Part No. 317177-A Rev 00
May 2004

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Passport 8000 Series Switch Software Release 3.7

NORTEL NETWORKS™

Copyright © 2004 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, PASSPORT, and Alteon are trademarks of Nortel Networks.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

SSH is a registered trademark and SSH Secure Shell is a registered trademark of SSH Communications Security Corp (www.ssh.com). The use of these trademarks is permitted to describe a product that conforms to the SSH standard and protocol.

Cisco and Cisco Systems are trademarks of Cisco Technology, Inc.

The asterisk after a name denotes a trademarked item.

Contents

Introduction

These release notes for the Nortel Networks* 8000 Series Switch Software Release 3.7 describe the hardware and software capabilities and features introduced in this release and known issues that exist in the release.

For information on how to upgrade your switch to Passport 8000 Series Switch Software Release 3.7, see "Upgrading Passport 8600 switch software" on page 23.

For information on how to upgrade your version of Device Manager, see *Installing and Using Device Manager* (part number 316341-B).

A list of related publications can be found on page 83. The Passport 8000 Series Switch Software Release 3.7 documentation suite can be found on the documentation CD included with your software or on the Nortel Networks technical documentation Web site, www.nortelnetworks.com/documentation. For more information, see the "Reading path" on page 83.

This document contains information about the following topics:

The information in these release notes supersedes applicable information in other documentation.

File names for this release

Table 1 describes the Passport 8000 Series Switch Software Release 3.7 software files and the hardware they support.

Table 1 Passport 8000 Series Switch Software Release 3.7 files and associated hardware

Module or file type	Description	File name
Boot monitor image	CPU and switch fabric firmware for the Passport 8600 routing switch and the Passport 8100 edge switch	p80b3700.img
Runtime image	The Passport 8600 image and the Passport 8100 image	p80a3700.img
3DES	Encryption module, which allows you to use Secure Shell (SSH)	p80c3700.img
DES	Encryption module, which allows you to use the Privacy protocol with SNMPv3	p80c3700.des
MIB	Passport 8600 switch and Passport 8100 switch MIB	p80a3700.mib.txt
SSL cluster upgrade	Passport 8600 clustered SSL modules self-installing runtime image/upgrade v3.7	p80s3700.pkg
SSL boot monitor	Passport 8600 SSL module boot monitor v3.7	p80s3700.img
SSL upgrade instructions	Passport 8600 SSL upgrade instructions v3.7	p80s3700.upgrade

Table 1 Passport 8000 Series Switch Software Release 3.7 files and associated hardware

Module or file type	Description	File name
SSL installation instructions	Passport 8600 complete software package v3.7	p80s3700.install
SSL diagnostics	Passport 8600 SSL diagnostics v3.7	p80s3700.diag
8100 Ethernet module image	Passport 8100 Ethernet code v3.7	p80e3700.dld
POS Ethernet code	Passport 8600 POS Ethernet Code v3.7	p80p3700.dld
ATM Ethernet code	Passport 8600 ATM Ethernet Code	p80t3700.dld
WebOS firmware image	WSM WebOS v10.0.30.7.0 firmware image for the Passport 8600 v3.7	wsm 1003070_mp.img
WebOS binary	WSM WebOS v10.0.30.0 binary image for Passport 8600 3.7	wsm1003070_bin.img
WebOS boot image	WSM WebOS v10.0.30.7 boot image for Passport 8600 3.7	wsm1003070_boot.img
Device Manager software image (Version 5.8.0.0)	Device Manager software image for Windows NT, Windows 98, and Windows 95	jdm_5800.exe

New hardware supported in this release

Table 2 describes the new hardware in this release.

Table 2 New hardware in this release

New hardware	Module part number	Where to find information	Document part number
8692SF Module	DS1404065	*Installing 8600 Switch Modules*	312749-H

8692SF Module

Passport 8000 Series Switch Software Release 3.7 introduces the Passport 8692SF Module. Dual 8692SF switch fabric modules enable a maximum switch bandwidth of 512 Gb/s. Using the Split Multi-Link Trunk (SMLT) protocol in the core, a redundant Passport 8600 switch with two 8692SF Modules can provide over 1 Tb/s of core switching capacity .

Note: You can install the 8692SF Module in slots 5 or 6 of the 8006, 8010, or 8010co chassis. The 8692SF Module is not supported in the 8003 chassis with Passport 8600 Series software Release 3.7.

Note: Passport 8600 Series software does not support configurations of the Passport 8692SF Module, and Passport 8690SF or Passport 8691SF Module installed within the same chassis.

To upgrade to the Passport 8692SF Module, see *Installing Passport 8600 Switch Modules* (part number 312749-H).

New software supported in this release

The Passport 8000 Series Switch Software Release 3.7 adds several significant features to support converged applications (for example, video/multimedia and VoIP) in the following areas:

- Reliability/availability
  - High Availability Layer 3 Phase 2
    - Filters
    - DHCP
    - UDP Forwarding
    - ECMP
    - Layer 3 dynamic routing protocols (RIPv1/v2, OSPF, route redistribution), VRRP
  - Routed SMLT (RSMLT)
  - IEEE802.3ad (also referred to as IEEE 802.3-2002 clause 43)
    - Standard support
    - IEEE 802.3ad/SMLT interaction
    - End-to-end failure detection or VLACP
  - STG/PVST+
- Security
  - IEEE 802.1xEAPoL (includes interaction with Optivity Policy Services (OPS) to support user-based policies)
  - New SNMPv3 agent with “inform” messages
  - CLI logging feature (provides the ability to track modifications made on the switch using CLI)
- Serviceability
  - Remote mirroring (ability to take traffic from a remote switch and send it to a central location in Layer 2 mode for analysis [using tools such as PCAP or IDS/IPS], thereby drastically reducing the cost of ownership)
  - MIB Ping (RFC 2925)
  - Default IP on management/out-of-band interface
  - DNS client

Specifically, this section includes the following topics:

Caution: The 8690SF module is supported only by SF/CPUs with at least 128 MB of memory. The 8690SF module contains only 64 MB of memory and therefore requires a memory upgrade. See your Nortel Networks representative for more information.

High Availability Layer 3 Phase 2

This release provides the second phase of the HA Layer 3. By adding the support of dynamic routing protocols (RIP, OSPF), the support of VRRP and filters, an 8600 chassis with 2 SFs (Switching Fabrics) is now able to recover quickly to an SF failover in a full Layer 3 environment (dynamic multicast routing protocols and BGP will be supported in a subsequent release).

Routed SMLT (RSMLT)

With SMLT, the switch can achieve rapid failover for network failures in Layer 2 environments. This improves availability and allows all links to be active simultaneously.

RSMLT, an extension for SMLT, provides rapid failover for Layer 3 networks, using Layer 3 protocols, such as IP-RIP, IP-OSPF, IP-BGP and IPX-RIP. RSMLT is not dependent on the routing protocol used in the network. The router redundancy is achieved by synchronizing the required forwarding information.

IEEE 802.3ad

IEEE 802.3ad-based link aggregation allows you to aggregate one or more links together to form Link Aggregation Groups, such that a MAC client can treat the Link Aggregation Group as if it were a single link. Although IEEE 802.3ad-based link aggregation and MultiLink Trunking (MLT) features provide similar services, MLT is statically defined, whereas IEEE 802.3ad-based link aggregation is dynamic and provides more functionality through the link aggregation control protocol (LACP). LACP dynamically detects whether links can be aggregated into a link aggregation group and does so when links become available.

IEEE 802.3ad/SMLT interaction

IEEE 802.3ad was designed for point-to-point link aggregation only. Nortel Networks provides extensions to support IEEE 802.3ad in SMLT configurations, thereby allowing any IEEE 802.3ad-capable device to be connected to an SMLT aggregation pair.

Virtual LACP

If an MLT link spans across a service provider network, a MLT failure on one side of the connection is not always detected. By providing an end-to-end failure mechanism based on the LACP protocol, the Passport 8600 provides a unique solution to improve network availability.

Cisco STP/STG/MLT interoperability

The Passport 8600 sends STP BPDUs on all the links of an MLT. Cisco has a different approach, where BPDUs are sent on one link only of the trunk group. This means the two proprietary implementations do not interoperate on an aggregated link with Spanning Tree. To overcome this, a new mode has been introduced in this release.

Per VLAN Spanning Tree plus (PVST+)

Nortel Networks Passport 8600 switches and Cisco System switches both support standards based 802.1d Spanning Tree in addition to supporting proprietary mechanisms for multiple instances of Spanning Tree. Unfortunately, using 802.1d Spanning Tree only provides one instance of spanning that may lead to incomplete connectivity for certain VLANs depending on network topology.

In a network where one or more VLANs span only some of the switches, 802.1d spanning may block a path that is used by a VLAN that doesn't happen to span across all switches.

To get around this issue, the Passport 8600 uses a tagged BPDU address associated with a VLAN tag ID. This ID is applied to one or more VLANs and is used among Passport 8600 switches to prevent loops. The same tagged BPDU address must be configured on all Passport 8600 switches in the network. Cisco Systems proprietary implementation of multiple Spanning Tree is called PVST/ PVST+ or “Per VLAN Spanning Tree,” using a Spanning Tree instance Per VLAN.

With software Release 3.7, the Passport 8600 switch can be configured using either of two methods: Passport 8600 tagged BPDU or PVST+.

Note: Only PVST+ (not PVST) is supported in the Release 3.7.

Similar to the Passport 8600 switch implementation of multiple STP instances, PVST+ uses the standard IEEE 802.1d Spanning Tree for VLAN 1; all other VLANs use PVST+ BPDUs. IEEE 802.1Q VLAN tagging is used to tunnel the multicast PVST+ BPDUs within a 802.1Q region. The standard BPDUs for VLAN 1 are all addressed to the well-known STP multicast address

01-80-C2-00-00-00, while PVST+ BPDUs in other VLANs are addressed to the multicast address of 01-00-0C-CC-CC-CD. IEEE 802.1Q VLAN tagging is used to tunnel the multicast PVST+ BPDUs within a 802.1Q region. PVST+ can be used to load balance the VLANs by changing the VLAN bridge priority.

Note: Nortel Networks is actively working on the 802.1w (RSTP) implementation and the 802.1s (IEEE standard for Multicast Spanning Tree Protocol) implementation. Please contact your Nortel Networks representative for more information.

IEEE 802.1x EAPoL

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access control protocol. This protocol is part of the IEEE 802.1x standard, which defines port-based network access control. EAPoL provides security by preventing users from accessing network resources before they have been authenticated. Without this authentication, users could access a network to assume a valid identity and access confidential material or launch denial of service attacks.

EAPoL allows you to set up network access control on internal LANs and to exchange authentication information between any end station or server connected to the Passport 8600 switch and an authentication server (such as a RADIUS server). This security feature extends the benefits of remote authentication to internal LAN clients. For example, if a new client PC fails the authentication process, EAPoL prevents it from accessing the network.

For information on configuring EAPoL, refer to *Configuring and Managing Security* (part number 314724-C).

Optivity Policy Server interaction with EAPoL

Nortel Networks provides a fully dynamic user-based policy configuration by interfacing EAPoL with the Optivity Policy Server (OPS). After authentication, rules (for example, denying access to a specific server or allowing access to a VoIP server with the highest level of QoS from 8am to 6pm) are dynamically assigned, based on the user ID.

For information on configuring EAPoL works with OPS, refer to *Configuring and Managing Security* (part number 314724-C).

SNMPv3 agent support for RFC compliance

The SNMPv3 agent engine code (Envoy 9.3) for the Passport 8600 switch provides full compliance with the following RFCs:

- RFC 2571
- RFC 2572
- RFC 2573
- RFC 2574
- RFC 2575
- RFC 2576

For information on configuring SNMPv3, refer to *Configuring and Managing Security* (part number 314724-C). For information on upgrading SNMP from versions 3.3 and 3.5 to 3.7, see "Upgrading SNMP from Release 3.3 to Release 3.7" on page 38 and "Upgrading SNMP from Release 3.5 to Release 3.7" on page 39, respectively.

CLI Logging feature (PCMCIA only)

This release allows you to track every CLI modification made locally or remotely (for example, via Telnet or SSH). A dedicated file is created on the PCMCIA and every modification to the configuration will be included into the file, with the following format:

```
Slot5  71  [05/01/03 19:38:07] CONSOLE rwa conf vlan 1
```

The file will be encrypted, and accessible only by **`rwa`** users.

Remote mirroring

Remote mirroring allows you to steer mirrored traffic through a switch cloud to a network analysis probe located on a remote switch. In a network, you can use remote mirroring to monitor many ports from different switches using one network probe device. This is accomplished by encapsulating mirrored packets in

a Remote Mirroring Encapsulation “wrapper.” The encapsulated frame can be bridged though the network to the remote diagnostic termination port. Remote mirroring Encapsulation “wrapper” is 20 bytes in length and consists of a Layer 2 destination address, Layer 2 source address, monitor tag, monitor EtherType, and Monitor Control. The original CRC-32 is stripped from a mirrored packet, and a new CRC-32 is computed over the entire encapsulated frame.

When the mirrored frame is 1522 bytes (1518 plus 4-byte 802.1p/q tag), the resulting maximum frame length is 1542 bytes. To support this, all the nodes in the network should have the capability to handle packets of size 1542. At the termination port, the encapsulation is removed before sending it out of the port. Source port for Remote Mirroring is called Remote Mirroring Source (RMS) while the destination port is called Remote Mirroring Termination (RMT).

MIB Ping

The MIB ping defined in the RFC 2925 is supported in this release. This MIB allows you to ping a remote device from the Passport 8600 switch and verify the connectivity from the switch itself.

Static IP address for management port

If the boot.cfg file is not present on the flash, the network management port (also referred to as the Out-of-Band [OOB] interface) is assigned a default IP address (192.168.168.168/24 for slot 5 or slot 3 and 192.168.168.169 for slot 6). If an IP address is already configured for this interface in the boot.cfg, the switch will use this address.

DNS client

Every equipment interface connected to a TCP/IP network is identified with a unique IP address. A name can be assigned to every machine having an IP address. The TCP/IP protocol does not require the use of names, but these names helps network managers quickly map IP addresses to these names.

Two methods are used by the Passport 8000 Series switch to establish the mapping between an IP name and an IP address: the flash/etc/hosts file and the DNS (Domain Name Service). The DNS is a hierarchical database that can be distributed on several servers (for backup and load sharing).

Mapping of IP name and IP address modifies the application to use a hostname instead of IP address. The hostname is converted to an IP address by the switch. If the entry for translating the hostname to IP address is not found in the hosts file, the switch queries the configured DNS server for the mapping from hostname to IP address. You can configure up to 3 different DNS servers: Primary, Secondary and Tertiary. The primary server is queried first, followed by the secondary and tertiary servers.

Nortel Networks does not provide a default hosts file on the system. The format is similar to the one used in a UNIX workstation. You can use the editor provided on the system to create, save, or modify such a file.

Supported software and hardware capabilities

Table 3 lists the supported software and hardware capabilities.

Table 3 Supported capabilities in the Passport 8600 switch (Release 3.7)

Feature	Maximum number supported
Hardware records	Non E / E Modules: 25 000 records M Modules : 125 000 records[1]
M Modules	Nortel Networks strongly recommends using 8691SFs or 8692SFs with M Modules
10GE	Release 3.7 does NOT support the combination of the following features and the 10GE Module: - IPX routing - SMLT - External MLT (Nortel Networks recommends that you use a Layer 3 routing protocol for resiliency, like OSPF, associated to ECMP, Equal Cost Multi Path) - Egress Mirroring Due to the internal architecture, Nortel Networks strongly recommends using 2 8691SFs/8692SFs per system using a 10GE Module (internal MLT of 8 Gig ports) for load sharing and redundancy.
VLANs	Passport 8100: 2013 Passport 8600: 1980
IP subnet based VLANs (Passport 8600 only)	200

Table 3 Supported capabilities in the Passport 8600 switch (Release 3.7) (continued)

Feature	Maximum number supported
IP Interfaces (Passport 8600 only)	• 500 (default) • 1980 (requires order number DS1411015: Passport 8000 Chassis MAC Address Upgrade Kit. License for reprogramming the chassis to a block of 4096 addresses for routed VLAN scaling)
RIP Routes (Passport 8600 only)	2500
OSPF Areas per Switch (Passport 8600 only)	5
OSPF Adjacencies per switch (Passport 8600 only)	80
OSPF Routes per switch (Passport 8600 only)	Non E / E modules: 15 000 M Module: 20 000
BGP (Passport 8600 only)	Number of peers: 10 Number of routes: - Non E / E Modules : 20 000 - M Modules : 119 000
DVMRP Interfaces (Passport 8600 only)	500
DVMRP Routes (Passport 8600 only)	2500
PIM Interfaces (Passport 8600 only)	500
Multicast source subnet trees (Passport 8600 only)	500
Multicast (S,G) DVMRP	1980
Multicast (S,G) PIM	500
IPX Interfaces (Passport 8600 only)	100
IPX RIP (Passport 8600 only)	5000
IPX SAP (Passport 8600 only)	7500
VRRP Interfaces (Passport 8600 only)	255
Spanning Tree Groups	Passport 8600: 25[2] Passport 8100: 1
Aggregation Groups - IEEE 802.3ad aggregation groups - Multi Link Trunking group (MLT)	Passport 8600: 32 Passport 8100: 6 Redirection: 3

Table 3 Supported capabilities in the Passport 8600 switch (Release 3.7) (continued)

Feature	Maximum number supported
Ports per MLT Note: all the ports MUST be of the same type (no mix of technology will be supported)	Passport 8600: up to 8 Passport 8100: up to 4
Permanent virtual circuits scaling (ATM)	Passport 8600 and Passport 8100: up to 500 permanent virtual circuits (PVCs) per chassis. • 256 RFC1483 bridged/routed ELANs per MDA • 500 RFC1483 bridged/routed ELANs per switch (12 more RFC1483 bridged ELANs per switch can be configured) • 64 PVCs per RFC1483 bridged ELAN • 1 PVC per RFC 1483 routed ELAN

1 The exact number is 125838. 2162 records are used by the system. With the record reservation feature, 8K records are pre allocated (see the documentation for more information) for some specific types of traffic (for example, MAC and ARP).

2 Nortel Networks supports only 25 STGs with Release 3.7. You can configure up to 64 (63 with the WSM Module) STGs, but configurations including more than 25 STGs will not be supported. If you do need more than 25 STGs, contact your Nortel Networks Sales Representative for more information about the support of this feature. With Release 3.7 (8600) and 10.0 (WSM), the WSM Module supports the tagged BPDU from the 8600 only with the default STG (STG ID 1).

Passport 8000 Series Software Release 3.7 does not support configurations of Passport 8100 modules and Passport 8600 modules simultaneously within the same chassis.

The Web Switching Module is not supported in Passport 8100 nor in 8100 module configurations.

3 The number of aggregation groups decreases when you install a WSM module into the chassis. Refer to the WSM configuration manual for more information about how to connect through the backplane and the logical configuration (VLAN/STGs)

Supported standards, RFCs, and MIBs

This section identifies the 802 standards, RFCs, and network management MIBs supported in this release.

Table 4 lists the supported standards.

Table 4 Supported standards

Supported standards	
802.3 CSMA/CD Ethernet	ISO/IEC 8802-3
802.3i 10BaseT	ISO/IEC 8802-3
802.3u 100BaseT	ISO/IEC 8802-3
802.3z	Gigabit Ethernet
802.3ab	Gigabit Ethernet 1000BaseT 4 pair Cat5 UTP
802.3ae	10 Gigabit Ethernet
802.1Q and 802.1p	VLAN tagging and prioritization
802.3ab	Gigabit Ethernet Over Copper
802.3x	Flow Control
802.1D	MAC bridges/spanning tree protocol
802.3ad	Link Aggregation Control Protocol
802.1x	Extended Authentication Protocol

Table 5 lists the protocol RFCs supported in this release.

Table 5 Supported protocol RFCs

Supported protocol RFCs	
RFC 768	UDP protocol
RFC 783	TFTP protocol
RFC 791	IP protocol
RFC 792	ICMP
RFC 793	TCP protocol
RFC 826	ARP protocol
RFC 854	Telnet protocol
RFC 903	Reverse ARP
RFC 1541 and 1542	BootP and DHCP
RFC 1542	BootP
RFC 1058	RIP version 1
RFC 1075	DVMRP
RFC 1112	IGMPv1
RFC 2236	IGMPv2
RFC 3376	IGMPv3
draft-holbrook-idmr-igmpv3-ssm-02.txt	IGMPv3 for SSM
RFC 2178	OSPFv2
RFC 1723	RIPv2
RFC 1771 and 1772	BGP-4
RFC 1745	BGP-4 and OSPF interaction
RFC 1812	Router requirements
RFC1965	BGP-4 Confederations
RFC1966	BGP-4 Route Reflectors
RFC 1997	BGP-4 Community Attributes
RFC 2270	BGP-4 Dedicated AS for sites/single provider
RFC 2385	BGP-4 MD5 authentication
RFC 2439	BGP-4 Route Flap Dampening
RFC 1866	Hypertext Markup Language v2.0
RFC 2068	Hypertext Transfer Protocol

Table 5 Supported protocol RFCs

Supported protocol RFCs	
RFC 2131	Dynamic Host Control Protocol (DHCP)
RFC 2338	Virtual Router Redundancy Protocol
RFC 2362	PIM-SM
RFC 3208 (draft-speakman-pgm-spec-04)	PGM
RFC 3569 (draft-ietf-ssm-arch-03.txt)	PIM-SSM
RFC 2474 and 2475	DiffServ
RFC 2597 and 2598	DiffServ per hop behavior
RFC 2138	RADIUS Authentication
RFC 2139	RADIUS Accounting
RFC 1591	DNS Client

Table 6 lists the ATM POS module RFCs supported in this release.

Table 6 Supported ATM POS module RFCs

Supported ATM POS module RFCs	
RFC 1332	IPCP
RFC 1471	LCP
RFC 1473	NCP
RFC 1474	Bridge NCP
RFC 1552	IPXCP
RFC 1661	PPP
RFC 1638	BCP
RFC 1989	PPP Link Quality Monitoring
RFC 2558	SONET/SDH
RFC 2615	PPP over SONET/SDH

Table 7 lists the network management MIBs and standards supported in this release.

Table 7 Supported network management MIBs

Supported MIBs	
RFC 1155.mib	SMI
RFC 1157	SNMP
RFC1213.mib	MIB for networks management of TCP/IP-based internets MIB2
RFC 1215.mib	A convention for defining traps for use with the SNMP
RFC 1493.mib	Definitions of management objects for bridges
RFC 1573.mib	Interface MIB
RFC 1643.mib	Definitions of managed objects for the Ethernet-like interface types
RFC 1724.mib	RIPv2 MIB extension
RFC 1757.mib	Remote network monitoring MIB (support of alarms, events, statistics, and history groups)
RFC 1389.mib	OSPFv2 MIB
RFC 1907	SNMPv2
RFC 2021	RMON MIB using SMIv2
RFC 2096.mib	IP forwarding table MIB
RFC 2233.mib	The interfaces group MIB using SMIv2
RFC 2674.mib	Definitions of management objects for bridges with traffic classes, multicast filtering and virtual LAN extensions
RFC 2932.mib	IPv4 multicast routing MIB
RFC 2933.mib	Internet Group Management Protocol MIB
RFC 2934.mib	PIM MIB
RFC 2571, 2572, 2573, 2574, 2575, 2576	SNMPv3
RFC 2674	Definitions of Managed Object for bridges with Traffic Classes, Multicast Filtering, and Virtual LAN extensions
RFC 2925.mib	Ping and Traceroute MIBs

Upgrading Passport 8600 switch software

General upgrade considerations

Warning: The configuration file generated with Passport 8000 Switch Series Software Release 3.7 contains options that are not backward compatible with Passport 8000 Series Software Releases 3.0.*x*, 3.1.*x*, 3.2.*x*, 3.3.*x*, or 3.5.*x*. Loading a 3.7 configuration file on a 3.0.x or 3.1.x run-time image generates errors and causes the image to abort loading the configuration file.

As a precaution, before you upgrade or downgrade your switch software, make a copy of the switch configuration file specified in the boot.cfg file, using the following command:

```
copy /flash/config.cfg/<device>/
config_backup.cfg
```

where *device* can be PCMCIA, flash, or an IP host.

- If the flash on your system has never been reformatted since the upgrade to the 3.2.2 Release (May 2002) or higher, Nortel Networks highly recommends that you do so before upgrading to the Release 3.7. In some very rare cases, you may not be able to access the switch files. The file access problem may be prevented if you perform this operation. (Q00736836)
- After you upgrade your Passport 8000 Series software, make sure you save the configuration file.
- Nortel Networks does not support different software versions, for example Releases 3.3.2 and 3.7, on the master and standby CPU. Also, the master and standby CPU must have the same amount of memory.
- When installing files on the on-board flash or PCMCIA, make sure that you verify flash capacity before downloading the files.
- With releases prior to 3.7, a switch coming from the factory first checks for the IP address of its management port (Out of Band or OOB) in the boot.cfg (flash). If it does not find one there, it checks the boot.cfg file in the PCMCIA.

In Release 3.7, the switch checks for an IP address using the following procedure:

a The switch checks the boot configuration file pcmboot.cfg in the PCMCIA. The pcmboot.cfg file, which has the same syntax as the boot.cfg file, must be created.

b If the switch does not find it in the pcmboot.cfg file, it checks for the address in the boot.cfg file in flash.

c If the switch does not find it in the boot.cfg file in flash, it checks for an address in the boot.cfg file in the PCMCIA.

d If the switch does not find it in the boot.cfg file in the PCMCIA, it attempts to get the IP address for the management port through BootP.

The default IP address for the management port is now 192.168.168.168/24 for slots 3 and 5, and 192.168.168.169/24 for slot 6.

- Because of the DNS implementation in Release 3.7, the CLI **`peer`** command is not available unless you add the peer IP address in a new file called flash/etc/hosts. You must create this file; no default file exists. You can manually create it using a simple text editor, like the one provided by the Passport 8600. See Figure 1 for an example of this file. For the CPU in slot 5, the peer address corresponds to 127.0.0.6. For the CPU in slot 6, the peer address corresponds to 127.0.0.5. Note that if you swap the CPU (going from slot 5 to 6), you have to manually modify the address in the file. (Q00880678)

Figure 1 Sample flash/etc/hosts file

```
198.202.188.44 inthp04.labpc.ernet.in labpc
206.236.134.194 inthp04.labpc1.ernet.in lacpc
198.202.188.174 ipksun05.accelar.wall.com ipksun05
198.202.188.34 dhcp.accelar.wall.com dhcpserver
127.0.0.6 peer cpuslot6
```

The following sections include:

Upgrading the boot flash image file

The following section shows an example of the input required to upgrade the boot flash image in your Passport 8000 Series switch and shows the command line interface (CLI) output as the upgrade is performed.

Caution: Do not attempt to downgrade an 8692SF image to Passport 8000 Series switch code that is earlier than Release 3.7. Doing so may yield unexpected results.

```
monitor#
monitor# boot /flash/p80b3700.img
Loading /flash/p80b3700.img ... xxxxxx to yyyyyyy (yyyyyyy)
Starting at 0x10000...

################ 8K CPU BOOT FLASH Update ################

File p80b3700.rom found in loaded image
File size: xxxxxx bytes
Number of flash sectors to be programmed: 10

WARNING: You are about to re-program your Boot Monitor FLASH
             image.  Do NOT turn off power or press reset
             until this procedure is completed.  Otherwise
             the card may be permanently damaged!!!

Press <Return> to stop monitor upgrade....
erased 10 sectors of bootflash
programmed bootflash
Verifying new BOOTFLASH Image...
xxxxxx matches, 0 mismatches
Update complete!

Press return to reboot

Copyright (c) 2002 Nortel Networks, Inc.
CPU Slot 3:    PPC 740 Map B
Version:       3.7.0.0/055
Creation Time: May 13 2004, 02:15:39
Hardware Time: May 15 2004, 11:10:44 UTC
Memory Size:   0x04000000
Start Type:    cold
/flash/ - Volume is OK
Loaded boot configuration from file /flash/boot.cfg
```

Upgrading the software image on a non-redundant 8600 CPU

Before upgrading your 8600 switch CPU:

- Save the configuration file currently used by the switch in memory by entering the following command *at the switch prompt:*

  save config file /<*device*>/<*config file name*>

- Copy the configuration file specified by the boot.cfg file, by entering the following command:

  copy /<*device*>/<*config file name*> /<*device*>/<*backup config file name*>

  where:

  device is flash or PCMCIA.

To upgrade the non-redundant 8600 CPU with the Release 3.7 software image:

1. Download the Passport 8600 CPU boot monitor and Passport 8600 runtime image to a TFTP server.
2. Copy the image and boot files from the TFTP server to flash using the following command:

   copy <*tftpServerIPAddr*>:<*filename*> /flash/<*filename*>

   For example, you use the following commands to copy the main image and boot files from TFTP server 10.10.10.1 to flash:

   ```
   copy 10.10.10.1:p80a3700.img /flash/p80a3700.img
   copy 10.10.10.1:p80b3700.img /flash/p80b3700.img
   ```

   Use the above commands to copy all other files (ATM, POS, and so forth).

3. Verify that the software has been copied to the CPU by using the following command:

   dir

4 Change the primary runtime image for the Passport 8600 using the following command:

config bootconfig choice primary image-file /*<location>*/filename

For example, use the following command to change the primary image file to p80a3700.img:

config bootconfig choice primary image-file /flash/ p80a3700.img

5 Save boot config using the following command:

save bootconfig

6 Boot the 8000 Series switch with the boot-monitor image you downloaded previously in Step 2.

Enter the following command to boot the p80b3700.img file from flash

boot /flash/p80b3700.img

The screen displays the following message:

```
WARNING: You are about to re-program your Boot Monitor
FLASH image. Do NOT turn off power or press reset until
this procedure is completed. Otherwise the card may be
permanently damaged!!!
```

7 Save the boot.cfg file to flash using the following **save** command:

save bootconfig

8 Reboot the switch using the CLI command **boot -y**.

Caution: The configuration file generated with software Release 3.7 contains options that are not backward compatible with software release 3.0.x, 3.1.x, 3.2.x, 3.3.x, or 3.5.x. Loading a 3.7 configuration file on a 3.0.x, 3.1x, 3.2.x, 3.3.x, or 3.5.x run-time image generates errors and causes the image to abort loading the configuration file.

Upgrading the software image on a redundant 8600 CPU in HA mode

Note: Hitless upgrade is not supported in a single chassis with two SFs.

Before upgrading in HA mode, be sure you set the `ha-cpu` and `savetostandby` flags to `true` (enabled). To check if these flags are set to `true`, use the CLI command **`config boot flags info`**.

To upgrade the redundant 8600 CPU in HA mode with the version 3.7 software image:

1. Telnet to the master CPU or connect to the console port using an external modem and save the current bootconfig and config on the flash of both CPUs using the following CLI commands:

   `save config`

   `save bootconfig`

2. TFTP both configuration files to a TFTP server on the network using the following commands:

   `copy /flash/boot.cfg <tftp ip address>:boot.cfg`

   `copy /flash/config.cfg <tftp ip address>:config.cfg`

3. Verify available flash capacity on both master and backup CPUs before downloading the files.

4. Disable the **`ha-cpu`** flag on the master CPU; the standby CPU reboots automatically - wait for the standby CPU to come back online.

5. Copy the 3.7 image to the flash of the master and the standby CPU.

   For the **master CPU**, at the prompt, use the following command:

   `copy <tftpserver IP address>:p80a3700.img /flash/p80a3700.img`

   Use the above command to copy all the other files, including the boot image (p80b3700.img).

For the **standby CPU**, at the prompt on the master CPU, use the following command:

```
copy /flash/p80a3700.img peer:/flash/p80a3700.img
```

Note: Because of the DNS implementation in Release 3.7, the **peer** command is not available unless you add the peer IP address in a new file called /etc/hosts. You must create this file; no default file exists. You can manually create it using a simple text editor, like the one provided by the Passport 8600. See Figure 1 on page 24 for an example of this file.

6 Verify that the software has been copied to the master and the standby CPU.

For the **master CPU,** from the master CPU prompt, use the following command:

```
dir
```

For the **standby CPU**, from the master CPU prompt, use the following commands:

```
peer telnet

dir
```

7 Make sure that bootconfig is set properly by entering the following commands:

```
config bootconfig choice primary image /<device>/
p80a3700.img

save bootconfig
```

8 Reboot the standby CPU in slot 6 by entering the following command:

```
boot p80b3700.img
```

This command also loads the new boot monitor image to the flash of the standby CPU. Wait for the standby CPU to come back online.

9 Reboot the master CPU in slot 5 by entering the following command:

```
boot p80b3700.img
```

This command also loads the new boot monitor image to the flash of the master CPU. The standby CPU in slot 6 becomes the master CPU.

10 Enable the `ha-cpu` flag for slot 6; slot 5 reboots automatically.

11 Reset slot 6; slot 5 becomes the new master.

12 Exit the **standby CPU** using the CLI command:

```
exit
```

13 On the **master CPU**, at the prompt, set the primary image choice to the new image file (this will automatically synchronize to the standby CPU in HA-mode) using one of the following commands:

If the software image is stored on the flash, enter:

```
config bootconfig choice primary image-file /flash/
p80a3700.img
```

If the software image is stored on the TFTP server, enter:

```
config bootconfig choice primary image-file <tftp-server
IP address>:p80a3700.img
```

14 On the **master CPU**, at the prompt, save the boot configuration and run-time configuration (the configurations are automatically saved to the standby CPU in HA-Mode) using the following command:

Note: Before upgrading in HA mode, be sure your **`ha-cpu`** and **`savetostandby`** flags are set to **`true`** (enabled). To check if flags are set to `true`, use the CLI command **`config bootconfig flags info`**. (In HA-mode, the **`verify-config`** flag is set to false automatically.)

```
save config
```

15 Boot the standby CPU and then the master CPU with the new boot monitor image.

a Enter the following command:

```
peer telnet
```

a For the **standby CPU**, at the prompt, use the one of the following commands:

If the software image is stored on the flash,enter

boot /flash/p80b3700.img

If the software image is stored on the TFTP server, enter:

boot <tftp-server IP address>:p80b3700.img

b For the **master CPU**, at the prompt, use the one of the following commands:

If the software image is stored on the flash, enter:

boot /flash/p80b3700.img

If the software image is stored on the TFTP server, enter:

boot <tftp-server IP address>:p80b3700.img

The screen displays the following message:

```
WARNING: You are about to re-program your Boot Monitor
FLASH image. Do NOT turn off power or press reset until
this procedure is completed. Otherwise the card may be
permanently damaged!!!
```

Special Instructions:

If the response from the switch does not show the file being saved to the standby, you may need to copy the bootconfig and config file using the following commands:

copy /flash/boot.cfg peer:/flash/boot.cfg

copy /flash/config.cfg peer:/flash/config.cfg

The `copy` command uses TFTP as the default protocol for transferring the files. To use FTP, set the FTPD flag on the destination CPU to true. On the source CPU, set the parameters `config boot host users` and `config boot host password` to match the login-name/password of the destination CPU. (FTP will not work without setting the two config boot host parameters). (Q00524265)

NOTE: if the peer is not recognized, you can use the internal IP address used by the system, which is 127.0.0.5 for slot 5 and 127.0.0.6 for slot 6.

Upgrading the software image on a redundant 8600 CPU in non-HA mode

Note: Before upgrading in non-HA mode, be sure your `ha-cpu` flag is set to `false` and `savetostandby` flag is set to `true`. To check the flag settings, use the CLI command **`config boot flags info`**.

To upgrade the software image on a redundant 8600 CPU in non-HA mode, follow these steps:

1. Telnet to the master CPU or connect to the console port using an external modem and save the current bootconfig and config on the flash of both CPUs using the following commands:

   ```
   save config
   save bootconfig
   ```

2. TFTP both configuration files to a TFTP server on the network using the following commands:

   ```
   copy /flash/boot.cfg <tftp ip address>:boot.cfg
   copy /flash/config.cfg <tftp ip address>:config.cfg
   ```

3. Verify flash capacity before downloading the files.

4. Download the new software to the **master CPU**, using the following commands:

   ```
   copy <tftp server ip address>:p80a3700.img /flash/
   p80a3700.img
   copy <tftp server ip address>:p80b3700.img /flash/
   p80b3700.img
   ```

5. Copy the new software to the **standby CPU** using the following commands:

   ```
   copy /flash/p80a3700.img peer:/flash/p80a3700.img
   copy /flash/p80b3700.img peer:/flash/p80b3700.img
   ```

Note: Because of the DNS implementation in Release 3.7, the **peer** command is not available unless you add the peer IP address in a new file called /etc/hosts. You must create this file; no default file exists. You can manually create it using a simple text editor, like the one provided by the Passport 8600. See Figure 1 on page 24 for an example of this file.

6 Verify that the software has been copied properly to the **standby CPU,** at the prompt of the master CPU, using the following commands:

```
peer telnet

dir
```

7 Exit the **standby CPU** using the following command:

```
exit
```

8 From the **master CPU**, change your `bootconfig choice primary-image` file to the new run-time image file using the following command:

```
config bootconfig choice primary image-file /flash/
p80a3700.img
```

9 Save the boot.cfg file **boot.cfg** file on both CPUs using the following command:

```
save bootconfig
```

If the file was not automatically copied to the **standby CPU**, use the following command:

```
copy /flash/boot.cfg peer:/flash/boot.cfg
```

10 Boot the **standby CPU.**

a Log in to the **standby CPU,** at the prompt of the master CPU, using the following command:

```
peer telnet
```

b Use the one of the following commands:

If the software image is stored on the flash:

```
boot /flash/p80b3700.img
```

If the software image is stored on the TFTP server:

```
boot <tftp-server IP address>:p80b3700.img
```

11 Exit the **standby CPU** using the CLI command:

```
exit
```

12 Boot the **master CPU** with the new boot image and the new run-time image, using the CLI command:

```
boot /flash/p80b3700.img.
```

The screen displays the following message:

```
WARNING: You are about to re-program your Boot Monitor
FLASH image. Do NOT turn off power or press reset until
this procedure is completed. Otherwise the card may be
permanently damaged!!!
```

Note: Nortel Networks does not support different software versions, for example, Releases 3.3.2 and 3.7, on the master and standby CPU. Also, both CPUs must have the same amount of memory

13 Telnet back to the standby CPU after a few seconds to verify that the new image is running. The run-time image is shown in the Nortel Network banner displayed before the login prompt, as shown in Figure 2.

Figure 2 Sample login banner

```
Passport-8610:6# peer telnet
Trying 127.0.0.5 ...
Connected to 127.0.0.5
Escape character is '^]'

**********************************
* Nortel Networks, Inc.          *
* Copyright (c) 1996-2003 *
* All Rights Reserved            *
* Passport 8010                  *
* Software Release 3.7.0.0       *
**********************************

Login:
```

14 Telnet to the master CPU to verify the new image.

Troubleshooting the upgrade

If the standby CPU is not running the new software, either repeat the previous procedure if the CPU will allow you to log in or use the console port on the standby CPU to stop at the boot monitor and fix the problem.

Most common failures are caused by incorrectly typing the image file name in the bootconfig file or because the software is not present on the flash on the standby CPU. Using the console port to stop at the boot monitor will allow you to reenter the bootconfig choice primary information if it has been incorrectly typed and verify that the software is present on the flash of the standby CPU. If the software is not present on the standby CPU, you may have to copy it from the master CPU to a PCMCIA card on the master and then move the PCMCIA card to the standby CPU. You can then either copy it to the flash or change the bootconfig choice primary to use the PCMCIA card.

Upgrading SNMP

Before you upgrade SNMP from Release 3.3 or 3.5 to Release 3.7, note the following SNMP upgrade considerations.

SNMP upgrade considerations

- Starting with Release 3.7, the CLI command **`save config file`** creates a hidden and encrypted file that contains community table information. For security purposes, the **`save config file`** command also removes references to the existing SNMP community strings in the newly created configuration file.
- If you have one CPU only and a pre-3.7 configuration file, and if you swap the CPU, all the password files, including the hidden file, will be lost. You must reconfigure your trap receivers and community strings every time you change the CPU module. (Q00878458)
- With Release 3.7, changes within the SNMP agent prevent JDM from registering for traps. (Q00880590)
- With Release 3.7, the trap receiver concept has been replaced by the notification originator application. This application monitors a system for specific events or conditions, and generates Notification-Class messages, based on these events or conditions. For more information about configuring the notification originator application, see *Configuring Network Management* or *Configuring and Managing Security.*
- The ability to edit certain SNMP parameters, such as community strings, using the CLI command **`config sys set snmp`** is no longer available. For instructions on creating an SNMPv1, SNMPv2, or SNMPv3 user, or changing the default community strings, see *Configuring and Managing Security.*
- When upgrading from Release 3.5 to Release 3.7, read-only (ro) user is mapped into ReadView with read-only access. (Q00889700)
- After performing the upgrade, Nortel Networks strongly recommends that you set a password for the initial USM.

Upgrading SNMP from Release 3.3 to Release 3.7

In the Passport 8000 Series Switch Release 3.3, you set SNMP community strings by using the following command (this command is now obsolete):

```
config sys set snmp community rwa <commstring>
```

After you save the configuration, this command appears in the configuration file. This behavior has changed in Release 3.7. The upgrade procedure is detailed in the following sections.

Non-High Availability

1 Change and save the bootconfig options to the appropriate Release 3.7 image by entering the following commands:

```
config bootconfig primary choice /flash/p80a3700.img
save bootconfig
```

2 Boot up the chassis and upgrade the Boot Monitor by entering the following command:

```
boot /flash/p80b3700.img
```

The SNMP upgrade procedure loads the SNMP configuration into the Runtime configuration.

3 Save the configuration by entering the following command:

```
save config file /flash/config1.cfg
```

When you enter this command, the following activities occur:

— Configurations related to SNMP trap receivers are automatically mapped into Release 3.7-compatible commands in config1.cfg.

— Configurations related to SNMP community strings are ported to a hidden and encrypted file. This file must exist for you to access the chassis via SNMP. From this point forward, information regarding SNMP community strings will be stored ONLY in this hidden file and WILL

NOT be found in configuration files. If you choose to swap the existing CPU Module with a new CPU Module, you must copy all hidden files to the new module, in addition to the regular files, in order for the SNMP strings to work correctly.

— Default strings such as “public” and “private” are translated as is.

— The default string “secret” for rwa is no longer applicable in Release 3.7.

— All “l1”, “l2”, “l3”, and “rwa” SNMP strings will now be “rw.” (Q00894703)

High Availability

Follow the standard procedure for the HA upgrade. Refer to “Upgrading the software image on a redundant 8600 CPU in HA mode” on page 29. The upgrade process creates identical hidden files on both CPUs. Failover between CPUs should appear hitless with respect to SNMP connectivity.

Upgrading SNMP from Release 3.5 to Release 3.7

In the Passport 8000 Series Switch Release 3.5, you set SNMP community strings by using the following command (this command is now obsolete):

```
config sys set snmp community rwa <commstring>
```

After you save the configuration, this command will NOT appear in the configuration file. However, the community strings are stored in a hidden file. This behavior has changed in Release 3.7. The upgrade procedure is detailed below.

Non-High Availability

1. In CLI mode, before performing the upgrade, change and save the bootconfig options to the appropriate Release 3.7 image by entering the following commands:

   ```
   config bootconfig primary choice /flash/p80a3700.img
   save bootconfig
   ```

2. Boot up the chassis and upgrade the boot-monitor by entering the following command:

   ```
   boot /flash/p80b3700.img
   ```

The SNMP upgrade procedure loads the SNMP configuration into runtime configuration.

3 After the reboot, save the configuration by entering the following command:

```
save config file /flash/config1.cfg
```

When you enter this command, the following activities occur:

- Configurations related to SNMP trap receivers are automatically mapped into Release 3.7-compatible commands in config1.cfg.
- Configurations related to SNMP community strings are ported from a hidden file to another hidden and encrypted file. This file must exist for you to access the chassis via SNMP. From this point forward, information regarding SNMP community strings will be stored ONLY in this hidden file and WILL NOT be found in configuration files. If you choose to swap the existing CPU Module with a new CPU Module, you must copy all hidden files to the new module, in addition to the regular files, in order for the SNMP strings to work correctly.
- Default strings such as “public” and “private” are translated as is.
- The default string “secret” for rwa is no longer applicable in Release 3.7.
- All “l1”, “l2”, “l3”, and “rwa” SNMP strings will now be “rw.” (Q00894703)

High Availability

The standard procedure for HA upgrade needs to be followed. Refer to “Upgrading the software image on a redundant 8600 CPU in HA mode” on page 29. The upgrade process creates identical hidden files on both CPUs. Failover between CPUs should appear hitless with respect to SNMP connectivity.

Configuring SNMP traps

In the Passport 8000 Series Switch Release 3.3 or 3.5, you configured traps by using the following command (this command is now obsolete):

```
config sys set snmp trap-recv <ipaddr> v2c public
```

where *ipaddr* is the IP address of the trap receiver.

With Release 3.7, you configure traps by creating SNMPv3 trap notifications, creating a target address to which you want to send the notifications, and specifying target parameters. Nortel Networks provides two default entries in the notify table: Inform and Trap. The tag values for these entries are informTag and trapTag, respectively. For more information about configuring SNMP traps in Release 3.7, see *Configuring Network Management* or *Configuring and Managing Security.*

1 Configure an SNMP notification, using the following command:

```
config snmp-v3 notify create <Notify Name> [tag <value>]
[type <value>]
```

In this example, the DefNotify identifies the notification and DefTag identifies the tag value that will be to used to select entries in the snmpTargetAddrTable:

```
config snmp-v3 notify create DefNotify tag DefTag type
trap
```

2 Configure an SNMP target address, using the following command:

```
config snmp-v3 target-addr create <Target Name> <Ip
addr:port> <Target parm> [timeout <value>] [retry
<value>] [taglist <value>] [mask <value>] [mms <value>]
```

In this example, you create the target parameter ID (TparamV2) along with the target address ID (TAddr1), link them with the taglist (DefTag) that you created in step 1, and define the trap receiver's IP address (198.202.188.207). You also specify 162 as the default UDP port used to send traps, a timeout of 1500, a retry of 3, a mask value of ff:ff:00:00:00:00, and specify a maximum message size (MMS) of 484.

```
config snmp-v3 target-addr create TAddr1
198.202.188.207:162 TparamV2 timeout 1500 retry 3 taglist
DefTag mask ff:ff:00:00:00:00 mms 484
```

3 Specify SNMP target parameters, using the following command:

```
config snmp-v3 target-param create <target param name>
mp-model <value> sec-level <value> sec-name <value>
```

In this example, you first specify that target parameter ID, TparamV1, is linked to the user name, readview, define the model as SNMPv1, and specify a security level of noAuthNoPriv. Next, you specify that target parameter ID, TparamV2, is linked to the user name, readview, define the model as SNMPv2c, and specify a security level of noAuthNoPriv.

```
config snmp-v3 target-param create TparamV1 mp-model
snmpv1 sec-level noAuthNoPriv sec-name readview

config snmp-v3 target-param create TparamV2 mp-model
snmpv2c sec-level noAuthNoPriv sec-name readview
```

Note: Because Release 3.3 and Release 3.5 support only SNMPv1/SNMPv2c trap configurations, when you upgrade to Release 3.7, the trap configurations are in SNMPv1/SNMPv2c.

Hotswapping the CPU module or I/O modules

When hotswapping the active CPU module in an 8600 Series switch with redundant CPU modules, wait until the redundant CPU module is stabilized before inserting any other modules. The redundant CPU module will display a login prompt on the console screen. If no console connection is available, wait for at least 30 seconds before inserting the replacement CPU module or before reinserting the removed CPU module.

In addition, during a CPU fail over, do not hot swap I/O modules until the new CPU becomes the master CPU.

Caution: Do not hotswap or insert modules in a Passport 8000 Series switch chassis while the switch is booting. Doing so might cause the module not to be recognized and may cause module initialization failure.

Caution: Nortel Networks strongly recommends that you make the backup CPU the master before removing the master CPU in an HA configuration. Removing the master directly could generate traffic distortion.

Securing your network

For additional security-related information, consult the *Important Security Information for the 8000 Series Switch* and *Configuring and Managing Security.* A list of the documents contained in the 3.7 documentation set is included at the end of these release notes.

Password encryption

In the Passport 8000 Series Switch Software Release 3.7 or higher, passwords are now stored in encrypted format and are no longer stored in the configuration file. If a configuration file saved prior to Release 3.7 or higher is loaded, any saved passwords from the configuration file will not be recognized. If the switch is booted for the first time with the software Release 3.7 or higher image, the password is reset to default values and a log is generated, indicating any changes.

Note: For security reasons, Nortel Networks recommends setting the passwords to values other than the factory defaults.

The boot monitor command **`reset-passwd`** resets passwords to their default values.

- To reset the passwords, use the following command at the boot monitor prompt:

  `reset-passwd`

- To change the passwords, use the following commands. All passwords are case sensitive.

  `config cli password <access-level> <username>`

```
Enter the old password:
Enter the new password:
Re-enter the new password:
```

High Availability Layer 3 considerations

- If you want to use High Availability (HA) mode, verify that the link speed/ duplex mode for the CPU module are 100Mb/s and Full Duplex. Use the following CLI commands to configure the link speed and duplex mode:

  ```
  config bootconfig net cpu2cpu speed 100
  config bootconfig net cpu2cpu fullduplex true
  ```

- If the link is not configured in 100Mb/s and Full Duplex mode, either you will not be able to synchronize the two CPUs or the synchronization may take a long time. Error messages may appear on the console. (Q00839619)
- In HA mode, Nortel Networks recommends that you not configure the OSPF hello timers less than a second, and the dead router interval less than 15 seconds.

SMLT network design considerations

- If you use LACP in an SMLT/Square configuration, the LACP must have the same keys for that SMLT/LAG; otherwise, the aggregation may fail if a switch failure occurs. (Q00789437)
- Use the following procedure when designing an SMLT network. For more information, refer to the section “Passport 8000 Series Switch Release 3.7 Implementation Notes” in the *Network Design Guidelines*.

  a To ensure proper IST connectivity, define a separate VLAN for the IST protocol:

  `config mlt 1 ist create ip <value> vlan-id <value>`

  Note: Do not enable a routing protocol on this VLAN.

b To ensure that IST will not be disabled inadvertently, disable CP-limit on the IST ports:

```
config ethernet <slot|port> cp-limit disable
```

c Keep CP-limit enabled on the SMLT ports and change multicast-limit value to 6000:

```
config ethernet <slot|port> cp-limit enable
multicast-limit 6000
```

Note: Nortel Networks recommends that you keep CP limit enabled on SMLT ports to protect the SMLT aggregation switches against unforeseen DOS attacks.

d Disable loop detect on SMLT ports:

```
config ethernet <slot|port> loop-detect disable
```

Note: For Release 3.7, Nortel Networks recommends that you disable loop detect; this recommendation is in direct contrast to that made for earlier releases.

e Enable tagging on SMLT links:

```
config ethernet <slot/port> perform-tagging enable
```

Note: Nortel Networks recommends that you enable tagging on SMLT ports and drop untagged frames to ensure that SMLT client switches with default configurations will not adversely affect SMLT aggregation switch behavior.

f Enable drop untagged frames on SMLT links:

```
config ethernet <slot/port> untagged-frames-discard
enable
```

Documentation corrections and additions

The section describes information that requires correction in the documentation in this software release or were not described in the documentation set, and also describes configuration considerations that would normally be included with a feature or protocol in the documentation.

Configuring Web Switching Module using Device Manager (314995-A)

Be aware of the following discrepancies between the JDM interface, the online help, and the corresponding *Configuring Web Switching Module using Device Manager* (314995-A) manual:

- The Edit >WSM Card -> Bridge -> Spanning Tree JDM menu tab includes the Bridge Max Age, Bridge Hello Interval, and Bridge Forwarding Delay fields. The online help and the manual lists the fields as Root Max Age, Root Hello Interval and Root Forwarding Delay.
- The Edit -> WSM Card -> L4 Switching -> Filters tab online help and the WSM manual contain two separate table entries for Network Address Translation.

  The Edit -> WSM Card -> L4 Switching -> URL Parsing -> Expressions tab contains field string, whereas the online help and the manual reference expressions instead.
- The Graph -> WSM Card -> General -> RIP tab includes the Bad RIP Packet IN field, while the online help and the manual reference the Bad RIP Packets Out field. In addition, the JDM interface contains the RIP routes aged Out field, while the online help and manual do not. (Q00901730)

Bugs fixed in this release

The section describes the bugs fixed in this release and discusses the following topics:

Hardware and platform

ATM

- The Passport 8600 now implements a heartbeat mechanism between the 8672 ATM Module and the CPU (869x) so that in the event of a CPU problem, the ATM Module is able to detect that the CPU is no longer available and will either go offline or at a minimum, will disable its ports (Q00764492-01).
- When two CPUs come up after a power reset both of them try to read their own and each others SEEPROM for synchronizing the M-mode information. This causes a SEEPROM contention, which results in an error. The switch now tries to read the information available in the DRAM if available (Q00724913-02).
- The Passport 8600 now replies with the correct IP address following an invAtmArp request (Q00794080-01).
- Changing VPI bits more than once is now properly handled (Q00711417-01).
- The ATM Module properly handles the following action: show port stat atmport. (Q00754633-02).
- Actual SCR is no longer 10% higher than configured SCR (Q00605263-01).

POS

- Link statistics are now correctly displaying the MTU and Bad FCS using CLI and JDM (Q00728824-02).
- The web interface now shows POS information if the first-slot MDA is not installed (Q00792436-01).

10GE WAN

- CVs are now inhibited during SES events, at Section, Line or Path (Q00443204).

WSM

- IP of max VLAN (4093) is now correctly added to IP interface table (Q00525239).
- The switch does not default if during parsing a configuration, it fails on an empty slot (Q00758487-01).
- The switch now properly gives the information related to a session dump when vlanbind is disable (Q00667455).
- WSM trunkfile is now saved on Backup SSF using JDM save runtime config (Q00753922-02).

CLI/Platform

- The Passport 8600 switch no longer stalls during a FTP session after entering the CLI command **`cd`** or **`change directory`** command to multi subdirectories (Q00793609-01).
- Issues related to the following message chRetsratTumx have been fixed (Q00785973-02).
- JDS Uniphase GBICs SX model # AA1419001 are now properly recognized as SX rather than GBIC other (Q00734289-02).
- I/O modules with the correct hardware revision working in a single SMLT configuration are now properly handled and do not go off line (Q00794449-01).
- 8608GBE does not resend auto-negotiation request anymore after the link is already established (Q00712539-02).
- When 3 invalid login occur on the standby CPU, the switch gives back the prompt after 60 seconds (Q00246377).

- PCMCIA-stop - the switch now creates a new sys log file on the PCMCIA after a deletion (Q00146985).
- Boot configuration and image files with different version numbers generate a message asking for an upgrade (Q00819773-01).
- The switch now correctly processes VLAN information when Optivity NMS 10.1.0.1 tries to get some parameters related to this VLAN(Q00756412-01).
- The switch now properly handles the situation when CLI times out after logging out from shell (Q00822386-01).
- The switch now properly handles the connection and reconnection of telnet sessions where in some cases it was not possible to either view or save the configuration (Q00687891-02).
- Hardware errors are now correctly reported using Syslog (Q00747226-02).
- The error message now correctly reflects the CPU slot number in a 3 slots chassis (Q00717309-01).
- After using the command **`boot -y`**, the following error message no longer appears: `ERROR Task=tShell unable to perform complete re-boot - the switch should be powered off (`Q00731156-02).
- In the following message, `ERROR: 335 duplicate upd port fwd entry`, the word udp is now correctly spelled (Q00420622-02).

HA

- The switch now correctly synchronizes information between both CPUs (Q00820508-01).
- The savetostandby flag does not stay to true after the ha-cpu flag is set to false (Q00468677).
- A notification is shown on the console when enabling HA-CPU (Q00246794).
- The CLI command **`trace auto-enable`** is now synchronized correctly with the standby. (Q00505814).
- The change of management port IP for the slave from master is now correctly synchronized (Q00816093-01).
- In HA, the CLI command **`show log`** file does not print the following error message: `malloc: 0x0 size 914144` (Q00503817).
- In HA, the mrdisc-neighbor table no longer shows the following message: `Robust-val` of 26987 (Q00536682).
- The Syslog function is now correctly synchronized between both CPUs (Q00481423).

- The **`Enhanced-oper-mode`** flag is now correctly synchronized (Q00677477-02).
- Copper links on 8600 and 8100 are now properly showing links down (Q00680128-02).
- The CLI command **`show log file tail`** is now properly handled by the switch (Q00887742-01).
- Multicast addresses can not be configured on the CPU OOB port anymore (Q00455019).
- It's now possible to add multiple VLANs to an MLT using a single command (Q00667521-01).
- The following message `Error: Invalid STG ID` is now similar to the one used by JDM (Q00728199-01).
- Console access is no longer lost when you ftp a file from the switch to a remote station (Q00805788-02).
- When PCMCIA gets full, and stops to write events to the syslog file, a flag on CLI indicates it (Q00495277).
- TFTP timeout values are now correctly handled (Q00525982).
- The CLI move command (**`mv`**) now works correctly(Q00715500-02).
- The CLI command **`show port info state`** now properly indicates which action has taken down a port (link flag, cp limit) (Q00759621-01).
- Trap will be sent on every degree increment starting from 50C. This trap has the WARNING type (Q00747245-02).
- SSL - you can now use the 8661SAM when the Enhanced Mode is enabled (Q00718767-01).
- After changing the status of the Web server, it is now correctly handled (Q00628134-02).
- A log message (insertion/removal) has been added related to GBIC insertion/removal (Q00750484-01).
- VLAN FDB show command enhancements (show port info fdb-entry) (Q00645813-01).
- The CLI command **`show-all`** option for a some CLI commands has been added (Q00607608).

Passport 8100 only

- The protocol messaging between the CPU and the I/O modules has been redesigned to add redundancy and robustness (Q00717615-02, Q00725468-02).
- The VLAN IP now correctly recovers after a brief broadcast/multicast storm (Q00771673-02).
- Removing/adding static FDB entries is now properly handled by the switch (Q00616972-02).
- 8100 UDP packet (NAS-IP ADDRESS) does now show the Virtual Mgmt address (Q00766258-01).
- MRDISC/IGMP (Q00599371-02).

Switch management

SNMP

- Trap is no longer reported as 'none' when VRRP critical link failed (Q00090944).
- SNMPv3 compliance fixes (Q00625534-02, Q00486134, Q00486800, Q00486792, Q00486966)
- When the link trap disabled, the message concerning port up/down no longer disappears in the log file (Q00758963-02).
- Static route entry is no longer corrupted with both mgmt/vlan IP configured (Q00754534-02).
- Static Route does deactivated after next hop switch is disconnected (Q00602080).
- When logging in using L2 access, you are not able anymore to add an IP address to a VLAN. If an existing VLAN with an IP address is configured on the box, a user can no longer log in as L2 and delete the entire VLAN (Q00605340-01).
- A new CLI command **`show vlan info fdb-entry <vid> mac <mac addr > ports < slot/ports ...slot/port>`** has been created (Q00783080).
- 802.1p bits are now properly handled by the PCAP (Packet Capture) engine (Q00638548-01).
- JDM now provides allowable range for some parameters when configuring OSPF for VLAN (Q00416785).

- A message is now prompted by JDM to reset BGP after applying policies (Q00516654).
- The broadcast mask in the following menu is now available: JDM:ip-> udpfwd-> broadcastinterface (Q00321906).
- A spelling issue is now fixed - invlaidVlanIdSpecified (Q00796126-01).
- It is now possible to modify the HelloInterval and RtrDeadInterval under VLAN > IP >OSPF (Q00533862-01).
- It is now possible to telnet to a HA-CPU switch after toggling TFTP from true to false and back to true (Q00729744-02).
- The NewEMMode has been changed to NewMMode under Edit-> chassis-> chassis (Q00525241).

JDM

- Help messages correction (Q00042271, Q00038220).
- Inputting wrong network into the prefix list in the policy screen no longer displays the message `no such instance` until the screen is refreshed (Q00656513).
- Mroute-HW information, specifically Prunes and Sources information, is now correctly displayed Q00710450).
- BGP Route Table shows AggregatorAS and AggregatorAddress correctly (Q00668539-03).
- It is not possible to configure an interface address with an invalid broadcast address (Q00224945).
- JDM now contains configurable trap variables for BGP (Q00155710).
- The upper limit for the `udpfwdlistid` parameter is now 1000 (Q00735116-01).
- It is now possible to dynamically enable Telnet via JDM (Q00775245-01).
- The SNMPv3 agent now properly handles incorrect msgVersion values (Q00486039).
- It is now possible using JDM to query and display new fields in the I/O modules SEEPROMs (Q00714574-01).
- All OSPF RMON alarms can now be set using JDM (Q00771267-01).
- JDM now allows to configure more than 8 character (64-bit) for the OSPF simple authentication-key (Q00418387).

- You can no longer see the following error message: `rcIpConfOspfHelloInterval.2101: Router dead-interval must be a multiple of the hello interval(`Q00533862).
- JDM now supports the following CLI parameter: `ether-type-for-svlan-level = 0x8100` (Q00655116).
- Peer and Peer Info have been combined under IP -BGP (Q00476770).
- In a configuration with a brouter port, you can now configure IP protocol based VLANs (Q00416781).
- A new set of MIBs objects have been defined for the rctraps with an extra 0 added. The rcTrap OIDs have been also modified to conform with the RFC (Q00786202-01).
- A tool called “net-snmp” no longer generates an error message indicating that mib.txt is not being properly written (Q00706902-03).
- The MIB walk tool is no more looping at the rcBridgeFdbProtectTable node (Q00849286-01).
- Spelling errors in a previous MIB file (mib.txt) have been fixed (Q00856982-01).
- Web server - the Route Preference mismatch has been fixed (Q00517857).
- While retrieving the VLAN ID from the community string, the switch now checks if the VID is 0. A change has also been made with respect to the maximum VLAN id which is considered valid for an SNMP packet. It was previously 0xffff (16 bits). Because a VLAN id requires only 12 bits (max 4095), this value is made to 0xffe. (Q00803791-01).
- In Edit> SnmpV3> VACM Table> Group Access Right tab, the ContextMatch column has been removed. When you do Insert, the ContextMatch field has been removed too (Q00625534-02).
- The etherHistorySampleIndex is now correctly displayed in JDM (Q00798173-01).
- SNMP USN table are correctly synchronizing auth and priv key between master and slave CPU. (Q00761477-02).
- The **`block-snmp flag`** is now consistent with other task boot flags (Q00540689).
- The CLI command **`config rmon info`** now correctly shows the util-method settings in **`info`** command (Q00410153-03).
- The -y option has been added to the boot command (Q00653361).
- Log messages have been added after a password change (Q00426094).
- The backup SSF now sends a trap if the primary fails (Q00044078).

Security

RADIUS

If you configure servers to the value specified by maxserver parameter, but you try to configure the parameter maxserver to a value that is less than the number of configured servers, the switch generates an error, prohibiting you from changing the maxserver value (Q00640573).

- RADIUS - Reply-Messages are now correctly displayed. (Q00714777-02).
- RADIUS - The CLI command **`radius accounting`** is no longer lost if Telnet timeouts (Q00631178-02).
- RADIUS - Radius Accounting does now send requests when the switch is soft reset (Q00697428).
- ACCESS-POLICIES - Defining an Access Policy Enable using the HTTP service now correctly allows SNMP session to the switch (Q00559345-02).
- SSH - When the flash is full, error messages are now consistent for RSA and DSA key generation (Q00489583).
- SSH - The following error message `Task=sshdSession Write failed: S_iosLib_INVALID_FILE_DESCRIPTOR` no longer appears (Q00528007).
- SSH - The switch now properly shutdowns the access after 3 failed login attempts (Q00743506-02).
- SCP is now properly working (Q00732183-01).
- LOGIN - The switch now properly handles login with 20 characters (Q00717514-03).
- GLOBAL MAC FILTERING - see 3.5.1/3.5.2 Release notes (Q00690165).

Layer 2

- Global MAC filtering is now possible. See 3.5.1 and 3.5.2 release notes for more detailed information (Q00690165-01).
- The fdb-filter does not allow to use QoS level 7 anymore (Q00611473-02).
- Adding a new MAC does not cause its QoS set to Level 1 instead of Vlan's QoS anymore (Q00611467-02).
- The CLI command **`help`** used for adding multiple VLANs to a MLT has been added (Q00746984-01).
- Users are now blocked from adding 1- > 2014 VLANs in a MLT at the CLI level (Q00739344-01).
- Toggling STP on MLT ports does not corrupt the MLT STP configuration anymore; STP does not fail anymore if one MLT link is pulled (Q00707298-02).
- As expected, the potential ports of any dynamic VLAN belonging to an MLT are ALL activated upon reception of any matching traffic on even one of them. But when the link on one of these activated MLT port is removed or disabled (gets deactivated) and re-inserted or enabled, it does not get activated. This is now fixed (Q00732497-01).
- The switch no longer generates an error message when adding multiple VLANs to a MLT using "-" (Q00746913).
- The switch now properly handles the situation when removing a VLAN twice from a MLT in one CLI command (Q00746987-01).
- The STP now converges correctly over MLT when port STP priority/cost change (Q00604730-02).
- The switch now properly handles the STP convergence after a reboot when multicast data is sent on all ports (Q00647889).
- The warning message `Disabling STP on port won't take effect dynamically. Please toggle the admin status of the port to make the change reflect` has been added (Q00732466-01).
- The STP designated bridge information is now correctly displayed with multiple MLTs (Q00677516-02).

SMLT

- By default, with Release 3.7, all IST ports have the cp-limit flag disabled. (Q00762494-01).
- SMLT and VRRP interaction (Q00581008-02).

- Untagged SMLT port no longer become tagged after switch reset (Q00673256-02).
- MAC table (Q00781427-02).
- STP on the SP-SMLT port can now be disabled after enable tagging (Q00773624-01).
- Single port-MLT no longer disregards SMLT ID when deleting from port (Q00776685-01).
- While deleting the SLT from a port the spanning tree flag for the port was not correctly set again. This is now fixed (Q00775714-01).
- The check which was allowing SMLT Port STG state to true if IST is not yet configured is no longer in the software (Q00776716-01).
- SMLT / ARP entries (Q00786962-01).
- SMLT / IST (Q00793474-01, Q00811474-01).

SVLANs

- Customer VLAN BPDU's were previously dropped at UNI after hitting the CPU. So there was no way to detect customer loops spanning across SVLAN core. This condition is now fixed and prevents loops in the customer network (Q00474734).
- All VLAN MAC entries are now correctly handled (Q00780486-01).

Layer 3

IP

General

- You now have the ability to send Radius packets with the CLIP address as the source IP address (Q00618908-01).

```
config radius

    attribute-value <value>

    enable <true | false>

    maxserver <value>
```

```
    sourceip-flag <true | false>
```

The **sourceip-flag** will be introduced to this context. By default, the flag will be set to false.

```
# config radius server

    create <ipaddr> secret <value> [port <value>] [priority
<value>] [retry <value>] [timeout <value>] [enable <value>]
[source-ip <ipaddr>]

    delete <ipaddr>

    set <ipaddr> [secret <value>] [port <value>] [priority
<value>] [retry <value>] [timeout <value>] [enable <value>]
[source-ip <ipaddr>]
```

source-ip (optional) is the new field in create and set commands.

If **sourceip-flag** is true and source-ip for the server is configured then source IP address in the RADIUS packet will be source-ip otherwise (either **sourceip-flag** is false or source-ip is not configured) as per current implementation.

- In previous releases, the validity of the source IP address or target IP address was checked by assuming its mask to be one of the natural classful masks. In some cases, this creates problems while checking if that IP address is broadcast/network address. The implementation has been changed to use the original mask value instead of the natural mask while doing all these checks. (Q00677629-01).
- The switch now properly shows correct ARP entries after one port in MLT is plugged/unplugged (Q00730341-02).
- The switch does rearp when ping snoop is enabled (Q00824486-01).
- All `show` commands now correctly display the total number of entries (Q00279795).
- The inconsistent number range on udpfwd interface assignment seen on previous releases is now fixed (Q00322145-04).
- Routing policy naming issue is now fixed (Q00572865-02).
- The management IP interface address is now correctly shown after a JDM change (Q00714147-02).

- The CLIP can now be used as a source ip when sending traps using the CLI command **`config sys set snmp force-iphdr-sender <true|false>`** (Q00749008).
- The switch now shows the right IGMP report on IP IGMP group table (Q00385116-03).
- IRDP - an error message has been rewritten (Q00506067).
- Users are now allowed anymore to create loopback addresses (Q00616972-02).

ARP

- You now have the ability to save non-default ARP threshold values (Q00638438-01).

VRRP

- The VRRP holddown timer does properly work when backup-master is enabled (Q00804509-01).
- After disabling IP Forwarding on the master CPU, the backup CPU now correctly becomes the master. (Q00747319-02).
- VRRP and other protocols interaction - IPX route injection (Q00297197).
- You now can add critical IP addresses for all VRRP VLANs (Q00626433-03).
- You no longer see the following error message `Task=tMainTask portGetPortNum: invalid physical port 0292` (Q00286645).
- Blocked ports (STP) now drop the VRRP advertisements packets (Q00624420).
- VRRP/Boot-relay functionality improvement: the PP8600 now tags the giaddress for all incoming Bootp requests to be the VRRP address as well as the physical VLAN address (Q00577589).
- A syslog error is now generated when duplicate IP issue exists in the ARP table (Q00733565-01)

RIP

- RIP timers are now provided per VLAN interface, and not globally (RIP Update interval, Route HoldDown Interval, Route Discard Interval) (Q00573636).
- The switch now correctly displays the RIP timeout value in show/ip/rip/info (Q00469135).

- The message `tMainTask rip2GarbageList has too many paths` is no longer shown on the console, but logged only (Q00436259).
- It is now possible to disable RIP triggered updates on interfaces (Q00590732-03).
- RIP triggered packet are now sent with the correct metric for default route (Q00590728-02).
- JDM/RIP: it's now possible to configure the RipTimeOutInterval (Q00502750-01).
- A consistency check has been added to check the IP forwarding. If IP forwarding is disabled, no RIP updates are sent. (Q00747348-02).
- Wrong network address was being added to the aggregated list in case of inject-lists. The reason was the natural class mask was used for calculating the network address. This issue is now fixed (Q00815198-01).
- When triggered update is enabled on a RIP interface which has a out-policy configured to announce injected network, a metric 16 trigger update is sent out when one of the contributing route goes down. However, during the regular update interval this route was advertised back with a valid metric. The switch now suppresses the triggered update which is using the injected network (Q00796647-04).
- RIP triggered updates for OSPF sourced routes are not longer getting poisoned during SPF (Q00780260-04).

OS

- A valid LSA type was previously reported as invalid (type 11). It is now correctly reported. (Q00552389).
- Routes learned via OSPF are no longer sent back to the next-hop router with a RIP metric 16 (Q00780105-04).
- A new message has been added when OSPF neighbors status changes (Q00490696).
- OSPF Accept Route Policy Set Metric (Q00726235-01).
- The E_Metric in CLI LSDB table gives (0 or 1) bit value instead of type 1 or 2. This has been corrected (Q00605652-01).
- The switch now correctly handles the situation when it receives an LSA with an invalid length field (Q00732593-02).
- All the interface parameters are correctly cleaned up after deletion (Q00419072, Q00422614).

- The number of SPF run per area now correctly matches the total number of SPF runs (Q00419224).
- AS External routes are now correctly classified as ECMP routes (Q00696568-02).
- The switch now correctly handles the case of large LSAs (Q00733550-02).
- The Passport 8600 no longer redistributes internal connection to WSM via OSPF (Q00722571-02).
- OSPF Hello packet with incorrect header checksum and no authentication as per configuration are now correctly handled and logged (Q00631551).
- In previous releases, the switch was accepting routes with NSSA inter area ASE Forwarding Address. This problem has been resolved by preventing the installation of type-7 whose forwarding address is inter-area route (Q00718895-02).
- Misconfigured OSPF area ranges can not corrupt the OSPF state anymore (Q00734760-02).
- SPF counts do not increase anymore on 'backbone area' which has no active interfaces (Q00642852-02).
- The Passport 8600 switch no longer generates unnecessary T3 LSAs when interface state changes (Q00716013-01).
- The range for OSPF dead interval is identical for different interface CLI configuration methods (Q00597317-01).
- The Passport 8600 does now translate type 7 LSA to type 5 when area type is changed from transit to
- NSSA (Q00644652-01).

BGP

- The following message `Task=tMain Task aggminus: count lost sync`, related to BGP aggregation policy, is no longer appearing (Q00668579-03).
- JDM now correctly allows you to do a restart soft-reconfiguration (Q00656508-01).
- Some optimization has been done to reduce the establishment of the sessions after a reboot with the BGP peers (Q00661603-04).
- All routes appear correctly in the routing table after reboots and power cycles. (Q00661613-03).

- The check for a disable sequence number is now handled properly (Q00656496-02).
- When a user deletes a community-list or as-path-list, corresponding entries in IPASACC_LIST are correctly deleted and the references in RMAP entries too (Q00739301-02).
- A CLI command has be added to view RIB-out for a particular neighbor. See the following example:

```
Passport-8610:5/show/ip/bgp/neighbor# ?

Sub-Context:

Current Context:

advertised-route <ipaddr> [<prefix>] [longer-prefixes]

    info [<ipaddr>]

    stats <ipaddr>

    route <ipaddr> [<prefix>] [longer-prefixes]
[community <value>]

Passport-8610:5/show/ip/bgp/neighbor# advert 10.124.10.2

Network/Mask       NextHop Address Loc Pref Org   Status

------------------ --------------- -------- ----- ------

3.0.0.0/8          0.0.0.0         100      INC   import

10.124.10.0/30     0.0.0.0         100      INC   import

20.20.20.0/24      0.0.0.0         100      INC   import

30.30.30.0/24      0.0.0.0         100      INC   import

90.164.99.0/25     0.0.0.0         100      IGP   import

90.164.100.0/24    0.0.0.0         100      INC   import
```

  (Q00503134-01)

- Deleting a nonexistent route policy no longer prompts a wrong error message (Q00504510-01).
- Applying a route policy does prompt to reset BGP peer in telnet session, and not only working with the console (Q00510171-02).
- Different spelling for **`default-local-pref`** in config and info (Q00515786).
- Misspelled `soft-reconfigurationin-in` in the CLI command **`config ip bgp neighbor info`** is now fixed (Q00519973).

- Imported routes has been enhanced in order to avoid routing confusion (Q00558225).
- MaskLen variable now works properly with BGP aggregation policy (Q00731343-02).
- Routes are now correctly updated in the routing table manager (Q00673364-02).
- An option has been created to disable/enable the Multi-Exit Discriminator selection process. (Q00212907-02).
- Deleting community or AS path list now correctly removes it from Route Policy (Q00684509-03).
- A warning message now displays when you enable and disable the **`comp-best-path-med`** flag (Q00731340-01).
- Deleting community or AS path list now correctly removes the match-community (Q00693795-02).
- Route change optimization (Q00745549-01)
- The switch now correctly handles the situation when a BGP summary is queried continuously after disabling OSPF (Q00834517-01).
- BGP neighborship is correctly formed when send-community is enabled (Q00834520-01).
- The switch now correctly handles the situation when BGP is restarted twice (Q00860084-01).
- The switch is now able to control MED comparison for Confederation. (Q00508131-01).
- An Accept Exact Match community problem has been fixed (Q00697210-03, Q00695317-03).
- BGP redistribute static routes do not fail anymore if destination static routes are reset (Q00768506-01).
- There is now an option to disable/enable Multi-Exit Discriminator selection process. (Q00212907-03).
- The switch does now correctly show the flap penalty decrement when displaying dampened routes. (Q00499554-01).
- BGP max-init-peers and max-txqueue-len are now configurable through SNMP (Q00506766).
- BGP Range for max-prefix in MIB file and CLI are now identical (Q00508531).

- BGP: the switch now correctly rearranges Path Attribute in ascending order (Q00176871-01).
- A policy that matches a prefix and a community now works properly (Q00668622-03).
- The switch correctly handles the situation of changing a BGP route preference and entering the CLI **`info`** command (Q00734276-01)

IPX

- The processing of the IPX table route has been optimized (Q00124151-01).
- When an MLT is created with port in a VLAN using IPX, the IPX circuit no longer goes down. (Q00707065-01).
- IPX policies netlist are now unsigned 32-bit integer values (Q00621388-02).

Bandwidth management

- Global MAC filters are now supported (CLI/JDM) (Q00688186-03).
- The switch now correctly handles the situation when attempting to refresh JDM after disabling IP Filter (Q00787885-02).
- The IP filter MIB agent now returns the correct FILTER-OCTETS value if exceeding 32 bits. (Q00247020).
- The switch now correctly handles the configuration of filters on more than 15 ports at the same time (Q00660402).

  Note: Using Optivity Policy Server for this configuration is required. Please contact your Nortel Networks representative for more information related to this unique application.
- The time required to configure global filters on the switch has been optimized (Q00655445).
- During the learning process, a couple of packets could have been forwarded even if their source MAC was in the blocked list. The switch now properly discards all these packets (Q00843690-01).
- Filters are now correctly removed from a list of ports if the module containing there ports has been removed from the chassis (Q00469599-01, Q00699154-01).
- A very specific error condition (combination of global filters configured on the same group of ports) is now fixed (Q00704569-01).

- The switch no longer forwards traffic to the next hop when this next hop is not available (Q00763557-01).
- Diffserv settings are now homogeneous across MLT ports when a port is added to an MLT (Q00428992-05).
- The switch now allows to modify DSCP of Multicast traffic with Global filters if the configured dst-ip or the src-ip of the global filter is Multicast IP (Q00509096).
- QOS does now correctly respects the drop precedence on egress using a 8648TX-E (Q00610096).
- Multimedia Stream DSCP for a Class Selector 5 filter are now properly set (Q00640968-02).
- Filters are properly executed in M-mode (Q00681716-02).
- Filters configuration issue after a reboot (Q00751601-02).

Multicast

General

- The CLI command **`show ip mroute-hw resource-usage info`** command was displaying “Multicast Hardware Record Usage” in the title. This has been changed it to “Multicast Hardware Resource Usage.” (Q00499770-02).

IGMP

- Passport 8100 only: when the last receiver leaves the group the stream is now correctly flooded to the mrouter (Q00607185-03).
- The current IGMP Static Join implementation now allows to enter the range of the multicast groups in the IGMP Static Join statement (Q00456123).
- A pseudo report to non-querier side is now sent while sending query so that configured static groups can also be learned by non-queriers (Q00626663-01).
- Passport 8100 only: IGMP static groups are now properly saved to the configuration file (Q00607037-03).
- When static IGMP join is configured on the switch for any multicast group, the “igmp cache” information is now correctly displayed (Q00525068, Q00525068-01).
- An IGMP sender port is no longer wrong after a STG change causing traffic interrupt (Q00643017-02).

- IGMP snooping no longer fails to forward certain multicast streams (Q00656807-02).
- The switch now correctly handles the situation when attempting to flush IGMP entry using JDM (Q00773756-01).
- Multicast access control allows user to configure an IP multicast enabled VLAN with an access policy that consist of several multicast groups. Multicast access control uses same prefix list as that of routing protocol. User can configure a range of multicast groups in the prefix list and use it while configuring the access policy (Q00525006).

DVMRP

- The switch now correctly handles the following trace command on IPMC (level 27 3) (Q00725018-01).
- The following error message `ERROR ipmSysSetEgressDiscSubnetGroup FAIL ModifyArIpmcGroupACBG 239.0.0.56 InVlanId 2501 AcbIndex 583` no longer appears (Q00696562-01).
- In some rare conditions, some multicast packets were lost in a SMLT configuration. This is now fixed (Q00728462-01).
- The CLI command **`show ip mroute route table`** does now show all the mcast entries (Q00079968).
- DVMRP does now prune routes properly and keeps next-hop mroutes forwarding (Q00687543-02).
- The switch now supports triggered updates for sending out prune messages to all possible neighbors if it detects that any links are down (Q00796628).
- Some additional log and events related to DVMRP have been added (Q00209980).
- Multicast software forwarding feature does not drop the first packets from the sender anymore (Q00650303-01).
- The following CLI command **`show ip mroute-hw [src <value>] [grp <value>]`** has been modified to fix a display issue (Q00739110-01).
- Route Discard Timer (Q00573585).

PIM

- The switch no longer generates the following error message with less than 512 PIM interfaces: `rcIpPimIfxTblEntryAdd` (Q00474713).

- The switch now correctly handles the situation when you disable PIM (Q00896709-01, Q00724182-01).
- Several issues related to timers accuracy have been fixed (Q00635727).
- The Cand-RP option is now configurable with the CLIP (circuit-less-ip-address) (Q00641642).
- The switch no longer the following error message when sourcing a configuration file with PIM hellointerval=1500 (Q00742329-01): `rcIpPimTblSet: Error setting PIM parameters.`
- In previous releases, when an active RP was going down and groups were converging to an alternate RP available in the network, and when the previous RP was coming back and active RP for the group was changing back, the mroute entry was incorrect. This is now fixed (Q00715345-01).
- In some rare cases, some multicast stream were taking some significant time to recover after a failover. This issue is now fixed. (Q00643017, Q00667453-02).
- The PIM-MBR feature is correctly handled after a switch reboot. (Q00689585-01).
- The show ip pim debug-pimmsg info command now displays source and group addresses (Q00669723-01)

PIM-SSM

- The switch correctly handles the aging out of IGMP records (Q00760476-01).

Known limitations and considerations in this release

The following topics describe issues known to exist in the Passport 8000 Series Switch Software Release 3.7 and include the following topics:

Hardware and platform

- Release 3.7 provides SMLT support of a switch that has a single CPU/Switch Fabric 869x module installed. This enhancement, also referred to as SMLT-on-single-CP functionality, is provided through a combination of new Ethernet I/O module revisions and a new control plane functionality. It requires that the switch contain specific hardware revision levels of E or M series I/O modules; these modules are listed in Table 8.

To verify the BackHwVersion HW revision of I/O modules, use the CLI command **`show sys info card`**. Compare the revisions against those in Table 8. You will need a revision number equal to or greater than the ones in this table.

Table 8 Hardware revision requirements for SMLT on single CPU

Part No.	Revision	Description
DS140411	11	Passport 8616SXE Routing Switch Module. 16-port 1000BASE-SX Gigabit Ethernet
DS1404024	7	Passport 8632TXE Routing Switch Module. 32 10/100TX plus 2 GBIC interface module
DS1404034	5	Passport 8616GTE Routing Switch Module. 16 port 1000BASE-TGigabit Ethernet
DS1404035	7	Passport 8648TXE Routing Switch Module. 48 10BASE-T/ 100BASE-TX Ethernet
DS1404037	7	Passport 8624FXE Routing Switch Module. 24 port 100BASE-FX Ethernet Layer 3
DS1404038	7	Passport 8608GBE Routing Switch Module. 8-port 1000 Base GBIC
DS1404044	7	Passport 8608GTE Routing Switch Module. 8 port 1000BASE-T Gigabit Ethernet
DS1404055	2	Passport 8632TXM Routing Switch Module. 32 10/100TX plus 2 GBIC Expanded Memory
DS1404056	2	Passport 8648TXM Routing Switch Module. 48 port 10BASE-T/100BASE-TX Expanded memory
DS1404059	2	Passport 8608GBM Routing Switch Module. 8-port 1000 Base GBIC Expanded memory
DS1404061	2	Passport 8608GTM Routing Switch Module. 8 port 1000BASE-TGigabit Ethernet Expanded memory

Note: The Passport 8608SXE Routing Switch Module - 8 port 1000BASE-SX Gigabit Ethernet (part number DS1404036) is not supported with this feature.

If the I/O modules you have are not of the required hardware revision level and you want to use the new SMLT-on-single-CP functionality, you can order an upgrade for your existing hardware using the part number A0537499.

You can enable or disable the SMLT-on-single-CP functionality by using the following CLI command:

```
config sys set smlt-on-single-cp <enable/disable>
[timer <value>]
```

(Q00854986, Q00815081-01)

- You cannot configure more than 5 static routes on the network management interface. (Q00694618)
- A minimum of 128MB are required to support the Passport 8000 Series switch software Release 3.7. An upgrade kit of 256MB is provided in the Nortel price list; this upgrade kit is not required for the 8691SF. However, because different memory sizes (for example, 256MB for the 8690SF and 8692SF; 128MB for the 8691SF) in the same chassis can cause unpredictable behaviors, Nortel Networks does not recommend nor support a mixed configuration (8690/8691/8692) in a chassis. (Q00723245)
- Nortel Networks does not recommend using the CLI command **`trace level 4 4`**. This command, which provides some very low level information about chassis manager tasks, can impact the overall behavior of the system. (Q00896409)
- Any I/O Module that comes up as faulty on the master CPU will not be synchronized to the backup CPU. All configurations associated with this I/O board will also not synchronize between the master and the backup CPU. (Q00890882)
- Nortel Networks does not support the 8691omSF with the Passport 8000 Series Switch Software Release 3.7. (Q00909840-01)
- When a POS port is reset, meaning administratively disabled and then administratively enabled, STP is disabled or enabled according to the BCP state. So, if BCP was enabled and STP was disabled, after a port is reset, STP will become enabled because BCP was enabled. In this scenario, you will need to manually disable STP. (Q00281408)
- Upon bootup or after a CPU failover, the error message `ERROR Task=tChasServ RTC update on standby CPU failed!` may appear. It has no negative impact on your switch. (Q00527144)

- After setting the `max-mac-count` command for a port, the switch incorrectly allows you to change this value to one that is less than the current mac count. (Q00850159-01)
- Although the copy and cp commands perform the same function, there are some minor differences: the **`copy`** command does not allow wildcard characters and does not display acknowledgement that the copy was successful; the **`cp`** command allows wildcard characters and displays acknowledgement that the copy was successful. (Q00785080)
- 8608 Gigabit ports may not initialize if there is a Kevlar 5112 Firewall connected to any of the ports. This same issue may occur if there is a port connected to other Alteon products, such as the Alteon 184 or 180e. The workaround is to disable AutoNegotiation on the Gigabit ports of both the Passport 8000 and the Alteon switch. (Q00538075)
- Disabling the Telnet daemon prevents any connection between the master and backup CPUs using the Telnet **`peer`** command. (Q00595763-04)
- Illegal or illogical IP addresses cannot be entered in the /etc/hosts filename. The existence of such addresses will create problems with the address/ hostname resolution. (Q00914252)

Switch management

Caution: SNMP community Index length of up to 10 characters and SNMP community string length of up to 30 characters are currently supported. (Q00899521)

Caution: The default community string “secret” for **`rwa`** user in Release 3.5 is no longer valid in Release 3.7. The default on Release 3.7 is “public” and “private.” (Q00895834)

Caution: If you connect to Device Manager and then remove or add a management route before you close Device Manager, the connection to the switch is lost. Nortel Networks strongly recommends closing Device Manager before deleting or adding a route. (Q00907359)

General

- The traceroute feature will be supported in Release 3.7.1 release. (Q00912303)
- When you save the configuration file to the backup file, the primary configuration file is saved too. (Q00915233)
- If a port is part of a MLT/multiple spanning tree groups, it is blocking for a spanning tree group and forwarding for all others, and the port state is toggled, the port routing operational status displays as disabled even if you have enabled routing on the switch.

SNMP

- Because the SysOR MIB is not currently supported, a specific test, used to verify that the agent properly handles unknown contextEngineID values, will fail when executed. The following messages appear:

  ```
  [FAILED] Remarks: get-request operation failed or had
  errors
  Received unexpected noSuchObject exception on get
  operation
  ```
  (Q00486049)
- Using some specific tests related to SNMPv3 compliance, you may experience some issues. (Q00788702, Q00788718, Q00788728, Q00788722, Q00788723)
- The usmUserStorageType object is not supported in Release 3.7. (Q00799662)
- The MIB mib-2.80.1.1.0 is not supported in Release 3.7; consequently, the snmp walk reply shows “noSuchInstance” for this MIB. (Q00849687, Q00849691)

- Because of security concerns, community strings in the community table are now shown as ********* strings. Community strings will be translated into the community table, using the new format, during the upgrade from Release 3.5 to 3.7. Because community strings are no longer displayed, you must remember their community strings. (Q00883778)
- The trap notify table is based on the IP address of the target station and not the type of user. Therefore, all users, whether or not they have trap tags defined, will receive traps as long as they are on the same workstation on which at least one user is configured to receive traps. (Q00905161)
- SNMP default strings displace non-default strings in the original indices. (Q00889713)

Device Manager

- SNMP inform messages cannot be sent to a Device Manager session because Device Manager does not have an SNMP engine ID assigned to it. (Q00851264)
- When using Device Manager, you cannot graph a port that is a member of VLAN running OSPF. (Q00897049)
- When the trap option in RMON is set to toOwner (RMON > Options), no traps are received at the Owner. The workaround for this is to set the option to toAll. (Q00908256)
- Device Manager and the CLI incorrectly allow you to configure a large IPX tick value (up to 2147483647). The actual maximum tick value that can be used is 65535. Do not enter a value higher than this. (Q00538439)
- Device Manager uses the default settings of the Java application launcher when it is launched. These default fits most operations, but in large configurations you may need to increase the default heap size setting in the Java application launcher from 64MB to 128MB (-Xmx128m) to avoid display issues or error messages, for example, `java.lang.OutOfMemoryError`.

  Example in a Windows environment:

  a Close Device Manager.

  b Change the shortcut as follows:

  "C:\Program Files\JavaSoft\JRE\1.3.1\bin\javaw.exe" -Xmx128m -cp dm_40.jar;1k_40.jar;2k_40.jar;om8k_40.jar;bs_40.jar;falcon_40.jar;jcchart450k.jar;sfc.jar com.baynetworks.fswitch.dm.DM.

Example in a Solaris environment:

a Close Device Manager.

b Change the shortcut as follows:

$java_cmd -Xmx128m -cp
1k_40.jar:2k_40.jar:om8k_40.jar:bs_40.jar:falcon_40.jar:jcchart450K.jar
:sfc.jar:dm_40.jar com.baynetworks.fswitch.dm.DM $*.

(Q00487953)

- You cannot modify the following values on the Insert Target Table dialog box: TAddress, TagList, TMask, and MMS. If you must change these parameters, use the CLI. Or, using JDM, you can remove the Target Table entry and recreate it with the new values. (Q00914179)
- When you attempt to configure a VLAN ID, an inconsistency exists between Device Manager and the CLI. Device Manager does not allow you to create a VLAN with a VLAN ID of 4094. However, you can create a VLAN with a VLAN ID of 4094 using the CLI. Nortel Networks does not recommend that you use VLAN IDs ranging from 4000 to 4095. These values should be reserved for spanning tree group (STG) IDs (Nortel multiple STGs implementation). (Q00912868)

RMON

- RMON is not properly synchronized between both CPUs in HA mode. Nortel Networks is working on this enhancement, which will be provided in the 3.7.1 release. Please contact your representative for more information. (Q00535146)

Bandwidth management

Filters

- When you enable filters on ports, the filters may affect ports other than those on which the filters were configured. This problem exists when the Filter Mode is set to Forward and the Port DefaultAction is set to Drop. For example, if you enable a filter set on port 9/12, the PC that connects to port 10/12 (8648TX(E)) can no longer send data to networks through which the default gateway for unknown destinations must be used. However, paths known locally or via OSPF work correctly. (Q00912316)

ATM

- When you apply filters to an ATM port and set its default action to drop, if an ARP entry for the next hop out of an ATM interface times out, the entry will never be relearned and all outbound traffic will be dropped from that interface. However, if you set the action to forward, the ARP entry never ages and no connectivity problems occur.

  The problem can be fixed by bouncing the ATM port or when ingress packets are received on the ATM interface or PVC. (Q00818603-01)

- The ATM card becomes disabled after it receives the following error message: `SW ERROR smMsgSend: failed take the wait Semaphore`. (Q00859608)
- If a DS3 ATM MDA is not seated properly on the ATM module baseboard, DS3 port status, port administrative status and port LED status may appear in an “up” states, however, the PVCs may remain in a down state.

  For troubleshooting purposes, use these suggested steps to verify if the MDA is properly seated (once the F5-OAM loopback feature is enabled, it can be used to detect such conditions):

  a Create an STG on the switch or use an existing group.

  b Create a VLAN under this STG group.

  c Add ATM ports to this STG and VLAN.

  d Create a PVC executing the CLI command `config atm <slot/port> pvc create 0.1`.

  e Enable F5-OAM on this PVC (0.1) by executing the CLI command **`config atm <slot/port> pvc f5-oam 0.1 enable`**.

  f Create an ELAN by executing the CLI command `config atm` **`<slot/port> pvc 1483 bridged create vlan-id 0.1`**.

g Configure the other end of the link and then execute the CLI command **sh ports info atm f5 <slot/port>** to verify the PVC is up. If it is not up, then remove, reseat and refasten the MDA. (Q00539342)

Caution: For a default VLAN when the aging-timer is set from the CLI, it is reflected correctly on Device Manager. When it is set from Device Manager, it is reflected correctly in CLI. But for a non-default VLAN this is not the case. For example, a change from the CLI is not reflected in Device Manager and a change in Device Manager is not reflected in the CLI.

Since the aging-timer functionality works correctly in the CLI, use the CLI to change the aging-time field. (Q00915466)

- For a default VLAN when the aging-timer is set from the CLI, it is reflected correctly on Device Manager. When it is set from Device Manager, it is reflected correctly in CLI. But for a non-default VLAN this is not the case. For example, a change from the CLI is not reflected in Device Manager and a change in Device Manager is not reflected in the CLI.

  Since the aging-timer functionality works correctly in the CLI, use the CLI to change the aging-time field. (Q00915466)

Layer 2

LACP

Caution: The fast periodic time value of 200 ms is not supported for this software release. The minimum supported fast periodic time value is 400 ms (Q00834573).

STP

- In some rare cases, when you enable the `perform-tag` flag on a MLT, the status reported by the CLI command **`show STP status`** is incorrect.

SMLT

- Multicast routing with PIM and DVMRP enabled is not supported on the edge switch of a Triangle SMLT configuration. In addition, IP multicast routing is not supported on SMLT square and cross configurations. However, IGMP snooping is supported and queries for a given VLAN must be placed on one switch only. (Q00072438)
- End-to-end multicast traffic stops after reconnecting the broken half of a square/cross SMLT. (Q00075866)

Layer 3

IP

ARP

- If an MLT port has a static ARP associated with it and if that port is moved out of the MLT, the static ARP will not remain with the MLT, but will be moved out with the port. (Q00647998-02)

BGP

- Nortel Networks recommends using an 8691SF or an 8692SF in a BGP configuration.
- BGP is not supported in HA Layer 3 mode.
- The FlapPenalty value does not get refreshed in a BGP route dampened window. (Q00804187)
- The Remain field is not visible from the BGP dampened Routes window in JDM. There is currently no MIB support for this parameter. (Q00804182)
- The BGP CLI command **`config ip bgp redistribute direct`** is not in compliance with the CLI nomenclature and should be **`config ip bgp redistribute local`**. (Q00528995)
- If OSPF is using a policy that has an as-list and community list configuration, the route policy server attempts to add the configured as-list and community list to the OSPF local list. However, because OSPF does not use the as-list and community list, it provides a null head pointer. The route policy server then adds the as-list and/or community list to its global list, and a duplicate as-list and/or community list appears in the configuration. This issue will be fixed in Release 3.7.1. (Q00684082)

- Disabling BGP does not remove redistributed BGP routes in the OSPF LSDB. Routers running OSPF continue to receive the redistributed BGP routes. To exit this condition, either reset OSPF or reset the OSPF redistribution with BGP disabled. (Q00683022)
- Match Community/AS Path will work in OSPF redistribution only when the same route policy is coupled with BGP. If you do not need this BGP redistribution, you may choose to mark its state as disabled (Q00693853, Q00173743-01)
- The maximum limit of “Max-prefix” (config ip bgp neighbor <neighbor IP>) is shown as 2147483647 but the actual value is 999999. (Q00915249)

HA (High Availability mode)

The following protocols are NOT currently supported in HA mode:

- ATM and POS modules
- WSM; however, WSM incorrectly stays online when HA-CPU is enabled (Q00495703)
- BGP; therefore, all redistribution parameters (policies) related to BGP are not synchronized in HA mode (Q00786353)
- Multicast dynamic routing protocols (DVMRP, PIM-SM, PIM-SSM, PGM)
- VRRP Fast Advertisement Interval feature; a consistency check prevents the feature from being enabled
- IPX routing
- RMON; it will be supported in the Release 3.7.1 (Q00912566, Q00913212)

OSPF

- Occasionally, you may see the following message when sending link state updates:

  ```
  OSPF ERROR ospfAddToReqList
  ```

  This message has no impact on the switch. (Q00861942)
- Currently, there is no alarm or trap sent if the synchronization between the 2 CPUs cannot be done. (Q00781173)
- The backup CPU does not display the correct information about the I/O module types if the initialization of the I/O fails. (Q00799826)

- Nortel Networks recommends that you do not enable or disable I/O slots during an HA failover. Wait for the `system ready` message on the master CPU before enabling or disabling an I/O slot. (Q00885940)
- If you change the **`ha-cpu`** flag, the switch saves the change to /flash/boot.cfg only on both the master and backup CPUs, even though both CPUs were booted up using pcmboot.cfg. Because the flag's status has been changed, the backup CPU immediately boots up with pcmboot.cfg. However, because the change to the **`ha-cpu`** flag was saved to boot.cfg, the HA status of the switch does not change. (Q00911908)
- No error message is displayed if you do not have matching software versions on the primary and secondary CPU and are in HA mode. (Q00248522)
- The robustness value may incorrectly display in the `show ip igmp mrdisc-nei` CLI output on the receiving switch. The incorrect value is then copied to the standby CPU. This value is for informational purposes only and does not affect the operation of your switch. (Q00536682-01)
- After a failover (HA enabled), if the new master CPU does not complete table synchronization prior to another failover, the new master CPU will reboot. (Q00157504)
- The bootconfig flag, **`verify-config`**, changes from true to false if you reboot a High Availability (HA) chassis with incompatible protocols. This behavior allows the switch to boot properly if the previous configuration contains features not supported by HA. (Q00883779)
- In HA mode, when you reset ECMP multiple times, and you perform HA failover, the switch displays the following message on the backup CPU: "wrong updateFDB." This condition has no affect on the switch. (Q00912709)
- When you remove a module during CPU failover, the switch resets. (Q00790435)

Link Aggregation Group (MLT/IEEE 802.3ad)

- When you add a port to an aggregation group, the values of the rate limiting parameters on the port remain the same (that is, they are not updated, based on the values configured for the other aggregation group ports). To work around this limitation, first add all the ports to the aggregation group, and then change the rate limiting values of any port. (Q00805119)
- When the timer expires, the LACP Partner operation is not removed. (Q00762380)

- If you use LACP in an SMLT/Square configuration, LACP must have the same keys for that SMLT/LAG (Link Aggregation Group). Otherwise, the aggregation may fail if a switch failure occurs. Nortel Networks recommends that the same key be used for the two devices participating in the SMLT/LAG. Also, the two devices participating in the SMLT/LAG must have the same LACP port configuration values for system-priority, timeout, and mode. (Q00789437)
- If OSPF is enabled, do not set the LACP periodic transmission timer to less than one second. (Q00787821)
- If you have two switches, A in active mode and B in passive mode, when you change the status of the active switch to passive, reconvergence takes about 90 seconds. During this time, traffic from switch B to switch A will be sent for up to 90 seconds, but will not be received by switch A. No traffic will be sent from switch A to switch B. (Q00821166)
- In a core full meshed environment using RSMLT, HA, LACP, and VRRP (edge), if a HA transition occurs (CPU transition from master to backup) or if the IST link goes down, all the LACP ports will transition. (Q00836591)
- To correctly enable tagging in LACP applications, you disable LACP on the port, enable tagging on the port, and then re-enable LACP. (Q00859567)
- When more than 2000 ARP entries are learned on a single port, port link changes (down/up) may cause time sensitive protocols, such as VRRP or LACP, to change states on other ports. (Q00890785)
- If an SMLT aggregation switch has LACP enabled on some of its MLTs, do not change LACP system priority after LACP is enabled on ports. If some ports do not get into desired MLT after dynamic configuration change, enter the CLI command **`clear-link-aggregation`** on the MLT. (Q00822182)
- LACP-enabled ports with the same key must have the same VLAN membership. On LACP-disabled ports with the same key, VLAN membership can be different. This usually happens when you add VLANs to or delete VLANs from these ports. But before LACP is re-enabled on these ports, VLAN membership must be the same for ports with the same key. (Q00857570)
- If you set the broadcast rate limit value on a disabled MLT port, the value is reflected on the other MLT ports, but the rate limiting of the active link is still done based on the older value. For example, if you have two ports with a rate limit value of 10, and then the active link will be limiting broadcast to 10. If one of the MLT ports is disabled, the other one becomes the active link and continues to limit the broadcast to 10. If the rate limit value is changed to 500

on the disabled port of the MLT, the rate limit value of the active port changes to 500, but this port still limits the broadcasts to 10 rather than allowing 500. This behavior continues even if the disabled port is later enabled. (Q00805123)

- While copying a large file from the PCMCIA to flash, the SMLT/LACP ports may transition. (Q00906148)

RSMLT

- If you are using RSMLT instead of VRRP, you need to configure the RSMLT holdup-timer to 9999 in order to provide indefinite peer backup. (Q00789564)
- When peer switches configured to use RSMLT do not have the same DHCP configuration, unexpected results can occur. If there is a discrepancy in the DHCP configuration, RSMLT will reroute the traffic, but users could lose the connectivity if at the same time, their DHCP lease expires and DHCP is not properly configured on both core switches. (Q00787428)
- IPX RSMLT failover time may be greater than 30 seconds. This is due to the RIP/SAP learning process. (Q00745690)

IPX

- Occasionally, a client cannot establish a session with the server. The problem may be a network latency issue with the Windows XP NetWare client version 4.90.0.0 for Windows XP. The problem is caused by setting the Auto_Frame detection parameter, which is found under the NwLink settings. Nortel Networks recommends not using this parameter. (Q00812779)
- Using Device Manager, the IPX encapsulation type of an interface cannot be changed, whereas the CLI allows you to do so using the following CLI command: **config vlan <*vid*> ipx encapsulation <*IPX-network-number*> <*encapsulation*>**. (Q00910444)
- Because of some Device Manager inconsistencies, Nortel Networks highly recommends that after you enable RSMLT using Device Manager to enter the CLI command:

  config vlan <vid> ipx rsmlt enable (Q00915467)

VRRP

- VRRP hotstandby (with WebOS software version 10.0.29.0) is not supported in this release. (Q00249554)
- Nortel Networks does not recommend using the same IP address for the VRRP logical IP interface and the physical IP interface. (Q00812854)

Multicast

General

- When using the Multicast Router Discovery protocol on a Passport 8100/8600 connected to other devices implementing this protocol, there could be interoperability issues given that the Passport 8600 implementation sends multicast router discovery messages to the 224.0.0.2 address (all routers address) based on the fact that early drafts did not define this destination address. Newer drafts (http://ietf.org/internet-drafts/draft-ietf-idmr-igmp-mrdisc-08.txt), define the destination address as the all hosts address of 224.0.0.1 and devices implementing Multicast Router Discovery protocol based on the latest drafts will not interoperate with the Passport 8100/8600, unless they are able to send and receive Multicast Router Discovery messages using the 224.0.0.2 address. (Q00309216)
- When you enter the CLI command **`query max response`**, the switch sets the wrong parameter value for an IGMPv3 interface. (Q00912706)

IGMP

- In a SMLT configuration, when multicast traffic ingresses on an IGMP snoop-enabled edge switch from a PIM or a DVMRP enabled IST switch, show ip igmp sender CLI output will always display the IGMP Querier port as the sender port even though data is actually ingressing on a different port of the MLT. There is no traffic loss due to this issue. (Q00668314)

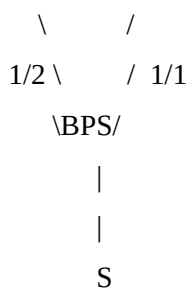
DVMRP

- Scaling with 500 DVMRP interfaces and 1980 VLANs with 512 neighbors or more will result in a high CPU utilization that could reach 100%. If you need to configure a large number of interfaces, you cannot have all these interfaces with DVMRP neighbors, but only attached to LANs without routers running DVMRP. (Q00646615)

- Before configuring DVMRP on an interface using Device Manager, please be sure that DVMRP has been globally and successfully configured (Q00912792).

PIM

- Non-DR switch receives double traffic when a receiver is connected to a non-DR switch and the unicast route (shortest path) towards the source is not through a DR switch. Both non-DR and DR switches create (*,G) and (S,G) records. (Q0086744)
- On a VLAN spanning more than 2 switches, `SPT path joins` are received on one port of the spanning VLAN. The messages on the VLAN port on which RP-to-source prune messages are received will not be properly pruned and will stay in a prune pending state (because of overriding joins received on the port in the SPT path). (Q00421566)
- The PIM MRtable incorrectly shows incoming traffic port when there is an SMLT fail over. (Q00664751)
- R1 and R2 are running PIM:
  - (non-DR)R1 ---------- R2 (DR)



  This issue happens with the BPS at the edge. The BPS always chooses to forward on the lowest link of the MLT. If we reboot the DR switch (traffic was flowing through 1/1), traffic recovers through 1/2.

  On R1, since it is getting data locally through 1/2, the source->upstream becomes NULL. When R2 comes back up, traffic starts flowing on 1/1 to R2. However, if the unicast route to the source subnet still lies through R1 (since R2 rebooted), joins to the source will go to R1 instead of R2. Now R1 has to send a join to R2 to receive traffic, but it will not do so since its source-> upstream is NULL (it thinks that the source is local).

The workaround for this issue is to always connect the lowest IP address (non-DR) to the lowest MLT port on the BPS. For example, in the above diagram, 1/1 should go to R1. On R1, we will always do FWD_TO_DR, so both R1 and R2 will receive traffic. Hence, whichever switch receives the join after a reboot, it will have traffic and be able to forward the same. (Q00658544)

Reading path

Note: The complete documentation set will be available June 3, 2004.

This section lists the documentation specific to the Passport 8000 Series Switch platform. To find the most up-to-date 8000 Series document, access the Nortel Networks customer support Web site, www.nortelnetworks.com/documentation.

Follow these steps:

1. Under By Product Family, select Passport.
2. Under Passport: General Availability, select Documentation under Passport 8000 Ethernet Switch Series: Passport 8600 Routing Switch.

Always look for the latest revision of your requested document on the Web.

You can print the listed technical manuals and release notes free, directly from the Internet. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

Related publications

This section describes common documentation related to the Passport 8600 switch.

Release notes and Important Information documents

These guides provide late-breaking information for installing, configuring, and managing your Passport 8600 switch.

Release Notes for the Passport 8000 Series Switch Software Release 3.7	317177-A
Important Information about the 8600 Series Switch Modules	316340-B
Important Security Information for the 8000 Series Switch	314997-C

Installation and User Guides

These guides provide instructions for installing the chassis and its components, installing and using the Device Manager software, and configuring various protocols on the Passport 8600 switch.

Adding MAC Addresses to the 8000 Series Chassis	212486-B
Installing and Maintaining the 8600 Series Chassis and Components	316314-D
Installing 8600 Switch Modules	312749-H
Installing a CPU Memory Upgrade	314832-B
Installing GBIC and Gigabit SFP Transceivers	318034-A
Getting Started	313189-D
Installing and Using Device Manager	316341-B
Managing Platform Operations	315545-C
Using Diagnostics Tools	317359-A
Using the Packet Capture Tool (PCAP)	315023-C
Using the 10 Gigabit Ethernet Modules: 8681XLR and 8681XLW	315893-C
Using the 8672ATME/ATMM Modules	209195-E

Reference and Configuration Guides

These guides provide reference and configuration information for the Passport 8600 switch.

Configuring Internet Membership Group Authentication Protocol (IGAP).	316343-B
System Messaging Platform Reference Guide	315015-C
Configuring QoS and IP Filtering	316433-C
Configuring IP Routing Operations	314720-D
Configuring IP Multicast Routing Protocols	314719-C
Configuring BGP Services	314721-C
Configuring Network Management	314723-C
Configuring IPX Routing Operations	314722-B
Configuring and Managing Security	314724-C
Configuring VLANs, Spanning Tree, and Link Aggregation	314725-C
Configuring the Web Switching Module using Device Manager	314995-B
Network Design Guidelines	313197-D

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.