NORTEL NETWORKS

Passport 7400, 15000, 20000

Overview

241-5701-030

Passport 7400, 15000, 20000

Overview

Publication: 241-5701-030
Document status: Standard
Document version: 5.2S2
Document date: March 2004

Publication history

March 2004

5.2S2 Standard
General availability. Contains information on Passport 7400, Passport 15000, and Passport 20000 for the PCR5.2 release.

Contents

Chapter 6
Passport services 117

List of figures

List of tables

Chapter 1
Passport introduction

Passport is a carrier-grade, integrated, toll-quality voice, data gateway and network product.

Passport delivers a powerful range of standard-based interfaces and services, including frame relay, ATM, and IP. Passport provides multiprotocol routing services, intelligent traffic management, and simultaneously supports voice, data, and video traffic.

Passport networks are scalable: networks scale easily from a few nodes to thousands of nodes. Passport redundancy and sparing capabilities mean that Passport provides the high reliability and redundancy required by today's networks.

Passport can simultaneously support multiple services using both frame and cell switching, and provides multimedia solutions from the backbone to the access layer.

Passport provides the high reliability and redundancy required by today's networks by supporting:

- a variety of equipment sparing schemes for electrical and optical interfaces
- SONET or SDH line automatic protection switching (APS)
- a means for upgrading switch software without interrupting some services being provided by the switch

- service software that can run uninterrupted, even when the hardware providing the service changes

Passport models

Passport offers a selection of products with different cost structures, scalability and functionality. You can choose the Passport platform with the services you require while managing your cost effectiveness and growth potential.

Passport hardware and software are modular. You can tailor the hardware and software components to meet the requirements of each site and to evolve to future technologies.

See the following sections for more information on the Passport models that are available:

- "Passport 7400 introduction" (page 16)
- "Passport 15000 introduction" (page 17)
- "Passport 15000-VSS introduction" (page 17)
- "Passport 20000 introduction" (page 18)

Passport 7400 introduction

The Passport 7400 series includes Passport 7420, Passport 7440, and Passport 7480.

Passport 7420 is a 3-slot Passport switch. It is ideal for branch or regional sites as a network consolidator device or tandem switch that feeds other sites. The Passport 7420 is also used for aggregation and switching traffic in radio access networks.

Passport 7440 is a 5-slot Passport switch. Like the 3-slot Passport it is ideal for branch or regional sites as a network consolidator device or tandem switch. In addition it offers the additional slot space for greater traffic capacity or hardware redundancy. This switch can also handle backbone applications in sites that do not require the high fanout of the 16-slot switch making it a cost-effective choice for service providers at smaller sites.

Passport 7480 is a 16-slot Passport switch that provides superior reliability and redundancy required by service providers. The 16-slot Passport switch offers two load-sharing buses and support for redundant power supplies. Passport processor cards also support sparing. Therefore, even in the unlikely event of a failure, Passport continues to deliver service.

Passport 7400 offers a full range of data services and enables customers to use a single ATM access link to transport voice, video, and data. Statistical multiplexing, voice compression, and silence and fax idle suppression techniques maximize bandwidth savings. Echo cancellation, comfort noise generation, and congestion handling techniques ensure that the Passport 7400 voice services deliver toll quality services.

Passport 15000 introduction

Passport 15000 is a multiservice ATM-based data switch that can be deployed as a backbone for existing Passport edge switch networks or as a service provider ATM backbone switch. In addition to ATM, it delivers a powerful range of standards-based interfaces and services, including frame relay and IP. Passport 15000 provides multiprotocol routing services, intelligent traffic management, and simultaneously supports voice, data, video and image traffic. It offers full redundancy, scalable high capacity, high-speed access and trunking, and optional SONET or SDH integration.

Passport 15000-VSS introduction

Passport 15000-Variable Speed Switch (VSS) is a combined edge (Passport 7480) and core (Passport 15000) multi-service switch. Passport 15000-VSS offers low-speed accessibility at the edge of a network and high speed switching at the core of a network.

In addition to ATM, Passport 15000-VSS delivers a wide range of standard-based high-speed interfaces and services, including frame relay, circuit emulation, voice, and Internet protocol (IP). These interfaces provide a wide variety of access and trunking speeds from channelized DS0 to OC-48.

Passport 15000-VSS provides high density scalability that includes

- more than 43,000 DS0’s in a network equipment building system (NEBS) frame compliant footprint
- high throughput, beyond 43 Gbit/s

The Passport 15000-VSS is DC powered. An external AC power rectifier provides power for AC requirements.

Passport 20000 introduction

The Passport 20000 Multiservice Switch is added to the Passport family of switches. It provides the same functionality and services as a Passport 15000 except for significant hardware improvements, especially with higher shelf (user) capacity.

The Passport 20000 can re-deploy FPs that were previously loaded with Passport Carrier Release (PCR) software 2.3 or later, and re-deploy CP3s with PCR 3.1 or later software provided the cards are migrated to the current PCR of the switch.

Passport century compliance

Passport switches are Century Compliant. “Century Compliant” or “Century Compliance” means that the product functions without any material, service-affecting non-conformance to the applicable Nortel Networks product specifications with respect to the operations performed by such product which are date dependent, provided that the identified baseline software and requisite hardware are installed, and the use conforms to the associated documentation. The statement that a product is Century Compliant should not be interpreted as a commitment to support such a product beyond its committed support window.

Chapter 2
Passport hardware

The basic hardware structure of Passport consists of a mounting apparatus, the shelf assembly, power components and the cards that plug into the shelf to provide functionality.

The Passport 7400 series of switches are physically different and do not share hardware with the Passport 15000 and Passport 20000 switches. See the following sections for more information about Passport hardware:

- “Passport 7400 hardware” (page 20)
- “Passport 15000 hardware” (page 25)
- “Passport 15000-VSS hardware” (page 28)
- “Passport 20000 hardware” (page 31)

Control processors and function processors have the same role on all Passport switches. The cards and modules that are intended to be used on Passport 15000 or Passport 20000 are physically different than the cards available for Passport 7400.

For more information on control processors, function processors and their uses see:

- “Passport control processors” (page 33)
- “Passport function processors” (page 33)

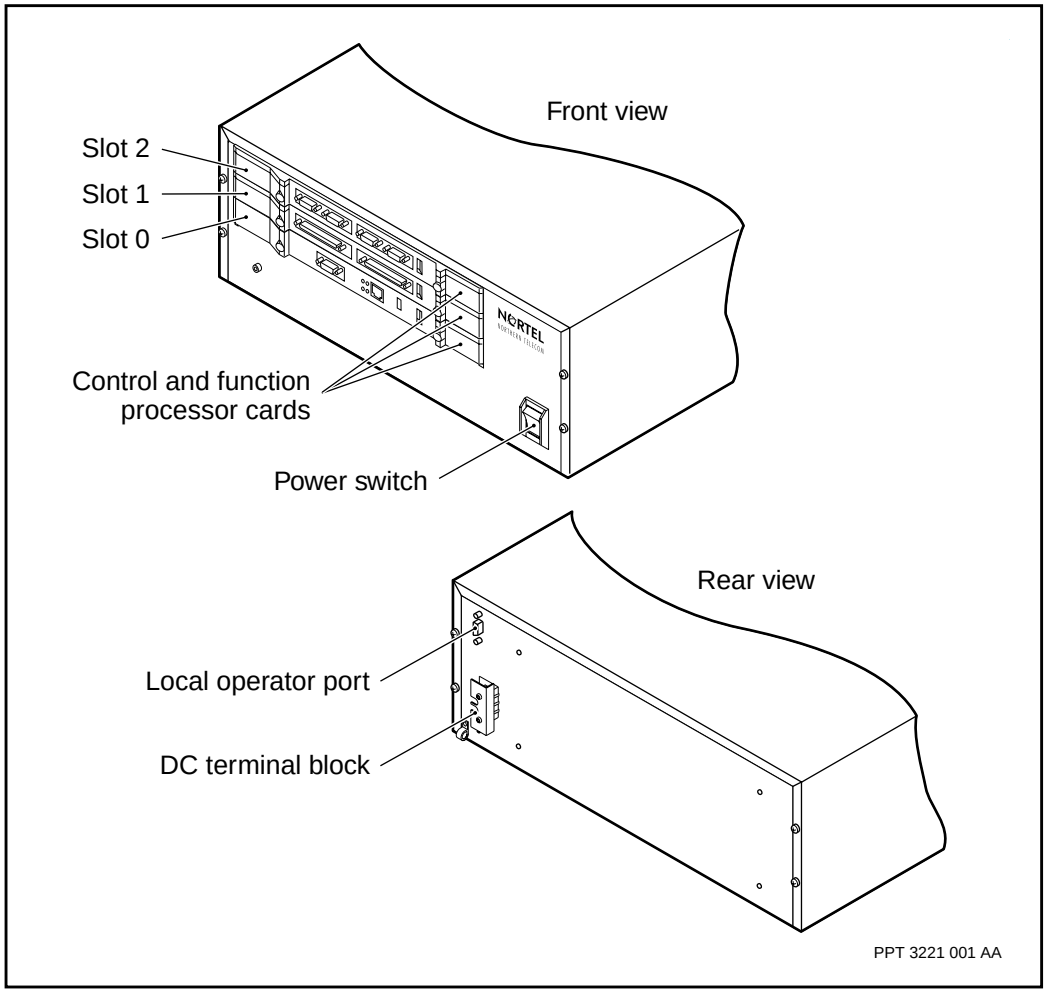
Passport 7400 hardware

The Passport 7400 switch is available in three models: See “Passport 7420 hardware” (page 21),“Passport 7440 hardware” (page 22) and “Passport 7480 hardware” (page 23). Each model supports Passport 7400 software applications and function processors (FPs).

Passport 7420 hardware

The 3-slot Passport 7400 switch supports a maximum of three processor cards: two FPs and one CP. For a detailed view, see the figure “3-slot Passport switch” (page 21). The Passport 7420 can be mounted as a stand alone unit either on a desk-top (horizontally) or on the floor (vertically). You can also install the Passport 7420 in a cabinet or standard 19” rack.

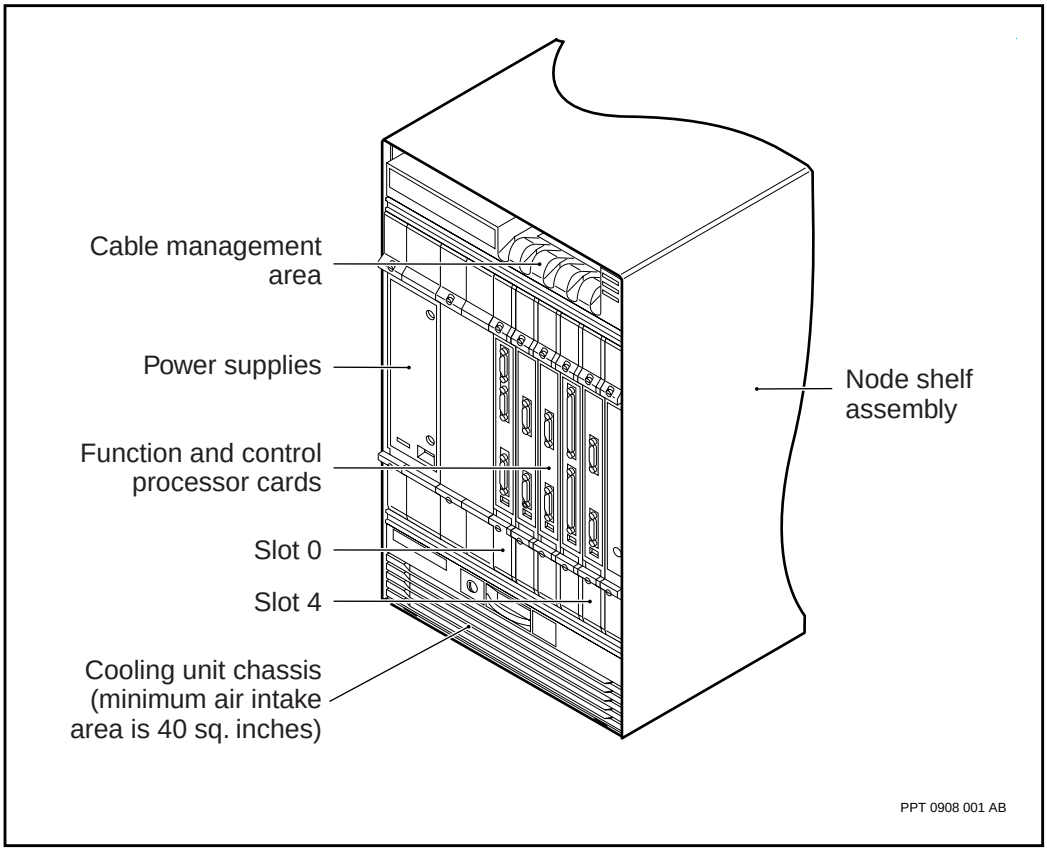
Figure 1
3-slot Passport switch



Passport 7440 hardware

The 5-slot Passport 7400 switch supports a maximum of five processor cards: four FPs and one CP. For a detailed view, see the figure “5-slot Passport 7440” (page 22). You can install the Passport 7440 on the floor as a stand-alone unit. You can also install this switch in a Passport cabinet or a 19-inch standard rack. A 19-inch rack holds a maximum of six 5-slot switches.

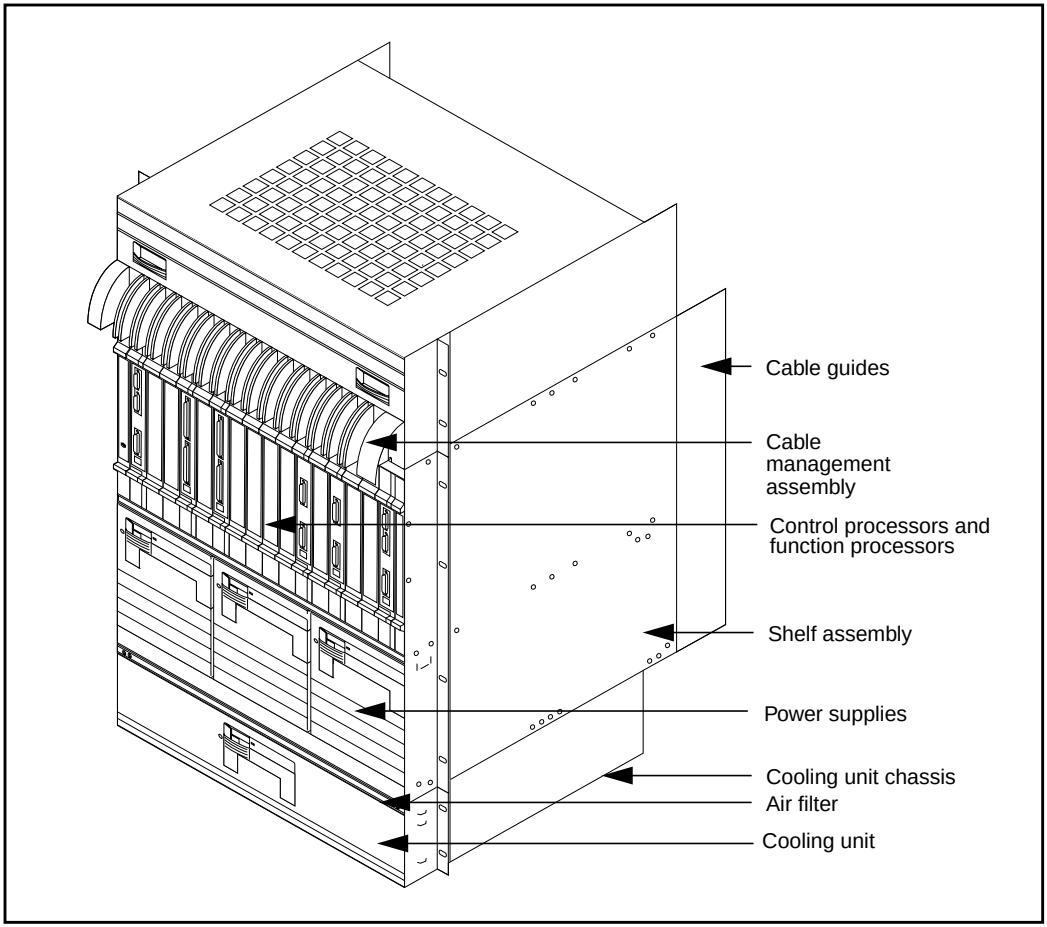
Figure 2
5-slot Passport 7440



Passport 7480 hardware

The 16-slot Passport 7400 switch supports a maximum of 16 processor cards: a CP with 14 function processors and a spare CP (or 15 FPs without a spare CP). For a detailed view, see the figure "16-slot Passport 7480" (page 23). You can install the Passport 7480 in a Passport or Passport seismic cabinet, or in a standard 19-inch rack. A standard 19-inch rack can hold two switches, or one switch and its related termination panels.

Figure 3
16-slot Passport 7480



For more information about Passport 7400 switch hardware, see the following documents:

- 241-7401-200 *Passport 7400 Hardware Description*
- 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*
- 241-7401-242 *Passport 7400 FP Cabling Specifications*

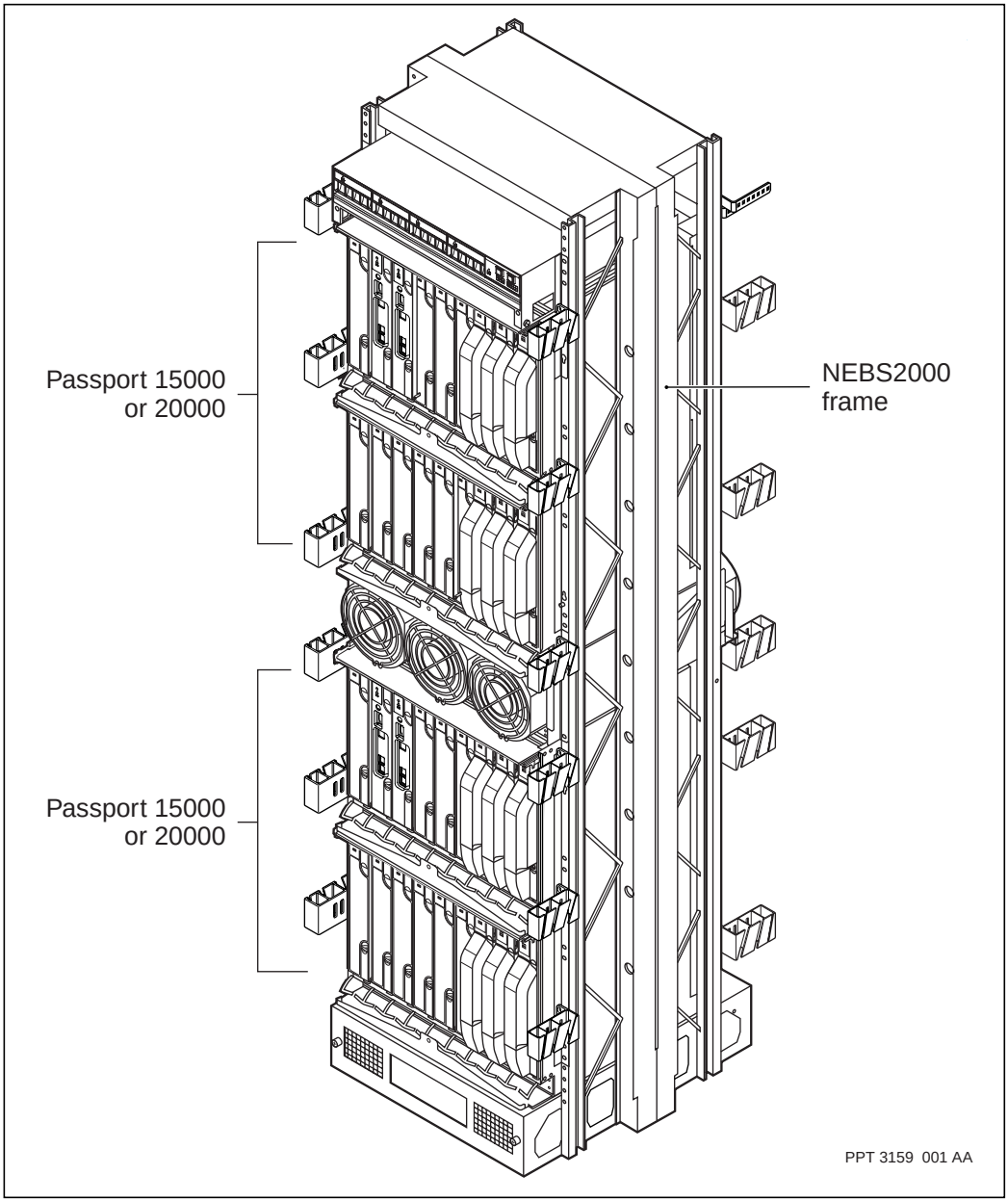
Passport 15000 hardware

The Passport 15000 is installed in a frame that can hold two independent switches. Each 18-slot Passport 15000 switch supports a maximum of 16 processor cards.

- slot 0 is dedicated for the primary control processor (CP) card
- fourteen slots are dedicated for function processor (FP) cards that are connected to fabric cards
- slot 1 is used for a redundant CP card or an FP when running non-redundantly
- two slots are reserved for future use

The two fabric cards interconnect the processor cards. Each processor card has redundant serial links to the two fabric cards.

Figure 4
Two Passport 15000 shelves in a NEBS 2000 frame



For more information about Passport 15000 switch hardware and the services they support, see the following documents:

- 241-1501-200 *Passport 15000, 20000 Hardware Description*
- 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade*

Passport 15000-VSS hardware

You install the Passport 15000-VSS switch in a network equipment building system (NEBS) frame that holds two independent switches: Passport 7480 in the upper part and Passport 15000 in the lower part of the frame. For a detailed view of Passport 15000-VSS, see “Passport 15000-VSS” (page 29).

Figure 5
Passport 15000-VSS

PPT 2912 001 AA

For more information about Passport 15000-VSS hardware see

- “Passport 7480 hardware” (page 23)
- “Passport 15000 hardware” (page 25)

You can connect Passport 7480 and Passport 15000 through an OC-3 FP on each node using a single-mode or multi-mode fibre cable. For more information about Passport 15000-VSS FP cards see, “Passport function processors” (page 33). For information on connecting the Passport 7480 and Passport 15000 nodes in Passport 15000-VSS, see 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade*.

A separate cabinet is required to house the Passport 15000-VSS sparing panels. See 241-1501-205 *Passport 15000, 20000 Site Requirements and Preparation Guide* for more information about the sparing panel requirements.

For information about

- preparing the site for Passport 15000-VSS installation, see 241-1501-205 *Passport 15000, 20000 Site Requirements and Preparation Guide*.
- installing and maintaining Passport 15000-VSS, see 241-1501-240 *Passport 15000, 20000 Hardware Installation, Maintenance and Upgrade*.

Passport 20000 hardware

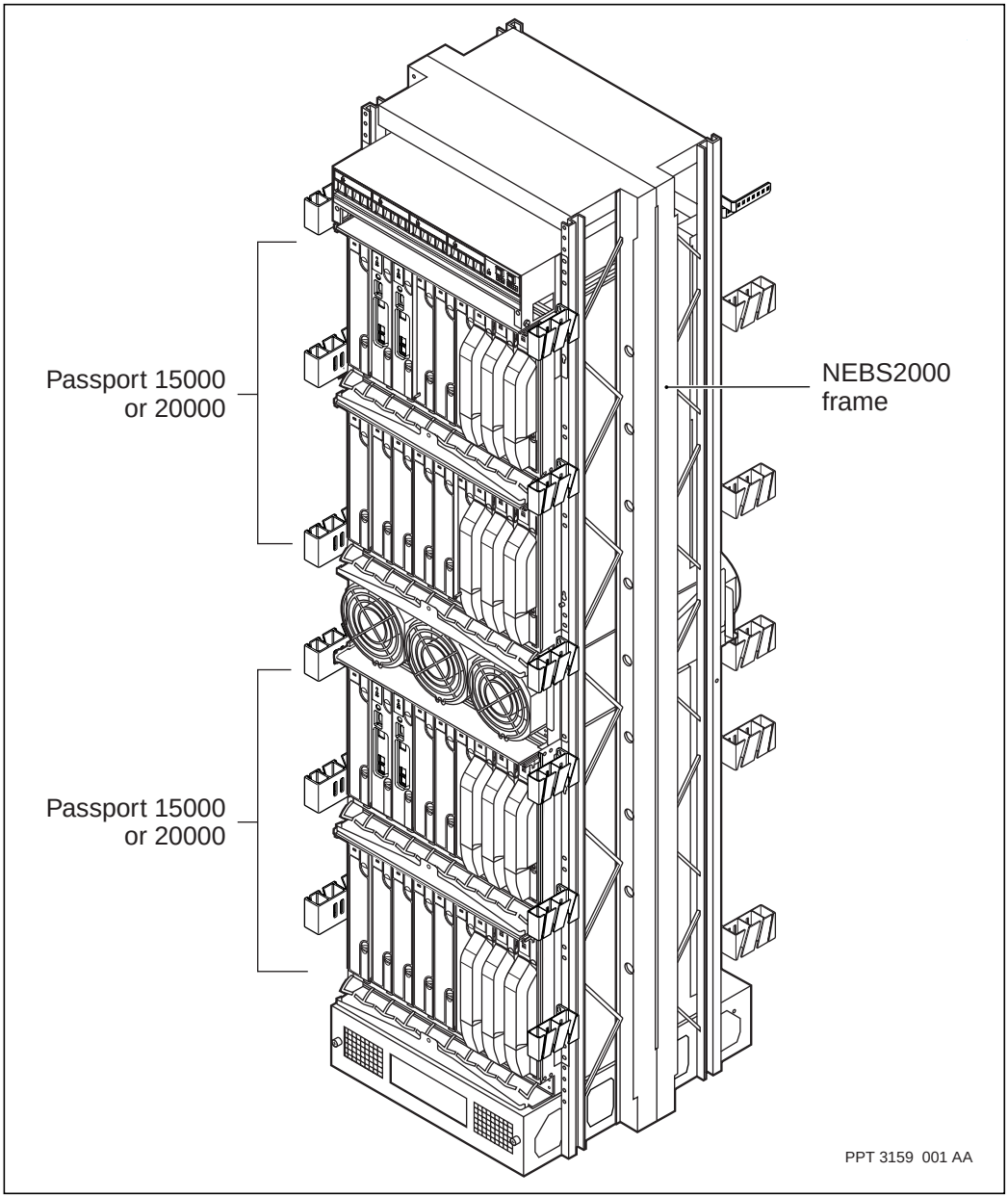
The Passport 20000 shares much of the hardware of a Passport 15000, including the methods of installing one in a rack or two in a NEBS 2000 frame. The breaker interface panel (BIP) is the same power distribution unit except the Passport 20000 version has 25 A breakers instead of 20 A. The power input feeds remain the same, however, a Passport 20000 and a Passport 15000 cannot be powered from the same BIP in the same frame.

The plug-in modules and fabrics at the rear of the Passport 20000 are redesigned for improved capacity, performance, or usability. The backplane is designed to accommodate fabrics of different capacities and is scalable to 160 Gbits/s. The initial 112 Gbits/s fabrics continue to load-balance and load-share with 70 Gbits/s of shelf (user) capacity so that either fabric can take over the load of its mate and FP traffic is maintained.

The shelf assembly of the Passport 20000 is designed to ship cards in place. This means that the control processor (CP3), function processor (FP), and fabric cards can be pre-loaded with software, placed in pre-determined slots (including filler cards), and shipped safely in a partially seated transportation position. Shipping in place means the cards can be powered up as soon as they are seated.

Information about the Passport 20000 hardware (and software) is the same as a Passport 15000 unless otherwise specified. From the rear, the look of the plug-in modules and fabrics has changed. From the front, a Passport 20000 looks very much like a Passport 15000.

Figure 6
Two Passport 20000 switches in a NEBS 2000 frame



For more information about the hardware of a Passport 20000, see 241-1501-200 *Passport 15000, 20000 Hardware Description*.

Passport control processors

The control processor (CP) card controls overall processing in the switch. Some of the basic functions it performs are booting the switch, collecting and maintaining shelf inventory and statistical data, as well as maintaining routing tables.

The card contains a standard core computing engine with a disk drive, as well as circuits to provide a Stratum-3 timing reference, the external clock synchronization interfaces (DS1/E1), and operation access ports (Ethernet, RS-232 interfaces).

The CP can operate in redundant mode. In redundant mode, two CPs must be installed. These two CPs contain duplicated information and are connected with redundant links. While one CP operates as the active card, the second card operates in warm standby mode to provide high availability. If the active CP should fail, the standby CP automatically takes over.

For more information on control processors see 241-7401-200 *Passport 7400 Hardware Description* or 241-1501-200 *Passport 15000, 20000 Hardware Description*.

Passport function processors

Function processors (FP) provide interface ports that connect network communications facilities to Passport switches. FPs support and execute real-time processes that enable service delivery.

The function of the FP is determined by the type of electrical or optical interface on the card, as well as the software running on the processor. Each type of interface provides circuitry and faceplate connectors specific to its function.

Some electrical FPs must be provided with special interface cables and a separate fanout panel in cases where there is insufficient faceplate area for standard connectors, or where FP sparing is required. Specific FP types are available for Passport to support specific link interfaces.

Many FPs use termination panels and support 1:1 sparing. Electrical FPs that support sparing require a sparing panel. Some optical FPs can support sparing without the use of a termination panel. Some termination panels also break out the ports of the FP so that each port has an access and termination point for customer equipment connections.

Each FP supports one or more services. For more information about Passport FPs and the services they support see 241-1501-200 *Passport 15000, 20000 Hardware Description*, 241-7401-200 *Passport 7400 Hardware Description*, or 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

Chapter 3
Passport software infrastructure

Passport software has five main classes: base, networking, trunking, access services, and packet voice gateway.

The base software provides basic system functions that support the remaining software. Base software functions include software management, command processing, file storage, data collection, port management, and network management interfaces. For more information, see “Passport base software” (page 35).

Networking software provides capabilities for forwarding a packet of information from its source to its destination. Networking software includes routing and congestion management functions. For more information, see “Passport networking software” (page 40).

Trunking software provides the capabilities for interconnecting Passport nodes. For more information, see “Trunking software” (page 49).

Access service software provides the communication functions of Passport such as frame relay, ATM and internet protocol (IP). See “Passport services” (page 117) for more information about the services supported on Passport.

Passport base software

The Passport base software system functions include command processing, shelf management, file storage, data collection, and network management interfaces. See the following sections for more information:

- “Command processing” (page 36)

Command processing

The base software controls and processes commands and enables you to configure the node. Components provide the infrastructure through which network operators and administrators interact with Passport. Components represent the hardware, software, and services on a Passport node. To modify a node's configuration, you change the value of component attributes. You can do this directly by entering commands in the text interface, or indirectly by using a network management device.

For more information about components, see 241-5701-060 *Passport 7400, 15000, 20000 Components*.

Data collection

The Passport data collection system (DCS) is the part of the base software that collects data for troubleshooting, performance tuning, and billing. For analyzing this data, it is transferred to the management data provider (MDP) on Preside Multiservice Data Manager. The data collection system collects the following types of network management data:

- alarms and state change notifications
- accounting records
- performance measurements
- operator logs and debug information
- SNMP traps that are alerts to fault conditions

File system

The Passport file system stores the software and configuration files that run the node, as well as data generated by the node. The file system contains up to two physical disks, one located on each of the control processors. When you install and configure a main and spare control processor, the disks on the control processors provide file system redundancy when the disks are synchronized.

For information about file system synchronization and redundancy, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*.

Network management interfaces

The network management interface system (NMIS) is the part of the base software that enables you to access a Passport node through a network management device. The NMIS also provides network management access security.

Passport supports four types of network management interfaces: local operator, telnet, fast management information protocol (FMIP), and file transfer protocol (FTP).

The local operator interface allows a co-located ASCII terminal to act as a local operator. The telnet interface allows remote operator sessions.

Preside Multiservice Data Manager can connect to a Passport switch through the Ethernet port on the switch's control processor.

The FMIP interface is Nortel Networks' proprietary management information protocol. An FMIP interface operates between a Passport switch and Nortel Networks' Preside Multiservice Data Manager.

The FTP interface allows file transfers to and from local disks.

For more information about Passport network management, see "Passport network management" (page 57).

Processor control system

The processor control system manages the processor cards. Specifically, it

- sequences system start-up
- determines when processor cards are available for service and loads them with the appropriate software
- monitors processor cards and invokes appropriate recovery procedures when problems are detected
- supports processor card sparing
- provides a control interface for the command processing system so that you can monitor the system and perform corrective actions, if necessary

Software control system

Passport software is stored at a distribution site that is remotely accessible by network nodes. The Passport software control system allows you to download software from the software distribution site to the Passport node.

This system manages the software installed in the shelf. Passport software has separate applications that contain the software for a distinct type of service. Each application has an associated version number. An application version can also have one or more patches, which enhance or correct its functionality. The Passport software control system manages these application versions and patches on the Passport node.

When the software is on the Passport node, the software control system allows you to configure software services and applications on processor cards.

For more information about the software control system, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*.

Passport 7400 bus control

Passport base software controls its two 800 Mbit/s buses. The bus enables the processor cards on the shelf to communicate. When both buses are in operation, the node runs in dual bus mode, where both buses share the traffic on the bus, and provide a bandwidth of 1.6 Gbit/s. If one bus becomes

disabled, the node is in single bus mode and traffic runs on the enabled bus. If necessary, Passport automatically switches between single bus mode and dual bus mode.

Passport 15000 or 20000 backplane control system

The Passport 15000 and 20000 backplane control systems control the two fabrics. The fabrics enable the processor cards on the shelf to communicate with other cards in the shelf. When both fabrics are operational, the node runs in dual-fabric mode and both fabrics share the transport of processor card cells. With a disabled fabric, the node is in single-fabric mode and all processor card cells run on the enabled fabric. Passport 15000 or 20000 automatically switches between single- and dual-fabric mode depending on the state of the individual fabrics.

The backplane control system provides a fabric component interface in order to allow the user to monitor or to perform corrective actions on the fabric. Any operator commands such as locking, unlocking, or testing the fabric are controlled by the backplane control system.

The two 56.3 Gbit/s fabrics of the Passport 15000 provide 40 Gbit/s shelf (user) capacity.

The two 112.6 Gbit/s fabrics of the Passport 20000 provide 70 Gbit/s shelf (user) capacity.

Port management

The port management function of the base software controls and manages the ports and channels on each processor card.

A logical processor is a logical entity that you map to one or more processor cards and to a group of software features. For each logical processor, you must configure the ports and channels that exist on the processor card. After you define the ports and channels of a logical processor, you can link them to the service that you require for that port or channel.

For information about logical processors, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*.

Passport networking software

Passport networking software provides routing capabilities. The Passport routing systems enable Passport to forward packets of information from a source to a destination. Passport supports both connectionless and connection-oriented routing.

The base routing system provides transport resource and topology management. For more information, see “Base routing system” (page 40), “Transport resource manager” (page 40), and “Topology manager” (page 45).

Passport supports the following connectionless routing systems:

- “Dynamic packet routing system (DPRS)” (page 48)
- “IP routing system” (page 48)

Passport supports the following connection-oriented routing systems:

- “Path-oriented routing system (PORS)” (page 48)
- “ATM routing system” (page 49)

For more information about Passport routing systems, see 241-5701-400 *Passport 7400, 15000, 20000 Networking Overview*.

Base routing system

The base routing system captures and maintains a view of the Passport network topology. The system calculates the best path based on characteristics that exist in all Passport nodes in the network.

The base routing system provides transport resource and topology management through the transport resource manager (TRM) and the topology manager.

Transport resource manager

The transport resource manager (TRM) is a subsystem of the base routing system. It is responsible for management and monitoring of link resources (Passport trunks and DPN gateways) on the node. TRM assists in handling link up and link down requests and is the intermediary between the Passport trunking and routing systems. It also manages the grouping of links into link groups. TRM resides in the network layer.

IP, DPN gateway, and frame/cell trunk are available only on Passport 7400 series switches. Passport 15000 and 20000 do not use these services.

TRM has the following features:

- Common point of access to node's view of connectivity: TRM provides a single location that gives a view of all the neighbor nodes, links, and link groups. TRM also makes link characteristics visible, collects statistics for links, and learns which LNNs are supported on a link.
- TRM provides the base support for topology regions. Topology regions are used to support very large networks by restricting the topology information that is shared within the network. TRM detects when neighbors are in different regions (region boundaries).
- TRM supports the link group concept. TRM builds and maintains the link group tables. Link groups allow cost effective and flexible Passport trunking options. Link groups enable multiple links, and therefore increased available bandwidth, between nodes. This function is similar to inverse muxing without extra hardware.

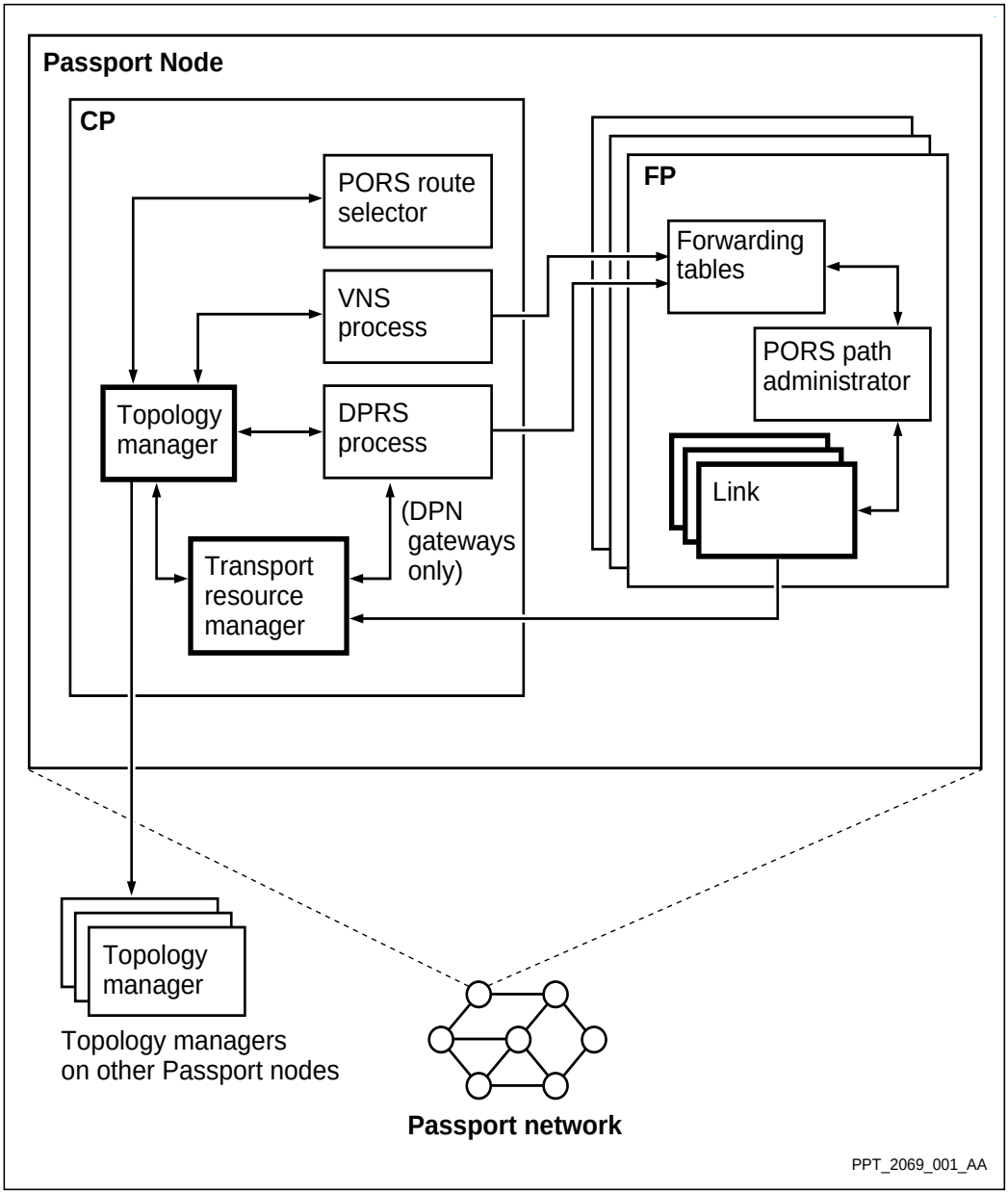
TRM and the network layer

TRM interacts with other components in the network layer and in the switching layer. TRM resides on the control processor of each node and handles information as follows:

- receives information from the link elements of the Passport trunking system located on the function processors
- sends information to the topology manager and DPRS component on the control processor

The figure "Passport base routing system - transport resource manager and topology manager" (page 42) highlights the interaction of base routing components.

Figure 7
Passport base routing system - transport resource manager and topology manager



Link information exchange

The transport resource management (TRM) subsystem on a switch interfaces with the local Passport trunking system to learn the status (up or down) of all usable links (Passport trunks and DPN gateways), their attributes to support various classes of routing (such as speed and delay), and the logical network that they support.

This information is required by two sources:

- the topology manager to learn the link state information, and DPRS to learn of gateways
- routing protocols to compute the metrics advertised for each of the available Passport links

TRM maintains the logical network connectivity between neighbor nodes.

Link group information exchange

The TRM subsystem organizes multiple links to neighbor nodes into link groups. TRM builds and maintains link group tables and link MPID tables. TRM broadcasts these tables to all processors on the shelf for use by the packet forwarding systems.

Link groups are used to carry DPRS traffic. PORS can make use of all the links in a link group to carry traffic. However, it treats each Passport trunk individually and does not make use of the link group concept.

There can be up to four links in a link group, and each node can support up to 255 link groups. Link groups, made up of Passport trunks or DPN gateways, are included in this total. Links in a link group may have differing characteristics, such as speed and delay, but support the same set of logical networks and maximum transmission unit (maximum packet size).

Preferred links include some or all links in a link group that carry traffic for DPRS. For example, a high delay satellite link in a link group would not be chosen as a delay preferred link if a terrestrial link also exists in that link group. TRM determines throughput and delay preferred links. DPRS packet forwarding uses both throughput preferred links and delay preferred links.

Bandwidth reservation and TRM

TRM also learns of the reserved PORS bandwidth of each link. The PORS bandwidth reserved on each link limits the number of PORS connections that can be established over that link. The total amount of peak or average reserved bandwidth for the connections cannot exceed the link's PORS reserved bandwidth.

DPRS calculates metrics based on the bandwidth available once the PORS reserved bandwidth has been subtracted from total available bandwidth. For more information see 241-5701-435 *Passport 7400, 15000, 20000 Path-Oriented Routing System Guide*.

The link override information is also learned by TRM for DPRS. If a link speed (bandwidth) or delay override is provisioned, the override is selected as the prevailing link bandwidth and or delay.

Topology regions

A topology region is an autonomous group of Passport nodes, where the complete topology of all Passport nodes in that portion of the network is known to the topology system. The topology of the rest of the network remains unknown to the Passport nodeIds within the topology region.

Provisioning topology regions within a network will improve network scaling because nodes only need to know the topology of their own region. Topology regions create greater network autonomy and make it possible to increase the size of networks by allowing nodes to be reused in different topology regions.

TRM provides the infrastructure to support topology regions by detecting neighbors that are part of a different region. The topology manager is not informed of such links.

TRM components

The *TransportResource (Trm)* component resides on all Passport modules and is responsible for managing link resources. This component acts as an intermediary between a link, and all the routing systems that use the links.

For *Trm* component state combination information see the table "Transport Resource Manager component state combination" (page 45).

Table 1
Transport Resource Manager component state combination

Combination (Administrative, Operational, Usage)	Details
Unlocked, Enabled, Active	The *TransportResource* component is operational and is communicating with each of the Passport trunks and gateways configured in the module. It is able to receive and process requests.

For more information on components, see 241-5701-060 *Passport 7400, 15000, 20000 Components*.

Topology manager

The topology manager system is an element of the base routing system, along with the transport resource manager system. The topology manager subsystem manages the topological view of the Passport nodes in the network.

A Passport node needs full knowledge of the network in which it is working. This knowledge encompasses two dimensions: the connectivity of other nodes, and the characteristics of interconnecting links and link groups between all nodes.

The Passport topology system has the following characteristics:

- Topology computes efficient paths for connectionless traffic and enables almost instantaneous rerouting when topology changes occur. Topology supports both the delay and throughput RCOS (DPRS delay and throughput).
- Topology distributes link attributes such as cost, delay, and bandwidth utilization to PORS. PORS uses this information to compute paths.
- Topology provides the base support for logical networks. Logical networks provide the capability to logically partition physical networks.

Topology manager and the network layer

Topology manager is located in the network layer. It retrieves information from and distributes information to other elements of the network layer.

The topology manager resides on the control processor of each node and handles information as follows:

- receives information from TRM located on the control processor
- sends information to the routing system components on the control processor and to the other topology managers on other nodes

The figure “Passport base routing system - transport resource manager and topology manager” (page 42) illustrates the interaction of base routing components.

Local node discovery

The topology manager interworks with TRM to learn local link characteristics and status such as all the link groups connecting to neighbors. TRM also notifies topology of any link state changes such as connectivity, bandwidth and delay. The topology manager updates its database with this local node information.

Neighbor discovery

Passport nodes automatically learn the network topology upon establishing connectivity to the network. When the topology system detects a link to a new neighbor node, it initiates the neighbor staging protocol. This protocol effectively synchronizes the topology databases on both nodes. This process ultimately ensures that up to date topology information is learned immediately and dynamically by new nodes as they join the network.

Network internal topology discovery

On each Passport node, the topology manager is responsible for learning the network topology. It propagates link state information about its own node to topology managers on all other switches within its topology region and maintains its own topological database. Each topology manager learns the complete network topology through this process such that the topology systems on all nodes maintain an identical view of the Passport network. This view includes all Passport nodes in the network (or the topology region if they are deployed in the network), and the links (or link groups) between them.

Path computation

The topology manager computes optimal paths through the network for each connectionless routing system using the shortest path first algorithm. The paths are generated by using a distributed link-state routing protocol based on

the IP standard OSPF (open shortest path first). The trees contain network path information. The topology manager provides the summary information to the routing manager for DPRS, and acts as a database for PORS.

Topology also provides quick, transparent recovery for all virtual circuits (VCs) or connectionless flows. Topology reacts quickly to network events and computes new paths to make use of new facilities and to avoid failures and congestion.

Supporting logical networks

Topology knows the logical network numbers (LNNs) for the link groups and carries this information to every node in the network.

Topology components

The *Topology (Top)* component is a subcomponent of *Routing (Rtg)* residing on all Passport modules. The *Topology* component maintains a topological database describing the Passport network topology in terms of nodes and connectivity between them. It computes the reachability costs to each Passport node for the different routing systems taking into account the underlying transport attributes (for example delay, throughput) of interest to them.

For *Topology* component state combination information see the table “Topology component state combination” (page 47).

Table 2
Topology component state combination

Combination (Administrative, Operational, Usage)	Details
Unlocked, Enabled, Active	Topology is exchanging routing protocol data units with Passport neighbors. It is capable of mapping additional Passport nodes in its topological database.
Unlocked, Enabled, Busy	Topology is operational, but its topological database cannot accept more Passport nodes. The number of Passport nodes stored in the topology database has reached the maximum network node number (256).

For more information on components, see 241-5701-060 *Passport 7400, 15000, 20000 Components*.

Dynamic packet routing system (DPRS)

Dynamic packet routing system (DPRS) uses a hierarchical addressing routing protocol and uses topology information to find the best routes to every destination address. Forwarding tables record these routes for use by the packet forwarding function.

For more information about DPRS, see 241-5701-425 *Passport 7400, 15000, 20000 Dynamic Packet Routing System Guide*.

DPRS supports frame relay services, and the transport of DPN-100 traffic across a Passport backbone network.

IP routing system

Passport supports the native routing of standard IP traffic with connectionless routing. It supports the following IP routing protocols:

- open shortest path first (OSPF)
- routing information protocol (RIP)
- border gateway protocol version 4(BGP-4) for IP

Passport's IP services support the following WAN services: ATM multiprotocol encapsulation service, frame relay DTE, point-to-point protocol, 10BaseT Ethernet, 100BaseT Ethernet, and gigabit Ethernet.

Path-oriented routing system (PORS)

The path-oriented routing system (PORS) provides a connection-oriented routing system that automatically establishes and maintains a connection. PORS supports switched and permanent connections. PORS transports traffic that responds to delay variance such as video, voice, and transparent traffic across Passport networks. At call setup time, PORS establishes a path and reserves bandwidth, allowing all packets to flow along the same path to the destination. PORS removes the path when it no longer needs the connection.

In conjunction with voice and transparent data services, PORS also utilizes the network clock synchronization, which synchronizes the clocks on both ends of a data path to a single master clock signal.

For more information, see 241-5701-435 *Passport 7400, 15000, 20000 Path-Oriented Routing System Guide*.

ATM routing system

The ATM routing system is a connection-oriented system. ATM routing provides dynamic runtime connection setup between Passport nodes, and allows Passport switches to interwork with other ATM switches. ATM routing provides the addressing, signaling, and routing facilities to support switched virtual connections (SVCs), soft permanent virtual connections (SPVCs), soft permanent virtual paths (SPVPs), and permanent virtual connections (PVCs). These networking capabilities allow you to set up ATM connections in real time.

Passport supports both IISP-based static routing and PNNI-based dynamic routing. However, a mix of routing types is not supported.

For more information, see the following documents

- 241-5701-700 *Passport 7400, 15000, 20000 ATM Overview*
- 241-5701-702 *Passport 7400, 15000, 20000 ATM Routing and Signaling Fundamentals*
- 241-5701-710 *Passport 7400, 15000, 20000 ATM Configuration Guide*
- 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide*

Trunking software

Passport trunking systems enable Passport nodes to connect to other Passport nodes and to DPN-100 nodes. Passport trunking systems include:

- “Passport trunks” (page 50)
- “Passport 7400 trunks for multi-service access” (page 50)
- “DPN gateways for Passport 7400” (page 50)

Passport trunks

Passport-to-Passport links are called trunks. A Passport trunk is a point-to-point or logical connection (ATM virtual channel connection) between two Passport nodes over which Passport proprietary routing protocols can run. Passport trunks use an ATM transport mechanism.

Passport trunks over ATM (previously called ATM logical trunks) encapsulate frame traffic into ATM traffic. The Passport trunk over ATM uses one or more ATM VCCs and standard ATM adaptation layer protocols based on ATM adaptation layer type one (AAL1) and ATM adaptation layer type five (AAL5).

For more information, see 241-5701-420 *Passport 7400, 15000, 20000 Trunking Guide*.

Passport 7400 trunks for multi-service access

Some function processors (FPs) for multi-service access (MSA) can be configured to provide SONET or SDH optical trunking through the one or two OC3/STM1 ports on the same FP. For the MSA FPs with two OC3/STM1 ports, only one carries traffic while the other backs it up with automatic protection switching (APS). Whether APS is enabled or not, port protection can also be set up through the dynamic packet routing system (DPRS).

Configuring the ports as trunks is described in 241-5701-420 *Passport 7400, 15000, 20000 Trunking Guide*. For information on which FPs can be configured for SONET or SDH optical trunking, refer to 241-5701-615 *Passport 7400, 15000, 20000 FP Configuration Reference*.

DPN gateways for Passport 7400

Links to other networks are called gateways. Passport-to-DPN trunking (DPN gateway) uses two DPN trunking protocols: universal trunk protocol (UTP), and light-weight trunk protocol (LTP) over frame relay. A DPN gateway can link to an access module (AM), resource module (RM), or an RM configured as a call-server resource module (CSRM). A gateway connection at the AM side is called a network link. A gateway connection at the RM or CSRM side is called a DPN trunk.

Passport addressing

This section provides background on addressing. The topics covered are as follows:

Role of addressing

An address uniquely identifies a network entity. This identifier may be unique within or outside a network, depending on the addressing plan. The network entity may be a Passport node, DPN-100 module, work station, telephone, service port, or other network device.

An important aspect of the addressing function is to identify and resolve any differences between address formats. Routers and servers translate external network addresses to Passport internal addresses. This address resolution allows connections to be established and packets routed.

Addressing features

The Passport system has several addressing features.

Compliance to external addressing plans

The Passport system supports addresses complying to the following standard addressing plans and formats:

- E.164
- X.121
- Internet Protocol (IP)
- Media Access Control (MAC)
- Network Service Access Point (NSAP)

Note: Data network address (DNA) is a Passport term for an address that identifies a device in a Passport network. DNAs conform to X.121 and E.164 numbering systems.

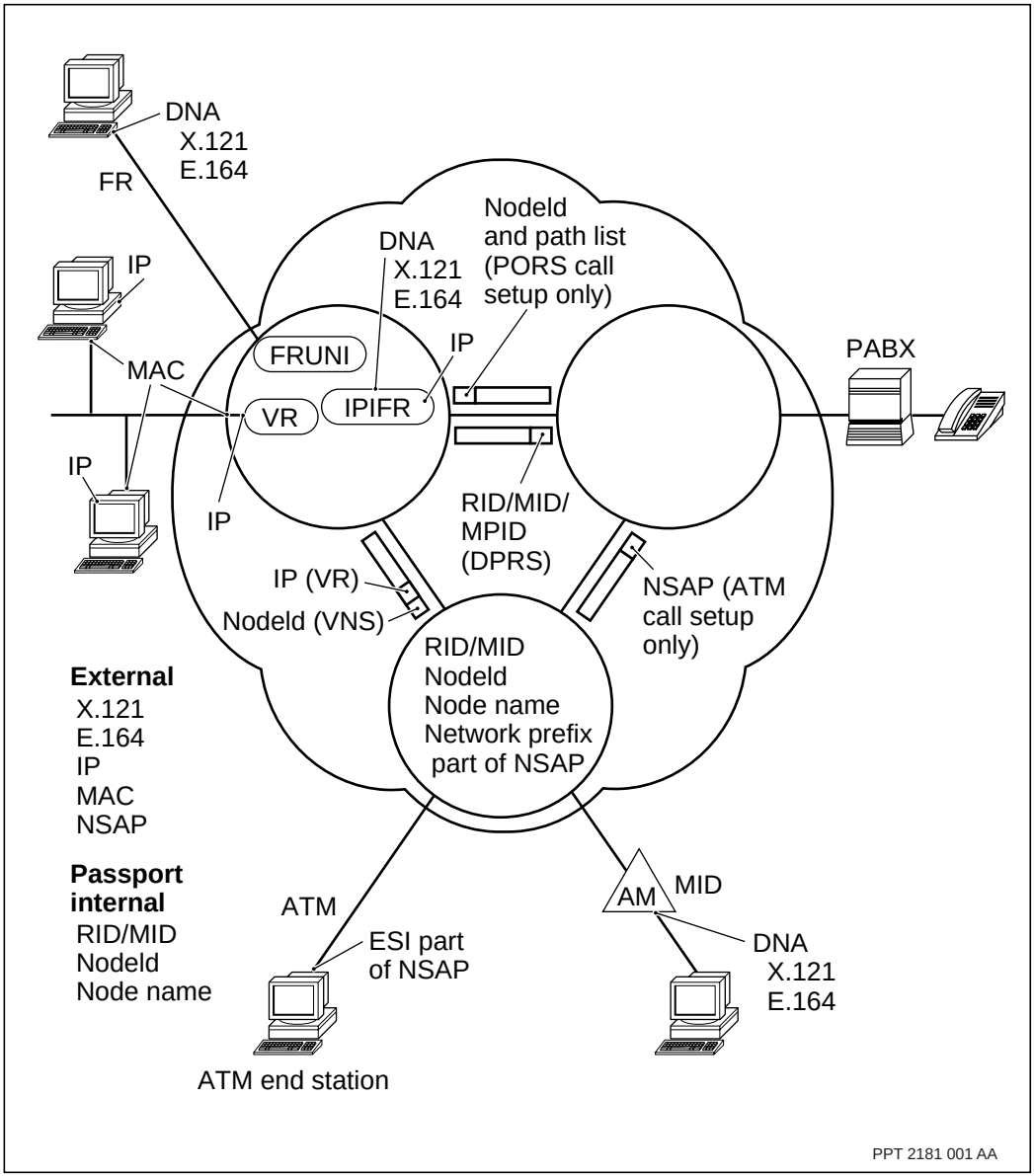
Support of Passport internal identifiers

The Passport system uses the following internal identifiers, which are used to optimize call establishment and packet routing:

- RID
- MID
- node identifier (nodeId)
- node name

See the figure “External addressing plans and Passport internal identifiers” (page 53) for the addressing plan usage for several network entities.

Figure 8
External addressing plans and Passport internal identifiers



Addressing mechanisms

This section describes the following addressing mechanisms:

- "External addressing plan formats" (page 54)
- "Passport internal identifiers" (page 54)

External addressing plan formats

An addressing plan, also known as an addressing scheme or numbering plan, defines a format for identifying an endpoint. The Passport system supports the most common external addressing plans recognized by ITU-T and IETF.

Passport services using the Dynamic Packet Routing System (DPRS) can accept the X.121 and E.164 addressing format for both international and national addresses. IP services use IP and MAC addressing formats. PORS services use X.121, E.164, and NSAP addresses. ATM services accept E.164 and NSAP addresses.

Passport internal identifiers

The Passport system supports external addressing plans by translating them when necessary to proprietary or internal identifiers for Passport network use.

Passport networks and nodes have several identifiers (see the table "Passport internal address information" (page 54)). The identifiers are provisioned by the network operator. Each identifier is used by the routing system, and in some cases for network management too.

Table 3
Passport internal address information

Level	Name	Length	Example	Use
Network	RID	7 bits	15	DPRS for routing
Node	MID	11 bits	275	DPRS for routing

(Sheet 1 of 2)

Table 3 (continued)
Passport internal address information

Level	Name	Length	Example	Use
	nodeId	32 bits	1244	PORS for call setup; and network management
	node name	12 character ASCII string	EM/Toronto	mnemonic for a node. Synonymous with nodeId within a region. PORS for call setup; network management.

(Sheet 2 of 2)

Note: Network management is outside the scope of this NTP.

RID/MID

DPRS uses the hierarchical routing identifier/module identifier (RID/MID) addressing system.

NodeId

The node identifier (nodeId) is an internal concept within base routing. NodeIds are stored in the topology database and used by the topology process to select the best routes to each nodeId for the DPRS and PORS routing systems. These routes are placed in the routing system's forwarding tables.

Node name

PORS BTDS, HTDS, and voice service use the node name addressing system for call set up. Node name is synonymous with nodeId and is used to determine nodeId.

Chapter 4
Passport network management

This section explains Passport network management in terms of

Network management functions

There are five functions of network management. Some network management devices enable you to perform all five functions of network management. Other devices perform a part of these functions.

For information about network management functions, see the following sections:

Fault management

Passport fault management includes monitoring a Passport node or network with a network management device. Passport generates alarms to indicate faults in a node or network. Passport also provides OSI state information that can help you determine the cause of a fault.

For general information on Passport alarms, see "Passport alarms" (page 69). For information on specific alarms, see 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*. For information on OSI state information, see 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*.

Passport also supports the Passport trace system (PTS). PTS is a tool that monitors incoming and outgoing data for a specific frame relay connection. PTS copies the data in real time and sends it to a remote receiver. You can configure a trace session to copy distinct types of frames.

For more information about PTS, see 241-5701-510 *Passport 7400, 15000, 20000 Trace Guide*.

Configuration management

Configuration management includes provisioning and software management. Provisioning modifies Passport components and attributes to add or delete services, or to change the behavior of the node or services. Software management configures and downloads software to Passport nodes to add or upgrade services or features.

Passport configuration management is dynamic, online, and does not require down time for processor cards. Passport stores provisioning data on each node. Each node stores its working configuration, and can also store different configurations. Network management devices can retrieve copies of these configuration files to create backups.

For information on configuring the base Passport system or managing the software running on your Passport node, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*.

Accounting management

The Passport data collection system collects information about the use of some services. You can use this data for billing customers.

In a redundant CP configuration, two fault-tolerant disks, each containing the same data, store accounting data for frame relay and ATM services. You can schedule time-of-day accounting to allow for modifications (for example, changes in tariff rates).

Passport also includes a call management capability that helps to prevent the loss of accounting records. This capability only applies to frame relay SVCs. The call management system only accepts a new call if there are enough system resources to process the call and its associated accounting records at the moment the call is made.

For more information about accounting, see 241-5701-650 *Passport 7400, 15000, 20000 Accounting Fundamentals*.

Performance management

The Passport data collection system collects statistics and real-time statistical data on a node-by-node basis to evaluate system performance. In a redundant CP configuration, two fault-tolerant disks, each containing the same data, store network planning statistics. The real-time statistics are not spooled to disk. They may be viewed in ASCII format through a network management interface system (NMIS) local or telnet session or retrieved by the MDM through an NMIS FMIP session.

A network management device can retrieve and analyze these statistics and real-time statistics to determine node or network performance. For more information on Passport performance management, see 241-5701-611 *Passport 7400, 15000, 20000 Data Collection Guide*.

Security management

Passport provides different levels of security that include user ID and password protection, command logging, an allowed-IP address list, and session control. For more information on Passport security management, see NN10600-605 *Passport - MDM Network Security: Operations*.

You can configure each Passport user ID with allowed interface types: local operator, FMIP, telnet, and FTP. You can provision a list of IP addresses to indicate network management devices from which a Passport node accepts a connection.

Note that both secure and non-secure FTP is supported between Passport and Preside MDM workstations. See the document Preside MDM Security User Guide 241-6001-040 for details.

Network management devices

You can configure and manage your Passport node or network with different network management devices. For more information, see the following sections:

- “Local or telnet devices” (page 60)
- “Nortel Networks Preside Multiservice Data Manager” (page 61)
- “SNMP-based network management devices” (page 61)

Passport enables you to connect to a network management device over several types of connections. See “Network management connections” (page 61).

Local or telnet devices

The most direct method for managing a Passport node is to use a VT100 terminal or a VT100 terminal emulator plugged directly into the V.24 port on any of the node’s control processors. This local access provides you with a text interface where you can enter commands and view alarms.

With a local VT100 terminal, you must be in the same location as your Passport node to manage it. Often this is not possible or practical. You can manage your node from a remote site using a telnet application. With telnet, you can log into Passport’s text interface from a remote workstation. You can enter commands and view alarms as if you were using the local VT100 terminal.

Local and telnet devices enable you to configure a node and to perform fault and security management with operations and maintenance commands.

For more information about Passport commands, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Nortel Networks Preside Multiservice Data Manager

Nortel Networks Preside Multiservice Data Manager provides a general description of a network. Common network management tools and procedures enable you to manage Passport, DPN-100, and SNMP devices. The graphical user interface can be customized so that you can adjust the look and behavior of the system. Preside Multiservice Data Manager is scalable and can manage networks that contain a number of network elements and subcomponents in many different locations. Nortel Networks Preside Multiservice Data Manager delivers the following capabilities:

- allows you to view and manage each Passport node or DPN-100 module as one of many integrated elements within the network
- provides standard network views and equivalent alarm and display systems for Passport and DPN-100
- provides fault, configuration, accounting, performance, and security management for integrated networks

Telnet, FTP, and the Passport proprietary protocol, the fast management information protocol (FMIP), transport information to Preside Multiservice Data Manager.

For more information about Preside Multiservice Data Manager, see 241-6001-801 *Preside MDM Overview*.

SNMP-based network management devices

You can use an SNMP-based management application to manage a Passport network. Passport supports SNMP-based management devices for surveillance and fault management. It also supports both standard and enterprise MIBs.

For more information about Passport SNMP, see 241-5701-300 *Passport 7400, 15000, 20000 SNMP Guide*.

Network management connections

To manipulate and view nodes in a network you must log into the network with a network management workstation. When you log into a Passport node, you are in Passport's text interface where you can view alarms and enter commands.

There are three ways to log into a Passport node:

- from the local VT100 terminal or VT100 terminal emulator
- from a telnet client (on a management workstation or another Passport node)
- from the Command Console in Preside Multiservice Data Manager

When setting up your local VT100 or terminal emulator, make sure it is set to 9600 bit/s, 1 stop bit, no parity. The keyboard shortcut Control-Q may need to be pressed to resume output after connecting the local VT100 terminal or VT100 terminal emulator.

Regardless of how you log in, you must provide valid user information for that node. In some cases, the IP address of the workstation you are using must be on the valid IP address list for the node. For more information, see 241-5701-600 *Passport 7400, 15000, 20000 Configuration Guide*.

For more information on logging into a Passport node, see the following:

- "Understanding the network management interface system" (page 62)
- "Logging into a Passport node from a local operator terminal" (page 65)
- "Telnet access to a Passport node" (page 65)
- "Connecting to a device using telnet" (page 68)

Understanding the network management interface system

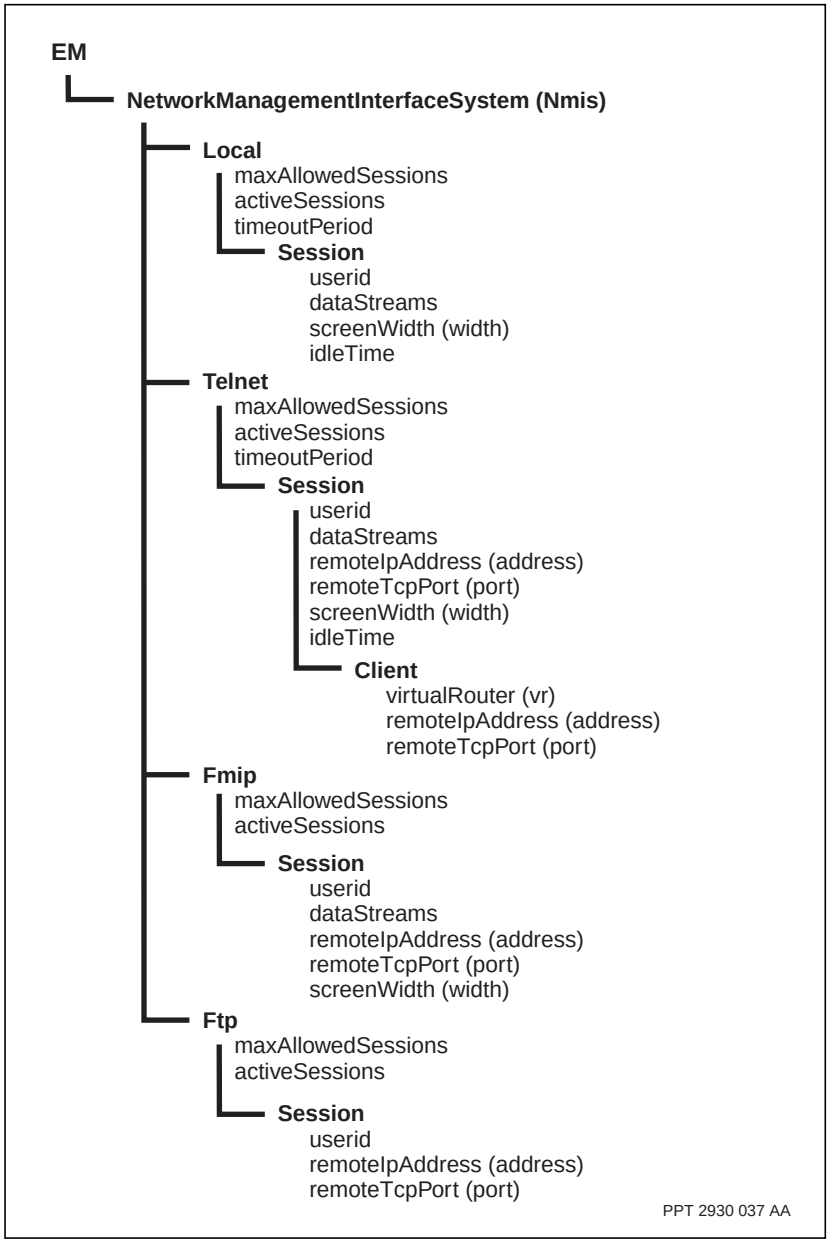
The network management interface system (NMIS) manages a number of network manager interfaces. Whenever you log into a Passport node, you use a session of a network management interface.

The figure "Network management interface components and attributes" (page 63) illustrates the components and attributes that represent the network management interface system.

See the following for more information on the NMIS:

- "Network management interfaces" (page 64)
- "Network management interface sessions" (page 64)

Figure 9
Network management interface components and attributes



Network management interfaces

There are four network management interfaces you can use to log into a Passport node:

- local (local operator)
- telnet
- FMIP
- FTP

Each of the interfaces has a corresponding subcomponent which represents the interface. All of the subcomponents have two attributes: *maxAllowedSessions* and *activeSessions*. The *maxAllowedSessions* attribute specifies the maximum number of simultaneous sessions the interface can have. The *activeSessions* attribute specifies the number of simultaneous sessions currently active on the interface.

> ***Note:*** The local and telnet subcomponents have an additional attribute: *timeoutPeriod*. For more information, see either "Idle local operator sessions" (page 65) or "Idle telnet sessions" (page 67).

Network management interface sessions

When you log into a Passport node through a management interface, Passport dynamically creates a *Session* subcomponent to represent your connection. It automatically removes the *Session* subcomponent when you log out of the node.

Each network manager interface has the following basic session attributes:

- *userid*
- *dataStreams*
- *width*

The *userid* attribute identifies the user ID of the user logged into the session. The *dataStreams* attribute identifies which data streams (alarms, SCNs, operator logs, debug information, or rtstats) Passport displays during the operator session. The *width* attribute identifies the maximum width of the operator command responses.

Remote access sessions (telnet, FMIP, and FTP) also include information about the remote connection. The *remoteIpAddress* attribute reports the IP address of the remote device, and the *remoteTcpPort* attribute reports the TCP port number on the remote device used for the session.

Logging into a Passport node from a local operator terminal

For information on how to log into a Passport from a local-operator terminal, see 241-5701-270 *Passport 7400, 15000, 20000 Software Installation Guide*.

Idle local operator sessions

The local *timeoutPeriod* attribute is disabled by default, meaning local sessions can remain idle indefinitely. This state of inactivity uses up system resources needlessly as well as offers a security risk since unauthorized access is a possibility. All terminations due to inactivity are logged and an override capability is available. For more information about timeoutProtocol, see 241-5701-060 *Passport 7400, 15000, 20000 Components*.

Telnet access to a Passport node

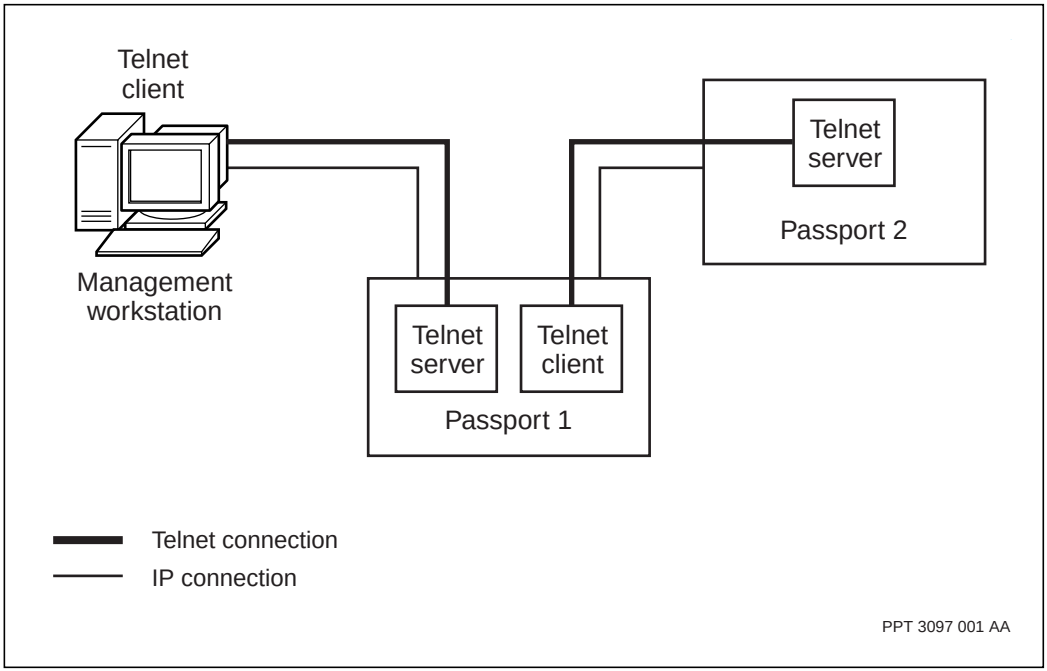
When you log into a Passport node using telnet on a management workstation, Passport acts as a telnet server. The telnet server accepts up to 12 incoming telnet connections for CP2 and up to 16 incoming telnet sessions for CP3.

Note: CP1 is not supported.

A Passport switch can also act as a telnet client, making outgoing telnet connections to telnet servers. Since Passport can behave as both a telnet client and a server, you can use the telnet Vr command on a Passport node to connect to another Passport node. You can also use the telnet Vr command to connect to any device supporting standard telnet access. The Passport node or device must be accessible through a management or customer virtual router.

The figure “Using telnet on a Passport node” (page 66) illustrates how you can use the telnet Vr command to connect from one Passport node to another. First you telnet to Passport 1 from a management workstation using a telnet client application. Once you are logged into the telnet server on Passport 1, you can use the telnet Vr command to establish a telnet connection to Passport 2. You are now using the telnet client on Passport 1 to connect to the telnet server on Passport 2.

Figure 10
Using telnet on a Passport node



Telnet client and server sessions

Passport can act as both a telnet client and a telnet server. It acts as a server when you use a telnet application to log into a Passport node. Up to 12 different users can simultaneously log into a Passport equipped with CP2. Up to 16 different users can simultaneously log into a Passport equipped with CP3.

Note: CP1 is not supported.

Passport acts as a telnet client when you use the telnet Vr command to establish a connection from a Passport node to another Passport node, or from a Passport node to any other device supporting standard telnet access.

An instance of a *Session* component represents a single telnet server connection. Once you have a telnet server connection, you can use the telnet Vr command to establish a telnet client connection. A *Client*

component represents this outgoing connection. The attributes of the *Client* component report the IP address and TCP of the remote device, as well as the virtual router used to access the remote device.

For more information on telnet Vr, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Idle telnet sessions

On Passport, up to 12 telnet sessions can be simultaneously active on a Passport equipped with CP2 and up to 16 telnet sessions can be simultaneously active on a Passport equipped with CP3. Sessions that are idle continue to use system resources. As a result, the timeoutPeriod attribute is introduced to allow users with *systemAdministration* access to determine how long telnet sessions can remain idle before they are terminated. This attribute is disabled by default, however, it can be provisioned to be anywhere between 5 and 120 minutes. By provisioning a value for this attribute, idle sessions will be terminated after a certain length of time so that new sessions can be initiated. Additionally, when sessions are idle there is a possibility for unauthorized access. This risk is reduced with the introduction of the *timeoutPeriod* attribute.

The *timeoutPeriod* is applicable to all sessions that are created after this attribute is set. The setting of the *timeoutPeriod* is limited to users with a command impact of *systemAdministration*. If the value of the *timeoutPeriod* is changed, only new sessions created after the activation will be affected.

Each session has a unique *idleTime* value indicating the amount of time the session has been idle, even if the *timeoutPeriod* is disabled. If the *timeoutPeriod* is provisioned, a warning will automatically be issued when an idle session is within one minute of its *timeoutPeriod*.

> ***Note:*** The *idleTime* attribute begins counting idle time after the user has received a final response and has not entered any new commands. It only applies to telnet sessions in server mode. Sessions that make use of telnet client, as well as sessions that run in startup mode, are exempt from inactivity tracking.

All terminations due to inactivity are logged and an override capability is available. The override capability allows users with a command impact of *systemAdministration* to disable the *timeoutProtocol* for specific user IDs. Those user IDs for which the *timeoutProtocol* has been disabled are exempt from inactivity tracking. The *timeoutProtocol* is enabled by default; therefore, when a *timeoutPeriod* has been configured, it applies to all telnet sessions.

Connecting to a device using telnet

To connect to Passport via telnet when working from a remote location, first ensure that

- The node has a properly configured virtual router.
- Your user ID is allowed outgoing telnet access. For information on allowing outgoing telnet access, see NN10600-605 *Passport - MDM Network Security: Operations*.
- The IP address of the device you are connecting to is accessible through a management or customer virtual router on the node. In other words, the IP address is within the address space of the specified virtual router.
- You have a user ID and password for the remote device.
- If you are connecting to another Passport node and that node has IP address checking enabled, the IP address of your node is on the valid IP address list.

Use the following command:

```
telnet -ipAddress(<remoteAddress>) Vr/
<virtualRouter_instance>
```

If you are connected to another Passport node, the connection is transparent. Command responses and alarms appear on screen as if you had directly connected to the node from a management workstation. If you are uncertain which Passport node you are connected to, use the me command.

Preside Multiservice Data Manager connections

You can connect your Passport node to Preside Multiservice Data Manager workstation in one of the following ways:

- connecting the node to Preside Multiservice Data Manager through a Passport-only network

- connecting the node directly to Preside Multiservice Data Manager
- connecting the node to Preside Multiservice Data Manager through the networking of IP services
- For Passport 7400 only, connecting the node to Preside Multiservice Data Manager through a DPN network

The Passport StartUp utility enables you to initially connect a Passport to a network management device through any of these connections.

For more information about StartUp, see 241-5701-271 *Passport 7400, 15000, 20000 Network Management Connectivity*.

Passport alarms

Passport provides a method for components in the system to asynchronously signal events or alarms to an external management device (for example, a VT100 terminal or a network management workstation).

Passport alarms are based on an event-driven system (that is, alarms are generated when certain events occur).

Common alarm situations include the following:

- a failure or fault occurs (this is a set alarm)
- a fault or failure condition has been fixed (this is a clear alarm)
- cases where conditions are transient or cannot be repaired (a message alarm may appear to inform you of the condition).

Alarm strategy

Passport alarms are designed to minimize the occurrence of multiple alarm generation in the event of a failure or error condition. In general, only the component that fails or detects the failure generates the alarm, thus preventing the generation of an entire chain of alarms from components associated with the failed component.

Note: There are some cases when a fault or failure results in the generation of more than one alarm.

Using state change notifications, the component that fails notifies other components above and below it on the component hierarchy to indicate that it is no longer in service. The related components do not generate an alarm because they have been notified of the change of state.

When the component is back in service, it clears its previous alarm and notifies its subcomponents (as well as other components that may be dependent on it) of its new state.

Alarms and customer identifiers

All Passport alarms contain a customer identifier (CID). The CID does not appear on the interface, but is essential in determining which alarms are displayed to which users. Alarms are displayed based on the CID of the user Id.

What causes alarms

Generally speaking, alarms occur in the following situations:

- degradation/quality of service conditions (for example, the onset of severe congestion)
- processing errors (for example, protocol errors)
- engineering alarms (for example, insufficient memory for a required component)
- out-of-service conditions (for example, hardware failures such as a functional processor or power supply failure)
- software errors (that is, an unexpected condition has been detected in software)
- administrative conditions (such as using the lock command to temporarily lock a component)
- security violations (for example, successive invalid logon attempts)

How are alarms cleared?

Clearing an alarm may involve taking one of several actions, or in some cases, no action at all. It may require that you act immediately to a condition in the network, call for help, change a piece of hardware or simply wait until the condition has cleared itself.

Note: You can report an alarm to Nortel Networks by opening a customer service request (CSR).

The following list describes some general methods for clearing alarms:

- issuing operator commands (refer to NTP 241-5701-045 *Passport 7400, 15000, 20000 Management System User Interface Guide* for details on issuing common commands)
- replacing hardware (for example, a control processor)
- taking no action—in some cases such as threshold alarms, no action may be required on the part of the user—the alarm clears itself if conditions return to normal

Note 1: Alarms can also be cleared using the Integrated Alarm Display. However, it clears only the alarm logs in Preside Multiservice Data Manager and not those at the Passport.

Note 2: These are only general remedial actions. For specifics on clearing individual alarms, refer to 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

What are state change notifications?

State change notifications (SCN) are intended primarily for use by network management systems for determining the impact of a certain failure.

When the OSI operational state or the OSI procedural status of a particular component changes, the system automatically generates an SCN. This information is used to update the network model.

For more information on OSI operational state and OSI procedural status, refer to “Operational state” (page 80) and “Procedural status” (page 83),.

How to interpret alarm information

Depending on your requirements, you may want to interpret an alarm as it appears on the text interface, in Preside Multiservice Data Manager, or as it is documented in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

For information on interpreting alarms as they appear on your text interface device, refer to Chapter “Interpreting alarms” (page 72).

SONET/SDH alarm handling on Passport 7400 has been improved to follow the hierarchical near end failure model such that it is now consistent with Passport 15000 and other transport equipment. In the case of an LOS for example, all the lower precedent alarms (LOF, AIS, RFI, UnusableTxClkRef) will not be raised.

Interpreting alarms

This section will help you interpret Passport alarms as they appear on a text interface device (that is, an ASCII-based terminal such as a VT100 or a telnet session). Included is an example to help you understand the fields and terms discussed in the chapter.

> ***Note:*** The format and contents of the user interface are subject to change over time.

Alarm screens

The sample screens and paragraphs in this section will familiarize you with the appearance of Passport alarms as they appear on a text interface device and the Alarm Display (AD) tool.

The section “Alarm fields” (page 75) provides a description of the fields that appear in the alarm formats shown below.

Alarm format on a text interface device

The figure “Alarm format on a text interface device” (page 73) shows the Passport alarm format used on a text interface device.

Figure 11
Alarm format on a text interface device

```
      <Component name>; <date> <time>
<status> <severity>  <type>  <cause>            <alarm index>
      ADMIN: <admin>   OPER: <oper>   USAGE: <usage>
      AVAIL: <avail>   PROC: <proc>   CNTRL: <control>
      ALARM: <alarms>  STBY <stdby>   UNKNW: <unknown>
      Id: <notifId>  Rel: [<relatedComp1>; <relatedComp2>; ...]
      [Com: <commentData>]
      [Op:  <operatorData>]
      Int: <process id>; <filename>; <linenumber>; <version>
           [<internalData>]
```

PPT 0001 001 AA

Alarm format on the Alarm Display

The figure "Alarm format using the Alarm Display tool" (page 73) shows the Passport alarm format used on the Nortel Preside Multiservice Data Manager Alarm Display (AD) tool.

Figure 12
Alarm format using the Alarm Display tool

```
<severity> <status> <NTP index> <date> <time> <component name>
ID: <notifId> TYPE: <type> CAUSE: <cause>
[CO: <commentData>]
[OP: <operatorData>]
[EX: <internalData>]
RAW: <raw> ADMIN: <admin> OPER: <oper> USAGE: <usage>
                  AVAIL: <avail> PROC:<proc>  CNTRL: <control>
                  ALARM: <alarm> STBY:<stdby> UNKNW: <unknown>
[REL COMP: <Related Component name>] <--one line per
          related component
INT: <process id>; <filename>; <line number>; <version>
```

PPT 0002 001 AA

The possible values for the RAW state are:

- insv (in service)

- oos (out of service)
- trb (troubled)
- unk (unknown)
- nex (non-existent)

Example of an alarm on a text interface device

The figure “Alarm on a text interface device” (page 74) shows an example of an alarm as it would appear on a text interface device.

Figure 13
Alarm on a text interface device

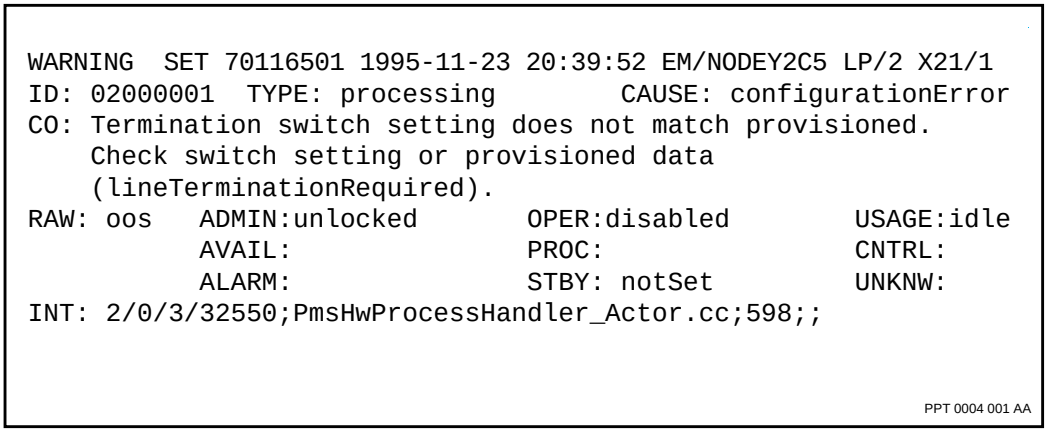
```
     Shelf Card/1; 1993-05-11 18:30:08.99
CLR  warning  equipment  processorProblem          11010001
     ADMIN: unlocked     OPER: disabled     USAGE: idle
     AVAIL: dependency   PROC: initializing CNTRL: SubjectToTest
     ALARM: alrmOutstdng STBY: coldst       UNKNW: false
     Id:    03        Rel: Shelf Card/13
     Com:   This is a hypothetical alarm.
     Op:    596F7572206E616D65206973206D7564
     Int:  1/9/215; dcsTESTApRecord.cc;255; user1.23.7
```

PPT 0003 001 AA

Example of an alarm on the Alarm Display

The figure “Alarm on the Alarm Display tool” (page 75) shows an example of an alarm as it would appear on the Alarm Display (AD) for Passport.

Figure 14
Alarm on the Alarm Display tool



Alarm fields

Alarm fields are described below in table format to assist you in interpreting alarms. The fields are listed in the order they appear on the text interface. The third column of the table “Alarm fields of the text interface” (page 76) gives an example of each field taken from the figure “Alarm on a text interface device” (page 74). Column 4 states whether the field is mandatory or optional.

A mandatory field must be present in the display, while optional fields may not be present.

Some fields are for internal use only and are noted as such in the description column of the table “Alarm fields of the text interface” (page 76).

Where necessary, subsections following the table describe fields in further detail (for example, the Alarm index field).

Table 4
Alarm fields of the text interface

Field	Description	Example from "Alarm on a text interface device" (page 74)	M/O
component name	The full name of the component needing repair, or detecting the fault. The component name can be used for hierarchically clearing alarms for its subcomponents (since the subcomponent name is derived from the component name).	Shelf Card/1	M
date and time	The date and time the alarm was issued.	1993-05-11 18:30:08.99	M
status	Indicates the status of an alarm. The possible values for this field include message (MSG), set (SET) or clear (CLR).	CLR	M
severity	Indicates the severity of the alarm. The value will be one of, critical, major, minor, warning, indeterminate, cleared. For further details, refer to ITU-T Recommendation X.733.	warning	M
type	This is a general explanation of why the alarm was generated. Possible values for this field include communications, quality of service, processing, equipment, environmental, security, operator, debug, or unknown. For further details, refer to "Type" (page 79).	equipment	M
cause	This provides another level of detail of why the alarm was generated. It is information given in addition to the general explanation given in the Type field. For further details, refer to 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.	processorProblem	M

(Sheet 1 of 3)

Table 4 (continued)
Alarm fields of the text interface

Field	Description	Example from "Alarm on a text interface device" (page 74)	M/O
Alarm index	An eight-digit number which is the principal alarm identifier. It consists of an IndexGroup and SubIndex. For further details see "Alarm index" (page 79).	11010001	M
ADMIN, OPER, USAGE	These fields describe the possible OSI states, that is, the administrative state, operational state, and usage state of the component. For information on OSI states, refer to "OSI states" (page 80). For component-specific OSI state combinations, refer to the appropriate Appendix in 241-5701-520 *Passport 7400, 15000, 20000 Troubleshooting and Testing*. Some of this information is also included in the user guides for the various services.	unlocked/disabled/idle	M
AVAIL, PROC, CNTRL, ALARM, STBY, UNKNW	These fields describe OSI status. Included in this group are availability status, procedural status, control status, alarm status, standby status, and unknown status. For information on OSI status, refer to "OSI status" (page 82).	dependency/initializing/ subjectToTest/ alrmOutstdng/coldSt/ false	M
Id	The system automatically inserts the notification Identifier. Notification identifiers are unique within each Passport.	03	M

(Sheet 2 of 3)

Table 4 (continued)
Alarm fields of the text interface

Field	Description	Example from "Alarm on a text interface device" (page 74)	M/O
Rel	A list of known related components. Usually it is only the supporting hardware name that the affected component resides on. For example the LP and possibly the card number. This field may appear as blank if there are no related components.	Shelf Card/13	O
Com	Comment data is additional data in ASCII format. It provides the operator with extra information in the form of a comment.The text appearing in this field is self-explanatory.	This is a hypothetical alarm.	O
Op	Operator data is hex-format data that an operator can use for additional information. If operator data exists, it is explained in the "details" section of the individual alarms in 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.	596F7572206E616...	O
Int	Internal data is additional information in Hex-format that can be used by internal support personnel. Contained within this field are the processId (Pid), filename, linenumber and version.	1/9/215; dcsTESTApRecord.cc; 255; user1.23.7	O
processId	Used internally	1/9/215	O
filename	Used internally	dcsTESTApRecord.cc	O
linenumber	Used internally	255	O
version	Used internally	user1.23.7	O

(Sheet 3 of 3)

Type

The following explains the values that can appear in the Type field:

- communications alarm indicates a problem related to communication (for example, protocol errors)
- qualityOfService alarm indicates a problem related to quality of service (for example, crossing thresholds)
- processing alarm indicates a problem related to processing data (for example, a memory problem)
- equipment alarm indicates a problem with the physical equipment (for example, a processor failure)
- environmental alarm indicates a problem related to the enclosure in which the equipment resides (for example, flood detected)
- security alarm indicates a problem related to security (for example, an unauthorized access)
- operator alarm indicates that some event was caused by operator action (for example, locking a component)
- debug alarm indicates that the event was for debugging purposes
- unknown alarm indicates that reason for the event is not known

Alarm index

The Alarm index consists of eight BCD digits. The first four digits are collectively known as the IndexGroup and the remaining four digits are known as the SubIndex.

The IndexGroup is a four-digit number representing logical groupings of alarms. For example, it may represent:

- an application service
- an internal subsystem
- a component type
- a component class
- a software module
- a similarity of event

The SubIndex is a four-digit number that has significance only within the IndexGroup.

OSI states

Passport uses component state definitions according to the OSI standards. OSI states mays be exhibited by any application. Components that do not provide any behavior do not require any component state variables defined.

Further details are found in ITU-T Recommendation X.731, Information technology - Open Systems Interconnection - Systems Management - Part 2: State management function.

A component has three high-level state variables: an operational state, a usage state, and an administrative state. These states are the primary factors affecting the management state of a component.

Operational state

The operational state of a component indicates whether the resource is physically installed and operational.

Not all types of components exhibit all possible states. For example, a component that has no visible dependencies on other components may not show the disabled operational state.

You cannot cause a component to change from one state to another. You can, however, gather information about the operational state of a component by using the appropriate operator command. Specific events associated with a component can cause specific transitions from one operational state value to another.

The two possible values for this attribute are:

- enabled—the component is partially or fully operable and available for use
- disabled—the resource is totally inoperable and unable to provide service

Usage state

The usage state of a component indicates whether the resource is actively in use at a specific time, and if so, whether it has spare capacity for additional users.

The usage state can have one of the following values:

- idle—the component is not currently in use
- active—the component is in use, and has sufficient spare capacity to provide for additional users simultaneously
- busy—the component is in use, but it has no spare operating capacity to provide for additional users at this instant. This is also used for components that have only one user. A component that has only one user typically exhibits an idle or busy state value.

  Note: Not all usage state values are applicable to every component.

Administrative state

Administration specifies the permission to use or prohibition against using the resource. These permissions are imposed typically through the System Administrator.

The administration state can have one of the following values:

- locked—indicates that the component is administratively prohibited from performing services for its users
- shutting down—use of the resource (or component is administratively permitted to existing instances only. While the system remains in the shutting down state, the manager may at any time cause the object to revert to the unlocked state. This simply provides a state when shutting down a component (or service)—existing users of the component may still be serviced, but any new users are denied the resource that the component provides.
- unlocked—the component is permitted to perform services for its users

  Note 1: The administration of a component operates independently of its operability.

Note 2: Some classes of components may exhibit only a subset of the possible administrative state values.

OSI status

In addition to the three state attributes, six status attributes also exist within OSI. The primary function of these attributes is to provide additional information about a component's operability and usage. These attributes are:

- alarm status
- procedural status
- availability status
- control status
- standby status
- unknown status

Alarm status

Passport implements this attribute as a read-only set-valued attribute. Possible values for the alarms status attribute are:

- empty set—the attribute value appears as empty.
- under repair—the resource is being repaired. The operational state can be either enabled or disabled.
- critical—one or more critical alarms indicating a fault or failure have been detected and have not been cleared. The operational state can be either enabled or disabled.
- major—one or more major alarms indicating a fault have been detected and have not been cleared. These faults can be disabling.
- minor—one or more minor alarms indicating a fault, have been detected and have not been cleared. These faults can be disabling.
- alarm outstanding—one or more alarms have been detected and have not been cleared. The condition may or may not be disabling. If the operational state is enabled, additional component-specific attributes may indicate the nature and cause of the condition.

Procedural status

Passport implements this attribute as a read-only set-valued attribute. Possible values for the alarms status attribute are:

- empty set—the attribute value appears as empty.
- initialization required—the resource requires initialization before it can perform normal function and this has not been initiated. The operator will initiate it. The operational state is disabled.
- not initialized—the resource requires initialization before it can perform normal functions and this has not been initiated. The resource will initialize itself autonomously. The operational state is either disabled or enabled.
- reporting—the resource has completed some operation and is notifying the results (for example, a test process) The operational state is enabled.
- terminating—the resource is in termination phase. If the resource does not initialize itself autonomously, the operational state is disabled; otherwise, it can be either disabled or enabled.

Availability status

Passport implements this attribute as a read-only set-valued attribute. The two most common values are failed and dependency, both of which only apply when the operational state is Disabled. Possible values for availability status are:

- empty set—the attribute value appears as empty.
- in test—the resource is undergoing a test procedure. If the administrative state is locked or shutting down, normal users are precluded from using it and the control status is set to reserved for test.
- failed—the resource has an internal fault that prevents it from operating. The operational state is disabled.
- power off—the resource requires power.
- off line—the resource requires a routine operation to be performed to place it on-line and make it available. The operational state is disabled.

- off duty—the resource has been made inactive by an internal control process in accordance with a time schedule. Under normal conditions, It should come back into operation through the same mechanism. The operational state can be either enabled or disabled.
- dependency—the resource cannot operate because some other resource on which it depends is unavailable. The operational state is disabled.
- degraded—the service available from the resource is degraded in some respect such as speed or operating capacity. However, the service remains available for service. The operational state is enabled.
- not installed—the resource is not present or is incomplete.
- log full—indicates a log full condition as specified by ITU-T Recommendation X.735. Passport components do not use this attribute.

Control status

Passport implements this attribute as a read-only, set-valued attribute. The control status may have the following values:

- empty set—the attribute value appears as empty.
- subject to test—the resource is available to normal users but tests may be conducted simultaneously, causing it to possibly exhibit unusual behavior to users.
- part of services locked—a manager has restricted a particular part of the service from users. The administrative state is unlocked (for example, incoming service barred).
- reserved for test—the resource is administratively unavailable because it is undergoing a test procedure. The administrative state is locked.
- suspended—service is administratively suspended to users.

Standby status

Passport implements this attribute as a read-only, single-valued attribute. The standby status may have one of the following values:

- empty—this is a non-standard value which is used to indicate that the component does not use the attribute or none of the other values apply.
- hot standby—not providing service but operating in sync mode to take over immediately status.

- cold standby—not providing service and not synchronized. It requires some initialization activity.
- providing service—the backup resource is providing service.

Unknown status

This attribute is used to indicate that the state of the resource represented by the managed object is unknown. When the unknown status attribute value is true, the value of the state attributes may not reflect the actual state of the resource.

Summary of Passport OSI state and status attributes

The following table provides a summary of Passport state and status attributes.

Table 5
OSI states and status attributes

Attribute	Values
Operational state	enabled, disabled
Usage state	idle, active, busy
Administrative state	unlocked, locked, shutting down
Alarm status	empty, under repair, critical, major, minor, alarm, outstanding
Procedural status	empty, initialization required, not initialized, initializing, reporting, terminating
Availability status	empty, in text, failed, power off, off line, off duty, dependency, degraded, not installed, log full
Control status	empty, subject to test, part of services locked, reserved for test, suspended.
Standby status	not set, hot standby, cold standby, providing service
Unknown status	true or false

Chapter 5
Passport provisioning system

This section covers the following topics about the Passport provisioning system:

Passport text interface

In the Passport text interface, you can enter commands to configure the node, control the state of system, and perform diagnostic tests. The text interface has two modes: provisioning and operational. In provisioning mode, you enter commands to configure the node. In operational mode, you enter commands to control the state of the system and to perform diagnostic tests. In both modes, you can view alarms, which indicate faults.

The following sections describe the characteristics of the Passport text interface:

Operational mode

When you initially log into a Passport node, you are in operational mode. Passport uses the following command prompt when you are in operational mode:

```
#>
```

where:
is a sequential number assigned to commands

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

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

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

Provisioning mode

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

```
PROV #>
```

where:
is the current command number

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

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

Provisioning views

The Passport provisioning system lets you safely modify the configuration of your node. All the data that makes up a Passport configuration is called a view. Using the provisioning system, you can load views, save views, modify views, and activate a view as the current node configuration. The figure "Provisioning system components and attributes" (page 90) illustrates the components and attributes that represent the provisioning system.

Passport has four types of views:

- current view
- edit view
- committed view
- saved view

The current view is the configuration that is currently running on your node. The edit view is the view that you are currently modifying using the provisioning system and that can potentially become the next current view. A saved view is the view that was saved on the file system. The committed view is the view Passport uses when the node restarts.

The current and edit views are stored in memory. The saved and committed views are stored on the file system. The figure "Location of Passport views" (page 91) illustrates this relationship.

For more information on the Passport provisioning system, see the following sections:

- "Current view" (page 91)
- "Edit view" (page 92)
- "Committed view" (page 94)
- "Saved view" (page 94)

Figure 15
Provisioning system components and attributes

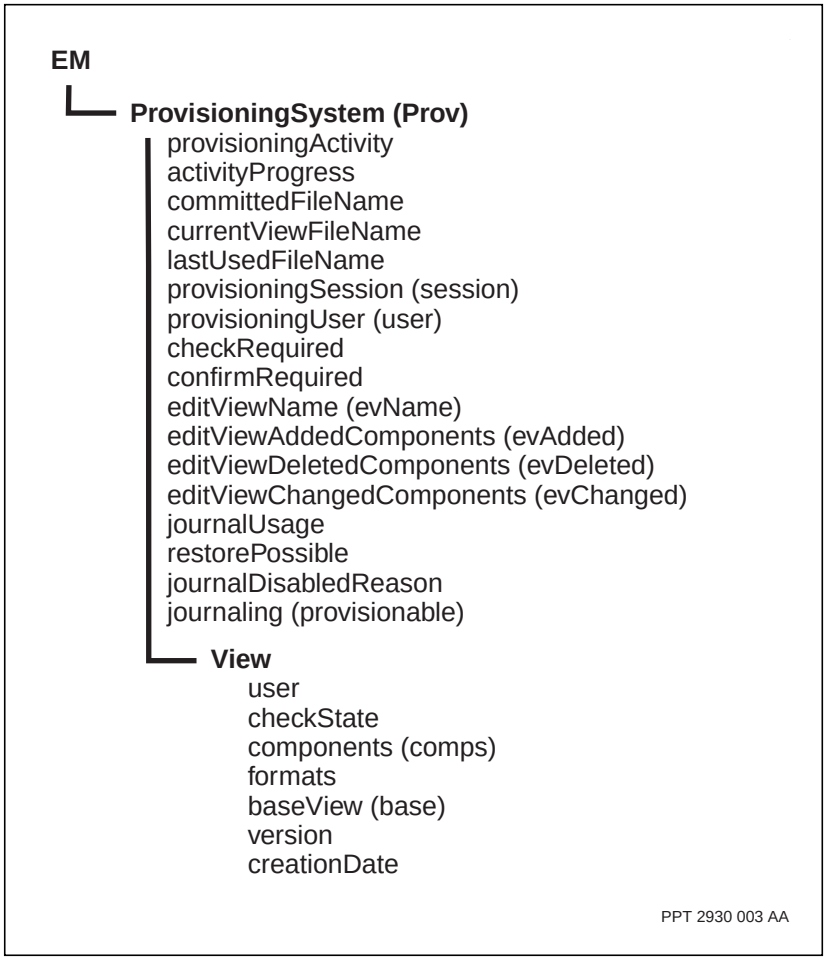
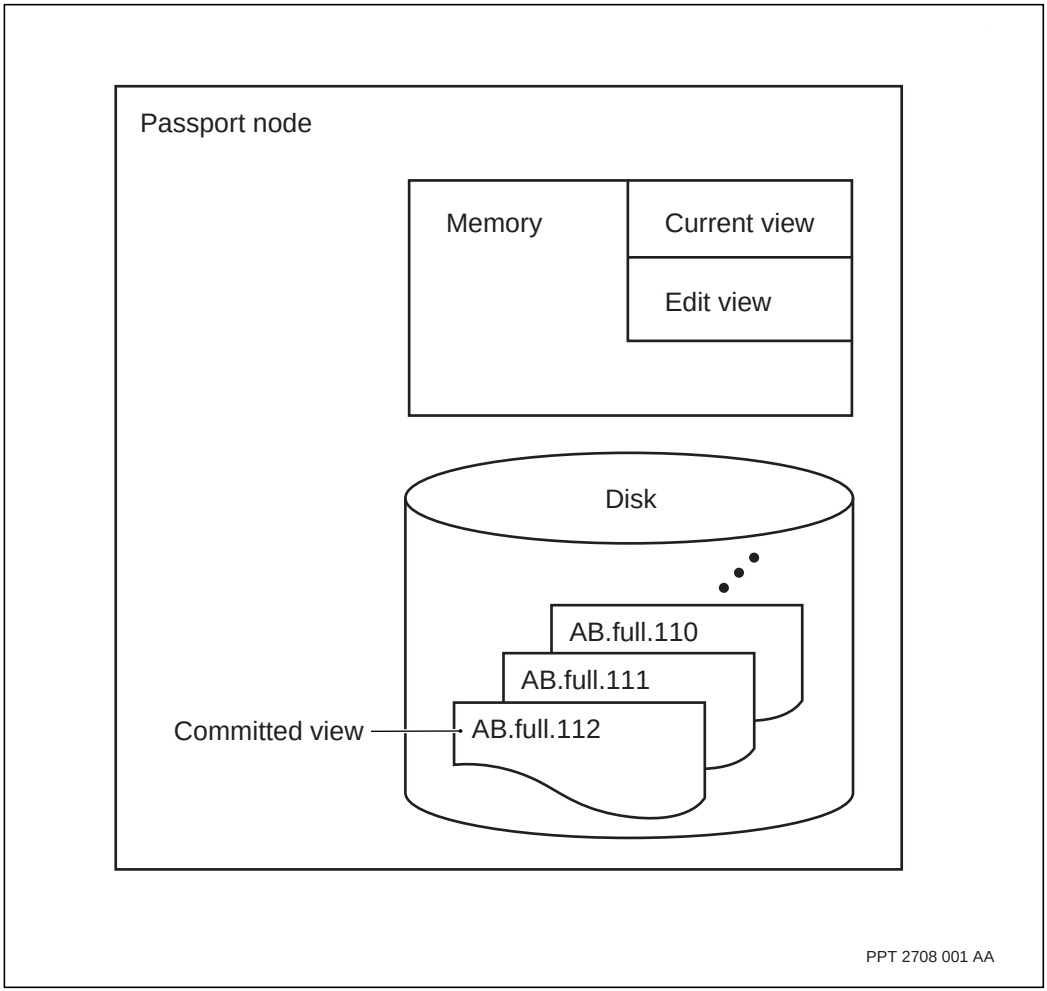


Figure 16
Location of Passport views



Current view

The current view contains the set of provisioned and operational data that defines the current configuration and operating parameters of the Passport node.

The provisioning system controls the provisioned data (provisioned components and attributes) which stores the current configuration. You can view and modify the operational data of the current view (operational components and attributes), but you cannot save it directly to the file system. All operational data, including any modification you have made, is lost when the node restarts, resets, or a control processor switchover occurs.

When you make configuration changes, you do not make them directly to the current view. You modify the edit view using the provisioning system. When you are satisfied with the edit view, you activate it as the new current view. If node recovery is enabled, then the changes you made are automatically journaled to the file system.

You can perform the following actions on the current view using the provisioning system:

- store the current view as a saved view
- commit the current view as the view to use if the node restarts
- copy the current view into the edit view

You perform these actions using provisioning commands.

The only way to change the provisionable components and attributes of the current view is to activate either the edit view or saved view. If you activate an edit or saved view but do not commit it, the committed view becomes the current view on a node reset, restart, or control processor switchover.

The *currentViewFileName* attribute of the *ProvisioningSystem* component indicates the name of the current view if it has been saved to the file system.

Edit view

The edit view is the set of provisioned data representing a node configuration which you can modify. You can make changes to the edit view using the provisioning system without affecting the current node configuration (current view). When you are satisfied with the edit view you can activate it, making it the current view.

Before you can activate an edit view, you must perform a semantic check on it. The semantic check verifies that all the settings in the edit view are self-consistent. If there are problems, the semantic check identifies them and indicates how to fix them. The semantic check also indicates any consequences of activating the edit view. For example, activating an edit view can cause a node restart.

To work with the edit view, you must start a provisioning session by entering into provisioning mode. The *provisioningUser* attribute of the *ProvisioningSystem* component indicates the user ID of the user currently in provisioning mode. Once in provisioning mode, you can perform the following actions to the edit view:

- apply changes stored in a saved view to the edit view
- delete non-permanent components
- add components
- set provisioned attribute values
- copy the current view into the edit view
- perform a semantic check of the edit view
- save the edit view to a saved view
- activate the edit view as the current view, making it the current node configuration

You perform most of these actions using provisioning commands.

The *editViewName* attribute of the *ProvisioningSystem* component indicates the name of the edit view if it has been saved. The *editViewAddedComponents*, *editViewDeletedComponents*, and the *editViewChangedComponents* attributes count the components in the edit view that were added, deleted, or changed from the current view.

When the node restarts, the edit view becomes identical with the current view and the commit view. Unless you save the edit view, any changes you made are lost.

Committed view

The committed view is a saved version of a current view that the node uses when it resets, restarts, or switches over from the active to the standby control processor.

The committed view provides a configuration that is known to work and will allow the node to initialize, as well as connect to the network. This configuration is important when you are trying to activate new configurations. If the new configuration is faulty, the committed view provides a configuration to which the node can return (roll back). After activating a new configuration, you have 20 minutes to confirm that the new configuration has successfully initialized and that the node is operating properly. If you do not confirm the activation within 20 minutes, Passport automatically restarts the node using the committed view.

In some instances, a committed view is not identical to the current view. When you activate an edit view as the current view, the current view and the committed view are different. The current view contains newly updated configuration data, while the committed view contains configuration data based on a previous current view.

Only when you commit the current view are the two views identical. Before you can commit the current view, you must save it to the file system. If you have a dual-CP node, the disks must also be synchronized.

The *committedFileName* attribute of the *ProvisioningSystem* component indicates the file name of the committed view.

Saved view

A saved view is a copy of the current view, edit view, or committed view stored on the file system.

You can save an edit view so you can reopen and change it later. Saving the edit view also means that your configuration changes are not lost in the event of a node restart.

An instance of the *View* component (a subcomponent of *ProvisioningSystem*) represents each saved view stored on the file system. The attributes of the *View* component detail the saved view, including its type, formats, and semantic check state.

There are two types of saved views:

- full saved views
- partial saved views

A full saved view includes all configuration data from either the edit or current view. You can load it into the edit view and activate it as the current view. You can also directly activate a full saved view as long as you semantically checked it before saving it.

A partial saved view includes all the configuration data for a component and all its subcomponents from either the edit or current view. You can load the component from a partial saved view into the edit view to add the component or change an existing component's configuration. You cannot activate a partial saved view.

A single saved view can have several formats. The format of the saved view depends on the options you used when saving the view and whether or not the view is the committed view. The table "Format of saved views" (page 96) describes the possible formats for a saved view.

Saved views are stored in subdirectories and files in the /provisioning directory. When you save a view, Passport assigns it a name, which becomes a subdirectory of the provisioning directory. The subdirectory contains the view in its various formats. For information on naming saved views, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Table 6
Format of saved views

Saved view format	Associated view	Contents and characteristics	Storage format
portable	Current or edit views	Includes all configuration data. A portable saved view can be moved from one Passport node to another, where you can load and further modify it.	Passport internal
ASCII	Current or edit views	Includes all configuration data. You can use views in ASCII format with non-Passport tools to generate configuration printouts.	ASCII
commit	Committed view	Includes all configuration data in the committed view. This format is in a Passport-internal format that enables fast activation.	Passport internal
delta	Edit view	Includes the changes made between the current view and the edit view. This format loads and saves faster than the other formats. You can also apply the changes stored in a delta view to the edit view. You can activate a view stored in this format only if activating it does not require a system restart.	Passport internal
part (partial)	Current or edit views	Includes all information about a component, including all its subcomponents and associated attributes. You can use views in partial format with non-Passport tools to generate configuration printouts.	ASCII

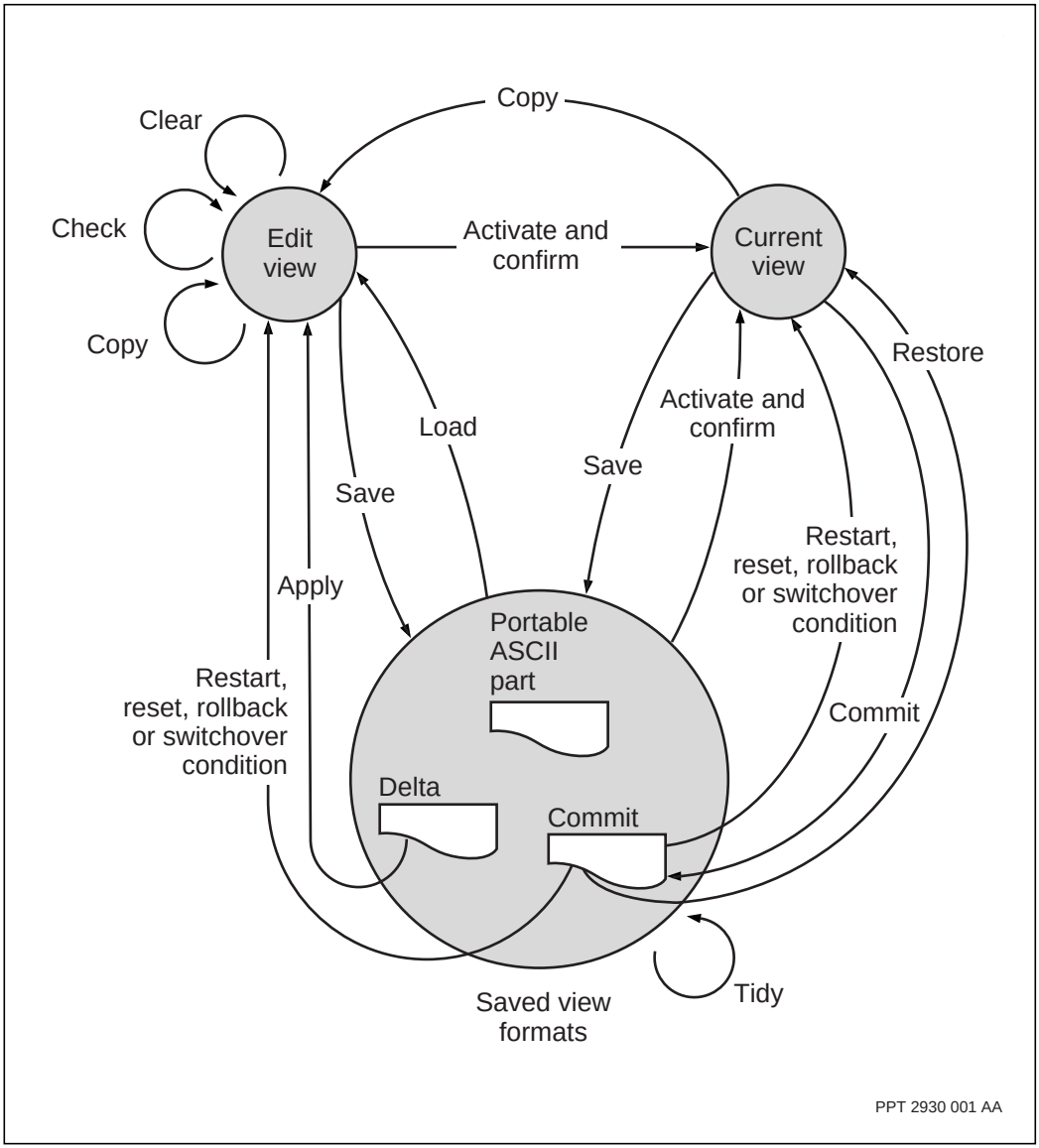
(Sheet 1 of 2)

Table 6 (continued)
Format of saved views

Saved view format	Associated view	Contents and characteristics	Storage format
pre-4.X provisioning files	Current and edit view	Includes all information about the Passport configuration. You can convert Pre-4.X provisioning files to portable or ASCII format (depending on the view type) by loading them into the edit view on the current release.	Passport internal
Note: Pre-4.X files are used with the Passport 7400 series only.			
(Sheet 2 of 2)			

The figure “Relationship between views and provisioning commands” (page 98) illustrates the relationship between provisioning commands and Passport views.

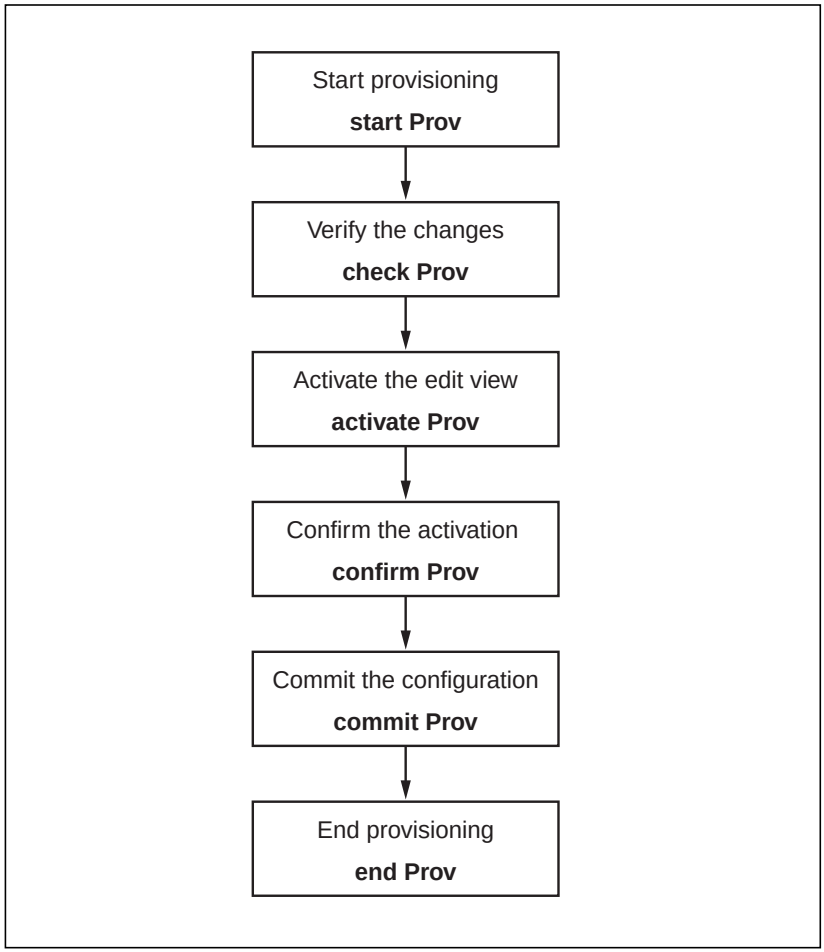
Figure 17
Relationship between views and provisioning commands



Activating and committing configuration changes

The figure “Flowchart for activating configuration changes” (page 99) illustrates the steps you follow when activating configuration changes.

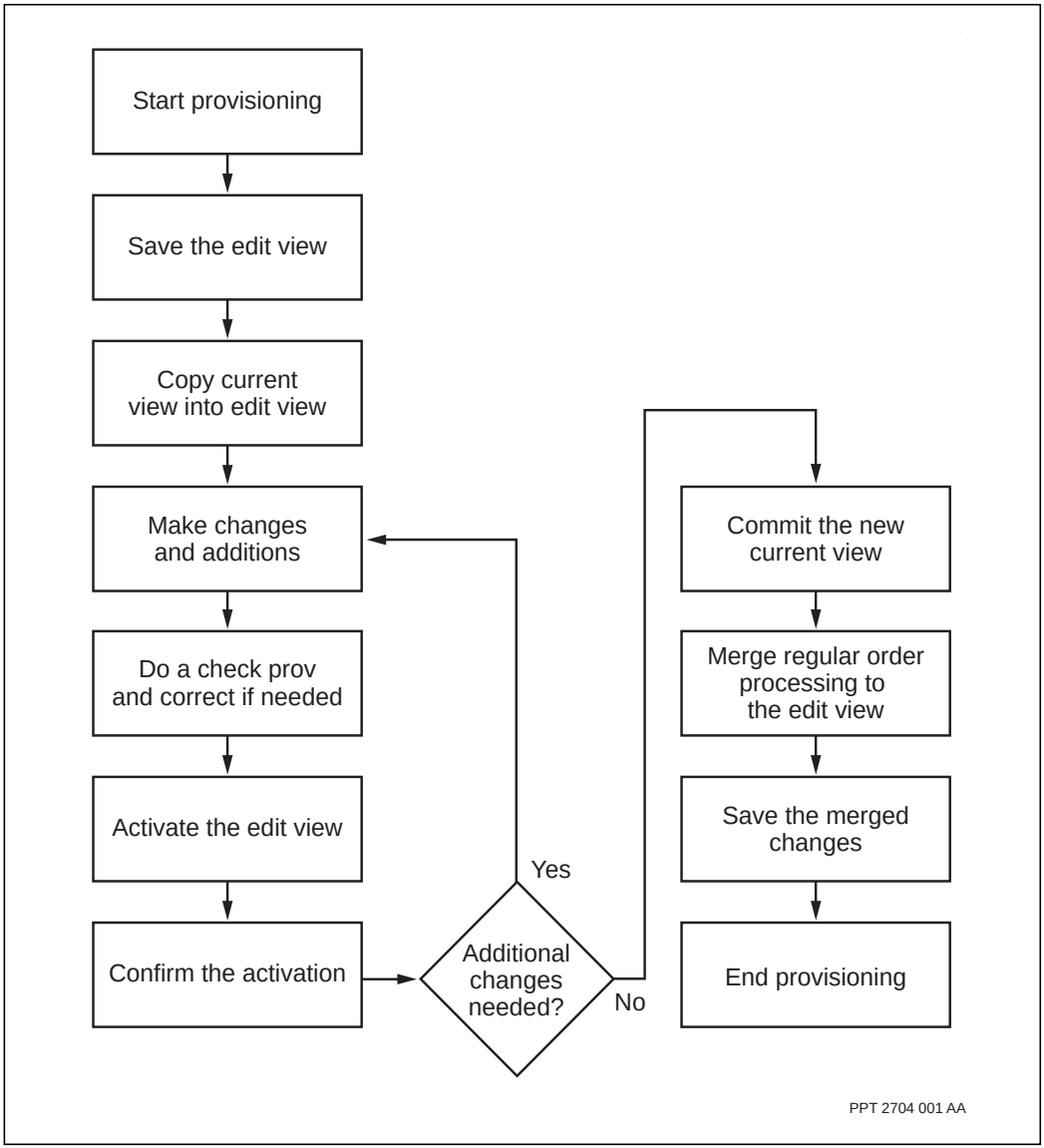
Figure 18
Flowchart for activating configuration changes



Configuring for immediate activation

Once you have completed your immediate activation, you apply the saved changes back into the edit view. The figure “Flowchart for immediate configuration” (page 101) illustrates the process.

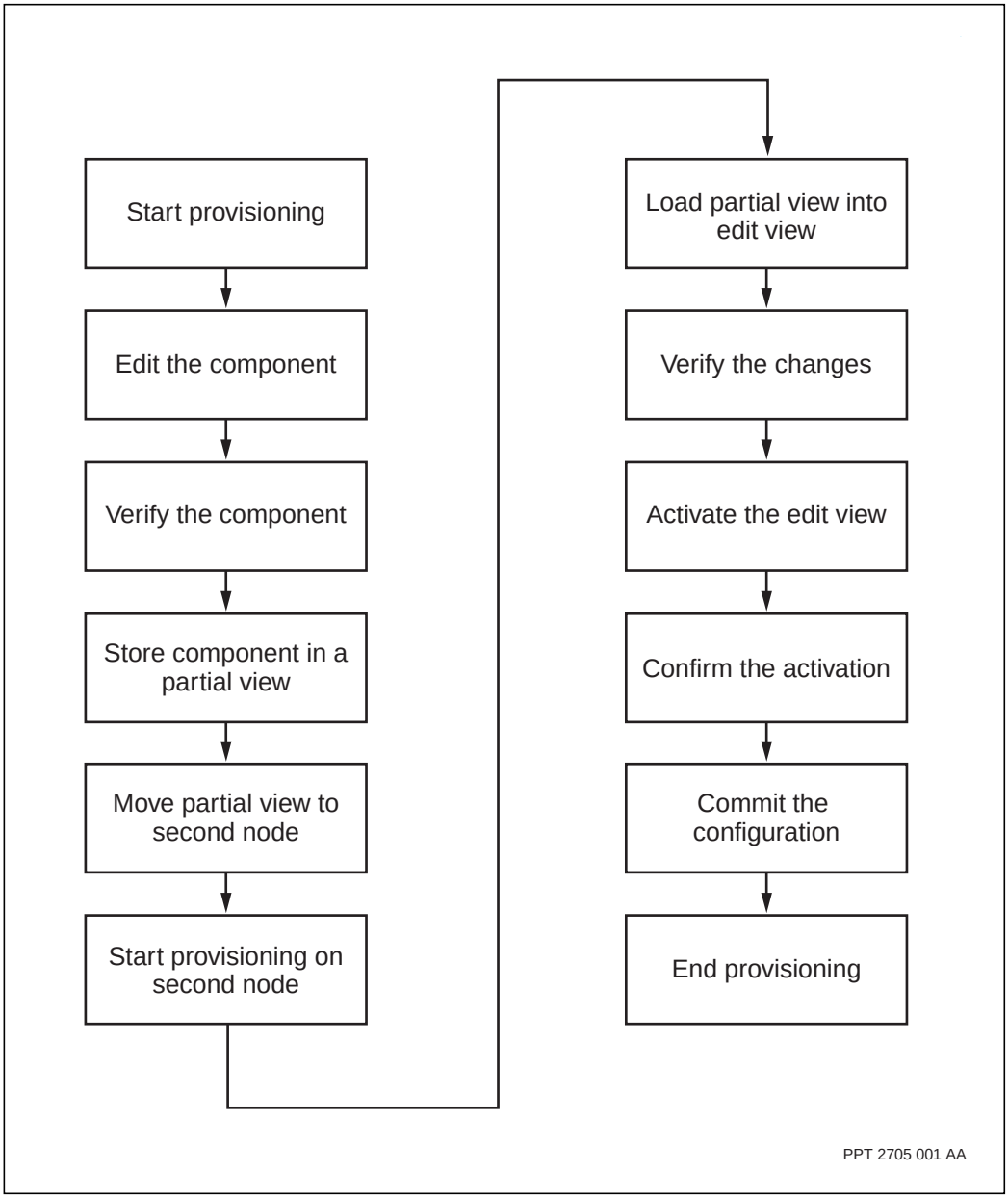
Figure 19
Flowchart for immediate configuration



Copying a component configuration to another node

The figure “Flowchart for using partial views” (page 103) illustrates the steps for developing a configuration for a component on one node and then using that configuration on other nodes in the network.

Figure 20
Flowchart for using partial views



Command basics

Commands are your main interface to Passport when you are working through a VT100 terminal (local interface) or a terminal emulator (telnet interface). They allow you to manage your Passport node, whether you are creating the initial configuration, monitoring alarms, performing maintenance, or adding new capabilities.

The following sections describe important concepts for successfully using Passport commands:

Components and commands

Components represent the hardware, software, and services on your Passport node. Passport commands are always directed at components. Almost every command requires you to specify a component. The commands that do not require a component are implicitly directed at the root component.

The following sections briefly describe components:

For more detailed information on components, see 241-5701-060 *Passport 7400, 15000, 20000 Components*.

Component hierarchy

Components are organized into a hierarchy. Most components have a parent component and one or more subcomponents. For example, the *Shelf* component is the parent of two *Bus* subcomponents. Each *Bus* component also functions as a parent component to a *Test* subcomponent.

The *EM* component is the top component in the hierarchy, and has no parent component. However, in most cases you do not have to specify the *EM* component, so its subcomponents—such as *Shelf* and *ProvisioningSystem*—become the highest in the hierarchy.

Types and instances

When working with components, it is important to understand the difference between component types and instances. A component type is a kind (or a class) of components. A component instance is a particular component of a component type. A type always has one or more instances.

You specify a component using both its type and instance value, separated by a slash (/). An instance value can be made of letters or numbers. For example, the *Card* component type uses numbers, starting at 0, for its instance values. The following text represents instance 0 of the *Card* component type:

```
Card/0
```

Certain component types, such as *Shelf*, can only have one instance. When you use these components, only specify the component type and not an instance value (and without the slash). To specify the *Shelf* component, enter the following:

```
Shelf
```

Multi-indexed components

Some components need more than one instance value to identify them. These multi-indexed components have their multiple instance values separated by commas (,). For example, the *View* subcomponent of the *VirtualRouter Snmp* component requires two instance values, as follows:

```
View/12, 1112
```

Component name

Since components are organized in a hierarchy, a complete component name includes type, instance, and hierarchy information. A component name consists of a number of type-instances pairs, starting from the root component (ignoring the *EM* component) and specifying all the components in the hierarchy. For example, the complete name of instance 0 of the *Card* component type is the following:

```
Shelf Card/0
```

The name of the *Test* subcomponent (which has only one instance) of *Card/0*, is the following:

```
Shelf Card/0 Test
```

Component class

In some cases, you do not need to know the particular instances of a component. A component class defines only the type and hierarchy information about a component, without the instance values. The component class for the *Test* subcomponent of *Card/0*, is the following:

```
Shelf Card Test
```

Attributes

Attributes hold the data associated with a component. For example, the type of card associated with a particular *Card* component is stored in the *cardType* attribute. If *Card/1* is a V.35 card, its *cardType* attribute is V35.

There are two kinds of attributes: operational and provisionable. Operational attributes hold data for monitoring the operation of the Passport node. Usually, the system automatically sets this data, which includes OSI state and statistical information. You can set the values of some operational attributes, but your settings will be lost when the node restarts.

Provisionable attributes hold the configuration data. These attributes define the general parameters and the specific services running on the node. The data in provisionable attributes is preserved during a node restart.

Groups

Related attributes are collected together in groups. For example, all the provisionable attributes of the *Card* component are part of the Provisioned group. Every attribute must be part of a group. Most components have a Provisioned group for its provisionable attributes and an Operational group for its operational attributes.

Verbs

Verbs combine with a component name to specify a command. The verb defines the action of the command. For example, you can combine the list verb with any component to list its subcomponents. To list the subcomponents of the *Shelf* component, use the list verb with the *Shelf* component:

```
list Shelf
```

Command syntax

With only a few exceptions, all commands have two parts: a verb followed by a component name. Some commands also allow you to specify options that modify the function of the command.

The following, then, is the general syntax for a command:

```
<verb> [-<option_name>]... <component_name>
```

Some commands—such as set, display, list, and find—also allow you to specify attributes and groups following the component name.

The following sections describe the syntax for parts of a command:

- "Component syntax" (page 107)
- "Option syntax" (page 108)
- "Attribute and group syntax" (page 108)
- "Saved view filename syntax" (page 109)
- "File and directory syntax" (page 109)

Component syntax

Most commands require a full component name, including type, instance and hierarchy information. The following is the syntax for a component name:

```
<type>/<instance> ...
```

For more information on component names, see “Component name” (page 106).

It is possible to replace instance values or a type-instance pair with a wildcard character in the Display and List commands. For more information, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Some commands, like Help, only require the component class, which has the following syntax:

```
<type>...
```

For more information on component classes, see “Component class” (page 106).

Option syntax

Options always appear between the verb and component parts of a command and begin with a hyphen (-). Some options allow you to specify values, which you must enclose in parenthesis. The syntax for an option with a value is as follows:

```
-<option_name>(<option_value>)
```

For example, when you use the help command, you specify a verb as an option value. To get help on the start verb for the Prov command, you would enter the following command:

```
help -verb(start) Prov
```

If a command can take more than one option, specify each option separated by a space. For example:

```
display -current -noTabular Lp/0
```

Attribute and group syntax

Attributes and groups always appear after the component. You can specify more than one group or attribute by separating them with a comma. The syntax is as follows:

```
<attribute>|<group> [, <attribute>|<group>]...
```

You can mix both groups and attributes in the same command. The following example specifies an attribute (activeCard) and a group (Provisioned):

```
display Lp/0 activeCard, Provisioned
```

Saved view filename syntax

Many of the provisioning commands allow you to work with a previously saved provisioning view. When you save a provisioning view on the file system using the save Prov command, its filename has a specific form. If you want to load the provisioning view, use the following syntax to specify its filename.

```
<name>.<type>.<sequence>
```

where:
<name> is the name of the view
<type> is either full for a full view, or part for a partial view
<sequence> is a three-digit number that differentiates views with this name and type

You would specify the 3rd iteration of the full provisioning view named Basic as follows:

```
Basic.full.003
```

When specifying the filename of a saved view, you must always include the name. If you only specify the name and type, Passport uses the most recent version of the view with that name and type. If you only specify the name, Passport uses the most recent full saved view, unless only partial saved views exist with that name. In that case, Passport uses the most recent partial saved view.

Saved view filenames are case sensitive.

File and directory syntax

Most file system commands require that you specify a file or directory as part of an option. If the file or directory is in the current working directory, you only need to specify its name.

If the file or directory is not in the current working directory, you will have to indicate where the file is located by using its path. You specify a path using a slash character (/) to separate directory names. The highest level, or root directory, is a single slash character (/). For example, to specify the spooled directory, which is a subdirectory of root, use the following syntax:

```
/spooled
```

You can specify a path absolutely, including the full path from the root directory, or relatively. When building a relative path use two dots (..) to refer to the directory above the current working directory. For example, to specify the info.txt file in the directory above the current working directory, use the following syntax:

```
../info.txt
```

You can use more than one set of dots, separated by slashes, to refer to directories more than one level above the current working directory. For example, to specify the info.txt file in the directory two levels above the current working directory, use the following syntax:

```
../../info.txt
```

In some cases, your relative path might simply be the current working directory. You can specify the current working directory using a single dot (.).

When you specify a path, enclose it in quotation marks (“ ”). If you do not enclose the path in quotation marks, Passport will misinterpret the slash (/) characters within the name.

Filenames and directory names are case sensitive. A filename can only contain letters, numbers, the . (dot) character, or the _ (underscore) character.

Command and response lines

There are four pieces of information for every command:

- command line
- component
- command response
- status line

The figure “Sample command and response” (page 112) provides an example of a sample command and all its associated information. The command line is where you enter a Passport command. The prompt for the command line changes depending on whether you are in operational mode (#>) or provisioning mode (PROV #>). In this example, the prompt indicates provisioning mode. For information on commands and their syntax, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

After you enter a command, Passport first responds with the full name of the component affected by the command. In the example, the command affects the *Shelf Card/0* component.

Following the component name is the particular response of the command. Depending on the command, the response can be one line or pages of information. In the example, the command responds with the provisionable attributes of the *Shelf Card/0* component.

The response is followed by a status line. The status line reports the status of the command (ok or command failed) and the date and time (in the YYYY-MM-DD HH:MM:SS.SS format).

If the command is unsuccessful, the status line indicates that the command failed and the response provides details on why it failed. When a command fails because you enter it incorrectly, Passport replaces the command response with the syntax error information. Syntax error information contains the following two pieces of information:

- invalid syntax
- input

The figure “Sample syntax error” (page 112) provides a sample of an incorrectly entered command. The invalid syntax line describes the syntax error. The description has the incorrect part (for example, verb, component, or attribute) of the command in curly brackets ({}) followed by an explanation. In the example, the command contains the incorrect component name *Cord* (instead of *Card*). The invalid syntax line explains that Passport does not recognize the component name.

The input line repeats the command you entered with curly brackets ({}) around the part of the command that Passport cannot interpret. In the example, the unrecognized word Cord has curly brackets around it.

Figure 21
Sample command and response

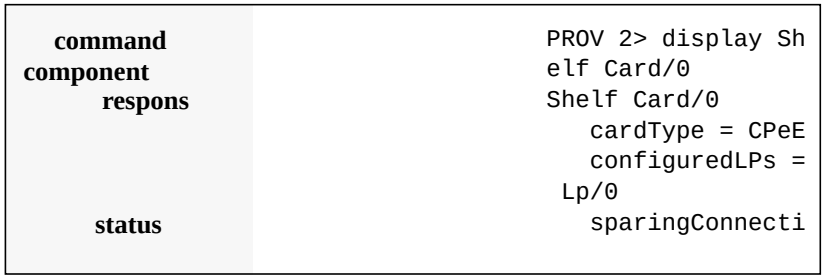


Figure 22
Sample syntax error

```
4> lock Shelf Cord/0
Shelf
Invalid syntax: {component name}
unexpected, value unrecognized.
         Input: lock Shelf {Cord}/0
command failed XXXX-09-
```

Command permissions

To execute a command, you must have the proper permission. Your permission depends on the userid or role you used to log into the Passport node. You can determine your current permissions using the Me command.

The required permission to execute a command depends on the verb and component that combine to form the command.

A Passport command has three types of permission:

- “Impact” (page 113)
- “Scope” (page 113)
- “Customer Identifier” (page 114)

You can determine the impact, scope, and customer identifier requirements of a command by looking up its verb and component in 241-5701-060 *Passport 7400, 15000, 20000 Components*. You can also use by using the help command. For more information on security, see NN10600-605 *Passport - MDM Network Security: Operations*.

Impact

The impact of a command is defined by its verb. To execute a command, you need to have an impact assigned to your userid equal to or greater than the required impact of the verb. The following table shows the five possible verb impacts, from highest to lowest.

Table 7
Verb impacts

Impact	Verbs that
Debug	Are executed by Nortel Networks personnel
System Administration	Change the security of the node
Configuration	Change the configuration of the node
Service	Maintain services
Passive	Display information about the node and services

Scope

The component defines the scope of a command. To execute a command, you need to have a scope equal to or greater than the scope of the component. The following table shows the three possible component scopes, from highest to lowest.

Table 8
Component scopes

Impact	Components that
Network	Affect the operation of the entire network
(Sheet 1 of 2)	

Table 8 (continued)
Component scopes

Impact	Components that
Device	Affect the operation of a Passport node
Application	Affect the operation of a single service application or access port
(Sheet 2 of 2)	

Customer Identifier

Most components have a provisionable customer identifier, that indicates the customer who is allowed to manage the component. The components that do not have a provisionable customer identifier have a default value of zero or use their parent's identification. To execute a command you need to have the same customer identifier as the component specified in the command.

Customer identifiers are numbers from 0 to 8191. Identifier 0 is reserved for the network owner.

Commands and operator modes

Passport has two operator modes: operational and provisioning. You use operational mode to monitor and maintain the node. You use provisioning mode to change the configuration of the node.

Commands can be associated with a particular operator mode. You can only use some commands, such as add and delete, while in provisioning mode. Other commands, such as display and list, work in both modes, but give different results in each.

For additional information on modes, see 241-5701-045 *Passport 7400, 15000, 20000 Management System User Interface Guide*.

Node recovery

The node recovery feature introduces automatic journaling of the current view. That is, a journal log file is created during each manual activation and contains a delta of the configuration changes between the current and edit views. This enables the current view to be manually recovered in the case of a switch reset through the restore Prov command, even if the current view has

not been explicitly saved by the user. This feature, in conjunction with the MDM Node Recovery tool, also enables the current view to be efficiently backed-up and restored in the case of a complete switch failure.

Only configuration changes that have been confirmed can be restored. Note that journal log files are not saved for null activations (where no configuration changes have been made) or for activations that will result in a switch reload, such as a software migration.

The saving of journal log files can become disabled in the following cases:

- when journal log file saving is disabled via provisioning
- when node recovery is enabled after being disabled, an initial commit must be done before the provisioning system can save journal log files (since journals are based on the committed view)
- too many log files were created since last the commit Prov was performed
- a file system error occurs (for example, disk is corrupted or disk is full)
- the file system is locked
- when it is the first manual activation after a switch reload and the current view is different than the committed view (for example, after a software migration, but before the commit)
- when the activation results in a switch reload activation (for example, a software migration activation)

When a new provisioning view is committed, all pre-existing journal log files are automatically removed by the system since the current view is now equal to the committed view and is thus saved.

The journal log files are saved in the following directory: /provisioning/journal/current. Note that this directory only exists if there are journal log files are created.

For information about Node recovery on Preside Multiservice Data Manager, see, 241-6001-807 *Preside MDM Passport/SNMP Devices Backup and Restore User Guide*.

The *maxNumberJournalFiles* attribute of the *ProvisioningSystem* component specifies the maximum number of journal files that can be saved.

The *currentJournal* attribute of the *ProvisioningSystem* component indicates the number of journal log files that have been saved since the last Commit Prov command was issued.

The *restorePossible* attribute of the *ProvisioningSystem* component indicates if it is possible to perform the restore Prov is possible. For more information about this command, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

The *journalDisabledReason* attribute of the *ProvisioningSystem* component indicates whether or not journaling is disabled.

Chapter 6
Passport services

Passport delivers a powerful range of standard-based interfaces and services. Passport services provide the support needed to simultaneously manipulate and manage any mix of voice, data, video and image traffic. Passport provides multiprotocol routing services and intelligent traffic management.

For more information on Passport services see the following sections:

Passport 7400 functionality is expanded by exclusively offering the following services:

Passport frame relay services

Frame relay is a fast access service that provides high-performance connectivity. Frame relay speeds the transmission of frames through the network by transferring processes such as flow control, validation, and error

checking to end devices. Frame relay supports only core communication functions such as transparency, multiplexing, congestion detection, and notification.

Passport frame relay services support both permanent and switched virtual circuits (PVCs and SVCs). PVCs are suitable for high use sites where you determine the connections ahead of time. SVCs establish and remove frame relay connections when required.

See the following sections for more information about Passport frame relay services:

- "Passport frame relay UNI service" (page 118)
- "Passport frame relay NNI service" (page 119)
- "Passport frame relay to ATM service" (page 119)
- "Frame relay ISDN switched access service for Passport 7400" (page 120)

Passport frame relay UNI service

The frame relay user-to-network interface (UNI) service provides a communications interface between a user device and the network. The Passport FR UNI service supports permanent virtual circuit (PVC), switched permanent virtual circuit (SPVC), and switched virtual circuit (SVC) connections.

A PVC is a predetermined logical connection. It remains in place even when not transmitting traffic.

An SPVC is a logical connection whose endpoints are configured by the user, but whose datapath is set up dynamically across networks.

An SVC is a logical connection that is established dynamically, on an as-required basis. User equipment signals the call to the desired destination, relieving the network provider of having to configure the connection. When the connection is no longer required, the subscriber application tears down the SVC.

For more information about the Passport frame relay UNI service, see 241-5701-901 *Passport 7400, 15000, 20000 Frame Relay Fundamentals*.

Passport frame relay NNI service

The Passport frame relay network-to-network interface (NNI) service provides a communication interface between two frame relay networks. This service transmits network status signaling information through the network, and provides end-to-end information about connections that span different frame relay networks. The Passport FR NNI service also ensures multi-vendor network compatibility with networks that conform to the FRF.2 Implementation Agreement.

The Passport FR NNI service supports permanent virtual circuit (PVC), switched permanent virtual circuit (SPVC), and switched virtual circuit (SVC) connections.

A PVC is a predetermined logical connection. It remains in place even when not transmitting traffic.

An SPVC is a logical connection whose endpoints are configured by the user, but whose datapath is set up dynamically across networks.

An SVC is a logical connection that is established dynamically, on an as-required basis. User equipment signals the call to the desired destination, relieving the network provider of having to configure the connection. When the connection is no longer required, the subscriber application tears down the SVC.

For more information about the Passport frame relay NNI service, see 241-5701-901 *Passport 7400, 15000, 20000 Frame Relay Fundamentals*.

Passport frame relay to ATM service

The Passport frame relay to asynchronous transfer mode interworking service (FR-ATM interworking service) transports frame relay traffic over ATM. FR-ATM interworking service improves connectivity between customer frame relay networks and end points, and ATM backbones and end points.

Passport FR-ATM interworking service connects frame relay permanent virtual connections (PVCs) to ATM PVCs. Passport FR-ATM interworking service supports the standard service interworking function (SIWF) FRF.8 and the standard network interworking function (NIWF) FRF.5.

Passport provides

- standard-based frame relay to ATM interoperability
- full local management interface capabilities at the user-to-network interface and network-to-network interface
- full traffic management capabilities
- support of many ATM physical interfaces

For more information about the Passport FR-ATM interworking service, see 241-5701-920 *Passport 7400, 15000, 20000 Frame Relay to ATM Interworking Guide*.

Frame relay ISDN switched access service for Passport 7400

The integrated services digital network (ISDN) technology provides a digital switched access path through an ISDN network. The frame relay ISDN switched access service can support B-channel circuit connections over primary rate interface links as required. The B channel supports the frame relay user-to-network interface (UNI).

Frame relay ISDN switched access service provides

- end-to-end digital transmission
- outbound signaling capabilities
- simple architecture multimedia service
- bandwidth sharing and bandwidth on demand

For more information about the Passport frame relay ISDN switched access service, see 241-5701-901 *Passport 7400, 15000, 20000 Frame Relay Fundamentals*.

Passport ATM services

Asynchronous transfer mode (ATM) is a cell-based switching and multiplexing technology that is a general purpose, connection-oriented data transfer mode. Passport ATM networks are interoperable with the bearer services of other public ATM networks.

Passport ATM supports both static and dynamic networking. Static networking uses permanent virtual circuits (PVC) that you provision on a hop-by-hop basis from end point to end point. Dynamic networking uses soft permanent virtual circuits (SPVC), soft permanent virtual paths (SPVP), and switched virtual circuits (SVC). SPVCs and SPVPs require provisioning at the source end-point only. SVCs are fully dynamic and require no end-point provisioning.

Passport supports three ATM interfaces in addition to the basic types. User-to-network interface (UNI 3.0, 3.1, and 4.0) is the interface between a customer premises equipment (CPE) and the network between nodes on the network edge. UNI uses an interim local management interface for dynamic address registration, and for link and physical layer status, configuration, and control. Interim interswitch signaling protocol (IISP 1.0) is the interface between Passport switches and other ATM switches. IISP builds on UNI and makes static routing possible in a dynamic network. Private network-to-network interface (PNNI 1.0) is the interface between Passport nodes and other ATM switches. PNNI makes routing in a dynamic network possible. PNNI increases network scalability and efficient address summarization.

Passport ATM provides quality of service traffic management. This service also provides automatic and initiated operations, maintenance, and testing capabilities to monitor and control the ATM infrastructure.

For more information about ATM on Passport, see 241-5701-700 *Passport 7400, 15000, 20000 ATM Overview*, 241-5701-702 *Passport 7400, 15000, 20000 ATM Routing and Signaling Fundamentals*, 241-5701-710 *Passport 7400, 15000, 20000 ATM Configuration Guide*, and 241-5701-715 *Passport 7400, 15000, 20000 ATM Monitoring and Troubleshooting Guide*.

Passport ATM services include

- “Passport ATM bearer service” (page 122)

Passport ATM bearer service

The Passport ATM bearer service allows ATM users and external equipment access to the Passport network.

The service provides sequence-preserving connection-oriented cell transfer between a source and destination with an agreed quality of service and throughput. An ATM bearer service connection can be part of a connection that extends into an external ATM network.

An ATM virtual channel connection (VCC) or a virtual path connection (VPC) provides the Passport ATM bearer service between two external ATM users. The external connection can be made with a Passport node or an external network. Each ATM hop in a network assigns VP and VC values to the connection.

For more information about the Passport ATM bearer service, see 241-5701-700 *Passport 7400, 15000, 20000 ATM Overview*.

Passport trunking over ATM service

A logical Passport trunk over ATM is a cell trunk that encapsulates frame trunk traffic through ATM adaptation layer 5 (AAL5) into ATM cells. These logical trunks reroute traffic around failures.

Logical Passport trunking over ATM provides a logical interconnection for Passport nodes over ATM facilities. This trunking service provides the ability to map many trunks to one ATM pipe in a point-to-point method. This service replaces the physical medium of ATM VCC trunks with multiple VCCs supported on a single interface (or port).

You can use the Passport trunking over ATM service instead of leased lines to interconnect Passport nodes. This feature provides the following advantages:

- economy
- high-speed (in excess of 155 Mbit/s) throughput
- increased trunking capacity

For more information about the Passport trunking over ATM service, see 241-5701-700 *Passport 7400, 15000, 20000 ATM Overview*.

Passport inverse multiplexing for ATM service

On Passport, the IMA functionality provides the capability to provision a logical UNI (UNI 3.0, 3.1, and 4.0) to group up to 28 DS1 channels belonging to a DS3 physical link. This allows Passport to support a bandwidth greater than what can be provided by a single DS1 link.

Inverse multiplexing for ATM (IMA) supports the transparent transmission of ATM cell data over IMA link groups. IMA transmits a single data stream of ATM layer cell traffic to multiple DS1 logical links for transmission across the network. At the remote end, IMA orders the cells into their original sequence.

Passport IMA service supports the ATM Forum Inverse Multiplexing for ATM specification.

For more information about Passport IMA service, see 241-5701-730 *Passport 7400, 15000, 20000 Inverse Multiplexing for ATM Guide*.

Passport AAL1 circuit emulation service

The ATM adaptation layer 1 (AAL1) circuit emulation service (CES) transports DS1 and E1 time division multiplexed (TDM) constant bit rate (CBR) data over an ATM network. The service transmits this data at the high-performance level of a dedicated (leased) circuit. Voice and video are examples of CBR data.

Passport AAL1 CES converts structured or unstructured DS1 or E1 circuit data to standard AAL1 cells. AAL1 CES transmits these cells across an ATM network. At the remote end, AAL1 CES converts the data to its original DS1 or E1 circuit form.

AAL1 CES provides

- multivendor interoperability for DS1 or E1 TDM circuits over ATM networks
- the maintenance of leased circuits while gradually evolving the network to full ATM capability

- full DS1 services over ATM networks without changing existing DS1 or E1 terminal equipment

For more information about Passport AAL1 CES, see 241-5701-720 *Passport 7400, 15000, 20000 AAL1 Circuit Emulation Guide*.

Passport IP services

Passport supports IP traffic routing and forwarding over a wide area network (WAN). Passport uses virtual routers (VR) to forward IP packets over a carrier network, and to provide traffic isolation for individual customers sharing switching and transmission resources. Each Passport node can support multiple VRs. In addition, carriers can provide differentiated classes of service for IP traffic and IP virtual private network (VPN) capabilities.

For more information about IP capabilities on Passport, see the following sections:

- "IP over ATM" (page 125)
- "IP over frame relay using frame relay DTE" (page 125)
- "IP over frame relay using IP-optimized DLCIs" (page 125)
- "IP over gigabit Ethernet" (page 125)
- "IP over point-to-point protocol (PPP)" (page 126)
- "IP routing protocols" (page 126)
- "IP class of service (CoS)" (page 126)
- "IP DiffServ" (page 126)
- "IP virtual private networks" (page 126)

For more information about Passport IP services, see 241-5701-805 *Passport 7400, 15000, 20000 Understanding IP* and 241-5701-810 *Passport 7400, 15000, 20000 Configuring IP*.

IP over ATM

Passport supports IP forwarding over ATM in accordance with RFC 1483. You can use the Passport ATM multiprotocol encapsulation (MPE) service to transmit IP frames to external routers or to VRs on different Passport nodes through an ATM network. By default, the frame forwarding decisions for IP traffic over ATM occur on the ATM IP FPs.

The Passport ATM MPE service supports two methods for carrying IP traffic over ATM adaptation layer 5 (AAL5). Logical link control (LLC) encapsulation allows each ATM connection under an ATM MPE interface to carry multiple protocols. Virtual circuit (VC) encapsulation allows each ATM connection under an ATM MPE interface to carry a single protocol type (that is, IP).

IP over frame relay using frame relay DTE

Passport supports IP forwarding over frame relay in accordance with RFC 1490. Frame relay data terminating equipment (FR DTE) access service provides the interface for the customer equipment to the Passport network by using a frame relay connection. You can use this service to connect multiple IP VPNs over a frame relay network.

IP over frame relay using IP-optimized DLCIs

Passport supports IP forwarding over frame relay in accordance with RFC 1490. An IP-optimized data link connection identifier (DLCI) can directly bind to a virtual router protocol port. This type of DLCI is linked to the Passport frame relay user-to-network interface (FRUNI), which eliminates the need for a frame relay DTE and simplifies provisioning.

Due to its flexibility and performance, using IP-optimized DLCIs is the preferred method for frame relay access to an IP VPN.

IP over gigabit Ethernet

Passport supports IP forwarding over gigabit Ethernet in accordance with RFC 894. Gigabit Ethernet is a high-speed facility that supports data transfer rates of up to one gigabit per second. It is used as a direct WAN access vehicle for large enterprises as well as an uplink for aggregating many lower-speed Ethernet end-customers. It is also used as an interface for trunking between edge service nodes and IP core networks.

IP over point-to-point protocol (PPP)

Passport supports IP forwarding over point-to-point protocol (PPP) in accordance with RFC 1661. PPP is a link layer protocol (LLP). It provides a simple, reliable method of transporting IP datagrams by encapsulating them into a high-level data link control (HDLC) frame.

PPP is designed for simple links that transport packets between two peers. These links provide full-duplex (simultaneous and bi-directional) operation and are assumed to deliver packets in order. PPP can provide a common solution for easy connection of a wide variety of hosts, bridges, and routers.

IP routing protocols

Each VR on the Passport node has a separate IP forwarding table and routing database to ensure the isolation of individual customer traffic. In addition to static routes, Passport supports the following dynamic routing protocols:

- routing information protocol (RIP)
- open shortest path first (OSPF)
- border gateway protocol version 4 (BGP-4)

IP class of service (CoS)

Passport supports differentiation of IP traffic for different levels of service. The Passport node examines layer 2, 3, and 4 parameters to classify each IP packet as it enters the node, and can forward these packets with different qualities of service over media that support multiple QoS.

IP DiffServ

IP DiffServ on Passport provides an IP differentiated services framework that delivers traffic management at each node in a network. Each virtual router can be configured to support a set of per-hop-behaviors for handling the flow of IP packets.

IP virtual private networks

An IP VPN consists of multiple customer VRs, each representing a private customer VPN site. Passport supports site-to-site intranet connectivity between customer VRs over the carrier network. Using IP VPN accounting you can measure the volume of IP data sent and received by VPN customers.

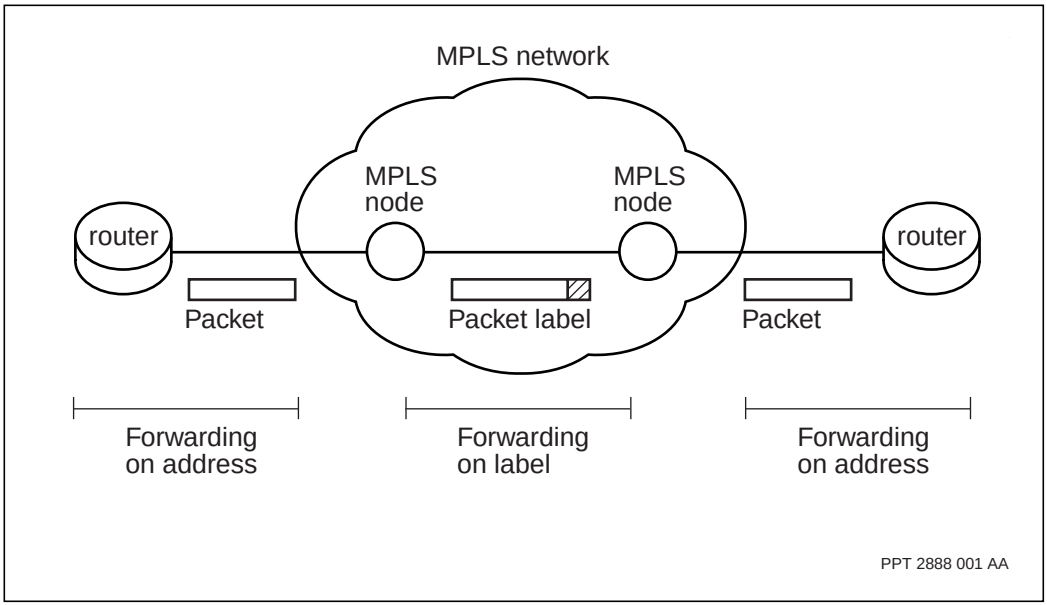
For more information about VPNs, see 241-5701-581 *Passport 7400, 15000, 20000 Basics: VPN Fundamentals* and 241-5701-582 *Passport 7400, 15000, 20000 VPN Configuration Management*.

Multiprotocol label switching

Multiprotocol label switching (MPLS) is a label-swapping, networking technology that forwards packet traffic over multiple, underlying layer-2 media. This technology integrates layer-2 switching and layer-3 routing by linking the layer-2 infrastructure with layer-3 routing characteristics. Layer-3 routing occurs at the edge of the network, and layer-2 switching takes over in the MPLS network core. See Figure 23, "MPLS technology," (page 127).

Essentially, MPLS forwards a packet by swapping labels at each node in its path. MPLS makes it possible to create new label formats without having to change routing protocols. For example, MPLS traffic can include internet protocol (IP), frame relay, ATM, and even optical waveforms.

Figure 23
MPLS technology



In its generic concept, MPLS can switch a frame from any kind of layer-2 link to any other kind of layer-2 link. At this stage in the development of its standards, MPLS supports ATM, frame relay, Ethernet, and point-to-point protocol (PPP). Because traffic flow is independent of the MPLS control protocols, MPLS will be able to support routing protocols that have not yet been defined without any need for the underlying forwarding hardware to change.

With MPLS, layer-3 traffic flows take advantage of the layer-2 traffic engineering abilities and quality of service (QoS) performance, without losing the benefit of existing best-effort, hop-by-hop routing.

MPLS is an emerging standard for network-layer packet forwarding, based on a number of signaling protocols proposed by the Internet Engineering Task Force (IETF). Among these protocols are the label distribution protocol (LDP), border gateway protocol (BGP), resource reservation protocol (RSVP), and constraint-based routing using LDP (CR-LDP). These signaling protocols distribute labels and forward MPLS traffic. The choice of protocol depends on factors such as the location and role of the switching node. In some cases, a node uses more than one distribution protocol.

Packet voice gateway

The Passport packet voice gateway (PVG) application is a carrier-grade integrated voice and data interworking service. Passport PVG creates a gateway between a time division multiplexed (TDM) network and a Passport ATM or IP network.

With Passport PVG, the central office switch still manages the call. However, instead of using TDM bearer channels to transport the traffic, traffic is routed to ATM bearer channels or IP circuits on Passport.

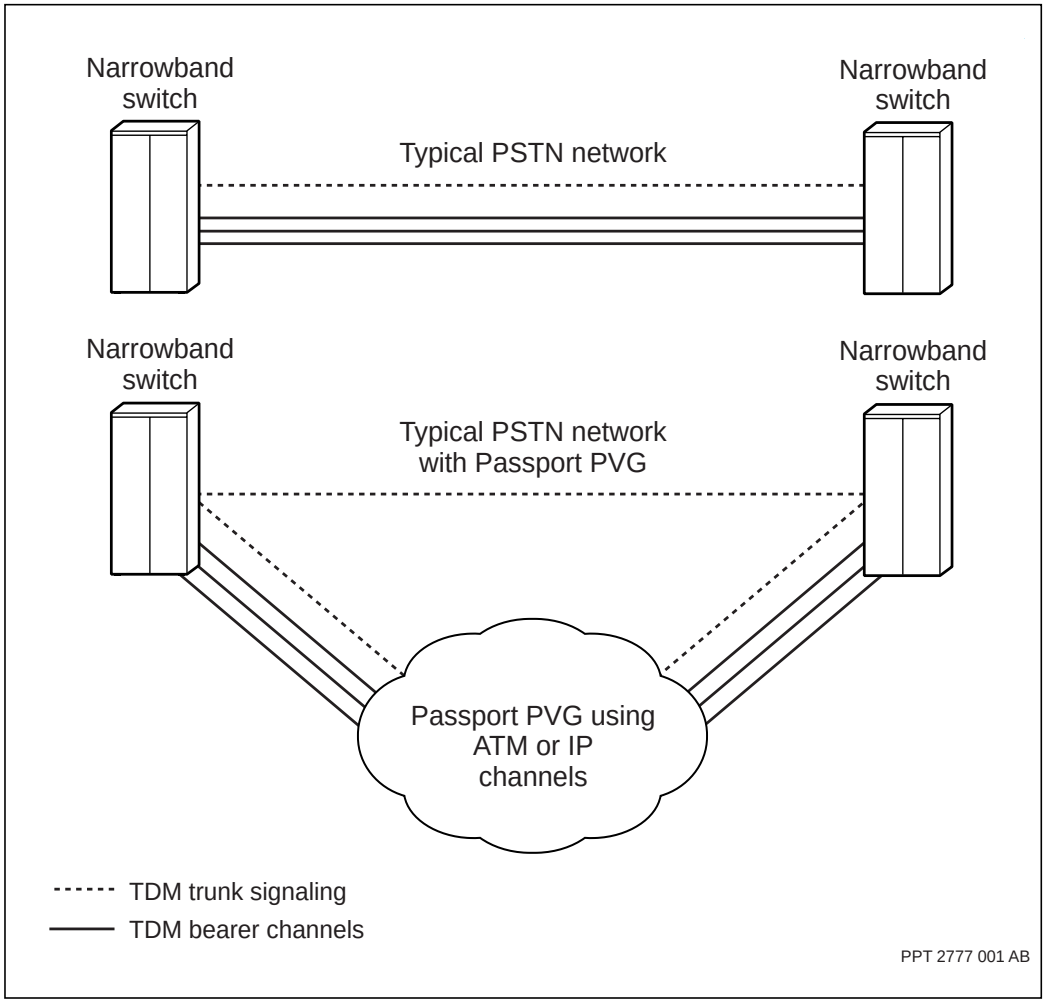
Statistical multiplexing, voice compression, adaptive differential pulse code modulation (ADPCM), silence and fax idle suppression techniques maximize bandwidth savings. Echo cancellation, comfort noise generation, and congestion handling techniques ensure that PVG also delivers toll-quality voice service. (Note that these service are not supported on all variants of Passport PVG.)

The figure “Passport Packet voice gateway configuration” (page 130) shows two scenarios. The top part of the figure shows a typical PSTN network, consisting of narrowband switches that transport TDM signaling trunks and TDM bearer channels.

The bottom part of the figure shows a PSTN network with PVG at work. TDM signaling trunks manage calls and ATM or IP channels transport voice and voice band data traffic over virtual connections. The virtual connections can consist of the following:

- permanent virtual connections (PVC)
- provisioned switched virtual connections (provisioned SVC)
- switched virtual connections (SVC)
- switched permanent virtual connections (SPVC)
- virtual router access point (VRAP)

Figure 24
Passport Packet voice gateway configuration



The following Passport PVG applications are available:

- “Non-switched PVG using ATM” (page 131)
- “Switched PVG using ATM” (page 131)
- “Switched PVG using IP” (page 131)

Non-switched PVG using ATM

In non-switched PVG, narrowband signaling arriving at the Passport switch is statically mapped to an ATM adaptation layer 2 (AAL2) channel. Similarly, each TDM time slot is statically mapped to a particular AAL2 channel identifier (CID) within an ATM virtual channel connection (VCC). Both are transported through the ATM network to another Passport switch. At the remote end, both are mapped back to TDM time slots and passed to another narrowband switch in the service provider network. In this application, narrowband signals do not terminate at the Passport switch, but rather travel transparently over the ATM network.

Switched PVG using ATM

In switched PVG using ATM, an interworking function (IWF) terminates narrowband signaling. This method allows Passport PVG to dynamically create voice and voice band data connections between the service provider's TDM network and the ATM network. Incoming TDM time slots are dynamically mapped to outgoing AAL2 CIDs within an ATM VCC for each call. This mapping can also occur in the reverse direction with incoming CIDs within ATM VCCs being mapped to outgoing TDM time slots.

Switched PVG using IP

In switched PVG using IP, an IWF terminates narrowband signaling similar to switched PVG using ATM. This method allows Passport PVG to dynamically create voice and voice band data connections between the service provider TDM network and the IP network. Incoming TDM time slots are dynamically mapped or switched to outgoing user datagram protocol (UDP) ports for each call. This mapping can also occur in the reverse direction, with incoming UDPs being switched to outgoing TDM time slots.

Multiservice voice platform for Passport 7400

Passport 7400 provides three types of multipurpose voice services:

- "Passport 7400 voice transport service" (page 132)
- "Passport 7400 DCME voice service" (page 132)
- "Passport 7400 Voice networking service" (page 133)

Passport 7400 voice transport service

The Passport voice transport service can multiplex voice traffic onto an integrated backbone network with other traffic types. The voice transport service is based on cell switching techniques. The switching system transmits cells when they contain important digitized voice information. When a voice circuit is inactive, the bandwidth allocated for the circuit is available for other traffic.

The Passport voice transport service handles voice, video, data, image switching, and transport. The service uses a concurrent frame and cell transport technology. To reduce overhead, the service transports data traffic that allows delay changes as variable length frames. The Passport voice transport service transports time-sensitive, constant bit rate (CBR) traffic, such as voice and video, across a Passport network in fixed length cells.

The Passport voice transport service uses a frame-cell trunk interrupting mode method to make sure that voice cells receive priority in an environment that contains a combination of voice and data traffic. The service also ensures that any delay variance introduced between voice cells does not have an effect on voice quality. Passport voice transport uses the path-oriented routing system (PORS) to provide end-to-end paths that allow calculated delay differences and maintain cell order in a selected path. Passport voice transport also uses network clock synchronization to allow the access lines at both ends of a transparent data connection to transmit cells at the same rate.

For more information about the Passport voice transport service, see 241-7401-750 *Passport 7400 Voice Transport Guide*.

Passport 7400 DCME voice service

The Passport DCME voice service communicates both the availability of transmission channels and bandwidth, for a range of call types, to international switching centers (ISCs). Supported call types include voice band (speech, modem, and facsimile), 3.1 kHz audio, and 64 kbit/s unrestricted.

The Passport DCME voice service allows two interconnected Passport nodes to emulate digital circuit multiplication equipment (DCME). International switching centers (ISCs) use DCME to process calls.

Passport provides DCME functionality through support of ITU-T Recommendation Q.50. For more information about the DCME voice service, see 241-7401-760 *Passport 7400 DCME Voice Service Guide*.

The Passport DCME voice service maintains a pool of pre-established path-oriented routing system (PORS) logical connections (LC) across a Passport network to manage bursts of calls from ISCs. And, the Passport DCME voice service can configure new LCs on request. To reduce the bandwidth necessary to transmit pulse code modulation (PCM) encoded audio traffic, the Passport DCME voice service uses compression encoding algorithms.

Passport 7400 Voice networking service

The Passport voice networking service provides routing of voice, modem, facsimile, and data calls through a Passport network to addresses (dialed numbers) provided by the calling PBX. The Passport voice networking service selects the best path through a Passport network using a switched virtual circuit (SVC). Voice networking sets up and tears down an SVC for each new call, releasing bandwidth in the network for subsequent calls. The Passport voice networking service uses the path-oriented routing system and the dynamic packet routing system to route calls between Passport nodes.

The Passport voice networking service allows you to define quality of service parameters based on the dialed number by using compression algorithms and both silence and idle period suppression techniques to increase bandwidth savings. Echo cancellation, comfort noise generation, network loss planning features, and congestion handling techniques provide toll-quality voice.

The Passport voice networking service supports a number of signaling protocols that allow it to communicate with a wide range of PBXs. The Passport voice networking service supports signaling based on both channel associated signaling (CAS) and common channel signaling (CCS) formats.

For more information about voice networking, see 241-7401-755 *Passport 7400 Voice Networking Guide*.

Transparent data services for Passport 7400

Passport transparent data services enable you to consolidate different traffic types over a Passport backbone to reduce bandwidth use and minimize costs. Passport transparent data services use path-oriented routing systems (PORS) and common Passport trunks that normally do not require additional equipment.

The Passport switch provides two transparent data services: bit transparent data service (BTDS) and high-level data link control (HDLC) transparent data service (HTDS). For more information, see the following sections:

- "Passport 7400 HDLC transparent data service" (page 134)
- "Passport 7400 bit transparent data service" (page 134)

Passport 7400 HDLC transparent data service

The high-level data link control (HDLC) transparent data service (HTDS) transmits data using any protocols, including proprietary protocols, that use HDLC at the link layer. The frames travel through an end-to-end connection without a change.

HTDS provides good transfer speeds, low bandwidth requirements, and low costs. Common Passport trunks provide this service without the need for additional customer equipment.

Path oriented routing service (PORS) provides the connection through determined fixed paths. These paths allow a minimum of delay differences in a connection. PORS maintains ordering but does not guarantee delivery. Higher layer protocols are responsible for frame recovery.

For more information about the Passport HDLC transparent data service, see 241-7401-770 *Passport 7400 HDLC Transparent Data Service Guide*.

Passport 7400 bit transparent data service

The bit transparent data service (BTDS) enables you to transmit constant bit rate data, such as video, across a network.

BTDS transfers data between user devices over permanent logical connections. At the source node, Passport formats the data into fixed length cells and transmits them across the network transparently. At the destination node, the cells are reformatted into the original data stream.

BTDS uses the path oriented routing system (PORS) service and network clock synchronization (NCS) service.

For more information about the Passport bit-transparent data service, see 241-7401-775 *Passport 7400 Bit Transparent Data Service Guide*.

Chapter 7
Passport customer services

See the following sections for information about Passport customer services:

Ordering procedures

The following information can help you to produce an order for your Passport hardware and software:

Ordering and delivering process

You can request only those Passport hardware assemblies required for your network. You can upgrade your network by ordering other Passport assemblies to install in your node.

Typically, you receive your Passport node in its bay, with most assemblies installed at your selected site. You must install the control processors and function processors.

Nortel Networks delivers software on CD-ROM to your selected site. The CD-ROM contains the software files described in the supplement report. The supplement report comes with the delivery.

As software changes, you automatically receive a software update on CD-ROM. The software update includes both current and new versions of supported base and application software. The software update replaces the previous release.

> ***Note:*** When you issue a service request (SR) for a software problem, you may receive an emergency fix. Nortel Networks updates fixes to the next version of an application that receives current support. See "Service requests" (page 141) for more information.

You can order documentation with each Passport node. The documentation is available in several formats, including paper and CD-ROM.

Order preparation guidelines and considerations

The following items are guidelines to help you prepare for an order. If necessary, see your account manager during the process.

- Complete all planning and engineering activities to determine your requirements. For more information about planning and engineering, see 241-1501-205 *Passport 15000, 20000 Site Requirements and Preparation Guide* or the 241-7401-200 *Passport 7400 Hardware Description*.
- Make sure that you identify each item and its dependencies.
- Determine your delivery requirements:
  - delivery date according to availability of the equipment
  - destination address of hardware, software, and documentation
  - destination address for billing and accounting information
- Determine your training and support needs.
- Determine licensing requirements for software use.
- Determine and procure additional products for supporting the Passport network (for example, workstations, text interface device, and printers).
- Consult with your Nortel Networks account manager to prepare a purchase order and other documents required to procure Passport.

Finding out more about the Passport products

Your account manager is your primary information resource for determining your needs and possible solutions.

The following resources can answer questions about Passport and other Nortel Networks products:

- Nortel Networks customer service representatives
- http://www.nortelnetworks.com

Nortel Networks support services

Nortel Networks support services can help you with training, problem reporting, and general requests. The following sections provide detailed information:

- "Passport courses" (page 139)
- "Nortel Networks training centers" (page 141)
- "Service requests" (page 141)
- "Nortel Networks technical support groups" (page 142)

Passport courses

Nortel Networks provides training courses in all aspects of Passport operations. These courses are currently evolving to meet customer needs and the expanding product requirements.

Currently Nortel Networks offers the following courses, although these offerings may be replaced as necessary:

- "Passport Overview" (page 140)
- "Operating and Monitoring a Passport Node" (page 140)
- "Provisioning and Maintaining a Passport Node" (page 140)
- "Passport Services, Nodal and Backbone Engineering" (page 140)
- "Passport services courses" (page 141)

For a complete list of courses available, or specific training material information, including schedules and registration details, contact your account prime, or one of the “Nortel Networks training centers” (page 141).

Passport Overview

This course is designed for anyone who needs an introduction to Passport and its functionality. The course covers the following topics: Passport architecture, Passport access services, routing systems overview and network management. It is presented in a downloadable self-study format.

Operating and Monitoring a Passport Node

This course is designed for anyone who needs to monitor and ensure continual operation of a Passport 7400, Passport 15000, or Passport 20000 node.

The course provides an in-depth knowledge of the Passport component architecture. Students develop the skills and knowledge to monitor the node through the use of surveillance tools, and respond to and interpret alarms. A brief overview of the available NMS surveillance tools is provided.

Provisioning and Maintaining a Passport Node

This course is designed for anyone who needs to provision, commission or maintain a Passport node.

The course provides an in-depth knowledge of Passport provisioning, maintenance and troubleshooting. Students will use the command line interface to provision and commission a factory-default Passport. Students will also learn and practice troubleshooting and maintenance procedures.

Passport Services, Nodal and Backbone Engineering

This course is designed for anyone involved in the engineering of Passport networks. After introducing Passport network engineering and a description of Passport hardware and routing systems, the course covers network engineering for both the node, and the backbone. The course also covers network engineering for the following services:

- ATM
- frame relay

- voice
- transparent data services

Passport services courses

There are several services-related courses which will be available for Passport. Please contact your regional training center for more information.

Nortel Networks training centers

Passport training is available on an on-going basis. To register, or for more information, contact one of the Nortel Networks training centers listed in the following table.

Table 9
Nortel Networks training center phone numbers

Area	Country	City	Number
North America (toll-free) *When you call this number, select a product, then choose whether you want information about training or documentation services*	1	877	662-5669
Asia Pacific	61	2	9325-5223
Europe, Middle East, Africa	44(0)	870	550-2501
Caribbean and Latin America			
Brazil	55	19	705-7979
Colombia	57	1	521-4222
Mexico	5	2	5480-8209
Sunrise, FL	1	954	851-8464

Service requests

A change request (CR) allows you to accurately define and report a problem to Nortel Networks. Nortel Networks produces the solution for you. On acceptance, Nortel Networks includes the solution in a future software release.

To open a CR, gather all information necessary to reproduce the problem and then request that your local Nortel Networks technical support group open a CR.

Nortel Networks technical support groups

Passport technical support is available from the Nortel Networks worldwide technical support groups that appear in the table below.

Table 10
Nortel Networks worldwide technical support groups

Area	Center	Address	Telephone
Canada	Training and Documentation Services	3500 Carling Avenue Ottawa, ON K1Y 4H7	Tel.: (877) 662-5669 Web: http:// www.nortelnetworks.com/td
United States	Training and Documentation Services	901 Corporate Centre Drive Raleigh, North Carolina United States 27607	Tel.: (877) 662-5669 Web: http:// www.nortelnetworks.com/td
United Kingdom	Nortel Networks Training Services	Maidenhead Office Park Westacott Way Maidenhead, Berkshire SL6 3QH	Tel.: +44 (0) 1628 438857 Fax: +44 (0) 1628 438894 Web: http:// www.nortelnetworks.com/ servsup/ets/
Asia/Pacific	Nortel Networks Technical Training Centre	Level 5, 380 St. Kilda Road Melbourne, Victoria 3004 Australia	Tel.: +61 3 9206 4646 Fax: +61 3 9206 4844

Passport 7400, 15000, 20000
Overview

Release 5.2

Publication: 241-5701-030
Document status: Standard
Document version: 5.2S2
Document date: March 2004
Printed in Canada

NORTEL NETWORKS