set trunk/<n> lowSpeedAlarmThreshold
   <expected-speed-of-leased-line>
   ```

   ```
   set trunk/<n> highSpeedAlarmThreshold
   <expected-speed-of-leased-line>
   ```

   If the measured speed decreases below the leased line speed, the Passport trunking system sets the low-speed alarm The alarm indicates that a leased line failure has occurred and the third-party device is either in backup mode or it is dialing up the backup lines. The alarm clears when the measured speed returns to the expected leased line speed.

If the measured speed increases above the leased line speed, the Passport trunking system sets a high-speed alarm. The alarm indicates that the third party device is using extra bandwidth that the third party device dialed up dynamically to accommodate the traffic peaks. The alarm clears when the measured speed returns to the expected leased line speed.

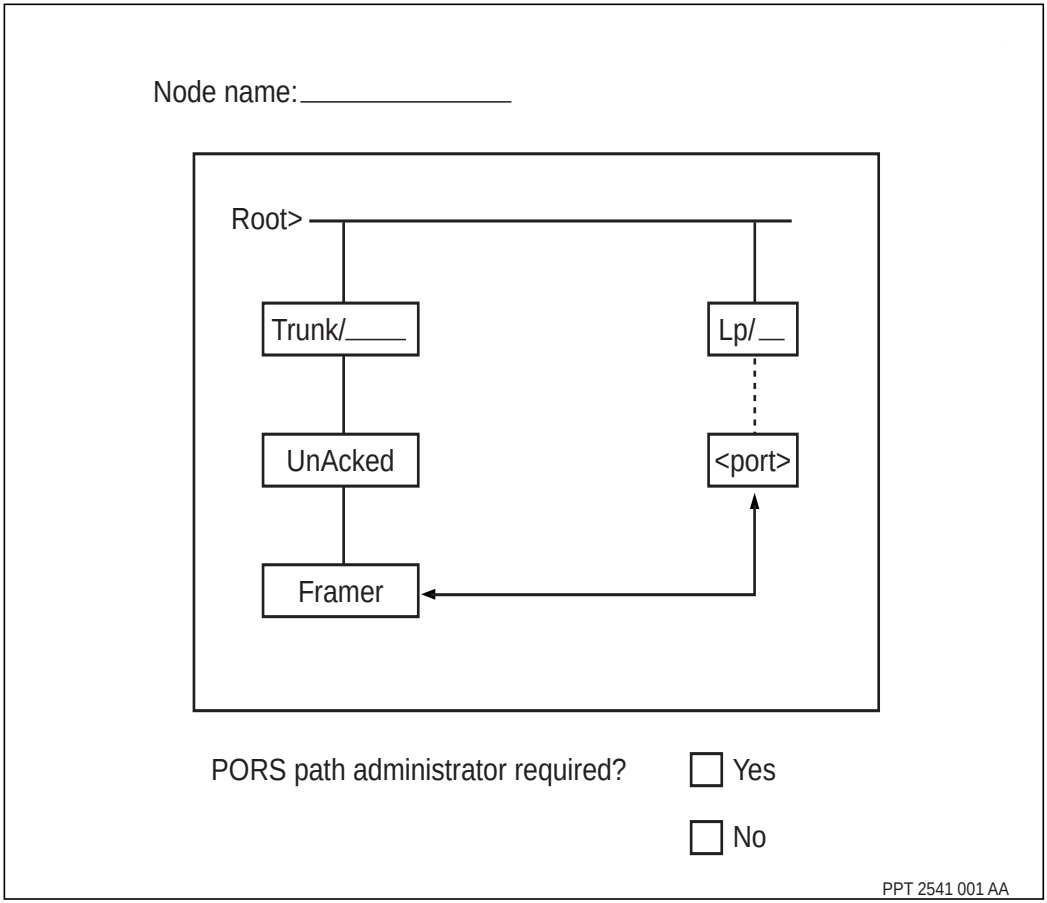
Variable definitions

Variable	Value
<expected-backup-speed, expected-speed-of-leased-line>	is the trunk speed reporting threshold values
<n>	is the instance value of the *Trunk* component between 0 and 65535
<seconds>	is the period of time

Provisioning worksheet for frame-cell trunks on a Passport 7400 series switch

This section provides examples of provisioning frame-cell trunks using the details in Figure 4, "Provisioning worksheet for frame-cell trunks," (page 39). The figure shows a diagram that you can use to record the details for your frame-cell trunk. Make copies of this page and use it. Give the copies to your network administrator to fill in the necessary blanks. These sheets closely match the format and sequence as followed in this guide.

Figure 4
Provisioning worksheet for frame-cell trunks



<port>: The exact *port* subcomponent to which the *Framer* component links depends on the type of function processor. See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* for provisioning information on the subcomponent for each FP.

Chapter 3
Provisioning ATM trunks

Provision Passport trunks over ATM to logically interconnect Passport nodes over ATM facilities.

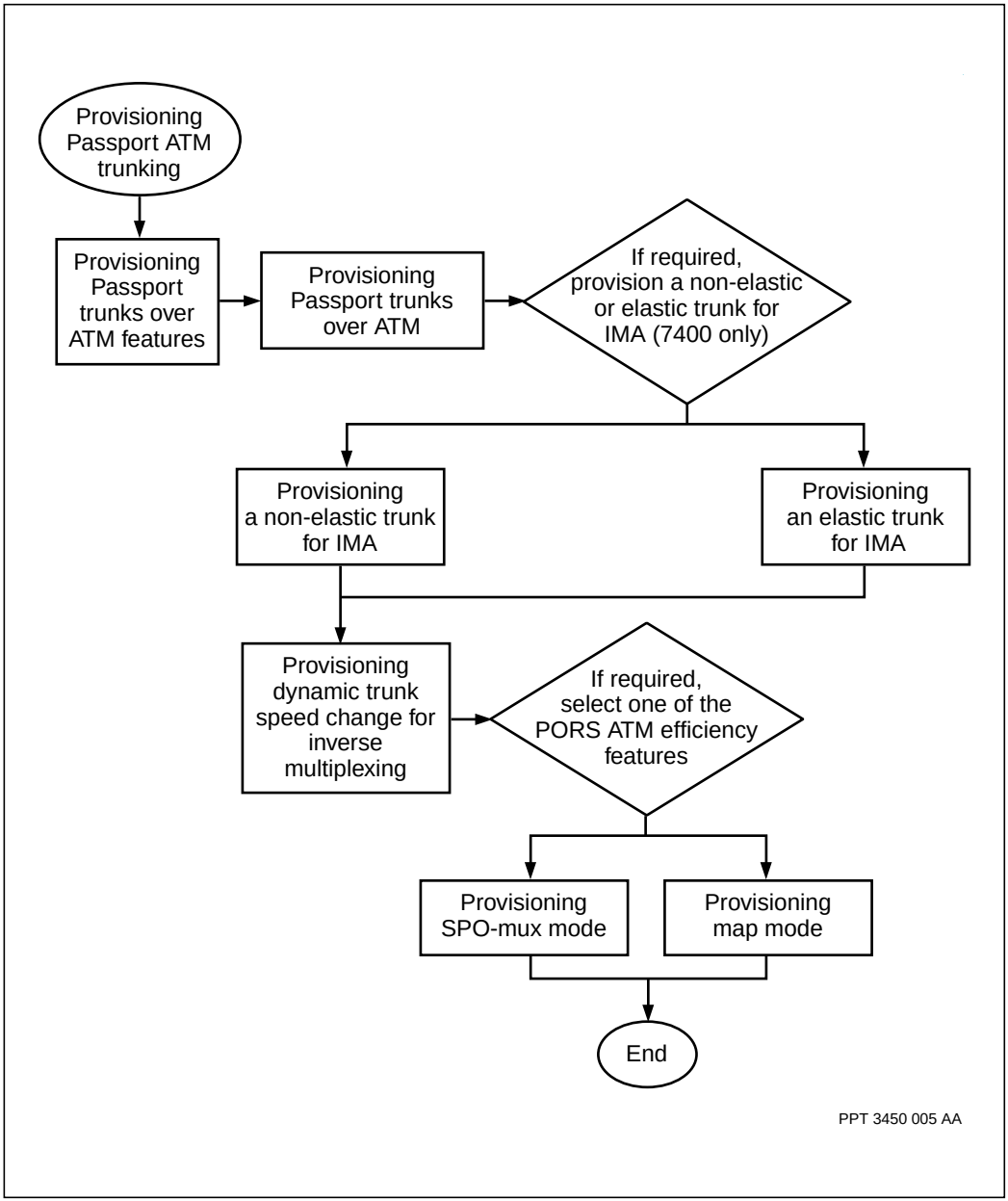
Prerequisites to provisioning ATM trunks

- If you are unfamiliar with provisioning ATM trunks concepts, see "Understanding Passport trunking" (page 97) and "Passport trunks over ATM" (page 135).
- Use the "Provisioning worksheet for Passport trunks over ATM" (page 60) to assist in determining appropriate configuration values.

Provisioning ATM trunks task flow

This task flow shows you the sequence of procedures you perform to provision ATM trunks. To link to any procedure, go to "Task flow navigation" (page 43).

Figure 5
Provisioning ATM trunks task flow



Task flow navigation

- “Provisioning Passport trunks over ATM features” (page 44)
- “Provisioning Passport trunks over ATM” (page 46)
- “Provisioning a non-elastic trunk for IMA” (page 49)
- “Provisioning an elastic trunk for IMA” (page 50)
- “Provisioning dynamic trunk speed change inverse multiplexing” (page 52)
- “Provisioning SPO-mux mode” (page 54)
- “Provisioning map mode” (page 58)

Provisioning Passport trunks over ATM features

You need to specify the Passport trunks over ATM features in the logical processor types feature list.

Prerequisites

- Ensure the required ATM interface and connection have been properly configured. See 241-5701-710 *Passport 7400, 15000, 20000 ATM Configuration Guide* for more information.
- Ensure an Lp/port has been provisioned for the *AtmIf* components used by the Passport trunk feature.
- Ensure the Network Administrator has supplied all of the appropriate provisioning information. This information includes such things as Trunk instance values, and the type of routing used (PORS, connectionless, or both).

  Note: Be aware that when a Passport trunk on a PQC-based FP is connected to another Passport trunk that is on a CQC-based FP, then the entire PQC-based FP reverts to software forwarding for dynamic packet routing system (DPRS). This results in a significant performance degradation. On a PQC12-based FP, it does not revert to software forwarding, but uses hardware forwarding instead; therefore, there is no performance degradation.

Procedure steps

1 Start provisioning mode.

2 Add the *AtmTrunks* component to the application software.

```
add sw lpt/atmtrk
```

3 Use the set command to specify the required features in the logical processor's feature list.

```
set sw lpt/atmtrk featureList ! atmTrunks porsTrunks
```

Note: You need PORS trunks in the feature list only if voice, video, or other connection-oriented traffic will use Passport trunks over ATM.

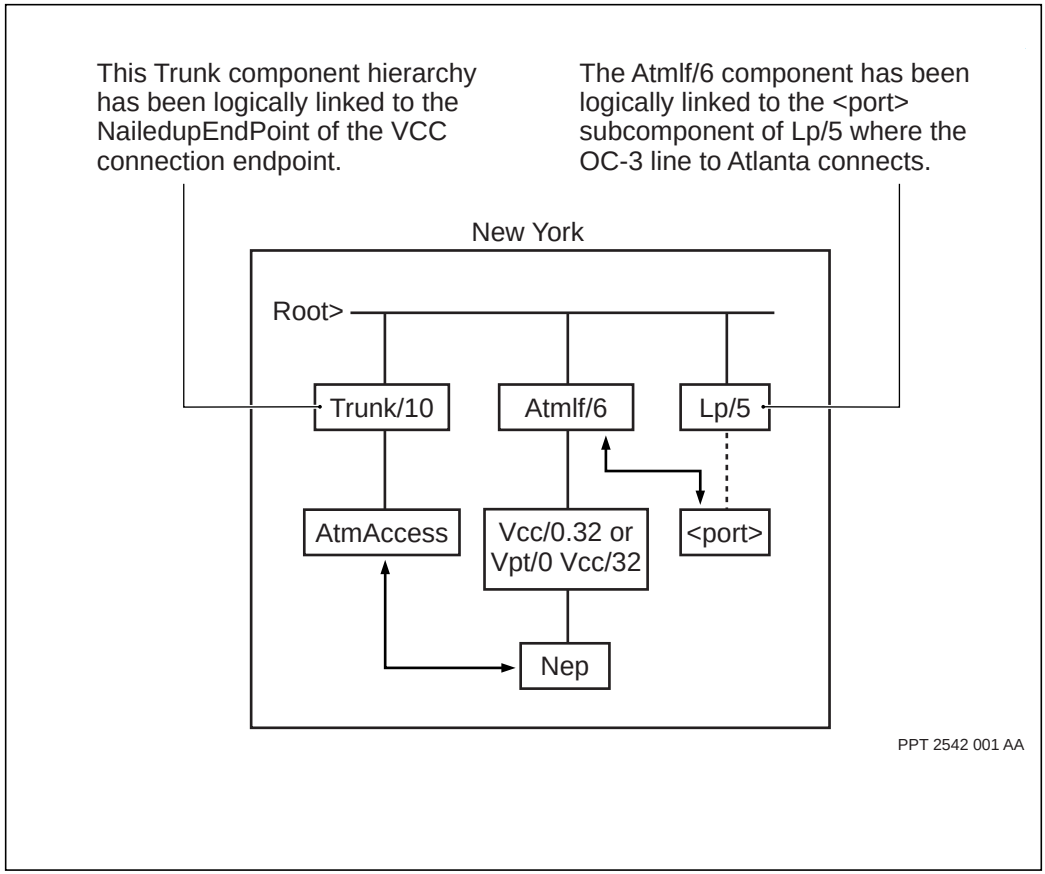
4 End provisioning mode.

When you have completed this procedure, the logical processor (*Lp*), *AtmIf*, *Vpt, Vcc* and *Nep* components are provisioned. See 241-5701-600

Passport 7400, 15000, 20000 Configuration Guide for information on provisioning logical processors (Lps) and 241-5701-710 *Passport 7400, 15000, 20000 ATM Configuration Guide* for detailed information on provisioning the ATM interface and connections.

Procedure job aid

Figure 6
Passport trunks over ATM component hierarchy example



Provisioning Passport trunks over ATM

Using values provided by your network administrator, provision Passport trunks over ATM.

Procedure steps

1. Start provisioning mode.
2. Add a *Trunk* component.

   add trunk/<n>

   The *Trunk* component has default values assigned to its attributes. Use the set command to alter these values.

   Note: The *Trunk* component provides the node-to-node connection. This component must be provisioned on both ends of the connection (on both Passport nodes).
3. Add an *AtmAccess* component.

   add trunk/<n> atm
4. If there is not already one configured, configure the ATM connection. The connection can be associated with the interface, or with a virtual path terminator. See 241-5701-710 *Passport 7400, 15000, 20000 ATM Configuration Guide* for details.
5. Use the SET command to alter the values assigned to the *Tm* component to satisfy the requirements of the *atmConnection*.

   set AtmIf/<m> [Vpt/<Vpi>] Vcc/<x> Vcd Tm txTrafficDescType 3

   set AtmIf/<m> [Vpt/<Vpi>] Vcc/<x> Vcd Tm txTrafficDescParm 1 <PCR>

   set AtmIf/<m> [Vpt/<Vpi>] Vcc/<x> Vcd Tm atmServiceCategory <service>

   The following restrictions apply when provisioning Passport trunks over ATM:

   - The only permissible value for both rxTrafficDescType attribute and txTrafficDescType is 3.
   - Passport trunks over ATM do not support unspecified bit rate (UBR), the default ATM service category on Passport.

- For the CBR service category, the txQueueLimit attribute must be at least 88 in order for the trunk to stage.
- For the rt-VBR and nrt-VBR service categories, the txQueueLimit attribute must be set to 0 or at least 88 in order for the trunk to stage (for values between 0 and 88 the trunk will not stage). Also, the minPerVcQueueLimit attribute must be set to at least 88 in order for the trunk to stage.

6 Add the *NailedUpEndPoint* component

```
add AtmIf/<m> [Vpt/<Vpi>] Vcc/<x> Nep
```

7 Link this application component to the *NailedUpEndPoint* component.

```
set trunk/<n> atmAccess atmConnection AtmIf/<m>
[Vpt/<Vpi>] Vcc/<x> Nep
```

8 If you are going to use PORS routing, add a *PathAdmin* (*Pa*) component.

```
add trunk/<n> pa
```

The *Pa* component has default values assigned to its attributes. Use the SET command to alter these values.

9 If you need utilization notification for Passport trunks over ATM over a provisioned bandwidth threshold, set the Passport trunks over ATM utilization alarm mechanism. Provision utilization thresholds for each *Trunk ATMAccess* component.

Note: The utilization calculation is provided for the AAL5 VCC only. It does not account for the traffic received by VCCs that are managed directly by the *Trunk PA* component. Traffic on the companion VCCs in SPO-mux mode and map mode trunks is not considered by the utilization alarm. As a result, the alarm threshold must be set according to the amount of DPRS and PORS AAL5-mux traffic that the link is likely to carry.

```
set trunk/<n> atm vccUtilAlarmStatus <status>

set trunk/<n> atm minorVccUtilAlarmThreshold <value1>

set trunk/<n> atm majorVccUtilAlarmThreshold <value2>

set trunk/<n> atm criticalVccUtilAlarmThreshold
<value3>
```

The Passport trunks over ATM utilization alarm mechanism is disabled by default.

An alarm threshold of 200% disables the alarm threshold.

When the critical alarm is received by Preside MDM, the trunk is marked as out of service. The trunk itself is still up but if the threshold is set correctly, the trunk is nearing saturation.

10 End provisioning mode.

Variable definitions

Variable	Value
<m>	is the *AtmIf* component instance value
<n>	is the instance value of the *Trunk* component between 0 and 65535
<Vpi>	defines the instance of the *Vpt* component.
[Vpt/<Vpi>]	is the *VirtualPathTerminator* component. Use this parameter if you are associating the virtual connection with a virtual path terminator.
<x>	defines the instance of the *Vcc* component. If the virtual channel is associated with an *AtmIf* component, <x> represents the VPI.VCI value. If the virtual channel is associated with a *Vpt* component, <x> represents VCI value.
<status>	is enabled or disabled
<value1>	specifies the minor alarm threshold percentage (0% to 200%)
<value2>	specifies the major alarm threshold percentage (0% to 200%)
<value3>	specifies the critical alarm threshold percentage (0% to 200%)

Provisioning a non-elastic trunk for IMA

Provision a non-elastic trunk connection which is either up with its full committed bandwidth or down. When the IMA link group capacity drops, some non-elastic connections in an ATM interface must be released according to the connection bandwidth control (CBC) algorithm. The order in which the non-elastic trunks release is based on their holding priority relative to other non-elastic connections. The trunk speed change reporting mechanism is disabled for non-elastic trunks. This feature is available for Passport 7400 series switches only.

Procedure steps

1. Start provisioning mode.
2. Set up the Passport trunk over ATM as non-elastic and disable the trunk speed change reporting mechanism, by clearing the list of thresholds.

   ```
   set trunk/<n> atmAccess bwElastic no

   set trunk/<n> speedReportingThresholds !
   ```

3. End provisioning mode.

Variable definitions

Variable	Value
<n>	is the instance value of the *Trunk* component between 0 and 65535

Provisioning an elastic trunk for IMA

Provision an elastic trunk for IMA where the ATM software admits a bandwidth elastic trunk regardless of the bandwidth available. If the bandwidth is available, the ATM software admits an elastic trunk at full bandwidth. If only part of the requested bandwidth is available, or if other elastic trunks must be reduced to make room for it, the ATM software admits the elastic trunk at reduced bandwidth.

The ATM software does not release an elastic trunk if the bandwidth available to the trunk is reduced. The elastic trunks allocated bandwidth is subject to change according to the connection bandwidth control (CBC) algorithm when the link group capacity fluctuates.

This feature is only available for Passport 7400 series switches

Procedure steps

1. Start provisioning mode.
2. Set up the *Trunk AtmAccess* component over IMA as elastic.

   `set trunk/<n> atmAccess bwElastic yes`
3. Set the threshold (in bit/s) for reporting the speed change.

   `set trunk/<n> speedReportingThresholds <level1, level2, level3, expected-normal-bandwidth>`
4. Set the period for delaying the speed change report. The default value is 30 seconds.

   `set trunk/<n> speedReportingHoldOff <seconds>`

   If required, you can set the speed change alarms to indicate when the FP experiences facility problems.

   The values of the speed alarm threshold attributes are expressed in bit/s.

   `set trunk/<n> lowSpeedAlarmThreshold <expected-normal-bandwidth>`

   If the measured speed decreases below the expected normal bandwidth, which can be the same as the PCR, the low speed alarm indicates a facility problem. The alarm clears when the measured speed returns to the expected normal speed.

   `set trunk/<n> highSpeedAlarmThreshold <threshold>`

Note: No high-speed alarm is set due to a speed increase.

Variable definitions

Variable	Value
<n>	is the instance value of the *Trunk* component between 0 and 65535
<seconds>	is the period of time
<threshold>	specifies the maximum value of normal speeds for the trunk. See 241-5701-060 *Passport 7400, 15000, 20000 Components* for the default value.

Provisioning dynamic trunk speed change inverse multiplexing

Provision the Trunk *speedReportingThresholds* attribute to control the behavior of the dynamic speed reporting mechanism. There is no default value but an empty value disables the mechanism. In the inverse multiplexing application, the trunk speed change reporting mechanism is enabled. Passport trunk speed variations are propagated to the routing systems.

This feature is available on Passport 7400 series switches only.

Prerequisites

- If you are unfamiliar with the concepts relating to dynamic trunk speed change, see “Dynamic Passport trunk speed change on Passport trunks over ATM” (page 147)

Procedure steps

1. Start provisioning mode.
2. Provision the Passport trunk according to “Provisioning Passport trunks over ATM” (page 46).
3. Set the threshold (in bit/s) for reporting the speed change.

   ```
   set trunk/<n> speedReportingThresholds
   <level1, level2, level3, ... level6,
   expected-normal-bandwidth>
   ```

4. Set the period for delaying the speed change report. The default value is 30 seconds.

   ```
   set trunk/<n> speedReportingHoldOff <seconds>
   ```

5. If required, you can set the speed change alarms can be set to indicate when the third-party device experiences facility problems.

   ```
   set trunk/<n> lowSpeedAlarmThreshold
   <expected-normal-bandwidth>
   ```

   If the measured speed decreases below the expected normal bandwidth, the low-speed alarm is set indicating a facility problem. The alarm clears when the measured speed returns to the expected normal speed.

   ```
   set trunk/<n> highSpeedAlarmThreshold <threshold>
   ```

   Note: No high-speed alarm is set due to a speed increase.

Variable definitions

Variable	Value
<level1, level2, level3, ... expected-normal-bandwidth>	defines the thresholds at which the trunk should report speed increases to the routing system. You should set expected-normal-bandwidth to the expected normal bandwidth for the trunk. Optionally, you can define up to six additional thresholds (<level1, level2, ...>) to control speed increase reporting at both lower and higher bandwidth allocation values.
<n>	is the instance value of the *Trunk* component between 0 and 65535
<seconds>	is the period of time
<threshold>	specifies the maximum value of normal speeds for the trunk. See 241-5701-060 *Passport 7400, 15000, 20000 Components* for the default value.

Provisioning SPO-mux mode

Provision a new VCC to use ATM efficiency on a Passport trunk over ATM. You can enable the SPO-mux mode transport capability by provisioning a new *Trunk* subcomponent and linking this subcomponent to a new VCC.

Note: To activate the PORS ATM efficiency feature you must provision both ends of the VCC.

Prerequisites

- You must have configured the required ATM interfaces and connections on the node before preforming this procedure. An ATM connection can be associated with and *AtmIf* or a *Vpt* component.For more information about ATM provisioning, see 241-5701-710 *Passport 7400, 15000, 20000 ATM Configuration Guide*.

Procedure steps

1 Start provisioning mode.

2 Configure the ATM interface and ATM connections as detailed in 241-5701-710 *Passport 7400, 15000, 20000 ATM Configuration Guide*.

3 Provision a new VCC to run voice or BTDS packet traffic.

```
add AtmIf/10 Vcc/0.35
```

Note: In this example the VCC is Vcc/0.35. If the VCC is associated with a virtual path terminator, the VPI value is the instance of the Vpt component. The VCI value is the instance of the Vcc component.

4 Add a *NailedUpEndPoint* (*Nep*) component under the Vcc connection.

```
add AtmIf/10 Vcc/0.35 Nep
```

Note: You can configure a VCC by provisioning attributes under the *Vcd* component.

5 Set the *endToEndLoopback* attribute.

```
set AtmIf/10 Vcc/0.35 Vcd endToEndLoopback on
```

The default value for the *endToEndLoopback* attribute is off. In this case, loopback is on since it provides a software continuity check. The check ensures that the VCC that is linked to the *Pa* component connects to its proper destination.

6 Set the type of traffic management for the transmit direction of the connection.

`set AtmIf/10 Vcc/0.35 Vcd Tm txTrafficDescType <txTdt>`

`set AtmIf/10 Vcc/0.35 Vcd Tm txTrafficDescParm <txTdp>`

When <txTdt> is 1 (the default value), you do not provision any traffic descriptor parameters.

When <txTdt> is 3, use parameter 1 of <txTdp> to specify peak cell rate (PCR) in cells/s for cell loss priority (CLP) 0 traffic and CLP1 traffic.

When <txTdt> is 6, use parameter 1 of <txTdp> to specify PCR in cells/s for CLP0 traffic and CLP1 traffic. Use parameter 2 of <txTdp> to specify sustained cell rate (SCR) in cells/s for CLP0 and CLP1 traffic. Use parameter 3 of <txTdp> to specify maximum burst size in cells.

7 Provision the *Trunk AtmAccess* component and attributes as outlined in Figure 6, “Provisioning Passport trunks over ATM,” (page 46).

8 Add a *Pa* component.

`add trk/10 pa`

The *Pa* component has default values assigned to its attributes. Use the set command to alter these values.

9 Add the *AtmAccess* component.

`add trk/10 pa atm`

Note: Make sure that you have fully provisioned Vcc/0.35 before attempting the next step.

10 Link the *atmConnection* attribute to the *NailedUpEndPoint* component.

`set TRK/10 pa ATM atmConnection AtmIf/10 Vcc/0.35 nep`

11 End provisioning mode.

Variable definitions

Variable	Value
<txTdp>	is a vector of five parameters. For PORS ATM efficiency, you can set one or three of the parameters.
<txTdt>	can be 1, 3, or 6. The default value is 1.

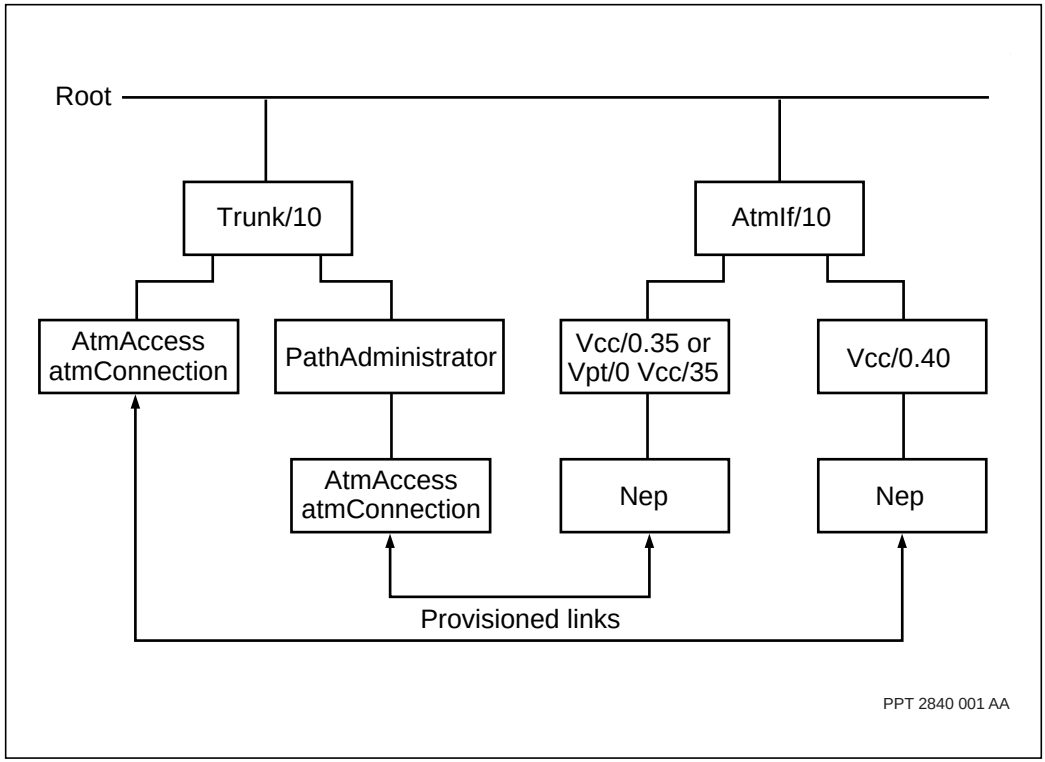
Procedure job aid

Figure 7, “Component hierarchy with sample links for ATM cell efficiency,” (page 57) illustrates the component hierarchy for the PORS ATM efficiency capability. In this figure, one Passport trunk over ATM is set up with two separate VCCs. One VCC is for voice or BTDS packet traffic and the other is for the rest of the traffic types. Other traffic types consist of frame relay, HTDS, and control traffic. To set up a VCC to carry these other traffic types you must set up direct AAL5 connections. You can do this by setting the *AtmConnection* attribute under the *AtmAccess* component and linking this to a specific VCC. In the example in Figure 7, “Component hierarchy with sample links for ATM cell efficiency,” (page 57), it is linked to AtmIf/10 Vcc/0.40.

To set up a VCC to carry only voice or BTDS packet traffic, set the *AtmConnection* attribute under the *AtmAccess* component which is located under the *pathAdministrator* component. Next, link these trunk attributes to a specific VCC as described above.

In the two-node Passport-to-Passport connection example in Figure 7, “Component hierarchy with sample links for ATM cell efficiency,” (page 57), it is linked to AtmIf/10 Vcc/0.35. You must repeat the provisioning steps in this procedure on both ends of the VCC to activate the ATM cell efficiency capability.

Figure 7
Component hierarchy with sample links for ATM cell efficiency



Provisioning map mode

Provision map mode if you want to map the calls to their own VCCs. You must set the *Pa AtmAccess mode* attribute to a value of map at both ends of the link.

Procedure steps

1. Start provisioning mode.
2. Provision the *AtmIf* component and its attributes as outlined in 241-5701-710 *Passport 7400, 15000, 20000 ATM Configuration Guide*.
3. Provision the *Trunk AtmAccess* component and attributes as outlined in “Provisioning Passport trunks over ATM” (page 46).
4. Add a *Pa* component.

   ```
   add trk/10 pa
   ```

   The *Pa* component has default values assigned to its attributes. Use the set command to alter these values.
5. Add the *AtmAccess* component.

   ```
   add trk/10 pa atm
   ```

   Note: Make sure that you have fully provisioned Vcc/0.35 before attempting the next step.
6. Set the *mode* attribute.

   ```
   set trk/10 pa atm mode map
   ```
7. End provisioning mode.

Determining the VCI range for a mapped call:
The difference between the *maxAutoSelectedVciForVpiZero* attribute and the *minAutoSelectedVciForVpiZero* attribute + 1, represents the maximum number of available dynamic VCCs. The value of the *Trunk Pa maxLc* attribute + 10 (the extra headroom provides for bumping and reduces clashing) must be less than this maximum number of dynamic VCCs. If not, the system raises an alarm 7018 0012, and disables map mode.

> ***Note:*** The VCI range is calculated in the same way for non-zero virtual paths: the *AtmIf CA maxAutoSelectedVciForNonZeroVpi* attribute replaces the *maxAutoSelectedVciForVpiZero* attribute and the *AtmIf CA minAutoSelectedVciForNonZeroVpi* attribute replaces the *minAutoSelectedVciFor VpiZero* attribute.

If you get an alarm, increase the *maxAutoSelectedVciForVpiZero* attribute under the CA component.

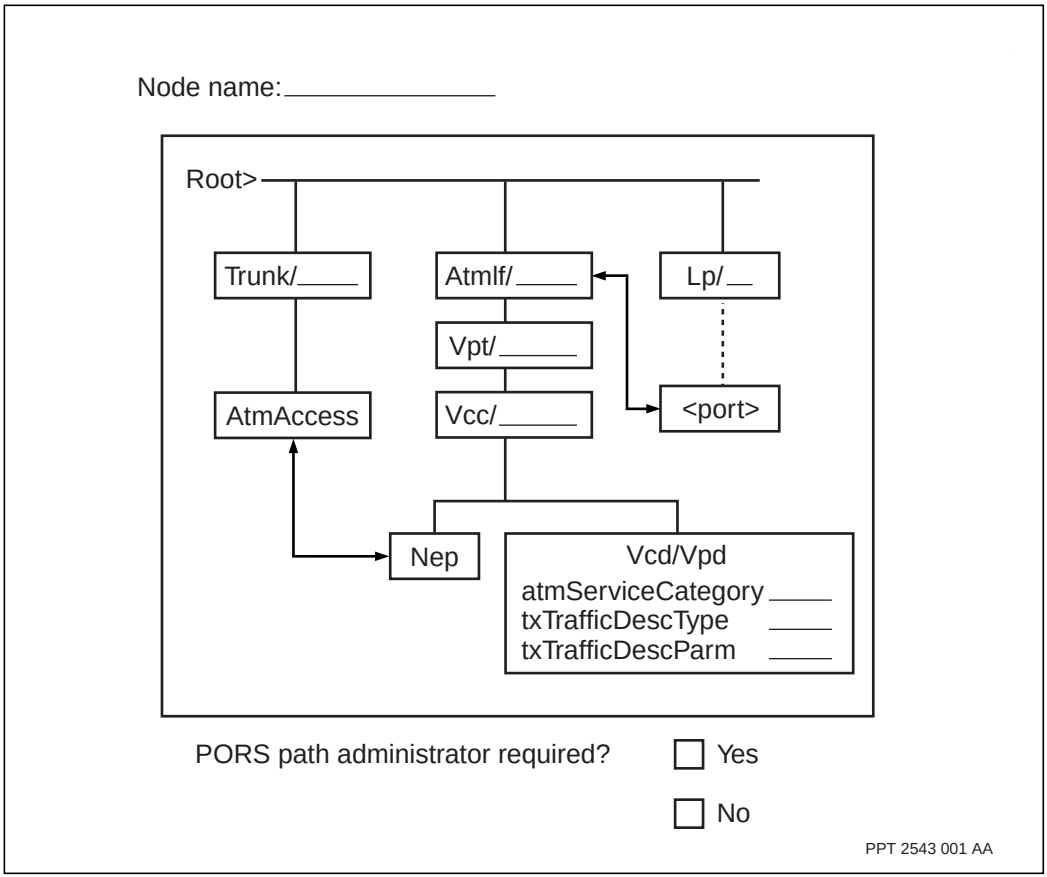
> ***Note:*** On CQC cards, the value for the *maxAutoSelectedVciForVpiZero* attribute must not exceed the number of VCCs allowed under the *conmap* component. If you wish to increase the *maxAutoSelectedVciForVpiZero* attribute, you may have to first increase the ranges in the *connmap component*.

For details, see 241-5701-710 *Passport 7400, 15000, 20000 ATM Configuration Guide*.

Provisioning worksheet for Passport trunks over ATM

This section provides examples of provisioning Passport trunks over ATM using the details in Figure 8, “Provisioning worksheet for Passport trunks over ATM,” (page 60). The figure shows a diagram that you can use to record the details for your Passport trunk over ATM. Make copies of this page and use it. Give the copies to your network administrator to fill in the necessary blanks. These sheets closely match the format and sequence as followed in this guide.

Figure 8
Provisioning worksheet for Passport trunks over ATM



<port>: The exact *Port* subcomponent to which the *AtmIf* component links depends on the type of ATM function processor. See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* for provisioning information on the subcomponent for each FP.

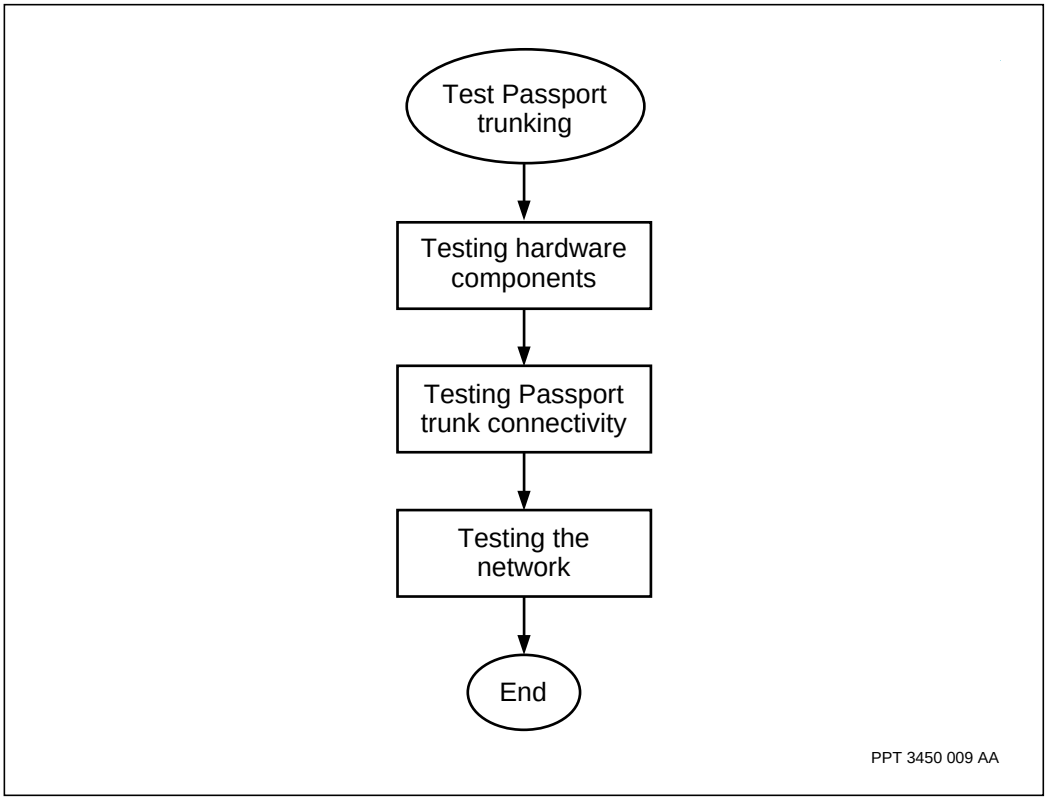
Chapter 4
Testing Passport trunks

Test Passport trunks to determine whether connections are provisioned and operating within expected parameters.

Testing Passport trunks task flow

This task flow shows you the sequence of procedures you perform to test Passport trunks. To link to any procedure, go to "Task flow navigation" (page 64).

Figure 9
Testing Passport trunks task flow



Task flow navigation

- “Testing hardware components” (page 65)
- “Testing Passport trunk connectivity” (page 66)
- “Testing the network” (page 67)

Testing hardware components

The first step in commissioning a Passport trunk is to use the test subcomponent functionality to determine the sanity of the physical portion of the connection.

For information on performing port tests, see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.

> ***Note:*** You must lock Passport trunks before performing port tests. For more information on Passport trunk disabling, see “Disabling a Passport trunk” (page 71).

For information on performing line tests, see of 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.

Testing Passport trunk connectivity

When the port and line tests are successful, verify the connection. Each Passport trunk expects to connect to a known port of a known node. This procedure tests the logical connection associated with a Passport trunk.

Procedure steps

1. Provision the Passport trunk at each end of the connection.
2. Set up each Passport trunk to alarm and disable if each Passport trunk does not provide a connection to each other's node.

   ```
   set trunk/<n> expectedRemoteNodeName <nodeName>
   ```

   ```
   set trunk/<n> remoteValidationAction disable
   ```
3. If the Passport trunk does not stage and does not issue an alarm indicating wrong remote then go to "Determining why a frame-cell trunk does not provide service" (page 94).
4. When the Passport trunk stages successfully verify the Passport trunk is connected to the expected remote Passport trunk with the expected facility speed and delay.

   ```
   display trunk/<n> remoteComponentName
   ```

   ```
   display trunk/<n> transport
   ```
5. Examine the Passport trunk statistics to verify connection quality.

   ```
   display trunk/<n> statistics
   ```

Variable definitions

Variable	Value
<n>	is the instance number of the Passport trunk between 0 and 65535
<nodeName>	is the remote node name

Testing the network

When the Passport trunk test is successful, verify the network connection. Each Passport trunk the routing system needs to know about the connection and exchange routing information with its counterpart on the remote node. This procedure tests the Passport-to-Passport connection associated with a Passport trunk.

Procedure steps

1. Verify the transport resource manager (TRM) knows about the Passport trunk and reflects the same operational attributes as shown by the Passport trunk.

   ```
   display trm lk/*
   ```

2. Verify the TRM knows about the node to which the Passport trunk connects and reflects the same operational attributes as shown by the Passport trunk.

   ```
   display trm lg/<nodeName>
   ```

3. Verify that topology knows about the node to which the Passport trunk connects and reflects the same operational attributes as shown by the Passport trunk.

   ```
   display rtg top node/<nodeName>
   ```

   ```
   display rtg top node/<nodeName> lg/*
   ```

4. Repeat these steps on the remote node.

Variable definitions

Variable	Value
<nodeName>	is the node name

Chapter 5
Monitoring Passport trunks

Gather information on the condition of Passport trunks to monitor trunk status and performance.

- “Monitoring Passport trunks tasks” (page 69)

Monitoring Passport trunks tasks

The following tasks show the procedures you can perform to monitor Passport trunks.

- “Determining Passport trunk component states” (page 70)
- “Disabling a Passport trunk” (page 71)
- “Re-enabling a Passport trunk” (page 73)
- “Alarms and state change notifications” (page 74)
- “Changing provisioned Passport trunk overrides” (page 75)
- “Setting Passport trunk protocol idle time out duration” (page 76)
- “Displaying Passport trunk statistics” (page 77)
- “SPO-mux mode operational procedures for PORS” (page 79)
- “Map mode operational procedures for PORS” (page 80)
- “Determining Passport trunk over ATM utilization for PORS” (page 81)
- “Definition of the IfTable” (page 82)
- “Support of SNMP enterprise MIBS” (page 83)

Determining Passport trunk component states

Determine the state and status of all the Passport trunks on a Passport node.

Prerequisites

- For information about OSI states for Passport trunks, see “OSI states for Passport trunks” (page 108)
- For more information on OSI model states in general, see 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

Procedure steps

1 Display the state and status of each operational Passport trunks on Passport node using the following command:

```
display trunk/* osi
```

The system displays information for each operational Passport trunk on your Passport node:

```
Trk/<n>
  adminState =
  operationalState =
  usageState =
  availabilityStatus =
  proceduralStatus =
  controlStatus =
  alarmStatus =
  standbyStatus =
  unknownStatus =
```

A Passport trunk is fully operational if the OSI model states in the displayed list appear as

```
  adminState = unlocked
  operationalState = enabled
  usageState = busy
```

If any other state indicators appear, then the Passport trunk is not fully operational. To detect any problems, you must understand how to interpret OSI model state attributes, such as *usageState*, *operationalState* and *adminState*.

Disabling a Passport trunk

The following procedure explains how to lock *Trunk* components. The -forever option locks the Passport trunk indefinitely rather than just for five minutes. The -force option forces the channels down rather than waiting.

CAUTION
Risk of node isolation
Locking a Passport trunk forever can result in node isolation.

Prerequisites

- for information about operational disabling of Passport trunks, see “Operational disabling of Passport trunks” (page 111)
- for information about restaging, see “The Passport trunk restaging mechanism” (page 112)

Procedure steps

1 Lock the Passport trunk.

```
lock trunk/<n>
```

This command sets the Passport trunk to the OSI model administrative locked state, disabling the Passport trunk for five minutes. Next, the Passport trunk returns to the OSI model unlocked state and attempts to restage with the remote network element. If the Passport trunk is supporting *LogicalChannel* subcomponents, it enters the OSI model administrative ShuttingDown state and waits for all of these channels to go away before it starts the disabling sequence. You can issue an unlock command during this time, returning the Passport trunk to the unlocked state so that it can continue to provide service.

2 Force a lock on a Passport trunk.

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

This command sets the Passport trunk to the OSI model administrative locked state, disabling the Passport trunk for five minutes. Next, the Passport trunk returns to the OSI model unlocked state and attempts to restage with the remote network element. If the Passport trunk is supporting *LogicalChannel* subcomponents, it enters the OSI model administrative ShuttingDown state and forces all of these channels to go

away before it starts the disabling sequence. You can issue an unlock command during this time, returning the Passport trunk to the unlocked state so that it can continue to provide service. Only LogicalChannels not yet disabled continue to provide service.

3 Lock a Passport trunk indefinitely.

```
lock -forever trunk/<n>
```

This command sets the Passport trunk to the OSI model administrative locked state, disabling the Passport trunk indefinitely. An unlock command is necessary to put the Passport trunk in the OSI model unlocked state for an attempt to restage with the remote network element. If the Passport trunk is supporting *LogicalChannel* subcomponents, it enters the OSI model administrative ShuttingDown state and waits for all of these channels to go away before it starts the disabling sequence. You can issue an unlock command during this time, returning the Passport trunk to the unlocked state so that it can continue to provide service.

Note: Use the lock -forever command carefully to avoid isolating a Passport node.

4 Force a lock on a Passport trunk indefinitely.

```
lock -force -forever trunk/<n>
```

This command sets the Passport trunk to the OSI model administrative locked state, disabling the Passport trunk indefinitely. An unlock command is necessary to put the Passport trunk in the OSI model unlocked state for an attempt to restage with the remote network element. If the Passport trunk is supporting *LogicalChannel* subcomponents, it enters the OSI model administrative ShuttingDown state and forces all of these channels to go away before it starts the disabling sequence. You can issue an unlock command during this time, returning the Passport trunk to the unlocked state so that it can continue to provide service. Only LogicalChannels not yet disabled continue to provide service.

Variable definitions

Variable	Value
<n>	is the instance number of the Passport trunk between 0 and 65535

Re-enabling a Passport trunk

If a Passport trunk has been disabled due to a lock -forever or lock -force -forever command, you can re-enable it using the unlock command. Alternately, if a Passport trunk has been disabled with a lock or lock -force command, it will re-enable itself within five minutes of being locked.

Prerequisites

- for information about operational disabling of Passport trunks, see “Operational disabling of Passport trunks” (page 111)
- for information about restaging, see “The Passport trunk restaging mechanism” (page 112)

Procedure steps

1 Unlock the trunk.

```
unlock trunk/<n>
```

Note: Issuing this command results in the Passport trunk attempting to restage.

Variable definitions

Variable	Value
<n>	is the instance number of the Passport trunk between 0 and 65535

Alarms and state change notifications

Passport trunks follow the Passport approach to the generation of alarms and state change notifications (SCNs). In general, the system generates only a single alarm when a fault occurs. If there is a problem with the physical layer, then the responsible component issues an alarm, while the state of the *Trunk* component changes. The *Trunk* component issues an SCN on behalf of the entire protocol stack using the hardware.

For additional information on Passport alarms and SCNs, see 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

Changing provisioned Passport trunk overrides

Passport trunk overrides consist of two provisionable *Trunk* attributes: *overrideTransmitSpeed* and *overrideRoundTripDelay*. These attributes override the operational *Trunk* attributes *measuredRoundTripDelay* and *measuredSpeedToIf* when reporting to the routing system for metric calculations. You can control the metrics calculated for this Passport trunk and in turn the routing behavior by using overrides.

If you change either the *overrideTransmitSpeed* or *overrideRoundTripDelay* attribute

- while the *Trunk* component is providing service, then these values are renegotiated with the remote Passport trunk with no disruption to the service
- while the Passport trunk is still staging, then the Passport trunk immediately restages

If there is a mismatch on two ends, the system issues the alarm 7005 0108 (overrideRoundTripDelay) or 7005 0109 (overrideTransmitSpeed). No change in metrics occurs until both ends are running with the same override values.

Setting Passport trunk protocol idle time out duration

Idle time out duration specifies the duration a Passport trunk stays enabled even if the Passport trunk receives no packets from the remote end. This attribute allows you to control the time required to disable the Passport trunk when the connection between the two ends of the Passport trunk is troubled.

The value of the provisionable *Trunk idleTimeOut* attribute determines the Passport trunk protocol idle time out duration. If the local Passport trunk does not receive any packets from the link for the period specified by this attribute, the Passport trunk enters Are You There (AYT) mode for up to two seconds. If the Passport trunk does not receive any packets from the remote end during the AYT mode it restages. If it does receive packets it exits AYT mode and continues to provide service.

The default value for *idleTimeOut* attribute duration is four seconds.

Displaying Passport trunk statistics

Passport trunks support spooled statistics which are split into different traffic types (DPRS or PORS). You can monitor each of these statistics groups through corresponding Passport trunk statistics subcomponents. These subcomponents are only present when the Passport trunk you are monitoring supports that traffic type.

These statistics provide counts for

- number of successfully forwarded packets
- unsuccessfully forwarded packets
- number of octets received

Procedure steps

1 Display statistics for all the Passport trunks on a Passport node using the following command:

```
display trunk/* stats
```

The system displays the following statistics for each Passport trunk on your Passport node:

```
Trk/<n>
  pktFromIf =
  discardUnforward =
  intPktFromIf =
  discardIntUnforward =
  pktFromIfByPrio =
  discPktFromIfByPrio =
  octetFromIfByPrio =
  trunkPktFromIf =
  discardTrunkPktFromIf =
  trunkPktToIf =
  discardTrunkPktToIf =
  areYouThereModeEntries =
  stagingAttempts =
```

2 Display statistics for DPRS and PORS traffic on a Passport trunk using the following command:

```
d trunk/<n> <stats>
```

Variable definitions

Variable	Value
<n>	is the Passport trunk instance
<stats>	is DprsStats, or PorsStats for DPRS and PORS traffic

SPO-mux mode operational procedures for PORS

The *mode* operational attribute on the *Trk*/n *Lch*/m component shows the following values:

- SPO-cell-mux, when a channel is using the new VCC
- AAL5-frame-mux, when a channel is using the existing AAL5 VCC
- frame-mux, on non-ATM FPs

Note: The *localConnection* attribute indicates that the connections are associated with a given provisioned VCC's NEP.

The following example shows the display option and output used on trk/70:

```
d Trk/70 LCh/* mode, localConnection

Trk/70 LCh/1
  mode = AAL5-frame-mux
  localConnection = atmif/70 vcc/0.100

Trk/70 LCh/2
  mode = SPO-cell-mux
  localConnection = atmif/70 vcc/0.101
```

Map mode operational procedures for PORS

The *mode* operational attribute on the *Trk*/n *Lch*/m component shows the following values:

- AALSPO-cell-map, when a channel is converting from or to small frames (VOICE or BTDS) going to or coming from the nextHop
- AAL5-frame-map, when larger frames (HDLC or frame relay) are going to, or coming from the nextHop
- cell-map, indicates that no conversion is required

The following example shows the display option and output used on trk/70:

```
d Trk/70 LCh/* mode, localConnection

Trk/70 LCh/1
  mode = AAL5-frame-map
  localConnection = atmif/70 vcc/0.141

Trk/70 LCh/2
  mode = AALSPO-cell-map
  localConnection = atmif/70 vcc/0.142

Trk/70 LCh/3
  mode = cell-map
  localConnection = atmif/70 vcc/0.191
```

Determining Passport trunk over ATM utilization for PORS

You need to provision a single VCC for the *PathAdmin* (*Pa*) component running in mux mode. The *Trunk* component statistics include all statistics.

The system dynamically allocates VCCs at run time for the *Pa* component running in map mode. You can determine the level of path-oriented traffic a particular Passport trunk over ATM is forwarding in map mode by displaying the ATM connection *statistics*.

Procedure steps

1 Display all Passport trunks.

```
display trk/*
```

2 Select a Passport trunk over ATM from the list, for example 821, and display all active PORS channels on that Passport trunk over ATM.

```
display trk/821 lch/*
```

3 Manually display the statistics for each VCC, for example 0.1234. (This step applies to connections under the ATM interface or virtual path terminators.)

```
display atmIf/82 vcc/0.1234 stats
```

Note: In this example the VCC is Vcc/0.1234. If the VCC is associated with a virtual path terminator, the VPI value (0) is the instance of the Vpt component. The VCI value (1234) is the instance of the Vcc component.

You need to manually add the statistics for all VCCs to determine the total amount of traffic on the Passport trunk over ATM for PORS.

Definition of the IfTable

The ifTable provides a basic model of a network device containing a set of interfaces. Currently, two RFCs define the ifTable and a proposal for its evolution:

- RFC 1213 Management Information Base for network management of TCP/IP-based internets: MIB-II
- RFC 1573 Evolution of the Interfaces Group of MIB-II

Passport supports ifTable entries for both unackTrunks and atmTrunks. For a detailed description of the ifEntries for the *Trunk* component, see 241-5701-300 *Passport 7400, 15000, 20000 SNMP Guide*.

Support of SNMP enterprise MIBS

Passport Trunks support SNMP Enterprise MIBs.

The following MIBs contains information specific to frame-cell *Trunk* components:

- nortelpp-trunksV1.BE0000.mib
- nortelpp-unackTrunksV1.BE0000.mib
- nortelpp-porsTrunksV1.BE0000.mib
- nortelpp-atmTrunksV1.BE0000.mib

The MIB nortelpp-atmTrunke1.mib contains information specific to Passport trunks over ATM components.

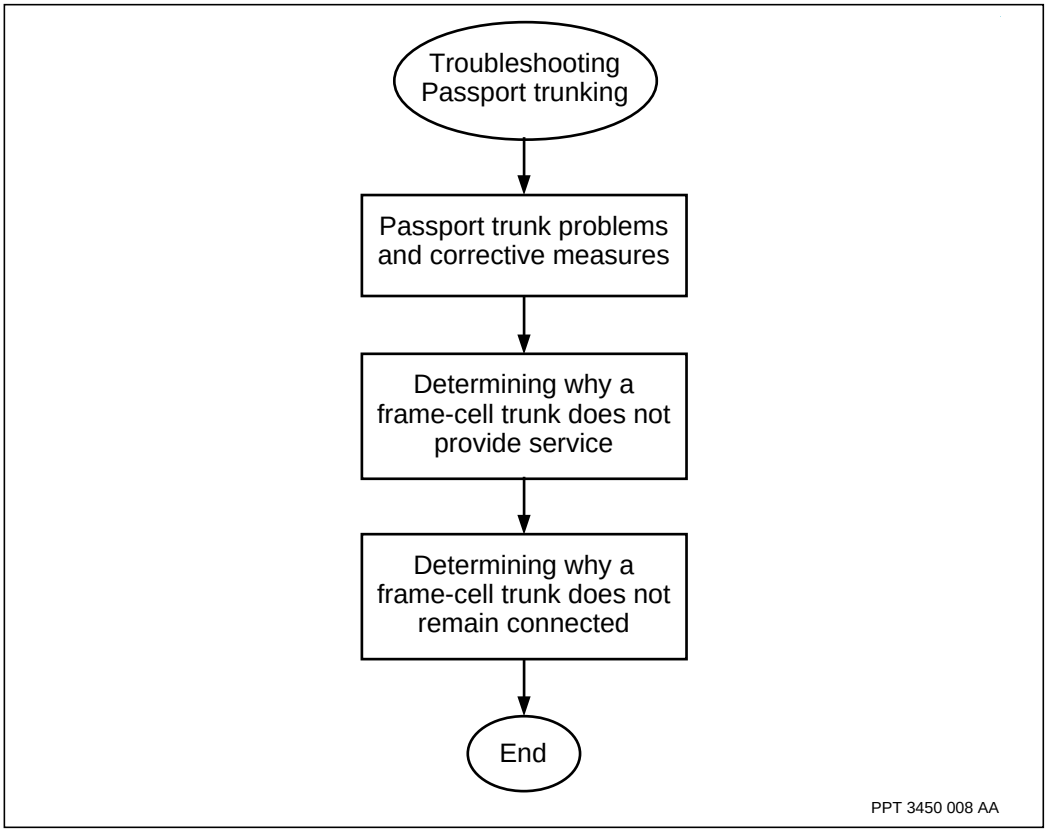
Chapter 6
Troubleshooting Passport trunks

The function processor (FP), the facility, or configuration errors can cause Passport trunk problems. Use the tasks and features in this section to the troubleshooting Passport trunks.

Troubleshooting Passport trunks task flow

This task flow shows you the sequence of procedures you perform to troubleshoot Passport trunks. To link to any procedure, go to “Task flow navigation” (page 86).

Figure 10
Troubleshooting Passport trunks task flow



Task flow navigation

- “Passport trunk problems and corrective measures” (page 87)
- “Determining why a frame-cell trunk does not provide service” (page 94)
- “Determining why a frame-cell trunk does not remain connected” (page 96)

Passport trunk problems and corrective measures

Table 1, “Handling problems with Passport trunks,” (page 87) provides guidelines on how to respond to problems that may occur when you are using frame-cell trunks for the Passport 7400 series switch and Passport trunks over ATM.

Table 1
Handling problems with Passport trunks

Problems	Probable causes	Passport trunk		Corrective measures
		Frame -cell	over ATM	
Passport trunk does not provide service	Processor module failure or port failure	Yes	Yes	Replace the function processor. See 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*.
	Facilities failure	Yes	Yes	Contact the service provider or Nortel Networks for assistance. See “Nortel Networks support services” in 241-5701-030 *Passport 7400, 15000, 20000 Overview*
	maximumExpectedRoundTripDelay is exceeded	Yes	Yes	Either increase the value of the *Trunk* attribute *maximumExpectedRoundTripDelay* (maximum by default) or correct the underlying facility to reduce RTD of the connection. The system issues an alarm (7005 0105) when this problem occurs.
	Incorrect hardware configuration	Yes	Yes	Run port and line tests to verify that the cable and connectors are functioning properly.

(Sheet 1 of 7)

Table 1 (continued)
Handling problems with Passport trunks

Problems	Probable causes	Passport trunk		Corrective measures
		Frame -cell	**over ATM**	
Passport trunk does not provide service		Yes	Yes	Verify the following hardware configurations: • cables and connectors at both ends are not faulty (would fail port and line test) • both ends have compatible clocking (Dte/Dce, Master/ Slave) • both ends have matching mapping, Cbit Parity
		Yes	No	• both ends have matching speeds; for example, V.35 X.21/HSSI of the Passport 7400 series switch are provisioned with the same lineSpeed values • X.21(only for the Passport 7400 series switch) line termination is on if speed >=2M or long cables in use
		Yes	No	• both ends have matching timeslots; for example, DS1 Chan or E1 Chan have the same values in timeslots

Table 1 (continued)
Handling problems with Passport trunks

Problems	Probable causes	Passport trunk		Corrective measures
		Frame -cell	**over ATM**	
		No	Yes	• both ends have matching speeds; for example, Vcc Vcds are provisioned with the same PCR values • both ends have VPI/VCI that match the traffic contract • both ends have matching VPI/ VCI
Passport trunk does not provide service	Framing errors as a result of • incorrect Framer provisioning • faulty hardware • mismatched connection bandwidth (port speeds) • facility problems	Yes	No	The Passport trunk protocol cannot stage or continually provide service if it is using a faulty connection. Check the integrity of the connection to see if it is providing service. Examine the *Framer* attributes contained in the *Framer statistics* group: • *aborts* • *crcErrors* • *IrcErrors* • *nonOctetErrors* • *overruns* • *underruns*

(Sheet 3 of 7)

Table 1 (continued)
Handling problems with Passport trunks

Problems	Probable causes	Passport trunk		Corrective measures
		Frame -cell	**over ATM**	
	Inconsistent Framer provisioning at each end of the connection	Yes	No	Verify that the remote and local *Framer* attributes match: • *framingType* • *dataInversion* • *frameCrcType* • *flagsBetweenFrames*
Passport trunk does not provide service	Inconsistent ATM provisioning at each end of the connection	No	Yes	The Passport trunk protocol is encapsulated into an AAL5 format (specified internally as the *AtmAccess* subcomponent). Verify that the remote and local VPI/VCI have the same attributes defined. The following attributes must match at both ends of the connection: • *txTrafficDescType* • *txTrafficDescParm* • *atmServiceCategory* • *trafficShaping* • *rxTrafficDescType* • *rxTrafficDescParm*

(Sheet 4 of 7)

Table 1 (continued)
Handling problems with Passport trunks

Problems	Probable causes	Passport trunk		Corrective measures
		Frame -cell	over ATM	
Passport trunk does not provide service	Cell errors as a result of • incorrect ATM provisioning • faulty hardware • mismatched connection bandwidth • facility problems	No	Yes	The Passport trunk protocol cannot stage or continually provide service if it is using a faulty connection. Check the integrity of the underlying VCC to see if it is providing service. See ATM Troubleshooting procedures in, 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide*. If the VCC is providing service, check for discard problems on the connection by examining the following attributes of the *VCC* component: • *txCellClp* • *txDiscard* • *txDiscardClp* • *rxCellClp* • *rxDiscard* • *rxDiscardClp*
	Invalid remote	Yes	Yes	The Passport trunk can only provide service if connected to another Passport trunk. Any other connection does not stage and does not provide service.

(Sheet 5 of 7)

Table 1 (continued)
Handling problems with Passport trunks

Problems	Probable causes	Passport trunk		Corrective measures
		Frame -cell	over ATM	
Passport trunk does not provide service	Mismatch of operational and expected remote NodeName	Yes	Yes	Passport trunks have provisionable attributes that specify the remote NodeName with which they are expected to stage. The attributes also specify whether to continue service if the remote differs. The system issues a set alarm when this situation occurs. Verify that the *expectedRemoteNodeId* attribute is either set properly or left blank (that is, set as “”).
Passport trunk goes down	There is a problem with the integrity of the connection.	Yes	Yes	Analyze alarms originating from the Passport trunk.
	The ATM layer is no longer providing service.	No	Yes	Analyze alarms originating from the Passport trunk and *VCC* components. If the VCC is no longer providing service, see the troubleshooting procedures in 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide*.
	Remote function processor is crashing	Yes	Yes	See 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

(Sheet 6 of 7)

Table 1 (continued)
Handling problems with Passport trunks

Problems	Probable causes	Passport trunk		Corrective measures
		Frame -cell	over ATM	
Passport trunk performance problem	Congestion, network instability, or trunk connectivity problems.	Yes	Yes	Sample the Passport trunk statistics several times to determine if the following statistics are increasing: • discardUnforward • discardTrunkPktFromIf • discardIntUnforward
Passport trunk does not come up	Total bandwidth is exhausted on the interface.	No	Yes	Change total bandwidth requests for the connection either by changing requested peak cell rates or by removing the connection.
	Routing rejects Passport trunk from staging	Yes	Yes	Check the regionIds and RIDs of the two nodes. If the regionIds are different, verify that RIDs are also different. Check if the number of Passport trunks in a link group exceed the maximum allowed by routing. The system issues an alarm (7005 0103) when this problem occurs.
Passport trunk fails intermittently, Passport node or transmission facility, or both loses synchronization, detects transmission errors.	A *lineType* attribute of D4 and a *zeroCoding* attribute of AMI and facility for Passport trunks carrying: IP traffic; a trunk packet payload that could include a long stream of zeros; or both.	Yes	No	Set the *lineType* attribute to ESF and the *zeroCoding* attribute to B8ZS under the *lp*/x *ds1*/y component.

(Sheet 7 of 7)

Determining why a frame-cell trunk does not provide service

Frame-cell trunks are supported on a Passport 7400 series switch. Passport 15000 and 20000 do not support frame-cell trunks.

Prerequisites

- The OSI model states provide valuable feedback for troubleshooting node problems. See “Determining Passport trunk component states” (page 70) for background information.

Procedure steps

1 To verify the status of the Passport trunk, issue the display command for the failed Passport trunk.

```
display trunk/<n> osistate
```

If adminState = unlocked, operationalState = enabled, and usageState = busy, the Passport trunk is operational. Go to “Determining why a frame-cell trunk does not remain connected” (page 96) to verify Passport trunk statistics.

If adminState = locked, consult with the operator who took the Passport trunk out of service to verify that you can now unlock the Passport trunk. Issue the unlock command. If the Passport trunk stages, the Passport trunk is operational. Exit this procedure or go to step 2 to verify the status of the logical processor.

If operationalState = disabled and availabilityStatus = dependency, there is a hardware failure. The possible failed components include the function processor, the individual port, and the Passport trunk facilities. Go to step 2 to verify the status of the logical processor.

If operationalState = disabled and availabilityStatus = failed, check the Passport trunk alarms.

If operationalState = disabled and availabilityStatus = inTest, check the Passport trunk statistics in “Determining why a frame-cell trunk does not remain connected” (page 96).

If operationalState = disabled and availabilityStatus is not dependency, failed, or intest, the Passport trunk never enabled. Go to step 2.

If operationalState = disabled and availabilityStatus = <empty>, the problem originates at the remote end. Repeat this procedure

("Determining why a frame-cell trunk does not provide service" (page 94)) at the remote end.

2 To verify the status of the logical processor (LP) issue the display command for the LP on the failed Passport trunk.

```
display lp/<m> osistate
```

Note: Determine the logical processor and port assignments by using the following command.

```
display -p trunk/<n> unacked framer
```

If adminState = unlocked, operationalState = enabled, and usageState = busy, the logical processor is operational. Go to step 3 to verify the status of the port.

If operationalState = disabled and availabilityStatus = dependency, there is a function processor failure. Go to the 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

3 To verify the status of the port, issue the display command for the physical port on the failed Passport trunk:

```
display lp/<slot> <interfaceType>/<port>
```

Example

```
display lp/10 v35/0
```

or

```
display lp/3 ds1/3
```

If the operationalState = disabled, go to "Testing hardware components" (page 65) to continue the troubleshooting analysis.

Variable definitions

Variable	Value
<interfaceType>	is the type of interface that failed
<m>	is the instance number of the failed logical processor
<n>	is the instance number of the failed Passport trunk
<port>	is the port number of the failed Passport trunk
<slot>	is the slot number of the failed Passport trunk

Determining why a frame-cell trunk does not remain connected

Frame-cell trunks are supported on a Passport 7400 series switch. Passport 15000 and 20000 do not support frame-cell trunks.

Changes in the facility (Framer) statistics at both ends can indicate hardware problems or a mismatch of local and remote provisioning.

Procedure steps

1. Issue the display command for the failed Passport trunk.

   `display trunk/<n> unacked framer`

   Examine the counts for the displayed errors.

2. Wait a few seconds and reissue the display command for the failed Passport trunk.

   `display trunk/<n> unacked framer`

   Examine the counts for the displayed errors. If any of these counts are increasing, use the appropriate port testing procedure in “Testing hardware components” (page 65) to isolate the problem to the port on the FP or the communications facility.

   If the Passport trunk discard statistics are increasing and the Passport 7400 is operational then check if the Passport trunk is congested and troubleshoot routing.

   If the Passport trunk discard statistics are stable and the Passport 7400 is operational then the Passport trunk is in a good state.

   If the counts are stable, the problem is likely located at the remote end of the Passport trunk. Move to that remote Passport node and continue troubleshooting. If the Passport trunk’s FP is crashing, see the section on determining the cause of an FP crash in 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.

Variable definitions

Variable	Value
<n>	is the instance number of the failed Passport trunk

Chapter 7
Understanding Passport trunking

This section describes the following trunking information:

- “Passport trunking terms” (page 97)
- “Passport trunking functions” (page 98)
- “Passport trunking architecture” (page 99)
- “Passport trunking mechanisms” (page 114)

For an introduction to Passport trunking, see 241-5701-400 *Passport 7400, 15000, 20000 Networking Overview*.

Passport trunking terms

Passport trunking terms are very specific. See Table 2, “Passport trunking terms,” (page 97) for definitions.

Table 2
Passport trunking terms

Trunking term	Trunking definition
trunk	generic term for a physical connection, not a Passport-specific term
Passport trunk	Passport-to-Passport connection supporting Passport core networking. Passport trunks support dynamic packet routing system (DPRS), and path-oriented routing system (PORS).
Trunk component	component type for a Passport trunk
(Sheet 1 of 2)	

Table 2 (continued)
Passport trunking terms

Trunking term	Trunking definition
inter-region Passport trunk	A Passport trunk which is a link between two border nodes in different topology regions.
Passport trunking system	software system that implements Passport trunking functions
frame-cell trunk	transport mechanisms used by Passport trunks to carry both frame and cell traffic on a frame-based interface. HDLC mode is a provisionable mode in which a frame-cell trunk can operate and that uses HDLC framing. Interrupting mode is a provisionable mode in which a frame-cell trunk can operate and that uses a modified HDLC-based framing. Interrupting mode allow highest priority data to interrupt traffic less sensitive to delay or traffic with a lower emission priority.
Passport trunk over ATM	transport mechanism used by Passport trunks to carry cell traffic on an ATM-based interface
Unacknowledged (UnAcked) subcomponent	component type for frame-cell trunks, both HDLC and interrupting modes
ATM link	standards-based ATM connection

(Sheet 2 of 2)

Passport trunking functions

A Passport trunk is a proprietary point-to-point protocol that connects two Passport nodes. The Passport trunking system provides this protocol and performs the following functions:

- implements Passport network layer functions in support of Passport trunks, such as reporting status of usable Passport trunks
- controls a protocol stack associated with a logical port on a function processor (FP) that provides interconnection to another Passport node or external network
- interfaces with the port management system (POMS)
- implements an unacknowledged protocol and supports ATM connections for Passport-to-Passport connectivity

- interwork with the node and network management systems through the component administration system (CAS) and the data collection system (DCS)

Passport 15000 and 20000 trunks over ATM can be provisioned on a spared LP as warm standby features. A warm standby application or feature can operate together with a hot standby application or feature on the same FP without affecting the ability of the hot standby application or feature to provide hitless services.

See 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide* for a description of hitless services and hot, warm and cold standby applications and features.

Passport trunking architecture

Passport-to-Passport links are called Passport trunks. A Passport trunk is a point-to-point or logical (ATM virtual channel connection [VCC]) connection between two Passport nodes over which Passport proprietary routing protocols are run. Passport trunks use two transport mechanisms: frame-cell and Passport trunks over ATM. Passport 7400 series switches use both frame-cell and Passport trunks over ATM. Passport 15000 and 20000 do not use frame-cell trunks.

- Passport frame-cell trunks transport data traffic (frame relay, and DPN-100) as frames, and constant bit rate traffic (voice, and video) as cells. The Unacknowledged (UnAcked) trunking protocol used for transmission is HDLC-based.
- Passport trunks over ATM (formerly called ATM logical trunks) are cell trunks that encapsulate frame traffic into ATM cells. The Passport trunk over ATM is carried on one or more ATM VCCs and uses standard ATM adaptation layer protocols based on AAL1 and AAL5.

The Passport trunking system interacts with several Passport software subsystems, as Figure 11, “Frame-cell trunks software architecture,” (page 101) and Figure 12, “Passport trunks over ATM software architecture,” (page 102) illustrate.

See the following sections for information on the Passport trunking architecture:

- "Passport software subsystems support of Passport trunking" (page 102)
- "Transport mechanisms support of Passport trunking" (page 104)
- "Passport trunks protocol stacks" (page 106)
- "Supported interfaces for Passport trunking" (page 113)

Figure 11
Frame-cell trunks software architecture

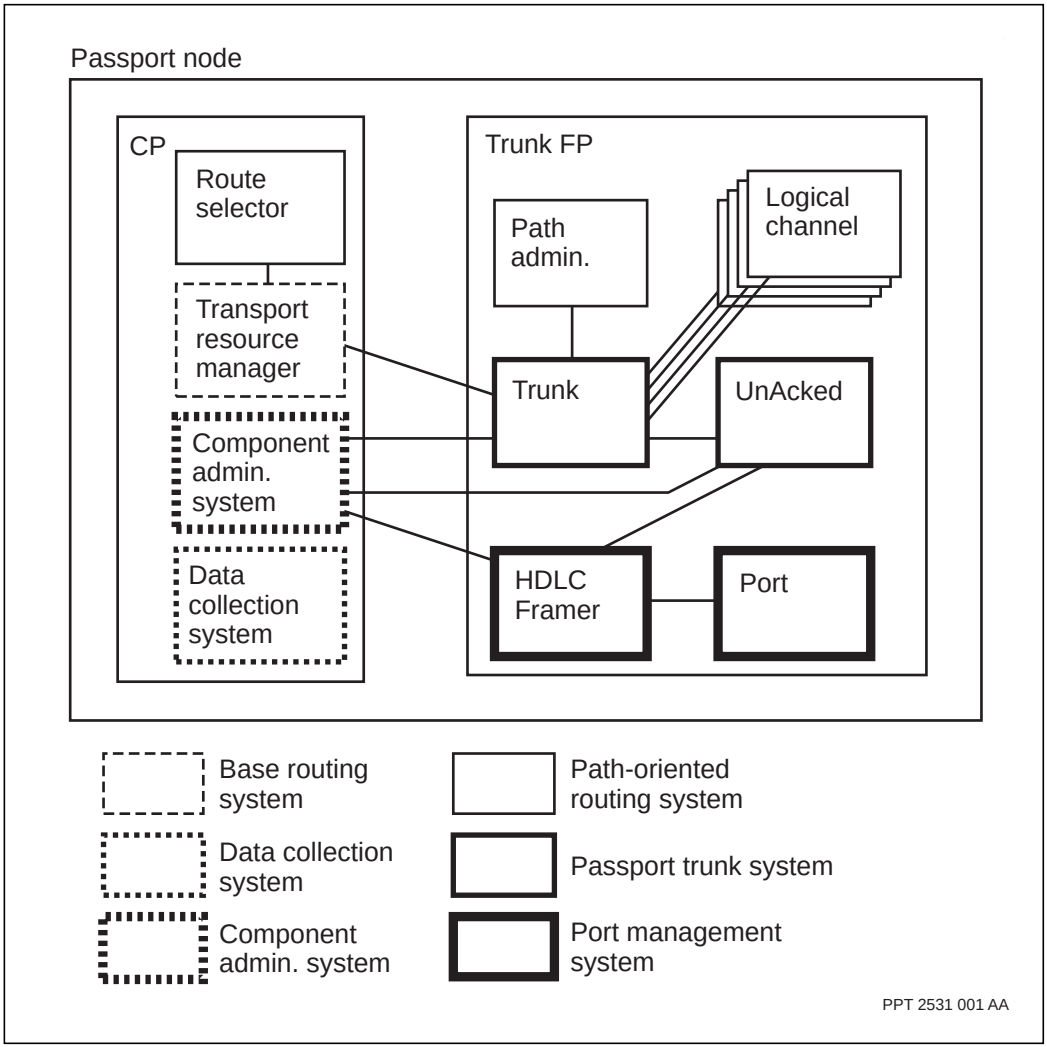
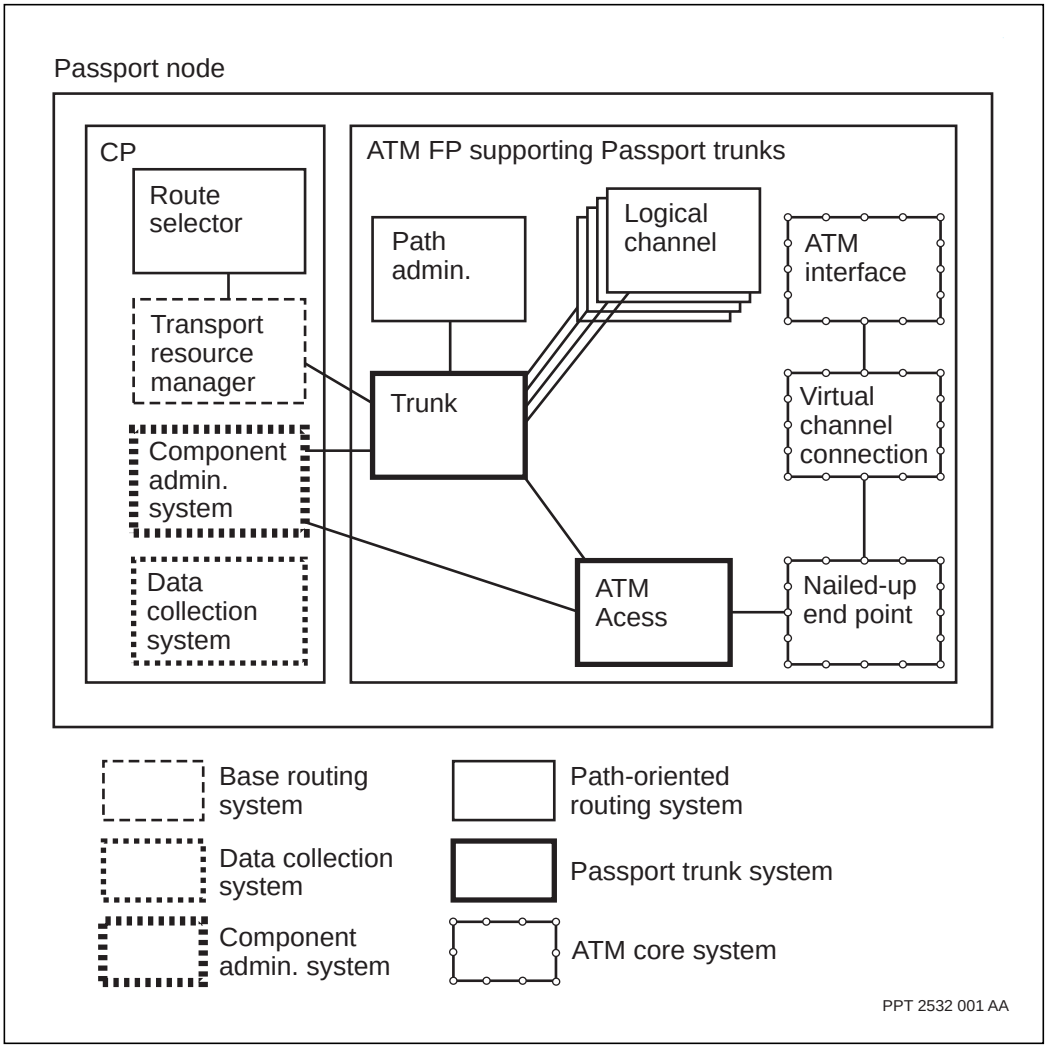


Figure 12
Passport trunks over ATM software architecture



Passport software subsystems support of Passport trunking

The following sections describe the software subsystems supporting Passport trunking:

- “Base routing system support of Passport trunking” (page 103)

Base routing system support of Passport trunking

Transport resource manager (TRM) in the base routing system interfaces with the Passport trunk system to learn

- the status (up or down) of all usable Passport trunks
- the Passport trunk attributes to support various classes of routing (throughput, delay, multimedia, cost)
- neighbor node information
- the maximum frame size

Base routing and the routing protocols use this information to compute the metrics for selecting routes.

Path-oriented routing system (PORS) support of Passport trunking

Interrupting trunks provide PORS with the interrupting hardware queue (used for voice and video delay-variation-sensitive traffic) and both the high and normal hardware queues. Route selector is responsible for choosing PORS connections (routes) through a module. Path administrator is responsible for setting up and controlling PORS connections on a Passport trunk. Logical channel, in conjunction with path administrator, controls a Passport trunk PORS connection.

Port management system (POMS) support of Passport trunking

POMS provides the Passport trunking system with the physical interfaces (ports) for transmitting and receiving traffic over Passport trunks. POMS is a software system that controls and monitors the physical interfaces supported by FPs. POMS also manages the physical lines from the Passport to other network elements and monitors the link for quality.

Data collection system (DCS) support of Passport trunking

Data collection system (DCS) collects and stores alarms, statistics, and state change notifications generated by Passport trunking.

Component administration system (CAS) support of Passport trunking

Component administration system (CAS) provisions and monitors the hardware and software components comprising Passport trunking. The Passport trunk system components interact with CAS for processing operator commands, handling alarms and statistics, and for interacting with the provisioning system.

Passport trunking system

The Passport trunking system has a layered architecture that spans two well defined OSI model protocol layers: the data link layer and the network layer. This architecture corresponds to the bottom of the Passport network layer and the top of the Passport switching layer. See “Passport trunks protocol stacks” (page 106).

ATM core system

The Passport switching layer contains the Passport ATM core system. See “Passport trunks protocol stacks” (page 106).

Transport mechanisms support of Passport trunking

Transport mechanisms can be acknowledged or unacknowledged. With unacknowledged trunks, receiving nodes do not acknowledge the receipt of packets. This method is optimal for high quality transmission lines (extremely low bit-error rates). Unacknowledged trunking reduces link processing and overhead (associated with acknowledgment), and provides for higher performance.

Highlights of unacknowledged trunks compared to acknowledged trunks are

- less trunk overhead and higher throughput
- interrupting capability

The transport mechanisms for unacknowledged Passport trunks are

- “Frame-cell trunks on a Passport 7400 series switch” (page 105)
- “Passport trunks over ATM” (page 105)

Frame-cell trunks on a Passport 7400 series switch

Frame-cell trunks use point-to-point connections, where bandwidth is dedicated to one user (directly over physical circuits). All frames use the HDLC-framed format when transmitting across the lines.

Frame-cell trunks are either HDLC-based or interrupting. The default mode is interrupting. The interrupting feature can be provisioned on each Passport trunk, on a port-by-port basis. This feature allows highest priority data to interrupt traffic which is less sensitive to delay or which has lower emission priority. Passport trunking supports three data emission priorities (priority of data as determined by its urgency). See “Traffic management for frame-cell trunks” (page 122) for more information.

Passport trunks over ATM

Passport trunks over ATM use bandwidth only when needed. The bandwidth appears to be dedicated. More bandwidth can be used if necessary and if available.

Passport trunks over ATM allow all non-ATM Passport services and DPN-100 traffic to travel transparently over ATM. The routing system uses Passport trunks over ATM in the same way as frame-cell trunks, replacing the unacknowledged sublayer with an ATM sublayer.

The ATM protocol consists of VCC access through ATM adaptation layer 5 (AAL5), or AAL short path-oriented (AALSPO) for voice. The ATM layer segments the frames into cells and transmits them across the VCC link. Each Passport trunk over ATM uses one or more ATM VCC.

Passport trunks over ATM are either direct or logical:

- direct Passport trunks over ATM connect Passport nodes directly together
- logical Passport trunks over ATM connect Passport nodes either through a series of Passport nodes or through an external ATM network

For more information on Passport trunks over ATM, see "Passport trunks over ATM" (page 135).

Passport trunks protocol stacks

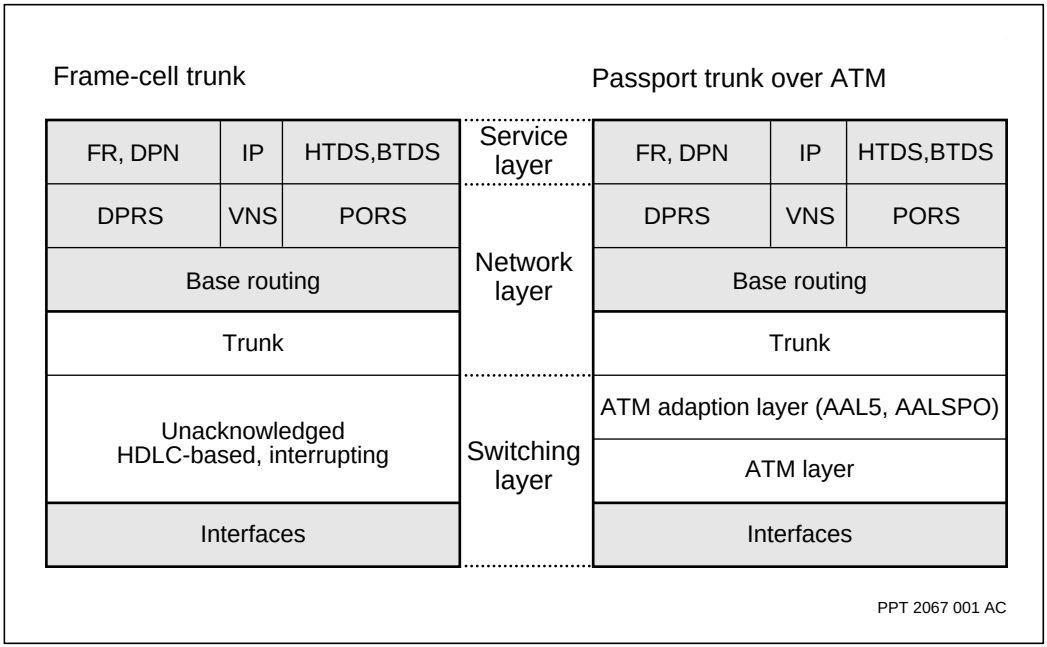
The Passport trunk architecture is a protocol stack. A protocol stack identifies a group of hierarchical functions divided into layers, in which each layer provides a service to the layer above it.

The Passport trunk over ATM protocol stack is similar to the protocol stack of frame-cell trunks. All the layers above the unacknowledged layer in the frame-cell stack and all the layers above the AAL layer in the Passport trunk over ATM stack are the same. The difference between the two stacks is the architecture of the switching group of layers. The HDLC-based stack is made up of the unacknowledged layer and the physical layer. The Passport trunk over ATM protocol stack is made up of the AAL5 layer, the AALSPO layer, the ATM layer, and the physical layer.

The following sections describe the Passport architecture layers:

- "Passport network layer" (page 107)
- "Passport switching layer" (page 108)

Figure 13
Comparison of Passport trunk protocol stacks



Passport network layer

The Passport trunk sublayer of the Passport network layer corresponds to the OSI model layer-three (L3) process (OSI model network layer). The Passport trunk sublayer is responsible for

- staging (establishing) the point-to-point Passport trunk
- providing an interface to the routing system independent of the Passport switching
- layer
- testing and managing the connection
- reporting link characteristics to base routing such as availability, connection bandwidth (speed), delay, remote node identification, three emission priority queue identifiers, static PORS attributes (such as cost, Passport trunk type, security), allocated PORS bandwidth, and number of currently established PORS connections

Base routing only supports protocol stacks with the Passport trunk protocol for Passport-to-Passport networking.

Passport switching layer

The Passport trunk sublayer of the Passport switching layer corresponds to an OSI model L2 process (OSI model data link layer). This sublayer provides

- the capability for transfer of packets across point-to-point links independent of the transmission facility used
- a pipe available to upper layers
- Passport trunk characteristics such as availability and connection bandwidth. Frame-cell trunks support three emission priorities: normal, high, and interrupting.
- the interface with the POMS which implements the OSI model physical layer for point-to-point Passport trunks
- access to channels of a service for logical Passport trunking

Frame-cell and Passport trunks over ATM are the only transport mechanisms supported. Transport mechanisms, such as FR, X.25, and IEEE 802.2 are possible future candidates.

OSI states for Passport trunks

The following sections have information on *Trunk* component states:

- "OSI model administrative state for Passport trunks" (page 108)
- "OSI model operational state for Passport trunks" (page 109)
- "OSI model usage state for Passport trunks" (page 109)
- "Summary of OSI model state combinations for Trunk, Unacknowledged, and AtmAccess components" (page 109)

OSI model administrative state for Passport trunks

The OSI model administrative state attribute (locked/unlocked) indicates whether the *Trunk* component is available for service. If the Passport trunk is out of service due to a lock command, then an unlock command is necessary to bring it back to service. After issuing the unlock, if the component does not come into full operation then you need to investigate the higher level components or subcomponents, and the states of the other two state attributes.

Note: *UnAcked* and *AtmAccess* components do not support lock/unlock commands and always have administrative states of unlocked.

OSI model operational state for Passport trunks

The OSI model operational state attribute (enabled/disabled) indicates the status of a Passport trunk's subcomponents. If any subcomponent is troubled then the operational state attribute has a value of disabled. The following are some of the most common scenarios:

- availabilityStatus = dependency indicates that the component has a dependency, such as a subcomponent, being disabled
- availabilityStatus = inTest indicates that the component is currently in test mode and trying to stage
- availabilityStatus = failed indicates that the component has detected either a loss of some resource, has encountered a protocol violation, or has lost communications with a remote component. The *Trunk* component issues a set alarm for any such failure.
- controlStatus = suspended indicates that the administrator has locked the component or some other software entity has disabled it

OSI model usage state for Passport trunks

The OSI usage state attribute (idle/busy) indicates whether the component is being used or not. There are several reasons why a Passport trunk usage state is idle, meaning that the component has no user:

- if the routing system is not using the *Trunk* component for its topologies
- if the *Trunk* component is not using the *UnAcked* or *AtmAccess* components
- if the remote Passport trunk is troubled

See Table 1, "Handling problems with Passport trunks," (page 87) and for assistance in troubleshooting.

Summary of OSI model state combinations for Trunk, Unacknowledged, and AtmAccess components

Note: The Unacknowledged components are specific to the Passport 7400 series switch.

Table 3, “Trunk component state combination,” (page 110), Table 4, “Unacknowledged component state combination,” (page 111), and Table 5, “AtmAccess component state combination,” (page 111) summarize the OSI model state combinations for *Trunk*, *Unacknowledged*, and *AtmAccess* component states, respectively.

Table 3
Trunk component state combination

Combination (Administrative, Operational, Usage)	Details
Unlocked, Disabled, Idle	External factors render the Passport trunk inoperable. The *Unacknowledged* or *AtmAccess* subcomponents reporting a link down is a possible cause. Bad line state and excessive line state changes are possible causes.
Unlocked, Enabled, Idle	The *Unacknowledged* or *AtmAccess* subcomponent is offering service and the Passport trunk is now staging with the remote.
Unlocked, Enabled, Busy	The *Trunk* component is in use. The component does not service any user (that is, any component) but has successfully joined packet routing.
Locked, Disabled, Idle	In addition to a lock/lock -force command being in effect, the *Unacknowledged* or *AtmAccess* subcomponent is reporting a link down. Bad line state and excessive line state changes are possible causes.
ShuttingDown, Enabled, Busy	A lock command is in effect. The *Trunk* component is waiting for any *logicalChannel* subcomponents to go away before entering the locked state.

Table 4
Unacknowledged component state combination

Combination (Administrative, Operational, Usage)	Details
Unlocked, Disabled, Idle	External factors render the *Unacknowledged* component inoperable. The *Framer* component reporting a link down is a possible cause.
Unlocked, Enabled, Idle	The *Framer* subcomponent is offering service and the *Unacknowledged* component is now waiting for the parent component to start using it.
Unlocked, Enabled, Busy	The *Unacknowledged* component is in use. The component services only one user (a *Trunk* component) at a time.

Table 5
AtmAccess component state combination

Combination (Administrative, Operational, Usage)	Details
Unlocked, Disabled, Idle	External factors render the *AtmAccess* component inoperable. The ATM connection reporting a link down is a possible cause.
Unlocked, Enabled, Idle	The ATM connection is offering service and the *AtmAccess* component is now waiting for the parent component to start using it.
Unlocked, Enabled, Busy	The *AtmAccess* component is in use. The component services only one user (a *Trunk* component) at a time.

Operational disabling of Passport trunks

You can disable a Passport trunk by using the lock command on either the *Trunk* component, or on the component controlling the port that the trunk is using. A disabled Passport trunk is available for port testing.

The Passport trunk must be locked before you can perform port tests. The *Trunk* component controls a logical port on a function processor. This *Trunk* component provides a connection to a *Trunk* component on another network

element. For details on *Trunk* components, see 241-5701-060 *Passport 7400, 15000, 20000 Components*. The system issues an alarm whenever a trunk becomes locked.

When you lock a Passport trunk for a port test, its operational state becomes disabled and its administrative state becomes locked. The administrative state becomes unlocked after five minutes even if the test is not complete. The operational state, however, remains disabled until the test is complete. Once the test is complete, the operational state changes to the enabled state and the Passport trunk attempts to become operational.

CAUTION
Risk of data loss
Locking a Passport trunk can result in the loss of data. To reduce the risk of data loss, do not lock a Passport trunk during peak periods of traffic.

The Passport trunk restaging mechanism

Passport trunks implement a backoff mechanism when restaging from a hardware-related fault. This mechanism reduces the amount of routing traffic generated by a Passport trunk that was repeatedly enabled and disabled.

The first time a Passport trunk is disabled due to a facility problem, the Passport trunk restages immediately. Following the second disabling the Passport trunk waits for 10 seconds after the facility is operational before attempting to restage. Subsequent failures result in the Passport trunk waiting for 20 and then for 40 seconds after the facility is operational before attempting to restage. This restaging mechanism cycles through the 10-, 20-, and 40-second periods until the Passport trunk is successful.

Once a Passport trunk is operating error-free for 10 minutes, the restaging mechanism resets to restage immediately before cycling through the 10-, 20-, and 40-second waiting periods.

See Table 6, “Passport trunk restaging scenarios,” (page 113) for restaging scenarios.

Table 6
Passport trunk restaging scenarios

Failure scenarios	Restaging description and times
Administrative Lock/Unlock of a *Trunk* component using a back-to-back facility	The locking of a Passport trunk on one end of a connection results in the other end of the Passport trunk detecting loss of communications and attempting to restage. When you unlock the Trunk, both ends of the Trunk stage immediately.
Administrative Lock/Unlock of a port component using a back-to-back facility	The locking of the port on one end of the connection results with a disabling of the facility. When you unlock that port, both Passport trunks use the backoff mechanism before restaging.
Failure of a back-to-back facility	Both ends of the connection detect the failure of the facility. When that facility is operational, both Passport trunks use the backoff mechanisms before restaging.
Administrative Lock/Unlock of a *Trunk* component using a modem or ATM facility	The locking of a Passport trunk on one end of the connection results with the remote Passport trunk detecting a loss of communications. When you unlock this Passport trunk, the other Passport trunk restages immediately.
Administrative Lock/Unlock of a port component using a modem or ATM facility	The locking of a port on one end of the connection results with the remote Passport trunk detecting a loss of communications. When you unlock this port, the other Passport trunk restages immediately.
Failure of a modem facility	The local Passport trunk detects the failure of a modem and the remote Passport trunk detects a loss of communications with this Passport trunk. When the modem is operational the local Passport trunk uses the backoff mechanism before restaging while the remote Passport trunk immediately attempts to restage.
Failure of an ATM facility	Neither Passport trunk detects the failure of an ATM facility but both detect a loss of communication with each other. When the ATM is operational both Passport trunks attempt to restage immediately.

Supported interfaces for Passport trunking

For information on which specific function processors (FP) support frame-cell trunks and which FPs support Passport trunks over ATM refer to 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference* or contact your Nortel Networks account representative.

Passport trunking mechanisms

The Passport trunking mechanisms detailed in this section are functions performed by the Passport trunking system and include the following:

Trunk component naming

Trunk components have a five-digit instance value. The range of *Trunk* component instances increased from four digits (1 to 1023) to five digits (0 to 65535). This feature allows customers and off-switch tools, such as network management tools, to implement more flexible naming conventions.

The following points describe a popular naming convention:

- the first digit (or two digits) represent(s) the card number
- the next digit represents the port number
- the final two digits represent the channel number

Using this naming convention with the longer instance value, allows for easier troubleshooting by network operators.

Trunk component instance synchronization

Both ends of a connection need to use the required software (P4.2) to incorporate the five-digit instance advantages. The instance value length is checked during Passport trunk staging (see "Passport trunk staging" (page 115)). If only one end of a Passport trunk uses a five-digit instance value, the local Passport trunk raises a major alarm because of the impact to the spooled statistics at the end with the older software. The impact is that the *remoteComponentName* attribute in the spooled statistics or on the operator console does not show the most significant digit in the Trunk instance. For example, *Trunk* component instance 12345 is shown as 2345. This result can affect the off-switch tools that use bulk data format.

Passport trunk staging

The process of staging a Passport trunk involves establishing the connection between Passports, and occurs after activating a Passport trunk. Staging occurs when a physical or logical (ATM) connection comes up between two provisioned Passport *Trunk* components (on different Passport nodes). Passport trunks also attempt to restage if the error rate on an existing Passport trunk exceeds a threshold.

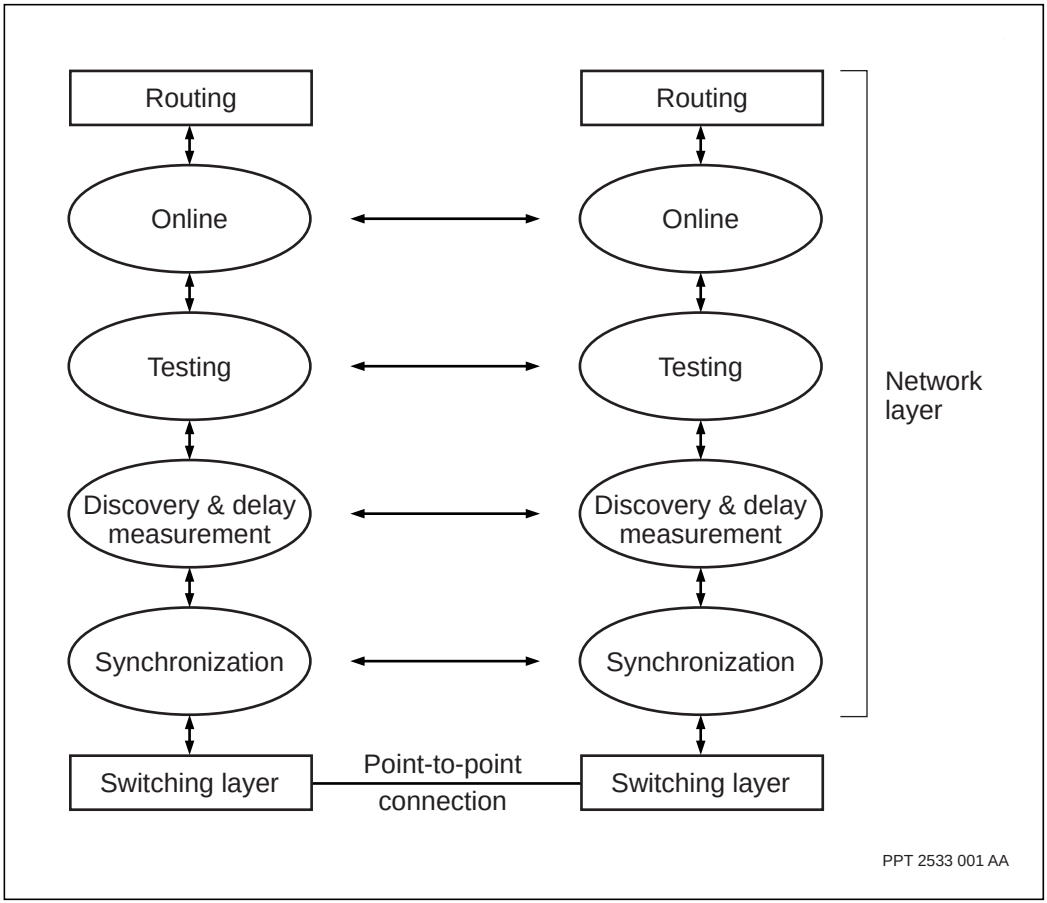
The staging method for the *Trunk* component starts with the interface (*Framer* or *AtmIf* component) indicating to its upstream component (*UnAcked* or *AtmAccess*) that the link connectivity has been established. The upstream component (*UnAcked* or *AtmAccess*) then performs its staging and testing before giving the same indication to the next upstream component (*Trunk*). Upon receiving an enable indication from a downstream component (*UnAcked* or *AtmAccess*), the *Trunk* component performs its staging protocol. The staging is complete when the Passport trunk joins the Passport routing system successfully.

The Passport trunk staging protocol performs the following tasks:

- “Synchronization” (page 116)
- “Discovery and delay measurement” (page 117)
- “Testing” (page 117)
- “Online monitoring” (page 117)
- “Interface with routing system” (page 118)

See Figure 14, “Tasks performed by the Passport trunk staging protocol,” (page 116) for an illustration of the trunk staging protocol tasks.

Figure 14
Tasks performed by the Passport trunk staging protocol



Synchronization

Synchronization ensures the local and remote nodes are aware of each other. The synchronization protocol transmits and receives Passport trunk up and ready packets with the remote node. For Passport trunks over ATM, these up and ready packets traverse the VCC provided by the *AtmAccess* subcomponent.

Discovery and delay measurement

After both ends of the Passport trunk have synchronized, each end sends an are-you-there (AYT) packet to exchange attributes such as remote node name. If the actual peer end name is different than the expected remote node name, an alarm appears and the validation action results. The *remoteValidationAction* attribute can be set to continue, where staging continues immediately, or to disable, where restaging occurs after a one-minute time out.

If the connection is deemed valid, then staging continues. One end measures round trip delay (RTD) in milliseconds using a 128-byte packet and then sends the measured value to the remote end.

Testing

The link quality test protocol transmits and receives 64 Passport trunk test packets of various lengths. For Passport trunks over ATM, the test packets traverse the atmConnection. If a packet is lost, the Passport trunk becomes disabled and attempts to restage.

The adjustment of the staging *Trunk idleTimeOut* attribute acts as a security timer in case packets are lost and the protocol is waiting. If staging is not done within the time specified, then the Passport trunk restages.

Online monitoring

The online monitoring protocol informs the routing system of the bandwidth and the delay associated with the Passport trunk connection. Online monitoring also provides the routing system with the remote node identification. The switching layer uses the enable indication message to provide information about the bandwidth to online monitoring. After the Passport trunk is online (available for use), monitoring continues for failure conditions.

The trunking system removes the Passport trunk or identifies it as failed if any of the following occurs:

- there is a looped-back condition
- the Passport trunk loses communication with its peer
- there is a physical failure, such as the loss of the carrier
- a user requests that the Passport trunk be terminated

The following describes the monitor mechanism that detects looped-back conditions and lost communications with a peer:

- The remote end sends a neighbor check packet every two seconds. When this packet arrives, the local end validates the remote node identification. The Passport trunk restages if the node identification does not match the staged value.
- If the local end does not receive a neighbor check for a period of four seconds, then the remote end transmits 40 AYT packets within a period of two seconds. If the local end does not receive a "Yes I Am" (YIA) packet, then the Passport trunk disables. If the local end receives a YIA packet, then the local end validates the remote node identification and continues to provide service.
- If both ends of the Passport trunk have agreed to use the enhanced Passport trunk neighbor check procedure then the Passport trunk no longer disables after four seconds without receiving a neighbor check packet from the remote Passport node.

You can adjust the *Trunk idleTimeOut* attribute to enable quicker rerouting or to be less reactive on slow or erroneous connections. For provisioning information, see "Setting Passport trunk protocol idle time out duration" (page 76).

Interface with routing system

The *Trunk* component gives an enable indication to its upstream component (routing system) to complete the staging process. This join request contains the remote component name, an RCOS table containing hardware IDs or software IDs or a mixture of the two.

Link quality mechanism

For network stability, Passport trunks need to disable in poor link quality situations. Line noise, equipment failure, and buffer overruns are some of these situations. Automatic disabling applications guarantee link quality and deliver traffic efficiently.

The link quality mechanism can be divided into two elements:

- "Link quality monitoring" (page 119)

• “Link quality policy” (page 119)

Link quality monitoring

The link quality monitoring determines when and how often a link between two Passport nodes experiences corrupted data packets being transferred. The *UnAcked* and *AtmAccess* components perform the link quality monitoring based upon raw statistics from the switching layer interfaces.

Link quality policy

The link quality policy judges link quality, and determines what to do when the quality is inadequate. The *Trunk* component has its own link quality policy called error threshold policy.

Two provisionable attributes exist under the *Trunk UnAcked* and *AtmAccess* components to support the link quality mechanism. The *maximumErroredInterval* attribute specifies the interval time over which the error threshold (as specified by *receiveErrorSensitivity*) must be continuously exceeded before the *UnAcked* and *AtmAccess* components can be degraded. The *UnAcked* and *AtmAccess* components issue an alarm once the error interval count exceeds the provisioned value. A *maximumErroredInterval* attribute value of zero (default) disables the mechanism.

The second attribute *receiveErrorSensitivity* is the allowable error rate beyond which the *UnAcked* and *AtmAccess* components can be degraded if it persists for a duration longer than the *maximumErroredInterval*. The threshold is expressed as a percentage of number of frames/cells in error per number of frames/cells received in the last interval (one minute). A *receiveErrorSensitivity* attribute value of zero disables the mechanism.

When the Passport trunk crosses the provisioned link error threshold, the Passport trunk automatically restages and issues alarms.

Cyclic redundancy checks for Passport trunks

For high availability, the Passport trunking system verifies the integrity of frames through cyclic redundancy checks (CRC) performed in hardware. The Passport trunking system discards frames with errors when the frames arrive from the link. Hardware provides CRC functionality.

Traffic management for Passport trunking

For information on traffic management see

- "Traffic management for frame-cell trunks" (page 122)
- "Traffic management for Passport trunks over ATM" (page 145)
- 241-5701-400 *Passport 7400, 15000, 20000 Networking Overview*
- 241-5701-705 *Passport 7400, 15000, 20000 ATM Traffic Management Fundamentals*

Passport trunk utilization alarm

The Passport trunk utilization alarm allows the operator to specify whether or not alarms should be generated when the link utilization crosses certain thresholds. There are three user-defined thresholds (one for a minor alarm, one for a major alarm, and one for a critical alarm), which you can provision.

This feature exists for both frame-cell trunks and Passport trunks over ATM. See "Provisioning frame-cell trunk features" (page 26) for frame-cell trunks, or "Provisioning Passport trunks over ATM features" (page 44) for Passport trunks over ATM.

Chapter 8
Passport frame-cell trunks

The frame-cell trunks mechanisms detailed in this section are functions performed by the Passport trunking system for Passport 7400 series switches. Passport 15000 and 20000 do not use frame-cell trunks. This section includes information on the following:

Data flow through the Passport system

Hardware and software control data flow through the Passport system.

Frames enter the Passport switch through the interfacing FP where they are stored in memory. Passport software then determines each frame's destination. The hardware then moves the frames through the processor without further software intervention. This approach increases overall Passport throughput.

Incoming and outgoing frames line up in queues. Queuing allows the Passport switch to handle the bursty nature of data and to implement parts of protocols that require, for example, frame reassembly.

Queues are also necessary for multiplexing different kinds of traffic on the same facilities. Higher priority queues are for delay-critical frame traffic. The highest priority interrupting queue is for delay-critical applications such as bit-transparent data service, voice, and frame relay multimedia traffic.

Traffic management for frame-cell trunks

The Passport trunking system provides traffic management functionality through the multipriority system (MPS). MPS is a queueing architecture that uses emission priorities to define the urgency of packet transfer and discard priorities to define importance of packet transfer. These two priority types work independently. See the traffic management chapter of 241-5701-400 *Passport 7400, 15000, 20000 Networking Overview* for a thorough explanation of this Passport feature.

Frame-cell trunk emission priority queues

How trunks handle traffic depends on the relationship between the frame-cell trunk mode, and the routing class of service of the traffic (for DPRS) or the service category of the traffic (for PORS).

You can provision frame-cell trunks to operate in HDLC mode or interrupting mode. Interrupting mode frame-cell trunks use three emission priority queues: interrupting, high, and normal. HDLC mode frame-cell trunks have two queues: high and normal. The interrupting queue has the highest priority, while the normal queue has the lowest.

For DPRS traffic, you provision the FRUNI TP with a routing class of service attribute. Each RCOS attribute has a specified emission priority (EP=0 for multimedia, EP=1 for delay, and EP=2 for throughput). The RCOS emission priority determines how the DPRS traffic will be handled on the frame-cell trunk.

On frame-cell trunks in HDLC mode, multimedia and delay traffic use the high priority queue, while throughput traffic uses the normal priority queue. On frame-cell trunks in interrupting mode, multimedia and delay traffic get split out such that multimedia uses the higher priority interrupting queue, and delay uses the high priority queue. Throughput traffic uses the normal priority queue.

Table 7, “Mapping between FRUNI TP and frame-cell trunk emission priority queue,” (page 123) provides an outline of the association between DPRS transfer priority and the frame-cell trunk emission priority.

Table 7
Mapping between FRUNI TP and frame-cell trunk emission priority queue

FRUNI TP	DPRS routing class of service (RCOS)	HDLC mode frame-cell trunk emission priority	Interrupting mode frame-cell trunk emission priority
TP 15	Multimedia (EP = 0)	High	Interrupting
:	Delay (EP = 1)		High
TP 0	Throughput (EP = 2)	Normal	Normal

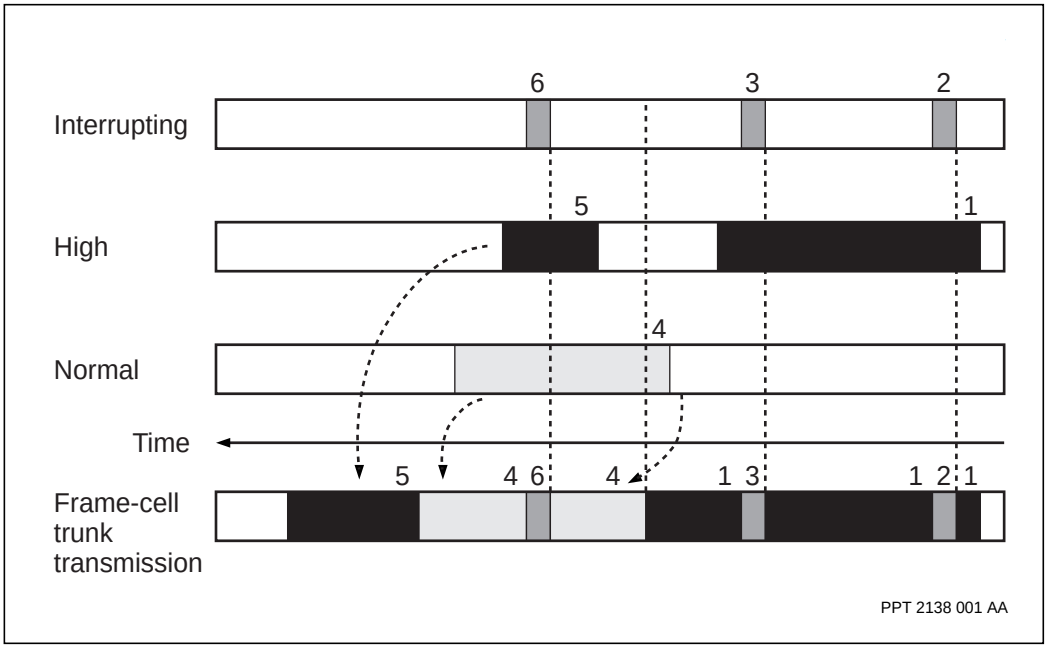
For more information on provisioning the FRUNI TP and routing class of service see 241-5701-902 *Passport 7400, 15000, 20000 Configuring Frame Relay*.

Passport trunks handle PORS traffic in much the same manner as the DPRS traffic. The difference is that instead of provisioning a transfer priority with a routing class of service, you provision the PORS traffic with a service category that reflects the emission and discard priority required for the traffic type. See 241-5701-435 *Passport 7400, 15000, 20000 Path-Oriented Routing System Guide* for more details on PORS traffic.

The Passport trunking system monitors frame-cell trunk emission queues for congestion and returns the congestion status to the forwarding tables. Remedial actions, such as re-routing traffic around congested areas, can be taken.

Each arriving packet lines up in an emission queue based on the delay priority indicator in its header. Figure 15, “Frame-cell trunk emission queues,” (page 124) shows an example of transmission from the three emission queues.

Figure 15
Frame-cell trunk emission queues



Frame-cell trunk congestion thresholds

Each queue in the Passport transmission trunking system supports four congestion levels or states: mild, moderate, heavy, and severe. Each congestion level corresponds to a threshold in terms of block count. The Passport trunking system compares current length of each queue against the threshold values to determine its congestion level. As frames and cells are queuing, the Passport trunk system informs the CPU when a queue has grown to a specified threshold value. When a frame or cell transfers from the ingress queue to the Passport trunk, the Passport trunking system compares the frame or cell discard priority with the Passport trunk congestion level. This comparison determines whether the queue accepts the frame or cell. In other words, the various congestion levels discard frames or cells when congestion persists.

Two sets of thresholds points exist for each congestion level. This arrangement prevents a large number of threshold interrupts if the queue length hovers close to a threshold. The set of upward thresholds is for an

increasing queue length. The set of downward thresholds is for decreasing queue length. When the queue length triggers the next congestion level by passing over an upward threshold, the congestion level only changes when the queue length has reduced below the corresponding downward threshold.

For the congestion threshold categories and the frame-cell trunk emission priority queue sizes in bytes, see Table 8, "Congestion thresholds on frame-cell trunks," (page 125).

> ***Note:*** The thresholds are converted values from number of blocks to bytes where each block is equal to 128 bytes for non-IP traffic. The block size for IP traffic is 256 bytes. For example, the first threshold (T1) on a 1536 kbit/s link is actually 347 blocks of 128 bytes which corresponds to 44416 bytes of shared RAM memory.

For more information on traffic management for frame-cell trunks, see 241-5701-400 *Passport 7400, 15000, 20000 Networking Overview*.

Table 8
Congestion thresholds on frame-cell trunks

Link speed	Emission priority	Upward thresholds (bytes)				Downward thresholds (bytes)			
		T1	T2	T3	T4	T1	T2	T3	T4
64 kbit/s	Normal	3968	8832	12416	14848	2688	7552	12416	13568
	High	2048	4352	6016	7296	1280	3456	5248	6528
	Interrupt	1024	2048	2944	3584	640	1664	2560	3200
256 kbit/s	Normal	6144	16128	22144	25984	4608	13824	20608	24576
	High	3072	7296	10496	12672	2048	6272	9600	11648
	Interrupt	1408	3456	4992	6144	1024	2944	4608	5632
384 kbit/s	Normal	8064	20992	30592	35968	6272	19328	28928	34304
	High	3840	9728	14336	17280	2816	8704	13312	16256
	Interrupt	1792	4480	6784	8320	1280	4096	6272	7808

(Sheet 1 of 2)

Table 8 (continued)
Congestion thresholds on frame-cell trunks

Link speed	Emission priority	Upward thresholds (bytes)				Downward thresholds (bytes)			
		T1	T2	T3	T4	T1	T2	T3	T4
512 kbit/s	Normal	9984	26880	39168	45696	7936	24960	37248	44032
	High	4736	12416	18304	21888	3584	11264	17152	20864
	Interrupt	2176	5760	8704	10624	1664	5632	8064	10112
1024 kbit/s	Normal	17536	49920	73216	85504	14464	47104	70528	82944
	High	8064	22784	34048	40704	6400	21248	32512	39296
	Interrupt	3712	10496	16128	19584	2944	9856	15360	18944
1536 kbit/s	Normal	44416	67456	100224	111232	42368	65280	97792	108672
	High	21120	31488	46464	51456	19072	29312	44032	48896
	Interrupt	11264	16256	23552	25984	9216	14080	21120	23424
1920 kbit/s	Normal	45056	68352	101376	112640	42624	65664	98432	109440
	High	21760	32512	47616	52864	19328	29824	44672	49664
	Interrupt	11904	17152	24704	27392	9472	14464	21760	24192
T3	Normal	78976	118528	175872	195584	69120	106624	160000	177792
	High	40448	12416	90112	100352	35456	54656	82048	91136
	Interrupt	29440	29440	48640	48640	26496	26496	44160	44160
E3	Normal	78976	118528	176872	195584	69120	106624	160000	177792
	High	40448	12416	90112	10352	35456	54656	82048	91136
	Interrupt	29440	29440	48640	48640	26496	26496	44160	44160

(Sheet 2 of 2)

Dynamic Passport trunk speed change for frame-cell trunks

The dynamic Passport trunk speed change feature enables Passport trunking and routing to adapt to changes in bandwidth without taking Passport trunks out of service. The Passport trunking system reacts to dynamic bandwidth changes and propagates this information to the routing system. The routing system uses this data to redistribute traffic to continue delivering quality of

service while simultaneously optimizing network resources. For provisioning information, see “Provisioning ISDN dial backup” (page 30), “Provisioning scheduled ISDN BWoD” (page 32), “Provisioning alarms for dynamic ISDN BWoD” (page 34), “Provisioning ISDN dial backup with scheduled BWoD” (page 35), or “Provisioning ISDN dial backup with dynamic BWoD” (page 37).

This section includes the following information:

- “Dynamic Passport trunk speed change feature highlights” (page 127)
- “ISDN dial backup” (page 128)
- “ISDN dynamic bandwidth on demand” (page 129)
- “Inverse multiplexing” (page 132)

Dynamic Passport trunk speed change feature highlights

The dynamic Passport trunk speed change feature enables a Passport system to interwork with third-party equipment to offer the following functionality:

- “ISDN dial backup” (page 128)

  This functionality resumes connectivity between two Passport nodes when a leased line failure occurs.

- “ISDN dynamic bandwidth on demand” (page 129)

  ISDN dynamic BWoD enables a Passport node to adapt to additional bandwidth when the capacity of the dedicated facility is exceeded.

- “Inverse multiplexing” (page 132)

  Inverse multiplexing enables a Passport trunk to support more than four physical connections between adjacent Passport nodes

V.11, V.35, and HSSI interfaces for frame-cell trunks support these third-party devices.

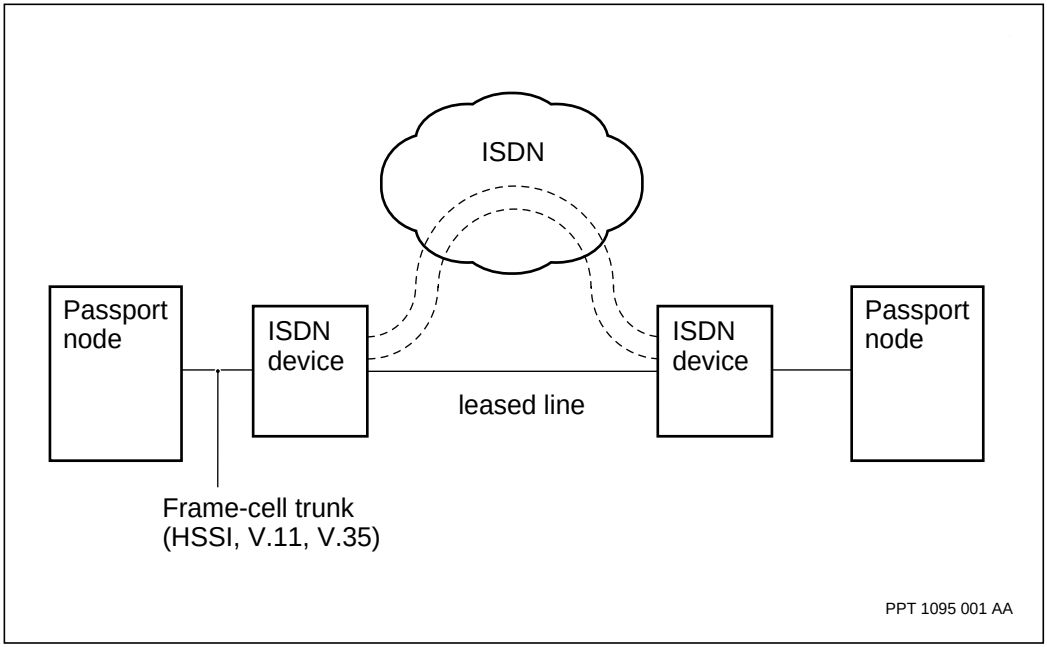
ISDN dial backup

For normal conditions, network traffic travels across a leased line. When the leased line fails, third-party ISDN equipment establishes a dialed-up connection as backup to carry the network traffic (see Figure 16, “Frame-cell trunking with third-party ISDN devices,” (page 128)).

In most cases, dial backup lines provide less bandwidth than the normal leased line. During these periods, the Passport network routes traffic with respect to the decreased bandwidth of the backup lines. Later, when the leased line becomes available again, third-party ISDN equipment releases the dialed-up connections, and the Passport network routes traffic with respect to the leased line bandwidth.

Note: The Passport port connected to the third-party IDSN device must be set to DTE.

Figure 16
Frame-cell trunking with third-party ISDN devices



Provisioning ISDN dial backup on a Passport 7400 series switch

In the ISDN dial backup application, the Passport trunk speed change reporting mechanism is enabled. The Passport trunk propagates speed variations to the routing systems.

When the leased line fails, the Passport trunk either disables and re-enables with a small amount of bandwidth or learns of a sudden bandwidth decrease. The Passport trunk reports the speed decrease immediately to the routing system. The routing system reacts to the speed decrease as soon as possible to avoid severe traffic congestion.

You can program the ISDN devices to automatically dial up a given number of lines at a time. In these cases, the dialed-up speed increases in steps. To avoid these transient speed updates from overloading the routing system, the Passport trunk speed change reporting mechanism allows you to customize the granularity and the frequency of the speed increase updates.

Reporting speed changes: The dynamic Passport trunk speed change feature has seven provisionable threshold levels for reporting the speed changes. In the ISDN dial backup application, the Passport trunk runs in one of two modes: normal speed and backup speed.

If only the normal speed provided by the leased line and one backup speed is provisioned as the threshold level, the Passport trunk reports the following speed increase to the routing system:

- when it has obtained the expected backup speed
- when it has obtained the normal speed provided by the leased line

The Passport trunk reports the current measured speed to the routing system if the next threshold level to the last reported speed, or the expected normal speed is reached and remains above that level after the hold-off time.

ISDN dynamic bandwidth on demand

To provide extra bandwidth for traffic peaks, dynamic bandwidth on demand (BWoD) is a more cost-efficient alternative than configuring extra bandwidth permanently. By dialling up extra bandwidth in response to high traffic levels, network planners and engineers can reduce facility cost.

As seen in Figure 16, “Frame-cell trunking with third-party ISDN devices,” (page 128), the frame-cell trunk bandwidth dynamically increases as the third-party ISDN devices dial up more connections. The dynamic increases can be

- “Dynamic increases—scheduled ISDN BWoD” (page 130)
- “Dynamic increases—dynamic ISDN BWoD” (page 130)

Dynamic increases—scheduled ISDN BWoD

In this configuration, extra bandwidth is required on a frame-cell trunk on a planned basis to respond to an anticipated peak in user traffic. For example, a particular application using the network can generate low levels of interactive traffic most of the time, but need to transfer large amounts of data from one host site to another on a daily basis for backup or consolidation purposes. To respond to this requirement, the third-party devices are set up to automatically dial up extra bandwidth between the two sites involved for the scheduled duration of the large data transfer.

When the scheduled BWoD occurs, the Passport network routes a higher volume of traffic through the frame-cell trunk where the bandwidth has been increased for that period of time. When the Passport network releases the extra dialed up bandwidth, the traffic over the frame-cell trunk returns to the reduced volume of traffic.

Dynamic increases—dynamic ISDN BWoD

If the traffic volumes vary widely in an unpredictable manner, frame-cell trunk congestion can occur during traffic peaks.

Through the third-party devices, the network can monitor traffic patterns and volumes and dynamically dial up extra bandwidth in response to traffic peaks.

If the third-party ISDN devices enable dynamic BWoD, the frame-cell trunk gets extra bandwidth to avoid or relieve congestion. If there is enough added bandwidth (as a percentage) the metric can be adjusted downward and the frame-cell trunk attracts more traffic.

Provisioning scheduled ISDN BWoD on a Passport 7400 series switch

In the scheduled ISDN BWoD application, the Passport trunk speed change reporting mechanism is enabled. The Passport trunk propagates speed variations to the routing systems.

You can program the ISDN devices to automatically dial up a given number of lines at a time. In this application, the speed increases in steps. To avoid transient speed updates from overloading the routing system, the Passport trunk speed change reporting mechanism allows you to customize the granularity and frequency of the speed increase updates.

Reporting speed changes: In the scheduled ISDN BWoD application, the Passport trunk runs in one of two modes: normal speed and peak speed. You can specify a maximum of seven values through the *speedReportingThresholds* attribute. The following procedure describes how to provision two thresholds (the expected speed of the leased line and the expected peak speed).

Provisioning ISDN dial backup with scheduled BWoD on a Passport 7400 series switch

In this application, the Passport trunk speed change reporting mechanism is enabled. The Passport trunk propagates speed variations to the routing systems.

Reporting speed changes: In the ISDN dial backup with scheduled BWoD application, the Passport trunk runs in one of three modes: normal speed, peak speed, or backup speed. Provision the expected backup speed, expected speed of leased lines, and the expected peak speed as the threshold values.

Passport trunks report only three speed increases to the routing system:

- when it has obtained the expected backup speed
- when it has obtained the normal speed provided by the leased line
- when it has obtained the expected peak speed

You can provision a maximum of seven threshold values for the *speedReportingThresholds* attribute.

Inverse multiplexing

Before inverse multiplexing, a maximum of four frame-cell trunks between Passport nodes were supported. If there was a requirement for more bandwidth than four DS1/E1 frame-cell trunks could provide, a DS3/E3 facility had to be installed between two Passport nodes. Now, inverse multiplexing supports cost-efficient configurations with multiples in excess of four DS1/E1 frame-cell trunks between two Passport nodes. There are two solutions provided for inverse multiplexing configurations:

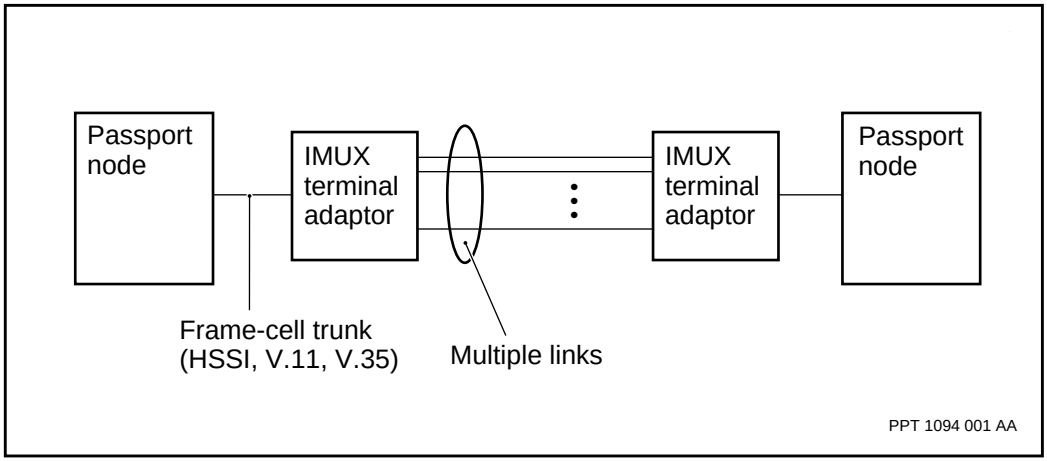
- “Inverse multiplexing on a Passport 7400 series switch” (page 148)
- “Third-party inverse multiplexing (IMUX) for frame-cell trunks” (page 132)

Third-party inverse multiplexing (IMUX) for frame-cell trunks

This configuration provides flexibility to the network provider when it is necessary to use third-party IMUX devices. The frame-cell trunk has the entire bandwidth of the IMUX as shown in Figure 17, “Frame-cell trunking with third-party IMUXs,” (page 133).

If third-party equipment detects additional or fewer links between the IMUXs, the third-party IMUX adjusts its clock which it provides to the Passport node to reflect the bandwidth changes. The bandwidth updates can then be propagated to the routing systems, which in turn takes the appropriate rerouting actions.

Figure 17
Frame-cell trunking with third-party IMUXs



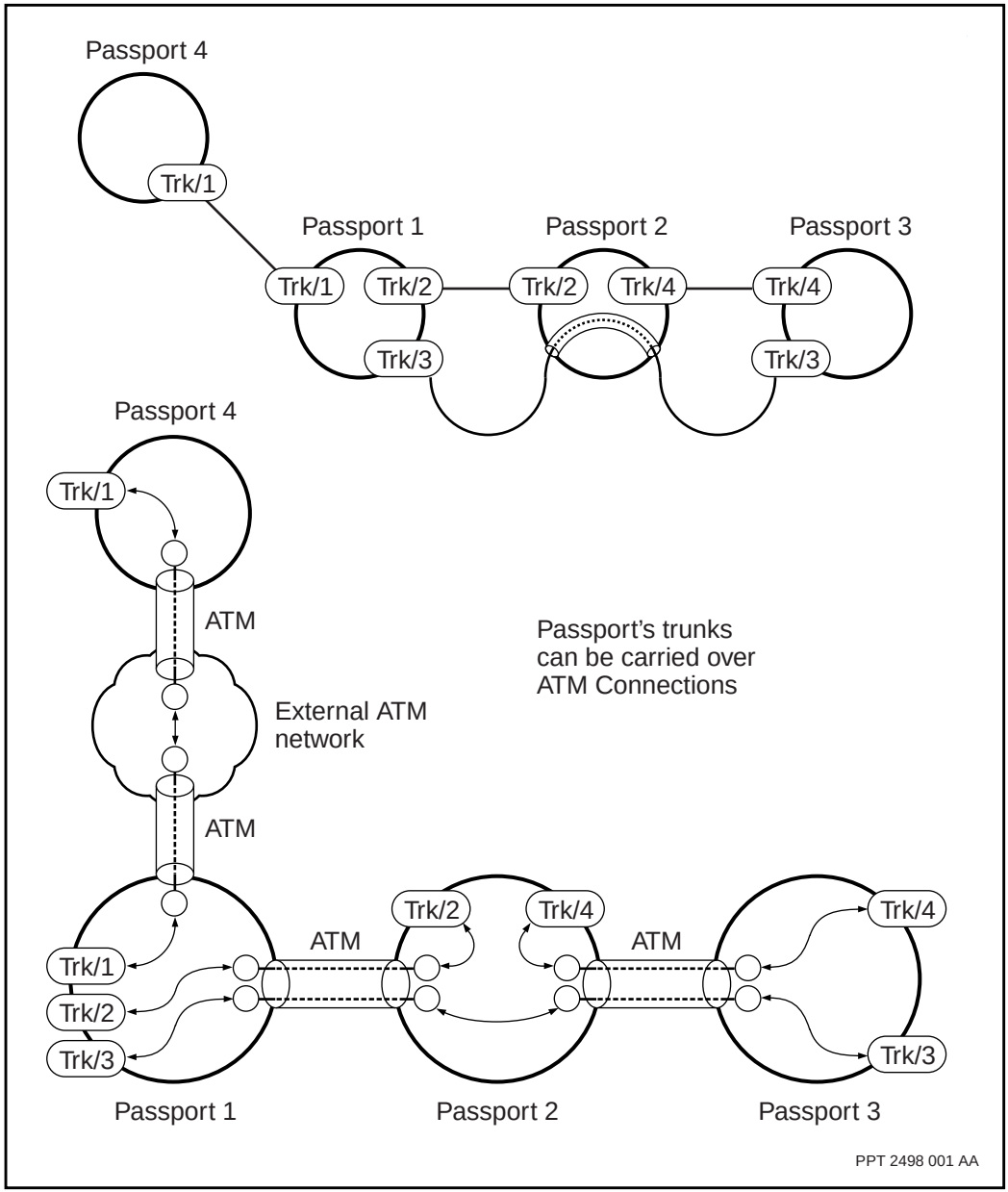
Chapter 9
Passport trunks over ATM

Passport trunks over ATM logically interconnect Passport nodes over ATM facilities as shown in Figure 18, “Passport trunks over ATM,” (page 136). This design offers the ability to map many trunks onto one ATM pipe in a point-to-point manner. This mapping is done by replacing the physical medium of traditional frame-cell trunks by an ATM VCC. A single interface (or port) can support multiple VCCs. Passport trunks over ATM allows all existing services to be carried. This transport mechanism also enables new service offerings to be carried prior to standardization of future adaptation protocols.

This section describes the following Passport trunks over ATM information:

- “Configuring Passport trunks over ATM” (page 137)
- “Passport trunks over ATM connection administration” (page 142)
- “Traffic management for Passport trunks over ATM” (page 145)
- “Dynamic Passport trunk speed change on Passport trunks over ATM” (page 147)
- “Engineering considerations for Passport trunks over ATM” (page 151)

Figure 18
Passport trunks over ATM



Configuring Passport trunks over ATM

You can implement Passport trunks over ATM using a variety of VCC configurations. These VCC configurations define whether the trunk is logical or direct. A logical trunk uses a VCC which in itself is a concatenation of VCC segments. A direct trunk uses a single VCC segment between two adjacent Passport nodes. These configurations include

- "Direct Passport trunks over ATM" (page 137)
- "Logical trunking over a Passport ATM network" (page 137)
- "Logical trunking over an external ATM network" (page 140)

Direct Passport trunks over ATM

Direct trunking between Passport nodes involves defining a Passport trunk over a VCC on an ATM facility that directly connects two Passport nodes (see Figure 19, "Direct and logical trunking over a Passport ATM network," (page 139)). Each VCC endpoint is located on the nodes at each end of the ATM facility. Therefore, only a single VCC segment is necessary to define the Passport trunk.

This way of interconnecting Passport nodes over ATM is the simplest to deploy. This setup only requires a replacement of the existing frame-cell point-to-point trunks with equivalent Passport trunks over ATM.

Traffic transfers to the software level at each tandem hop along the path to the destination. Unlike logical trunking (see "Logical trunking over a Passport ATM network" (page 137) for more information), direct Passport trunks over ATM do not take advantage of the ATM hardware forwarding capabilities of Passport.

If you provision the Passport trunks for map mode (see "Map mode" (page 167)), PORS paths use hardware forwarding.

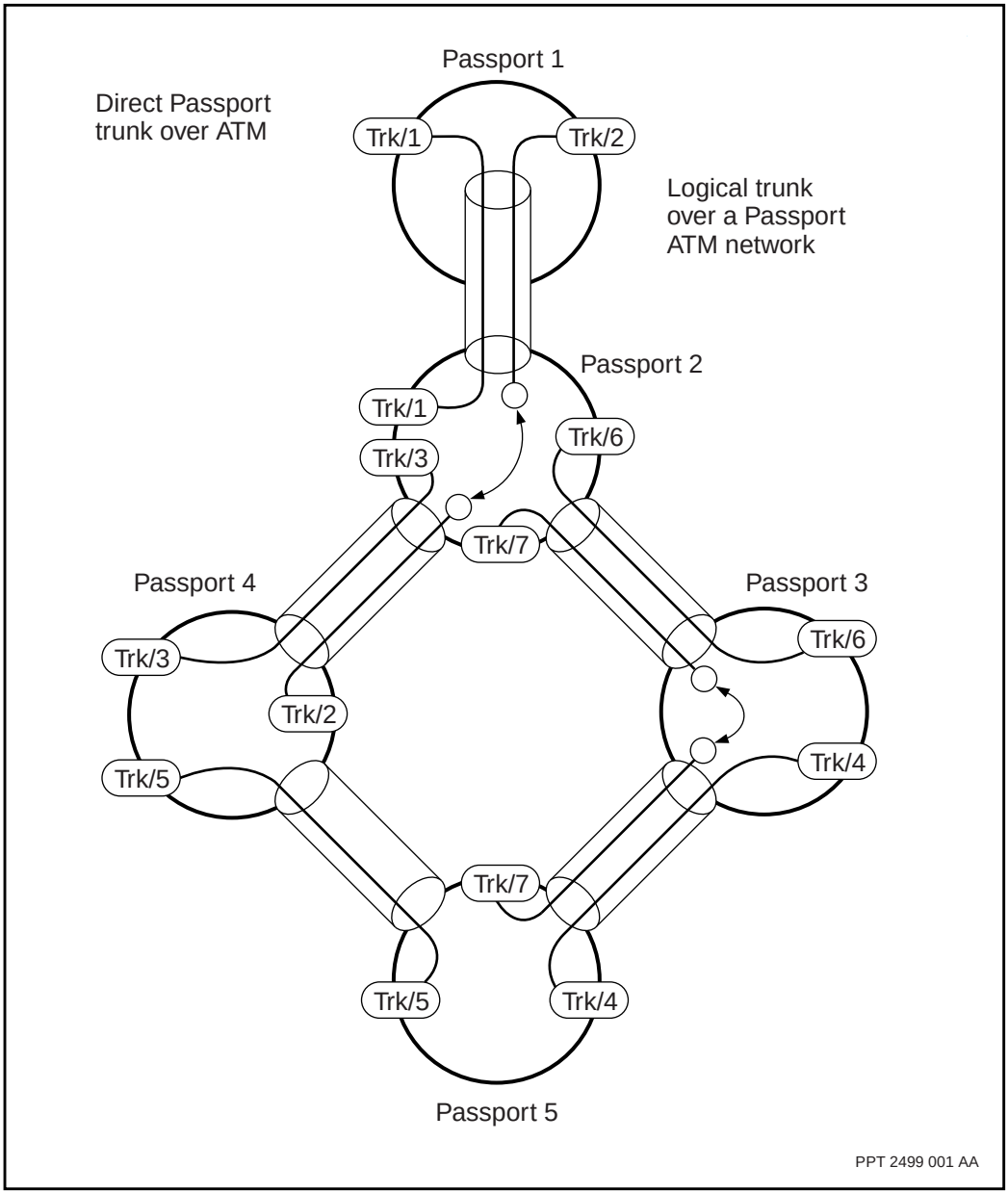
Logical trunking over a Passport ATM network

Logical trunking over a Passport ATM network involves defining a Passport trunk over an ATM bearer service that passes through one or more intermediary Passport nodes (see Figure 19, "Direct and logical trunking over a Passport ATM network," (page 139)). The ATM bearer service consists of an ATM VCC with nailed up relay points defined at tandem nodes along the

path between the source and destination of the VCC. A single interface can support multiple Passport trunks over ATM to provide connectivity to multiple remote Passports.

If you use this logical trunking configuration, you can achieve the full benefits of ATM through the use of ATM hardware forwarding at each of the tandem hops of the Passport trunk. This configuration effectively provides a cut-through mechanism at the tandem nodes along the VCC of the logical trunk which can significantly improve performance at these tandem hops.

Figure 19
Direct and logical trunking over a Passport ATM network



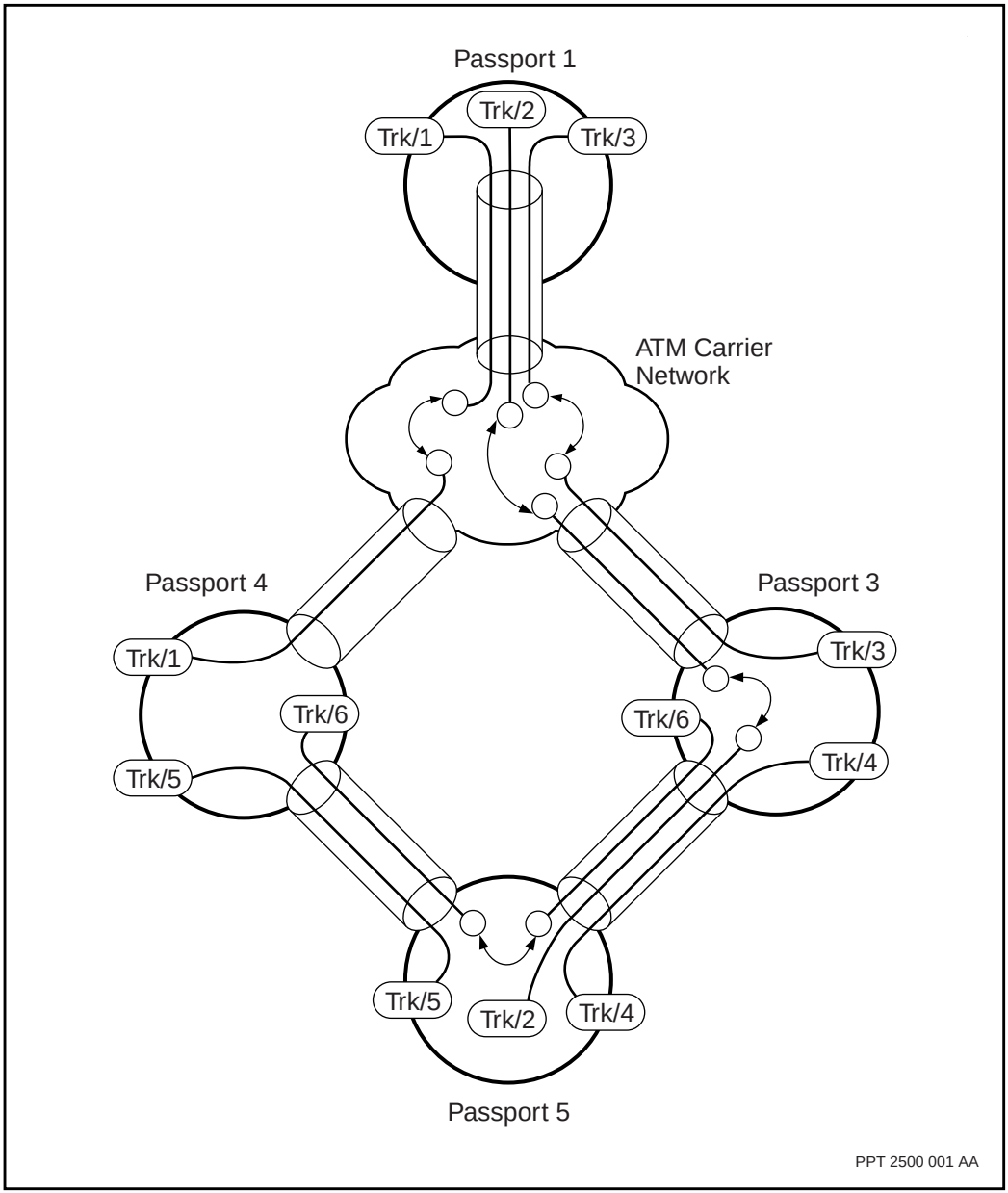
Logical trunking over an external ATM network

In a Passport trunks over ATM scenario with an external ATM network, the logical trunks are on ATM connections that run through an external ATM network (see Figure 20, “Logical trunking over an external ATM network,” (page 141)). The external ATM network views the Passport nodes as customer premise equipment (CPE). An ATM UNI connection to the third-party network is necessary. Multiple Passport trunks over ATM can be supported on a single interface to provide connectivity to multiple remote Passports.

For Passport trunks over ATM across an external ATM network, consider that the external ATM network can have usage parameter control (UPC) turned on at the interface. Ensure that traffic meets the ATM traffic contract guarantee of no loss of traffic at the ingress point to the ATM network. This guarantee can be achieved through the use of traffic shaping on the Passport trunk VCC. For more information see “Traffic management for Passport trunks over ATM” (page 145).

For the trunk to stage, the external network must set an appropriate cell delay-variance tolerance (CDVT) value.

Figure 20
Logical trunking over an external ATM network

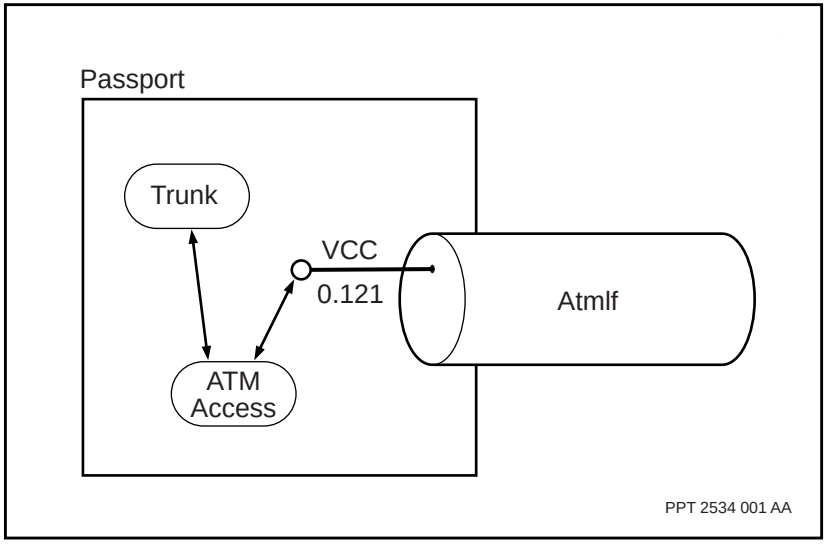


Passport trunks over ATM connection administration

For the ATM switching layer to interwork properly with the network layer, the switching layer needs to relay the connection administration information to the network layer.

The *AtmAccess* component links Passport trunks over ATM to ATM VCCs (see Figure 21, “Passport trunks over ATM connection administration,” (page 142)).

Figure 21
Passport trunks over ATM connection administration



The *AtmAccess* component controls the following functions for the trunk:

- provides the logical linking point for the ATM connection.

  This component provides to its parent *Trunk* component an anchor point for the logical link to the *Vcc* component. The Vcc component can be associated with an *AtmInterface* component or a *VirtualPathTerminator* component.

- provides a mechanism to relay VCC configuration information to the *Trunk* component

  When a *Trunk* component links to an ATM VCC using the *AtmAccess* component, the *AtmAccess* component forwards VCC configuration information from the VCC to the *Trunk* component.

- provides provisioning access

  Any provisioning change to the *atmConnection* attribute of the *AtmAccess* component results in the Passport trunk disabling and restaging. Changes to bandwidth attributes of a VCC result in the VCC going to disabled status and the Passport trunk disabling. On restoration of the VCC to enabled status, the Passport trunk restages and reports the new bandwidth availability to the routing system.

- reports available bandwidth to the *Trunk* component

  The AtmAccess component relays the available bandwidth of the ATM switching layer to the *Trunk* component. The *AtmAccess* component calculates the bandwidth available to the Passport trunk by converting the transmit cell rate of its VCC to a form recognized by Passport trunks. Depending on the value of the *AtmAccess* attribute *vccReportingBw*, the cell rate can be either

  — the peak cell rate (PCR) or current cell rate (CCR)

  — the actual cell rate (ACR)

The unit of measurement for PCR is cells per second (cells/s) but the Passport trunk and topology systems work in bandwidth units of bits per second (bps). The *AtmAccess* component converts the PCR value to a bandwidth value

measured in bits/s using the conversion formula of 1 cell/s = 384 bit/s. The reported VCC bandwidth is indicated by the value of the trunk attribute *measuredSpeedToIf*.

- relays status information

  While the VCC is in operation, the *AtmAccess* component indicates to the Passport trunk if the status of the VCC changes from enabled to disabled. A Passport trunk status can be either up or down, that is, a Passport trunk that is up is operating as intended, while a Passport trunk that is down is not functioning at all.

  You can determine the status of the ATM connection in several ways depending on the type of failure. In the case of an interface failure at the ATM port, all VCCs on the port are down. As well, an ATM connection can also be down because of network or remote end problems. You can detect these problems by the alarm indication signal/remote defect indication (AIS/RDI) or loopback functions provided by the ATM layer.

  When an RDI or AIS OAM cell arrives at the terminating connection (Passport trunk connections are always terminating) or if loopbacks fail, the *AtmAccess* component receives the failure notification and relays it to the Passport trunk as a connection failure. Therefore, it is preferable that you provision VCCs used by Passport trunks with end-to-end loopback enabled.

  Note: If you provision a Passport trunk VCC on an ATM interface or under a virtual path terminator that is connected to an external ATM network, and end-to-end loopback is enabled, the VCC can become disabled.

- relays delay information

  Passport trunks measure round-trip delay (RTD) during the discovery phase of the Passport trunk staging protocol. Passport trunks calculate RTD in microseconds then round to the nearest 100 microseconds. Routing calculates all delay metrics using this delay value in 100s of microseconds. Trunking and routing attributes are displayed in milliseconds with one decimal point.

Traffic management for Passport trunks over ATM

Passport ATM networks can support many applications, such as voice, video, multimedia, file transfer, and interactive communication. Each application has unique traffic characteristics (in terms of rate and density variation) and performance needs (in terms of cell-frame delay and cell loss). The applications used define the service requirements for each subscriber. The communication needs of these applications can be translated into a set of traffic characteristics based on the required quality of service (QoS) classes and the traffic descriptor types. Traffic management functions help ensure that the QoS objectives for each subscriber are met. Traffic management must also maximize the service provider's use of network resources so that the service offering is cost effective.

Traffic management topics introduced in this section include

- "Usage parameter control (UPC)" (page 145)
- "Traffic shaping" (page 146)
- "Emission priority" (page 146)
- "Congestion indication" (page 147)

For more information on traffic management see

- "Traffic management for frame-cell trunks" (page 122)
- 241-5701-400 *Passport 7400, 15000, 20000 Networking Overview*
- 241-5701-920 *Passport 7400, 15000, 20000 Frame Relay to ATM Interworking Guide*
- 241-5701-705 *Passport 7400, 15000, 20000 ATM Traffic Management Fundamentals*

Usage parameter control (UPC)

UPC is the set of actions taken by the network to monitor and control traffic, in terms of both the traffic offered and the validity of the ATM connection at the end-system access. The main purpose of UPC is to protect network resources from traffic demands in excess of those defined through the traffic contract, which can affect the QoS of established connections. UPC detects violations of negotiated parameters and takes appropriate actions, such as cell tagging and cell discarding.

Traffic shaping

Traffic shaping smooths-out traffic bursts. This traffic management strategy regulates the emission interval of cells in the transmit direction. Traffic shaping is useful for ensuring conformance of transmitted traffic to subscribed traffic parameters, or to ensure conformance at a subsequent interface. Traffic shaping is recommended when connecting to an external ATM network, where the connection can be policed.

Emission priority

Traffic management for Passport trunks over ATM also includes the emission priority system. The single virtual channel implementation enables all traffic types to flow through a single ATM emission queue.

Passport trunks over ATM handle traffic according to the emission priority of the VCC to which the trunk is provisioned. Each Passport trunk over ATM is provisioned to a VCC. On ATM FPs, each VCC has a service category (CBR, VBRrt, VBRnrt) with a specified emission priority of high, medium or low. On ATM IP function processors, the emission priority of the service category is provisionable, and can be assigned any of eight emission priorities from EP0 (high) to EP7 (low). For details on the carriage of frame relay traffic over ATM see 241-5701-920 *Passport 7400, 15000, 20000 Frame Relay to ATM Interworking Guide*. For details on ATM traffic management for ATM IP and CQC function processors see 241-5701-705 *Passport 7400, 15000, 20000 ATM Traffic Management Fundamentals*.

Multiple emission priorities provide the proper emission requirements for different traffic types. Voice traffic, for example, has strict emission delay requirements of less than 20 milliseconds. For trunks running the equivalent of E3 rates and below, the voice traffic must have a higher emission priority than data. This priority ensures there are no unacceptable emission delays due to voice frames being queued behind long or multiple data frames.

Passport trunks over ATM have a single emission queue, capable of carrying both DPRS data traffic and isochronous traffic such as HTDS, voice, and BTDS on the same trunk. This can result in the delay requirements of the isochronous traffic not being met. This problem can occur due to queueing delay if the data rate is low, or if large frames are present, or both.

Engineering the Passport trunk service category and the number of Passport trunks, or both provides the proper emission requirements for various traffic types. Sometimes the emission requirements for isochronous traffic cannot be met on a single ATM connection. If the requirements cannot be met, different traffic types can be divided over two or more ATM connections, each of which you can provision with an appropriate quality of service. For example, you can provision one Passport trunk over ATM with a service category that specifies only data traffic, while you can provision a second one with the service category that specifies only higher priority real-time traffic (such as voice service and BTDS).

Note: Passport trunks over ATM do not support unspecified bit rate (UBR), the default ATM service category on Passport. For a description of the ATM service categories available on Passport, see 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide*.

Congestion indication

Passport also forwards congestion indication from ATM traffic to Passport trunk traffic using explicit forward congestion indication and forward congestion indication (EFCI-FCI) mapping.

Mapping occurs when an incoming AAL5 frame is being reassembled and at least one of its cells contains an EFCI indication. The Passport trunk sets the FCI bit in the Passport packet, if the bit needs to be set. Mapping occurs automatically and requires no provisioning.

Dynamic Passport trunk speed change on Passport trunks over ATM

The dynamic Passport trunk speed change feature is supported on Passport 7400 series switches only. Passport 15000 and 20000 do not support this feature.

The dynamic Passport trunk speed change feature enables Passport trunking and routing to adapt to changes in bandwidth without taking Passport trunks out of service. For the frame-cell feature description, see “Dynamic Passport

trunk speed change for frame-cell trunks" (page 126). For provisioning information, see "Dynamic Passport trunk speed change for frame-cell trunks" (page 126).

This feature also supports Passport trunking on the integrated Passport Inverse Multiplexing for ATM (IMA). For details on IMA, see 241-5701-730 *Passport 7400, 15000, 20000 Inverse Multiplexing for ATM Guide*.

Inverse multiplexing on a Passport 7400 series switch

The following solutions are provided for inverse multiplexing configurations:

- "Integrated inverse multiplexing on ATM facilities carrying Passport trunks" (page 148)
- "Third-party inverse multiplexing (IMUX) for frame-cell trunks" (page 132)

For an introduction to inverse multiplexing see "Inverse multiplexing" (page 132). For provisioning information for the dynamic trunk speed change IMA feature, see "Provisioning a non-elastic trunk for IMA" (page 49), and "Provisioning an elastic trunk for IMA" (page 50).

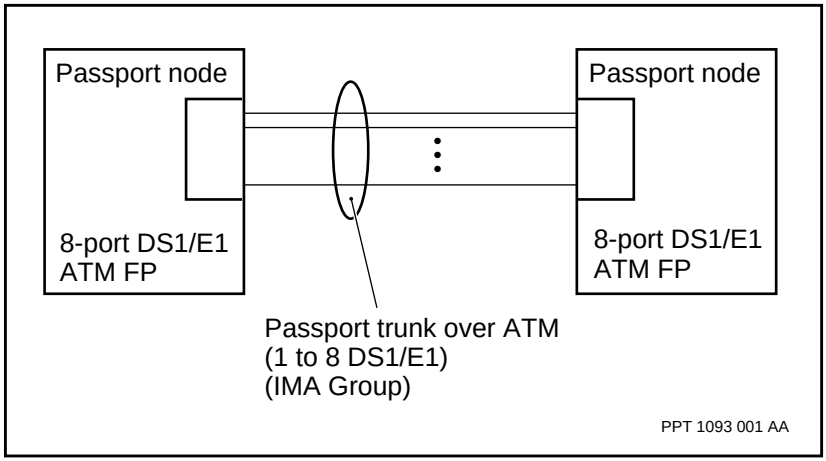
Integrated inverse multiplexing on ATM facilities carrying Passport trunks

The Passport system supports an integrated inverse multiplexing solution through the Passport inverse multiplexing for ATM (IMA) feature. This feature is supported on Passport 7400 series switches only. Passport 15000 and 20000 do not support this feature.

For a list of all FPs that support this feature, refer to 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Figure 22, "Passport trunking over ATM on eight-port DS1/E1 ATM IMA FPs," (page 149) shows how eight-port DS1/E1 ATM FPs support an IMA link group. The IMA group bandwidth is the aggregate of up to eight ATM DS1/E1 physical links. Passport series trunks over ATM that are part of the IMA link group use VCCs which share the bandwidth on the IMA group.

Figure 22
Passport trunking over ATM on eight-port DS1/E1 ATM IMA FPs



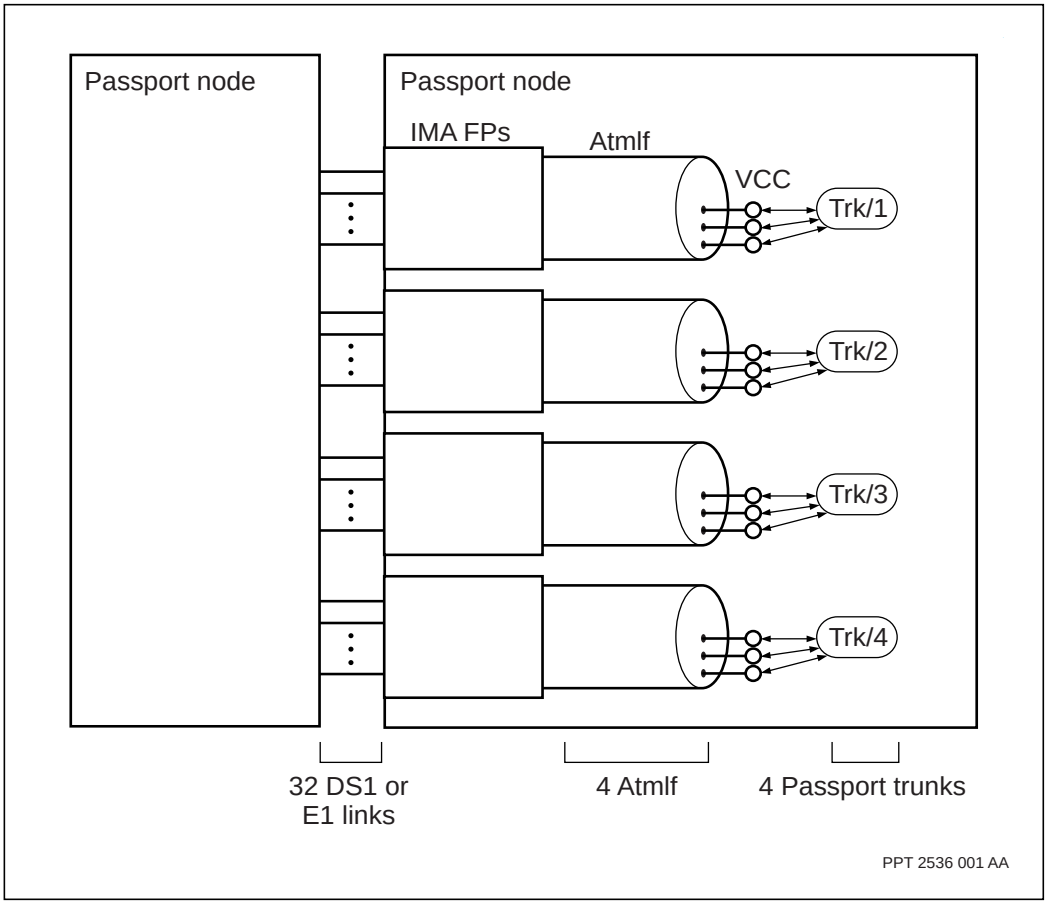
IMA technology greatly increases the number of DS1 or E1 links that can be supported between two Passport nodes. Without IMA

- Up to four Passport trunks are possible between two Passport nodes.
- Each Passport trunk runs over its own physical link.

With IMA, up to 32 physical DS1 or E1 links are possible (see Figure 23, "IMA support of links between Passport 7400 series switches," (page 150)). This maximum number results from the following configuration:

- Four trunks each carry one or more ATM VCCs.
- Each ATM VCC is part of one of the four ATM interfaces.
- Each of four *AtmIf* components consists of eight DS1 or E1 links in an IMA group.

Figure 23
IMA support of links between Passport 7400 series switches



If IMA detects additional or fewer links between the IMA FPs, the IMA group bandwidth can fluctuate. The software informs the Passport trunk of the bandwidth change. The bandwidth update can be propagated to the routing systems which in turn takes appropriate rerouting actions. PORS, and DPRS, provide dynamic bandwidth updates.

Only direct Passport trunks over ATM composed of nailed-up single-hop permanent virtual circuits (PVCs) can be configured as bandwidth elastic connections. Elastic connections can lose and regain bandwidth in response to changes in bandwidth available over an IMA link group.

The Passport trunking system admits a newly added non-elastic trunk at full bandwidth. The Passport trunking system readmits a released non-elastic trunk at the full original bandwidth.

The Passport trunking system admits a newly added elastic trunk at full or reduced bandwidth. The Passport trunking system readmits a released elastic trunk at the full or reduced original bandwidth.

Use an elastic trunk when the connection must stay up over the IMA link even though it is susceptible to reduced bandwidth. For elastic trunks, use either PORS map mode or AAL5 mux mode. Do not use PORS SPO-mux mode on an elastic trunk. In SPO-mux mode, the connection bandwidth controller (CBC) cannot guarantee that the trunk VCCs will remain up when the IMA group experiences bandwidth reductions.

For non-elastic trunks only, a trunk is released according to the holding priority. Use non-elastic trunks when you can apply the CBC holding priority.

An elastic or non-elastic trunk can be released due to

- a critical provisioning change that affects the trunk or VCC
- a locked trunk (local or remote-end lock)
- a trunk restage due to a faulty facility

For details on how ATM connections (including elastic connections) respond to dynamic bandwidth over an IMA link group, see 241-5701-700 *Passport 7400, 15000, 20000 ATM Overview* and 241-5701-702 *Passport 7400, 15000, 20000 ATM Routing and Signaling Fundamentals*.

Engineering considerations for Passport trunks over ATM

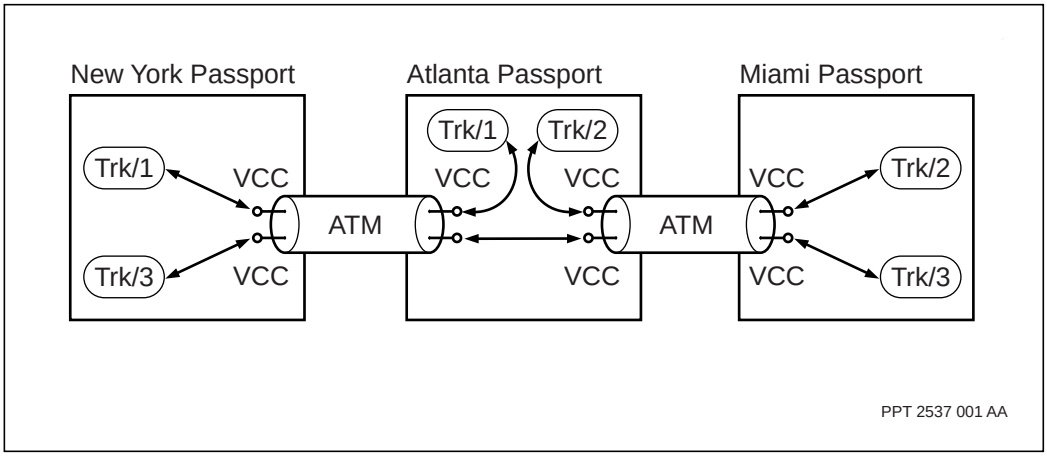
In order to maximize network efficiency, Passport trunks over ATM must be engineered with the following considerations in mind:

- “Maximizing connection performance” (page 152)

Maximizing connection performance

To maximize connection performance in a Passport network, increase the number of logical trunks and decrease the number of direct trunks where trunk concatenation is necessary. For a Passport network, if you are planning to implement a logical Passport trunk over ATM, ensure that you have concatenated the VCC links of the connection before logically linking the trunk component to the interface component (as opposed to concatenating several trunks). See Figure 24, "Increasing connection performance by using logical Passport trunks over ATM," (page 153). In this example, the Passport node in New York connects to Atlanta by Passport trunk 1 and Atlanta connects to Miami by Passport trunk 2. If you add Passport trunk 3 to logically connect New York to Miami, you can achieve better performance between those two nodes. Traffic tandeming through Atlanta does not then go through software processing (that is, hardware cell relays it).

Figure 24
Increasing connection performance by using logical Passport trunks over ATM



Increasing node connectivity

As illustrated in Figure 24, “Increasing connection performance by using logical Passport trunks over ATM,” (page 153), both the New York and Miami Passport nodes have increased their number of neighbors. One benefit of this is that it provides additional redundancy. For example, if Passport trunk 2 is disabled yet the ATM interface is still operational then the Miami Passport node is not isolated from the network as it still has connectivity to the New York Passport node.

Preside Multiservice Data Manager connectivity on tandem nodes

In Figure 24, “Increasing connection performance by using logical Passport trunks over ATM,” (page 153), if Passport trunk 1 and Passport trunk 2 do not exist and the Atlanta Passport node is only for ATM bearer service such as the tunneling of Passport trunk 3, then the Atlanta node is not accessible for Preside Multiservice Data Manager operations through the Passport network. To achieve connectivity, the Atlanta node too needs to have a direct connection between the Passport node and the Preside Multiservice Data Manager workstation. Or, it requires a direct Passport trunk over ATM (either Passport trunk 1 or Passport trunk 2) to connect to the Miami Passport node.

Trunk metrics

Even though a logical trunk looks like a single hop to the routing system, the logical trunk can actually tandem through service nodes. If the associated metrics to this Passport trunk are substantially in excess of service requirements, the existing override features of the Passport trunk can alter them.

Configuring trunks over ATM VCCs

Configuring Passport trunks over ATM to support different traffic types requires additional engineering effort because each Passport trunk over ATM offers one emission priority. To achieve different emission priorities over Passport trunks over ATM within a given Passport trunk group (that is a pair of connected Passport nodes), each Passport trunk over ATM must use a different VCC providing a different ATM service category.

For a more detailed explanation on these configurations, see the *Passport Engineering Notes and Guidelines*.

Passport trunks over ATM bandwidth

The *AtmAccess* attribute *vccReportingBw* determines how the bandwidth of a VCC is reported to the parent Passport trunk:

- If its value is pcr (the default value), the PCR or current cell rate (CCR) is reported.
- If its value is acr, the best measurement of the actual cell rate (ACR) is reported. The ACR is the minimum of the PCR, CCR, and actual shaping rate (ASR).

The actual reported bandwidth also depends on other factors:

- whether there is a requested shaping rate (RSR) in effect
- whether traffic shaping is in effect
- whether elastic bandwidth has been provisioned for the Passport trunk

Table 9, “ATM factors and reported cell rate,” (page 155) shows the relationships between these factors and the value of the reported cell rate. When the *vccReportingBw* attribute is set to pcr, the VCC reported bandwidth is either PCR or CCR. The CCR is reported when the VCC bandwidth is

reduced below the PCR. When the *vccReportingBw* attribute is set to acr, the minimum of the PCR, CCR, or ASR is reported. The actual cell rate is never higher than the PCR. When traffic shaping is in effect, the ASR is shaped at the next rate lower than the PCR, CCR, or RSR.

Table 9
ATM factors and reported cell rate

Factor	**Value**							
RSR	N	N	N	N	Y	Y	Y	Y
trafficShaping	N	N	Y	Y	N	N	Y	Y
bwElastic	N	Y	N	Y	N	Y	N	Y
Reported cell rate when vccReportingBw=pcr	PCR	PCR/ CCR	PCR	PCR/ CCR	PCR	PCR/ CCR	PCR	PCR/ CCR
Reported cell rate when vccReportingBw=acr	PCR	PCR/ CCR	min. of PCR, ACR	min. of PCR/ CCR, ASR	PCR	PCR/ CCR	min. of PCR, ACR	min. of PCR/ CCR, ASR

Chapter 10
Passport routing over ATM

You can adapt all of Passport's non-ATM services to ATM using Passport trunks over ATM. This functionality is achieved by taking advantage of the existing Passport routing architecture. ATM networks using DPRS, and PORS on Passport trunks over ATM can carry all Passport non-ATM services. Passport also allows a smooth migration toward ATM by allowing the co-existence and interworking of frame-based and ATM-based trunks.

For some PORS services on Passport trunks over ATM, you can achieve additional high performance end-to-end through hardware forwarding along the ATM path of the connection. For example, Passport delivers an end-to-end high-speed voice over ATM solution by using the ATM hardware to adapt and switch voice traffic through the ATM function processor (FP).

This section describes the following Passport routing systems for Passport trunks over ATM, including the PORS efficiency features:

DPRS on Passport trunks over ATM

The Passport Dynamic Packet Routing System (DPRS) is responsible for routing Passport traffic such as frame relay, and DPN-100. The DPRS routing system does not differentiate between the routing behavior of frame-cell and Passport trunks over ATM. However, the ability to route DPRS traffic on Passport trunks over ATM provides significant advantages.

DPRS can quickly reroute around trunk failures when routing on Passport trunks over ATM. This capability supports resilient frame relay connectivity with minimal administration. Passport trunks over ATM also provide the ability to map many frame relay DLCIs into a single ATM virtual channel connection (VCC). This mapping simplifies the administration for ATM for frame relay services for each connection. DPRS on Passport trunks over ATM provides the ability to use ATM to full advantage without significant impact to the existing network infrastructure. DPRS on Passport trunks over ATM offers concentration of low-speed/high-density frame relay, and provides for rapid transfer with hardware forwarding and high speed Passport trunks.

Passport trunks over ATM carry DPRS traffic using AAL5 to convert frames to ATM cells. DPRS traffic routing can also be configured to run on spare equipment. See “Spared Passport 15000 and 20000 Trunks over ATM” (page 182) for details.

PORS on Passport trunks over ATM

This section describes the following Passport trunks over ATM information for PORS:

- “PORS ATM efficiency” (page 159)
- “AAL5-mux mode” (page 162)
- “Short path-oriented multiplexing (SPO-mux) mode” (page 164)
- “Map mode” (page 167)

Passport trunks over ATM carrying PORS traffic can also be configured to run on spare equipment. See “Spared Passport 15000 and 20000 Trunks over ATM” (page 182) for details.

Passport PORS ATM efficiency consists of the SPO-mux and map modes. This section includes additional PORS ATM efficiency information:

- “PORS traffic mapping to internal discard and emission priority” (page 171)
- “PORS ATM efficiency migration strategy” (page 175)
- “PORS ATM efficiency impacts” (page 176)
- “PORS ATM efficiency engineering guidelines” (page 176)

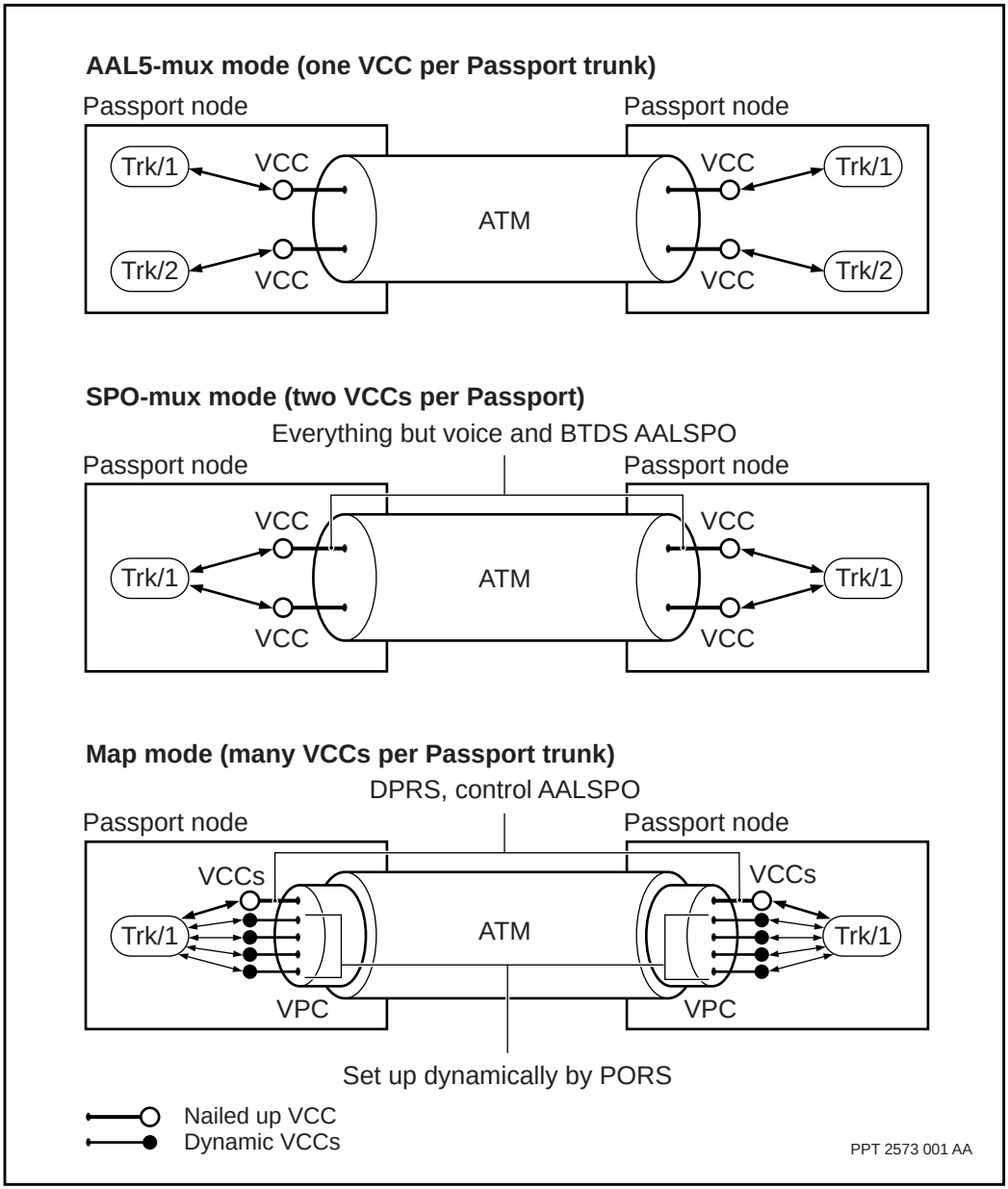
PORS ATM efficiency

You can provision PORS applications such as voice and BTDS to optimize bandwidth on Passport trunks over ATM.

PORS ATM efficiency modes

You can provision PORS ATM efficiency using one of three transport capabilities or modes. See Figure 25, “Mapping Passport trunks to ATM VCCs,” (page 160) for a comparison of the three modes. The last two modes listed are in the PORS ATM efficiency category:

Figure 25
Mapping Passport trunks to ATM VCCs



PORS ATM efficiency characteristics

PORS ATM efficiency has the following characteristics:

- increased throughput
- efficient transportation across frame-cell trunks and Passport trunks over ATM
- supported on all ATM functional processors (FPs)
- supported for path-oriented services

PORS ATM efficiency adds to the existing bandwidth saving capabilities available on the Passport voice service such as silence suppression and voice compression. For information on these capabilities, see 241-7401-750 *Passport 7400 Voice Transport Guide*.

See the Release Notes for maximum throughput per ATM FPs and maximum VCCs.

Table 10
PORS ATM efficiency usage

Mode	# VCCs for each Passport Trunk	ATM conversion method	When to use
AAL5-mux	1	AAL5	if little voice traffic and desire simplest administration
SPO-mux	2	AAL5 for PORS, DPRS data and control traffic; AALSPO for voice, BTDS traffic.	if voice traffic exists but map mode not appropriate
map	separate VCC for each call	AAL5 for DPRS and routing control traffic; AAL5 for PORS HTDS; AALSPO for voice and BTDS traffic.	if not limited by available VCC quantity if okay to have whole VPC through external ATM network

AAL5-mux mode

In this mode each Passport trunk links to a single ATM VCC, as Figure 26, "AAL5-mux mode," (page 163) illustrates. AAL5 encapsulation converts all traffic carried by the trunk to ATM cells.

AAL5 adds an eight-byte trailer, and 1 to 47 bytes of padding to each frame or Passport cell to be converted to ATM cells. This method is inefficient for Passport voice service since each Passport voice cell (44-byte payload) ends up requiring two ATM cells (40 bytes of padding). BTDS can be defined to use Passport cells with 84 bytes of payload. This method results in the Passport BTDS cell fitting evenly in two ATM cells with no padding.

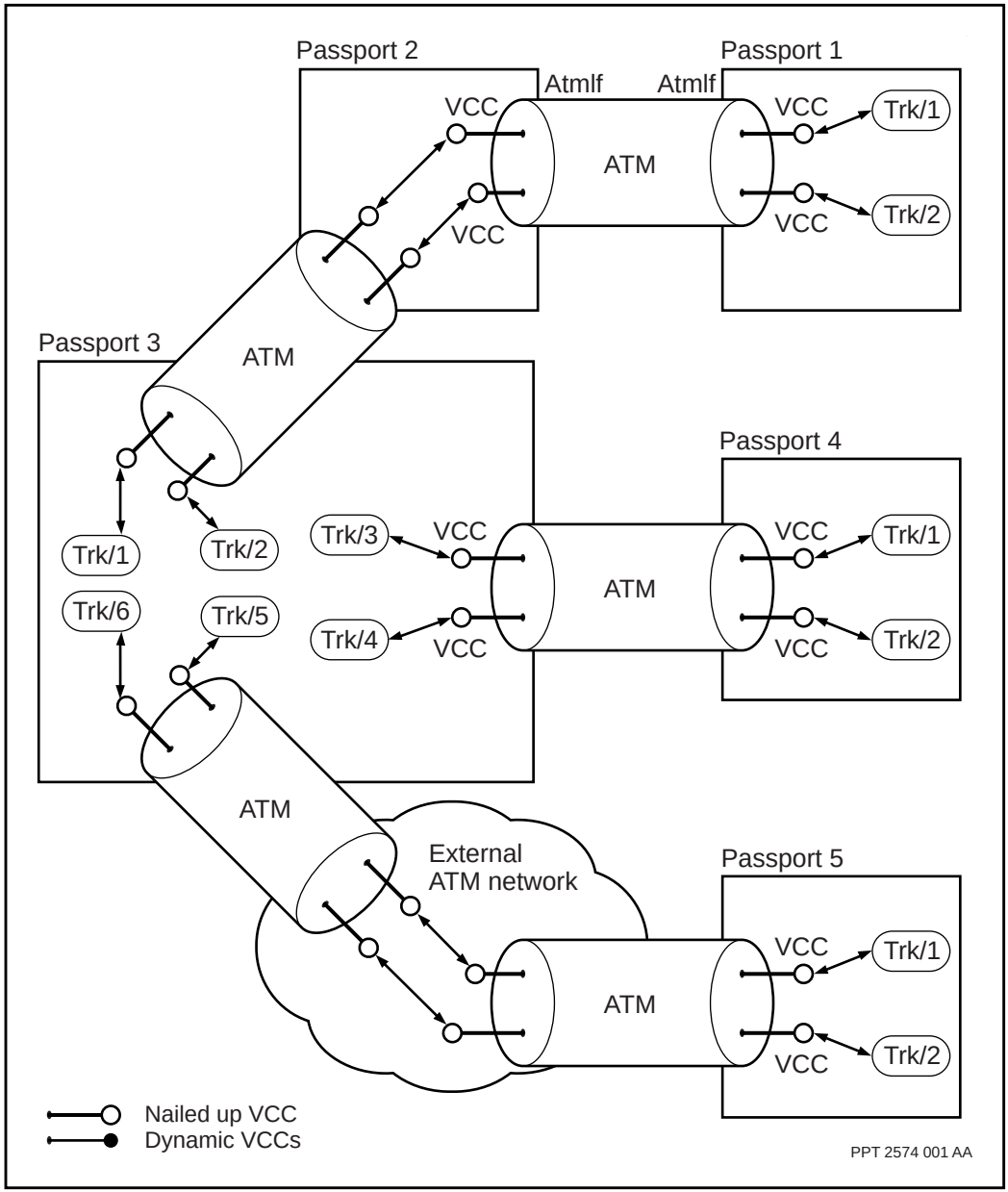
All connections between Passport trunks and ATM VCCs are nailed up. These VCCs can be over a direct ATM connection between two Passport nodes, or can pass through a tandem Passport node or an external ATM network.

Depending on the service mix offered on the Passport nodes, you can define one or more Passport trunks, each to carry traffic requiring a different class of service. One of the Passport trunks must be configured to carry frame traffic such as DPRS traffic and PORS HTDS traffic. The other must be defined to carry voice and BTDS traffic. The VCC for the Passport trunk carrying voice and BTDS traffic must be defined with a QOS such as rt-VBR, which has a higher emission priority. This definition allows the voice and BTDS traffic to jump ahead of frame traffic to reduce the delay variance for the user data.

At tandem sites, where nailed up ATM VCCs carry Passport trunks through the Passport node, ATM cell relay forwards the traffic. Hardware performs the ATM cell relay and the relay is extremely fast.

At tandem sites where the ATM VCCs terminate at Passport trunk components, the CPU performs the Passport frame and cell forwarding. CPU forwarding throughput is considerably less than hardware-only forwarding for ATM cell relay.

Figure 26
AAL5-mux mode



Short path-oriented multiplexing (SPO-mux) mode

For the SPO-mux mode, you configure the Passport trunk to use two ATM VCCs, an AAL5-mux VCC, and a SPO-mux VCC, as Figure 27, “SPO-mux mode,” (page 165) illustrates. The path administrator (Pa) adds and manages the new VCC.

The AAL5-mux VCC, usually called the parent VCC, uses AAL5 encapsulation to carry large frame PORS, DPRS data and control traffic. The SPO-mux VCC, uses AALSPO encapsulation to carry Passport voice or BTDS cells, which are 45 bytes of payload or less.

The SPO-mux mechanism carries voice over ATM efficiently. These 45-byte frames plus a 3-byte PORS routing header, and a 5-byte ATM header are exactly 53 bytes, as shown in Figure 28, “Conversion of voice or BTDS packets into ATM cells using SPO-mux mode,” (page 166). The 53-byte frames transport as pure cells (that is, no adaptation layer). The 45-byte payload results in 53 bytes on the link instead of 106 bytes when using the ATM adaptation layer 5 (AAL5) protocol.

To use SPO-mux mode transport, the applications must inform PORS that they are using frames no larger than 45 bytes. The maximum transmission unit (MTU) of the service and a new call flag to the VC sends this message to the PORS VC at call setup time.

Figure 27
SPO-mux mode

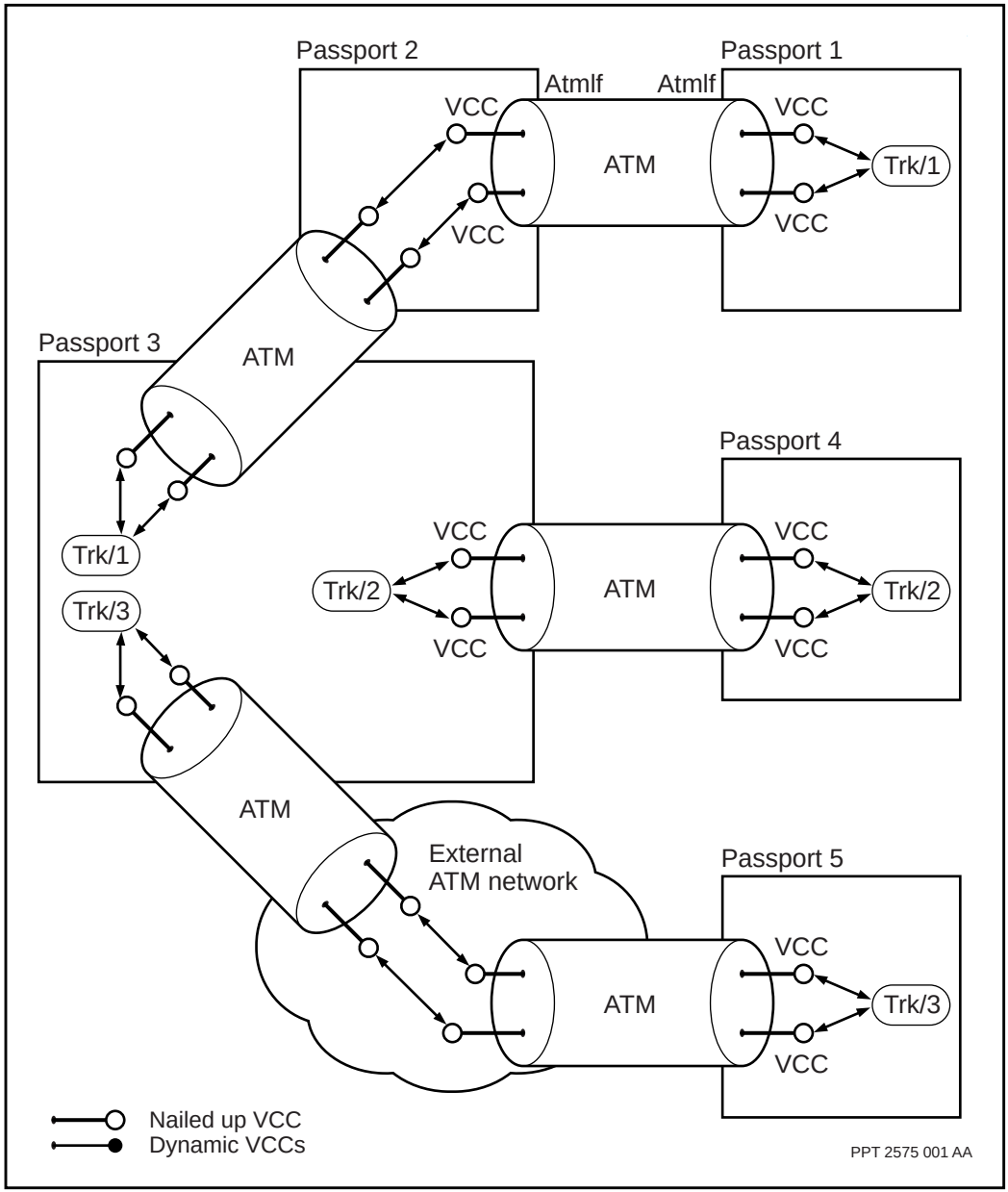
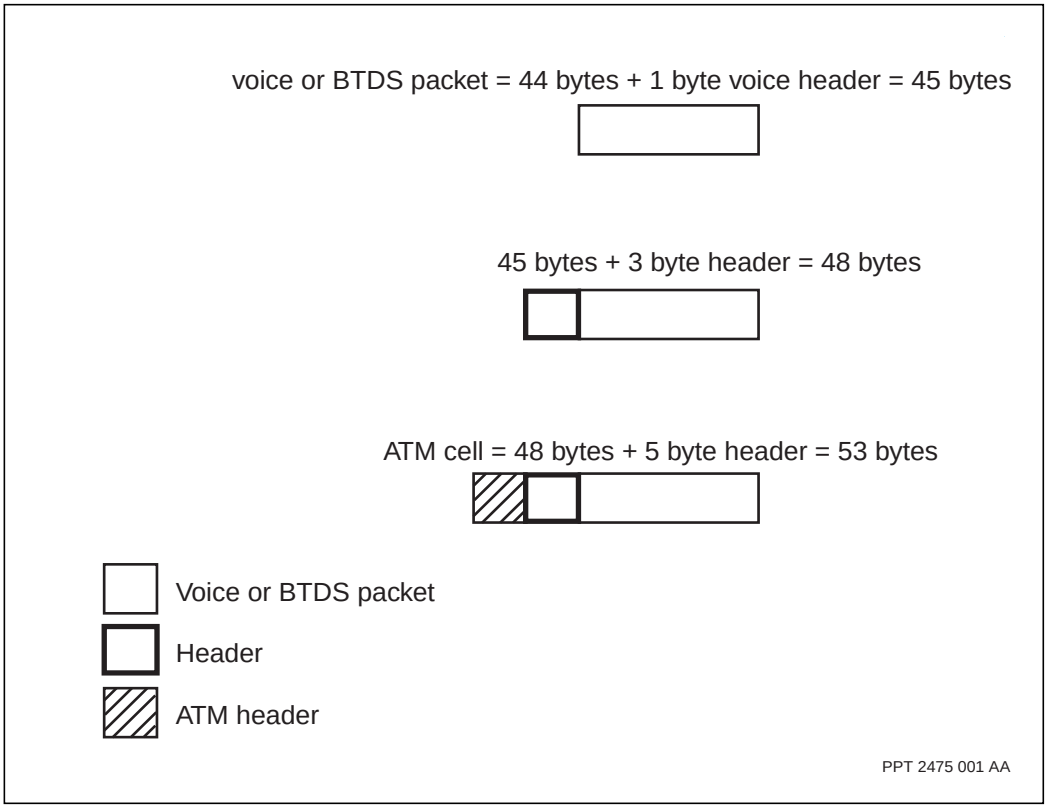


Figure 28
Conversion of voice or BTDS packets into ATM cells using SPO-mux mode



All connections between Passport trunks and ATM VCCs are nailed up. These VCCs can be over a direct ATM connection between two Passport nodes, or can pass through a tandem Passport node or an external ATM network.

At tandem sites, where nailed up ATM VCCs carry Passport trunks through the Passport node, ATM cell relay forwards the traffic. Hardware performs the ATM cell relay and the relay is extremely fast.

At tandem sites where the ATM VCCs terminate at Passport trunk components, the CPU performs the Passport frame and cell forwarding. CPU forwarding throughput is considerably less than hardware-only forwarding for ATM cell relay.

Map mode

Map mode allows a much larger number of VCCs for each Passport trunk, as shown in Figure 29, “Map mode,” (page 169):

- one AAL5-mux VCC to carry DPRS and routing control traffic using AAL5 encapsulation
- multiple AAL5-map VCCs to carry PORS HTDS and BTDS traffic using AAL5 encapsulation. For each HTDS or BTDS path, PORS sets up a separate ATM VCC, in the same VPC as the AAL5-mux VCC.
- multiple AALSPO-map VCCs to carry voice and BTDS traffic, using AALSPO encapsulation. For each voice and BTDS path, PORS sets up a separate ATM VCC, in the same VPC as the AAL5-mux VCC.

The AAL5-mux ATM VCC is nailed up. The AAL5-map VCCs and the ALSPO-map VCCs are dynamically created and managed by the PORS path administrator. Map mode trunks can be defined on direct ATM connections between two Passport nodes. If you define map mode trunks over external ATM networks you must provision a whole VPC.

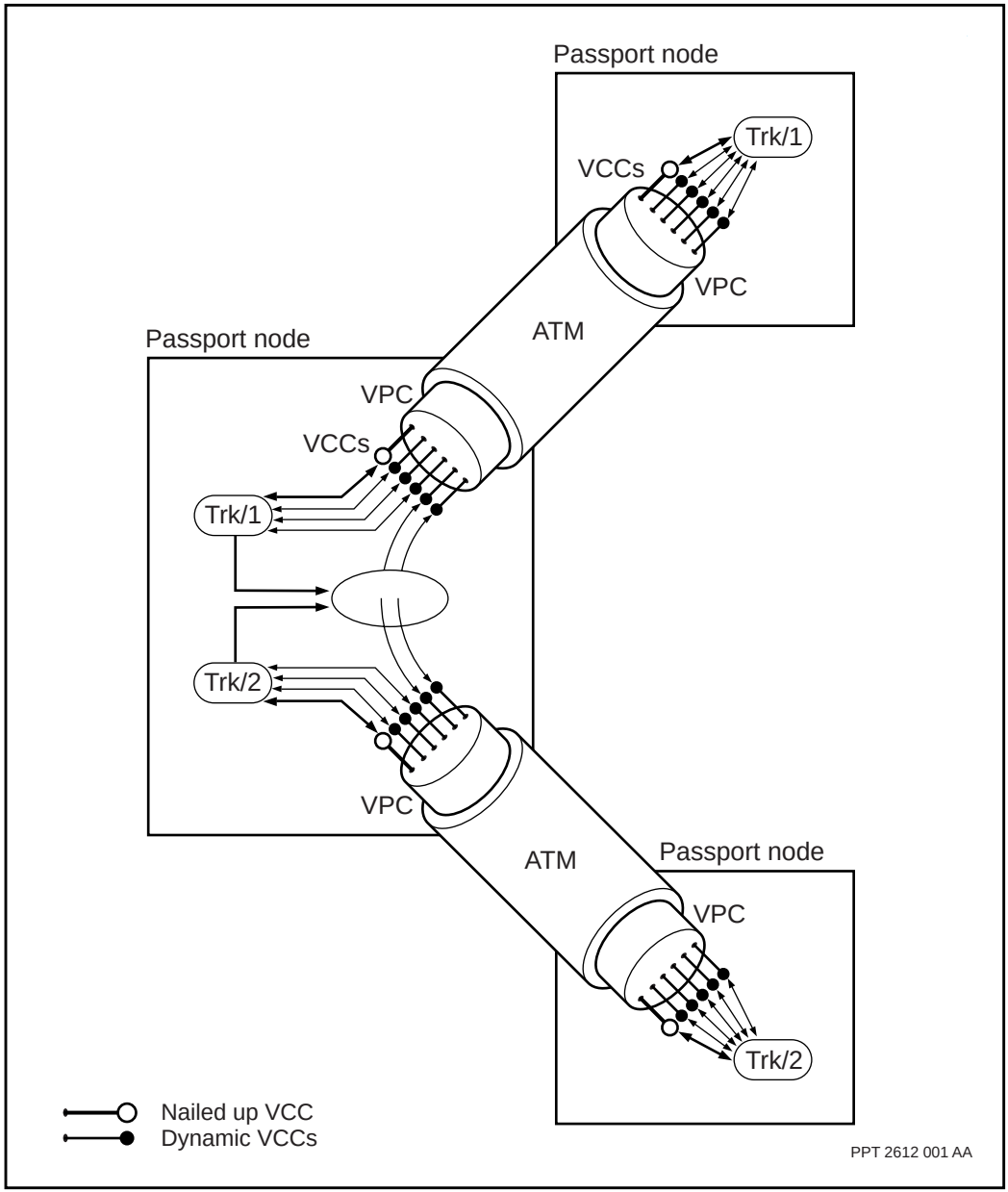
When a PORS path tandems through a Passport node the PORS path administrator creates logical ATM relay points on the VCCs and connects them together for the duration of the time the path is up. These connections share the available connection address space with ATM SVCs, SPVCs and PVCs. This allows the PORS traffic to use ATM cell forwarding at the tandem Passport nodes.

> ***Note:*** In order for PORS connections to establish on map mode trunks, the value of the *connectionPoolCapacity* attribute, under the *Lp Eng Arc Ov* component, must be set to a positive value. For details, see the Resource Management chapter of 241-5701-710 *Passport 7400, 15000, 20000 ATM Configuration Guide*.

DPRS and control traffic must use CPU forwarding at the tandem sites. This is because the traffic is multiplexed onto a single ATM VCC and the CPU is required to demultiplex it and make forwarding decisions.

All the map VCCs are created in the same VPC where the AAL5-mux ATM VCC is defined.

Figure 29
Map mode



Map mode introduces three new kinds of mapping:

- AAL5-map
- AALSPO-map
- cell-map

The following sections detail map mode:

- "Role of the path administrator in map mode" (page 170)
- "Selecting the map mode type" (page 170)

Role of the path administrator in map mode

You can use all three kinds of mapping at the same time under the same *Pa* component depending on the circumstances at call setup. When provisioned for map mode, the *Pa* component maps all calls to individual VCCs. In this mode, the provisioned Passport trunk over ATM AAL5 VCC only carries PORS and other routing control traffic and never PORS data.

Selecting the map mode type

The selection of the map mode depends on the following:

- voice or BTDS, or other application
- to what type of link or service you are forwarding data

A voice or BTDS service triggers the use of AALSPO-map at all frame or cell boundaries along the path (that is, everywhere that conversions from frame to cell are necessary such as endpoints or tandem hops from or to frame-based FPs). Other services trigger the use of AAL5-map at all frame or cell boundaries along the path.

At cell-to-cell boundaries along the path, pure cell mapping occurs regardless of the MTU. It is the use of cell relay at tandem points that reduces the end-to-end delay since segmentation and reassembly does not occur at these tandem points.

> ***Note:*** Cell relay is only possible to another *Pa* component in mapped mode. Otherwise, cell or frame conversions occur by hardware at this boundary using the appropriate AAL5-map or AALSPO-map protocol.

PORS traffic mapping to internal discard and emission priority

In map mode, PORS can specify the traffic mapping for traffic on mapped ATM VCCs. The PORS PLC emission and discard priority provisionable attributes specify the ATM QoS for these ATM VCCs.

Traffic mapping depends on the traffic flow direction (from the link or toward the link) and the traffic type (frame or cell relay traffic). This section describes the following information:

- “Receive mapping—cell relay” (page 171)
- “Receive mapping—frame” (page 172)
- “Transmit mapping—cell relay” (page 173)
- “Transmit mapping—frame” (page 174)

Receive mapping—cell relay

For traffic received from an ATM link, the cell loss priority (CLP) value from the ATM cell header and the PORS PLC discard priority for the connection determine the internal discard priorities of each cell. Once the FP receives a cell from the link, it compares the cell's internal discard priority with the memory congestion state. If the discard priority is greater than the memory congestion status, the FP discards the cell. If the discard priority is less than the memory congestion status, the FP allocates memory for the cell. See Table 11, “Receive mapping: queue selections based on mapping conversions,” (page 172), for a summary of mapping queue selections.

Next, the cell joins the appropriate bus queue. Before queueing the cell, the FP compares the cell's internal discard priority value with the bus congestion state. The FP discards the cell if its discard priority value is greater than the bus congestion state. The PLC emission priority determines the bus emission priority. See Table 12, “Receive mapping: PORS PLC emission priority to bus emission priority,” (page 172), for a summary of the receive mapping to bus emission priority.

Table 11
Receive mapping: queue selections based on mapping conversions

Mapping mode	Queue
AAL5-map to AAL5-mux	bus
AAL5-map to frame	bus
AAL5-map to AALSPO-mux	processor
AALSPO-map to AAL5-mux	bus
AALSPO-map to frame	bus
AALSPO-map to AALSPO-mux	processor

Table 12
Receive mapping: PORS PLC emission priority to bus emission priority

PLC emission priority	Bus emission priority
0	high
1	normal
2	normal

Receive mapping—frame

For traffic received from an ATM link, the CLP value from the ATM cell header and the PLC discard priority (of the service associated with the ATM VCC) determine the internal discard priorities of each cell.

As with receive mapping for cell relay, once the FP receives a cell from the link, it compares the cell's internal discard priority with the value for the memory congestion state. If the discard priority is greater than the memory congestion status, the FP discards the cell along with any other cells belonging to the same frame.

Once the frame has been reassembled from ATM cells, the frame can directly join a processor queue or a bus queue. See Table 11, “Receive mapping: queue selections based on mapping conversions,” (page 172), for a summary of mapping queue selections.

The transporting cell's CLP and the PLC discard priority determine the frame's discard priority. Before queuing the frame, the FP compares the frame's internal discard priority value with the processor or bus congestion state depending on which destination queue is selected. The FP discards the frame if its discard priority is greater than the queue's congestion state.

See Table 13, “Receive mapping: PLC discard priority and CLP to (internal) discard priority,” (page 173), for a summary of receive mapping to internal discard priorities. For AAL5, the frame CLP (internal) is set to 1 if the CLP in any of the constituent ATM cells is equal to 1.

Table 13
Receive mapping: PLC discard priority and CLP to (internal) discard priority

PLC discard priority	CLP	Discard priority
0	0	internal control (0)
1	0	very important (1)
	1	least important (3)
2	0	important (2)
	1	least important (3)
3	0	least important (3)
	1	least important (3)

Transmit mapping—cell relay

For ATM cell relay traffic, the cell's CLP and the PLC discard priority determines the discard priority. See Table 14, “Transmit mapping: PLC discard priority and CLP to (internal) discard priority,” (page 174). The discard policy uses the discard priority when the cell demands resources that are congested (such as, link and memory).

The CLP value is the same for ATM cell relay traffic in the transmit direction.

For transmitted cells, the emission priority selects one of the three link emission priority queues. The PORS PLC emission priority determines the emission priority. See Table 15, “Transmit mapping: PORS PLC emission priority to link emission priority,” (page 174), for a summary.

Table 14
Transmit mapping: PLC discard priority and CLP to (internal) discard priority

PLC discard priority	CLP	Discard priority
0	0	internal control (0)
1	0	very important (1)
	1	least important (3)
2	0	important (2)
	1	least important (3)
3	0	least important (3)
	1	least important (3)

Table 15
Transmit mapping: PORS PLC emission priority to link emission priority

PLC emission priority	Link emission priority
0	high
1	medium
2	low

Transmit mapping—frame

For frames in the transmit direction, the emission priority selects one of the three link emission transmit priority queues. The PORS PLC emission priority attribute, as provisioned for the service associated with the ATM connection to which the frame is forwarded for processing, determines the emission priority. See Table 15, “Transmit mapping: PORS PLC emission priority to link emission priority,” (page 174), for a summary of transmit mapping.

The internal discard priority is already set when the FP receives the frame from the bus. The discard policy uses the internal discard priority when demand for the resources (link and memory) exceeds capacity. The frame's priority determines the internal discard priority. The discard priority of the frame determines the CLP value of the cells comprising the AAL5 frame. See Table 16, “Transmit mapping: discard priority to CLP (for AAL5 frames),” (page 175), for a summary of the discard priority to CLP.

Table 16
Transmit mapping: discard priority to CLP (for AAL5 frames)

Discard priority	CLP
0	0
1	0
2	0
3	1

PORS ATM efficiency migration strategy

You do not have to provision both ends of the trunk simultaneously since the PORS ATM efficiency feature reverts back to routing over the AAL5 VCC unless both ends are properly provisioned. The *Pa* component detects the difference in provisioning and issues the following warning message:

```
MSG warning operator configurationError 7018009

Com: my atmConnection is not responding or is not
connected to same peer PA as my parent trunk’s
atmConnection.

Calls requesting it will default to AAL5 over parent
trunk.
```

It then defaults back to its original behavior until you provision the far-end *Pa* component to use this feature.

If the neighbor *Pa* component is running the proper version of software, it also detects that its peer wants to perform SPO-mux mode routing. If it has not been provisioned for this feature yet, it issues the following warning message and reverts to the default behavior, just like its peer:

```
MSG warning operator configurationError 70180010

Com: Neighbor not provisioned for mapped mode routing
but I am.

Calls requesting it will default to AAL5 over parent
trunk.
```

There is a shorter trunk outage if you reprovision both ends simultaneously.

PORS ATM efficiency impacts

The PORS ATM efficiency feature has no impacts on existing Passport features and there is no difference in voice quality.

There are performance costs associated with running a network where some nodes support the PORS ATM efficiency feature and some do not.

If any nodes along the path are not provisioned with the PORS ATM efficiency feature, the routing system has to disable the feature on the nodes which have this feature provisioned. This disabling process causes additional overhead activity on the routing system. In order to avoid this scenario, all nodes along the path must have the feature provisioned.

PORS ATM efficiency engineering guidelines

The ATM FP (regardless of interface type) can run at a particular sustained rate (packet/s). At the sustained rate, CPU utilization is close to 100%. The Passport FPs must be subjected to less than 90% sustained CPU utilization, including short bursts of up to 90% in either direction (on the order of several seconds). Sustained bursts results in data loss and possibly control frame loss on the FP. This loss causes an FP's trunk to oscillate up and down every few minutes.

Operating outside of these guidelines can result in the loss of small amounts of data whenever control traffic is present. For example, the voice service can experience clicks and pops when you issue display commands on an overly busy FP.

Note: The ATM bearer services do not require CPU intervention for forwarding on ATM FPs. This CPU utilization limit applies only to PORS or connectionless packets requiring CPU intervention for forwarding.

PORS ATM efficiency bandwidth guidelines

You require the AAL5-mux VCC's bandwidth and the reserved PORS bandwidth to determine the amount of available PORS bandwidth for the SPO-mux mode trunk. The defined PCR for the Passport trunk determines the AAL5-mux VCC bandwidth. The PA uses the calculated PORS bandwidth to decide if a connection may or may not be admitted. The PA never looks at the SPO-mux VCC's bandwidth for this decision.

From a routing perspective, all bandwidth must be represented by a single number for a given PA. This requires special consideration when you decide how to allocate bandwidth to the SPO-mux VCC. Here are some bandwidth strategies for various scenarios (see Figure 30, "ATM efficiency bandwidth guidelines," (page 178)):

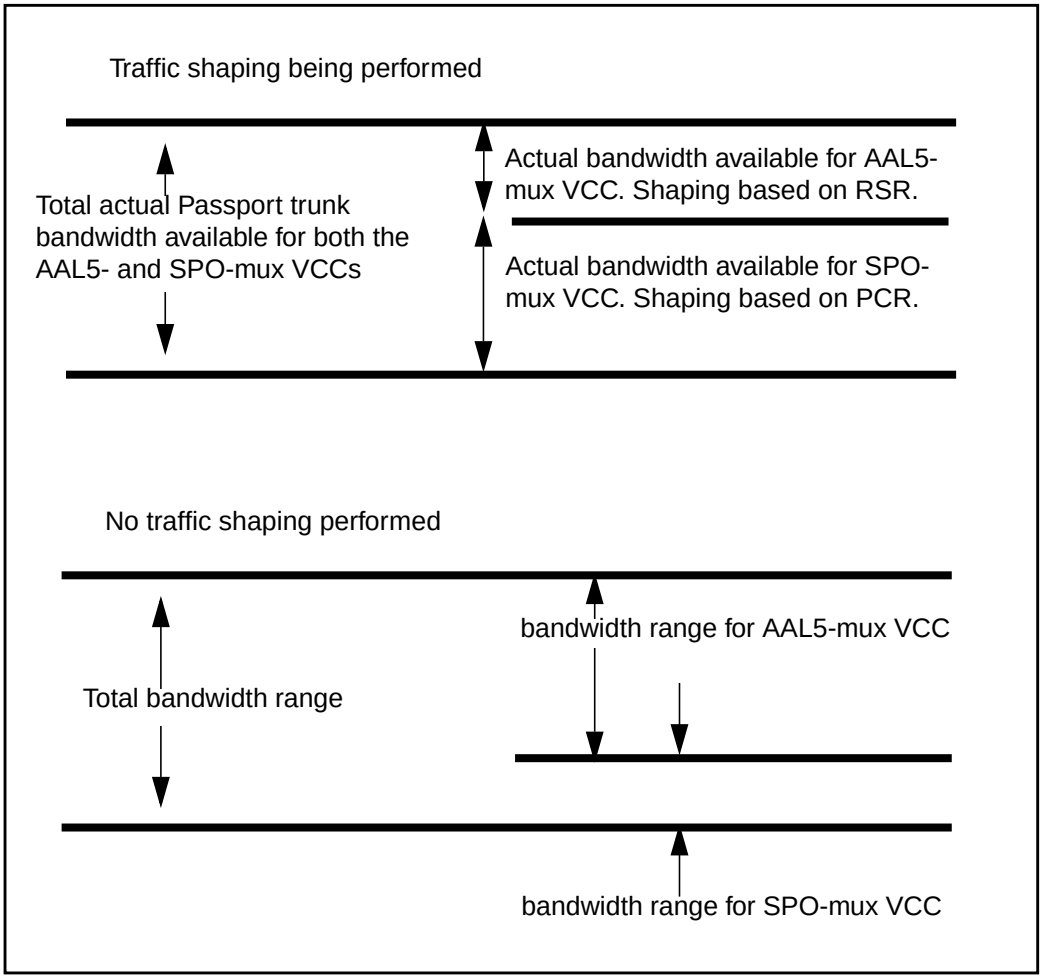
- Shaping of AAL5-mux and SPO-mux VCCs

  When you set up policing for the Passport trunk over ATM VCCs, you must also shape the individual VCCs. For the AAL5-mux VCC, the PCR value must consider the total reservable bandwidth requirements for PORS and DPRS traffic. The requested shaping rate and the amount of traffic that will be carried over this connection determines the AAL5-mux VCC shaping rate. Typically the total Passport trunk bandwidth minus the PCR of the SPO-mux is the AAL5-mux VCC shaping rate. The SPO-mux VCC shaping rate must consider the sum of the PORS traffic that will be carried by this connection.

- No policing or shaping of AAL5-mux and SPO-mux VCCs

  For the SPO-mux VCC, assign the PCR value to 0 cell/s or another low value. Assign the PCR of the AAL5-mux VCC to account for all remaining Passport trunk bandwidth. This approach avoids over reserving connection bandwidth from the ATM bandwidth pool.

Figure 30
ATM efficiency bandwidth guidelines



PORS ATM efficiency recommendations

Use the following guidelines to set up the PORS ATM efficiency feature:

- Set up the bandwidth for the two VCCs as outlined in “PORS ATM efficiency bandwidth guidelines” (page 177).

- Set the *endToEndloopback* attribute to on. This setting provides a software continuity check to ensure that the VCC that is linked to the *Pa* component is connected to its proper destination. See “Provisioning map mode” (page 58).
- Provision the feature on all the nodes along the path. See “PORS ATM efficiency impacts” (page 176) for more information.

PORS ATM efficiency known limitations

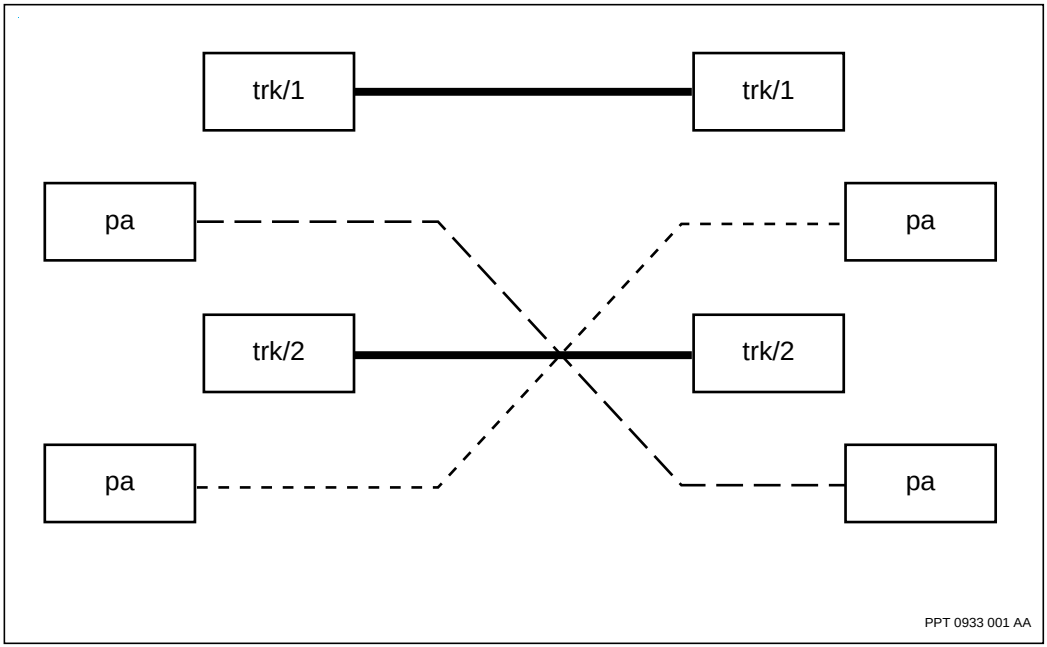
The following sections describe the limitations of this feature:

When a PA VCC is not connected to the same place as Passport trunk VCC

If the VCC that is linked to the PA is not connected to the proper destination, there is no detection or alarm for this situation and circuits fail to operate. In Figure 31, “Trunks (trk/1 and trk/2) with cross-connected PAs,” (page 180), two trunks PAs are accidently cross-connected. The calls complete but do not carry data. In addition, queries to the logical channel (LC) of a voice service which uses the PA’s VCC results in time-outs in the round trip delay that causes the call to be torn down and re-established over the same facility. Until integrity and connectivity checks are available on the second circuit, careful engineering is necessary to avoid this problem.

Route the PA’s VCC and the Passport trunk’s VCC identically whenever possible to avoid this limitation.

Figure 31
Trunks (trk/1 and trk/2) with cross-connected PAs



PA VCC must be provisioned for endToEndLoopback

The only continuity check made on the PA's VCC is by the VCC itself using the endToEndLoopback option of the VCD. While this software detects a break in the VCC, it takes over 30 seconds which for most voice calls is too long. The trunk's VCC has internal software that detects a break in approximately six seconds. There is no equivalent software in the PA which can do continuity checks with higher precision. For this reason, it is best to route the trunk's VCC and the PA's VCC over the same physical facilities whenever possible. This solution ensures that a breach to one breaches the other and that continuity problems on the PA's VCC do not go undetected for too long. It is also best to share the physical resources for the two VCCs for bandwidth sharing reasons. See "When a PA VCC is not connected to the same place as Passport trunk VCC" (page 179).

No integrity checking on voice calls

There is no room in the voice packets for LRC or CRC bytes. A voice packet can be corrupted when it traverses an ATM link without being detected. For the voice service, you can get a corrupt sample instead of a completely missing cell.

Allocating static VCCs over dynamic VCCs

When PORS dynamically uses a VCC with this feature, it reserves the VCC as a PORS VCC. When you provision a static VCC in this space, it does not come up since it is an invalid VCC. When PORS is done with the VCC, it releases the VCC. The static VCC does not come up until activation of the AtmIf takes place. (When PORS releases the connection, the ATM software does not check for the released VCC.) At present, the only way for ATM software to realize that the connection has been released, is to activate a provisioning change on the *AtmIf* component.

To avoid this limitation, do not provision static VCCs over dynamic VCCs.

Passport 7400 series switch BTDS efficiency

You can provision BTDS to optimize bandwidth on Passport trunks over ATM for Passport 7400 series switches. You can provision the larger cell size to take advantage of the AAL5 transport mode on FPs that support AAL5, or the smaller cell size for the SPO-mux mode. A larger BTDS cell size provides the following benefits:

- increased BTDS throughput
- efficient transportation across frame-cell trunks and Passport trunks over ATM

The smaller cell size provides the benefits of SPO-mux mode.

For details on the BTDS efficiency feature, see 241-7401-775 *Passport 7400 Bit Transparent Data Service Guide*. For information on which FPs support AAL5, refer to 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Spared Passport 15000 and 20000 Trunks over ATM

Passport 15000 or 20000 trunks over ATM can be provisioned on a spared LP as warm standby features. A warm standby application or feature can operate together with a hot standby application or feature on the same FP without affecting the ability of the hot standby application or feature to provide hitless services. See 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide* for a description of hitless services and hot, warm and cold standby applications and features.

Although Passport trunks over ATM can be provisioned as warm standby features, DPRS and PORS routing is interrupted during an equipment switchover. DPRS and PORS routing becomes available after:

- the switchover to the standby FP is complete
- Passport trunks over ATM are re-established

Passport 7400, 15000, 20000
Trunking Guide

Release 5.2

Publication: 241-5701-420
Document status: Standard
Document version: 5.2S1
Document date: November 2003
Printed in Canada

NORTEL NETWORKS