Part No. 316811-C Rev 00
December 2004

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Passport 8300 Series Switch Software Release 2.1

316811-C REV 00

NORTEL NETWORKS™

Copyright © 2004 Nortel Networks

Trademarks

Restricted rights legend

Statement of conditions

Nortel Networks Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Introduction

These release notes for the Nortel Networks* Passport 8300 Series switch Software Release 2.1 describe the hardware and software and any known issues that exist in this release. They are based on REL2.1 and Java Device Manager (JDM) 5850.

A list of related publications can be found on page 45. The Passport 8300 Series switch Software Release 2.1 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/support. For more information, see the "Reading path" on page 43.

The following topics are discussed in this document:

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

File names for this release

Table 1 describes the Passport 8300 Release 2.1 software files and the hardware they support.

Table 1 Passport 8300 Release 2.1 files and associated hardware

Module or file type	Description	File name
Boot monitor image	CPU and switch fabric firmware for the Passport 8300 switch. Supported on Passport 8393SF modules	p83b2100.img
Runtime image	The Passport 8300 image. Supported on Passport 8393SF modules	p83a2100.img
Pre-boot monitor image	Pre-boot monitor image	p83f2100.img
MIB (private)	Passport 8300 private MIB	p83a2100.mib
MIB zip file	Passport 8300 MIB	p83a2100.mib.zip
Input/output modules download file	Supported on Passport 8348TX, 8348TX-PWR, and 8324GT	p83r2100.dld
Encryption module for SNMPv3 (includes DES encryption capabilities)	Supported on the Passport 8393SF modules	p83c2100.des
Device Manager software image for Windows (Version 5.8.5.x)	Device Manager software image for Windows NT, Windows XP, Windows 2000, Windows 98, and Windows 95	jdm_5850.exe
Device Manager software image for UNIX (Version 5.8.5.x)	Device Manager software image for Solaris Device Manager software image for HP-UX	jdm_5850_solaris_sparc.sh jdm_5850_hpux_pa_risc.sh
Device Manager software image for Linux (Version 5.8.5.x)	Device Manager software image for Linux	jdm_5850_linux.sh

Before upgrading the switch from a previous release

Before upgrading to Passport 8300 Switch Series Software Release 2.1, take special note of the following cautionary messages.

- The configuration file generated with Passport 8300 release 2.1 software may contain options that are not backward compatible with Passport software releases 2.0.0.1 and 2.0.1.0.
- After you upgrade your Passport 8300 series software, make sure you save the configuration file.
- When installing files on the on-board flash or PCMCIA, make sure that you verify flash capacity before downloading the files.
- 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 CLI command:

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

  where device can be the local PCMCIA or a remote PC host.

Upgrading the switch to the Release 2.1 software

Refer to *Upgrading to the Passport 8300 Series Switch Software Release 2.1* (part number 318769-B) for the detailed procedures to upgrade the switch.

Note: Read the entire upgrade procedure before attempting to upgrade the switch. Upgrade procedures cause interruption of normal switch operation. Back up your runtime configuration and boot configuration before starting the upgrade process.

New Passport 8300 hardware

Table 2 describes the new Passport 8300 hardware in this release.

Table 2 New Passport 8300 hardware

New hardware	Module part number	Where to find information	Document part number
Passport 8306 (6-slot PoE chassis)	DS1402008	Installing and Maintaining the Passport 8306 and 8310 Chassis	316795-B
8302AC low power supply	DS1405?16 (The question mark represents country code variants A–F.)	Installing an AC Power Supply in the Passport 8300 Series Chassis	316797-B
1000 BaseT SFP	AA1419043	Installing GBIC and Gigabit SFP Transceivers	318034-A

Passport 8010/8006 chassis support

You can use Passport 8300 modules with the Passport 8010 and 8006 chassis. The following requirements must be adhered to, however:

1. The Passport 8010 and 8006 chassis require 4096 media access control (MAC) addresses to use the Passport 8300 modules. The upgrade kit (DS1411015) that allows you to increase the MAC addresses on your Passport 8300 switch to a total of 4096 MAC addresses is available for this purpose. For more information about this kit, see *Adding MAC Addresses to the Passport 8000 Series Chassis* (part number 212486-B).
2. The Passport 8300 switch fabric modules (8393SF) are limited to one switch fabric per Passport 8010 or Passport 8006 chassis. This single switch fabric in the 8010 or 8006 chassis can be in either slot 5 or 6. Dual switch fabric modules in these chassis are not supported. Only Passport 8310 and 8306 (10-slot and 6-slot PoE chassis) support dual switch fabric configurations.

3 The Passport 8010 and 8006 chassis do not support Power over Ethernet (PoE) capabilities on the PoE module. Therefore, the PoE feature is not available in these chassis.

Note:

1. You can use the Passport 8348TX-PWR module in these chassis. Be aware, however, that when the 8348TX-PWR module is operating in the 8010 or 8006 chassis, it operates as a Passport 8348TX module.

2. In an 8010 or 8006 chassis, you cannot mix Passport 8300 modules with Passport 8600 or 8100 modules.

Supported SFPs

Table 3 lists the transceivers supported by the Passport 8300.

Table 3 Supported SFP transceivers

Model	Product number
SFP transceivers:	
1000BASE-SX (LC Type)	AA1419013
1000BASE-SX (MT-RJ Type)	AA1419014
1000BASE-LX (LC Type)	AA1419015
1000 BaseT SFP	AA1419043

Table 3 Supported SFP transceivers (continued)

Model	Product number
CWDM SFP GBICs:	
1470nm/Gray	AA1419025 AA1419033
1490nm/Violet	AA1419026 AA1419034
1510nm/Blue	AA1419027 AA1419035
1530nm/Green	AA1419028 AA1419036
1550nm/Yellow	AA1419029 AA1419037
1570nm/Orange	AA1419030 AA1419038
1590nm/Red	AA1419031 AA1419039
1610nm/Brown	AA1419032 AA1419040

Features supported in this release

The Passport 8300 is the next generation of cost-effective, Power over Ethernet (PoE)-enabled, modular Ethernet switches. Delivering high density 10/100/1000 connectivity, high-performance Layer 3 switching, industry-leading resiliency, security and services, it is the solution for enterprises seeking to extend the intelligence of their network from the network core to the edge. Its hardware and software capabilities provide the PoE, quality of service, and feature set to enable voice over IP, video and multimedia applications.

New hardware in this release

8306 PoE chassis

The Passport 8306 PoE chassis is a 6-slot (2 slots for switch fabrics and 4 slots for I/O cards) chassis that supports PP83xx modules and power supplies. The chassis uses the same metalwork as the 8006 chassis, but consists of a modified backplane to support PoE.

8302AC - low power supply

The 8302AC power supply allows customers to deploy Passport 8300 switches in the same power infrastructure as the PP81xx/PP86xx switches. The power supply essentially will be the same as the 8301AC with a limit on the available PoE. The power supply is designed to maximize the available PoE with design targets of 200W @110v and 400W @ 220v.

The 8302AC power supply uses the same power cords as the 8004AC supply currently shipping on the PP81xx and PP86xx platforms.

➡ **Note:** The 8302AC power supply requires V2.1 software in order for the system to recognize it properly. If the system has a version of software prior to V2.1 and is booted with the 8302AC power supply in place, PoE will not be available.

1000 BaseT SFP

Passport 8300 Release 2.1 supports the 1000BaseT SFP (AA1419043) with the existing supply base. Testing and qualification ensures that all 8 slots on the 8393F can be populated with the 1000 BaseT SFP.

New software features in this release

DHCP Relay

The Dynamic Host Configuration Protocol (DHCP), an extension of the Bootstrap Protocol (BootP), is used to dynamically provide host configuration information to the workstations. To lower administrative overhead, network managers prefer to configure a small number of DHCP servers in a central location. Using DHCP servers requires the routers connecting to the subnets or VLANs to support the BootP/DHCP relay function so that hosts can get the configuration information from servers several router hops away.

The following differences between DHCP and BootP are specified in RFC 2131 and include functions that BootP does not address:

- DHCP defines mechanisms through which clients can be assigned a network address for a finite lease (allowing for reuse of IP addresses).
- DHCP provides the mechanism for clients to acquire the entire IP configuration parameters needed to operate.

DHCP uses the BootP message format defined in RFC 951. A packet is classified as DHCP if the first four octets in the options field are 99, 130, 83, 99, and the fifth octet is 53. The first four octets are referred to as the “Magic Cookie,” while the fifth is the DHCP message type code. The remainder of the options field consists of a list of tagged parameters that are called “options” (RFC 2131).

BootP/DHCP clients (workstations) generally use UDP/IP broadcasts to determine their IP addresses and configuration information. If such a host is on a network or a subnet segment (or VLAN) that does not include a DHCP server, the UDP broadcasts are by default not forwarded to the server located on a different network segment or VLAN. The 8300 must be configured to overcome this issue by forwarding the broadcasts to the server through virtual router interfaces. The router interfaces can be configured to forward DHCP broadcasts to other locally connected network segments or directly to the server’s IP address (transformation of the broadcast to an unicast). DHCP must be enabled on a per-routable-interface basis. A maximum of 10 DHCP servers can be configured per device.

User-defined protocol-based VLAN enhancements

This enhancement is required to allow flexibility in configuring user-defined protocol-based VLANs. It is especially important for the Passport 8300 switch because of the limitation in the number of VLAN records available in the system. The requirements are the following:

- Allow ranges for user-defined protocol-based VLANs. The range could be a contiguous range or any set of protocol types, up to 8 maximum.
- Allow the reuse of some existing protocol types from the predefined list of protocol-based VLANs. This will allow flexibility for customers to use a subset of predefined protocol-based VLANs, such as some of the DecOther and not all. This will also consume fewer VLAN records in the hardware. Refer to Table 5 on page 20 for the protocol-based VLAN record consumption.
- Allow to choose encapsulation type for the configured protocol-based VLANs.
- A port can belong to a user-defined protocol-based VLAN with protocol types that match existing predefined protocol-based VLANs, or configured user-defined protocol based VLANs, as soon as they are not configured on that port at the same time. Consistency checks should be provided to prevent a customer from configuring the same protocol type of protocol-based VLAN on the same port.
- With the exception of DecOther, the currently non-allowed protocol types (illegal) should also be non-allowed with this enhancement.

Extensible Authorization Protocol (EAP) enhancements

Guest VLAN

This feature allows users to accept stations from partners connected to a temporary VLAN, known as the Guest VLAN. If the station initiates an EAP authentication and authentication is successful, the station is redirected to the corporate VLAN defined by the network manager. This feature provides both flexibility and security.

Multiple Hosts Multiple Supplicants

Legacy or standard EAP does not allow the presence of multiple EAP supplicants on the same physical port. In some configurations, network managers do not want to allocate a port per station. This feature reduces the cost of ownership by allowing multiple stations to share the same physical port. Every EAP session will be individually monitored to guarantee maximum security.

EAP and non-EAP supplicants on the same port

This enhancement allows customers to combine EAP supplicants and non-EAP supplicants on the same port. This is particularly important in cases where a station is connected to a VoIP phone which itself contains a switch. The station can use EAP for authentication. Because not all IP phones currently support EAP, network managers will use the MAC address of the phone to secure the traffic from that device. Up to eight non-EAP devices can be connected at the same time.

Custom Auto-Negotiation Advertisements (CANA)

This feature allows you to limit the maximum speed that can be negotiated on a given Ethernet port. It is especially useful on the 10/100/1000 ports, but should be supported on all types of ports. You can set the ports not to negotiate above a given speed (10 or 100 Mbps) so that users attached to these ports do not get higher bandwidth than that allowed for their systems.

In Release 2.1, you can enable or disable auto-negotiation. When auto-negotiation is disabled, the hardware is configured for a single (fixed) speed and duplex value. When auto-negotiation is enabled, the advertisement made by the product is a constant value based upon all speed and duplex modes supported by the hardware. When auto-negotiating, the product will select the highest common operating mode supported between it and its link partner.

In several situations, it is beneficial to be able to auto-negotiate a specific speed and duplex value. In this situation, the product can allow for attachment at an operating mode other than its highest supported value. For instance, if the product only advertises a 100 Mbps full-duplex capability on a specific link, then the link will only go active if the neighboring device is also capable of auto-negotiating a

100 Mbps full-duplex capability; this can prevent mismatched speed/duplex modes if customers disable auto-negotiation on the neighboring device. Based upon the advertisement made, the link partner would negotiate to select the highest common operating mode.

Auto-negotiation must be enabled per port and allows you to set a maximum speed for auto-negotiation on that port.

Auto MDI/MDI-X

This capability allows the detection of the crossing of the pairs attached to a given port (MDI or MDI-X) and automatically adapt to this setting. There is no CLI, NNCLI or Device Manager requirement for this feature, and it has to be implemented on the driver of the hardware to allow this detection automatically and configure the port accordingly.

“Spinning slash” on code download

When downloading code to flash from a TFTP server, a spinning slash appears on the console to enable customers to see the progress of the download and to ensure that the switch is responding. In Release 2.0, the software does not show anything during the download, leading customers to consider that the switch is not responding. The spinning slash function is provided for any download operation, including those at the boot monitor.

Supported software and hardware capabilities

Table 4 lists the known limits for the Passport 8300 software release 2.1 and JDM 5.8.5.0 of the Passport 8300 Series switch software. These capabilities will be enhanced in subsequent software releases.

Table 4 Supported capabilities in the Passport 8300 Series switch (Release 2.1)

Feature	Maximum number supported
VLANs	Up to 4,000 VLANs. 200 have been tested and are officially supported in release 2.1.0
Protocol-based VLANs	12 records, 50 VLANs maximum
ARP Records	2500

Table 4 Supported capabilities in the Passport 8300 Series switch (Release 2.1) (continued)

Feature	**Maximum number supported**
IP interfaces	Up to 500 IP interfaces. 200 have been tested and are officially supported in release 2.1.0
Local next hops	500
Static routes	1000
Spanning Tree groups	Up to 64. Groups 1 through 25 have been tested and are officially supported in release 2.1.0
Aggregation groups • 802.3ad static aggregation groups	31 • For 8348TX ports, you can use only Link Aggregation Groups 1-7 • For 8324 ports and CP I/O ports, you can use Link Aggregation Groups 1-31.
Ports per aggregation group **Note**: All the ports MUST be of the same type (no mix of technology is supported)	4
IGMP maximum number of unique groups	1800

The Passport 8300 supports VLAN IDs from 1- 4000.

Note: Jumbo Frames are not supported in Release 2.1. Thus, you should not use the **mtu** command in the NNCLI Global configuration mode. (Q00876423)

Hot-removal/hot-insertion of Passport 8300 modules

In general, after you hot-insert or hot-remove a Passport 8300 module, you must wait 30 seconds before performing another hot-insertion or hot-removal of a module.

Hot-removal of master CPU

In a dual CPU configuration, both CPUs require the same set of images at all times. When you insert a new CPU in the Passport 8300, you should ensure that it has the same set of boot and runtime images as the existing CPU.

Removing the master CPU can result in a configuration loss for the removed CPU if it is replaced in the Passport 8300 switch. To avoid this situation, follow these instructions if you need to remove a master CPU from an 8300 chassis:

1. Perform a soft reset on the master CPU to cause failover to occur.
2. Wait until the new master comes up and the old master becomes the standby.
3. Remove the standby CPU. If you need to re-insert this CPU, you must wait at least 60 seconds.

Note that if you remove the master CPU without following this procedure and then save the configuration after removal, the new configuration will not contain the removed CPU configuration. You will then need to reconfigure the CPU ports.

To avoid this issue, back up the existing configuration file before saving any configuration. After you insert the removed CPU, you can then reboot the switch with the backup configuration file to restore the configuration. For more information, see “Guidelines for Warm Standby on the Passport 8300” in the *Network Design Guidelines (316809-B)*.

Protocol-based VLAN limitations

The Passport 8300 switch supports a maximum of 12 protocol VLAN records (Ethertypes). After you create a protocol-based VLAN, you can create additional ones by using the same protocol without consuming extra records.

For example, you can configure 20 ipx802.3 VLANs and 11 IP VLANs on different ports. The 12 record limitation applies to the total number of records used and one VLAN type consumes the necessary records a single time- even if you create several VLANs of the same type.

Note that all protocols do not take the same number of records. Table 5 shows the number of records that each specified protocol VLAN takes.

Table 5 Number of records for specified protocol VLANs

Protocol	Number configurable	Actual number of records per VLAN
IP	6	2
ipx802.3	12	1
ipx802.2	12	1
ipxSnap	6	2
ipxEthernet2	6	2
appleTalk	3	4
decLAT	12	1
decOther	1	9
sna802.2	12	1
snaEthernet2	12	1
netBios	12	2
xns	6	2
vines	12	1
IPv6	12	1
rarp	12	1

When creating user-defined, protocol-based VLANs, you can optimize the number of records used if you limit the encapsulation types. This depends on what encapsulation is used by the traffic matching the protocols in your network. Every encapsulation type that is used consumes an additional VLAN record.

Documentation corrections and additions

BSAC Server for Radius authentication superseded by Steel-Belted Radius Server (SBR)

BSAC server is now owned by Funk Networks and is sold as Steel-Belted Radius Server (SBR). The SBR Version 4.0 or above has a module that supports EAP.

Chapter 5 of *Configuring and Managing Security using Device Manager* (317346-B) and Chapter 10 of *Configuring and Managing Security using the NNCLI and CLI* (316804-B) describe how to use BSAC Server for Radius authentication. The procedures stated for preparing a BSAC server to support Radius authentication are still valid for SBR. However, you must perform the following steps to enable EAP authentication:

1. Ensure the RADIUS authentication and accounting ports match between the SBR Server and the 8300 switch.
2. Edit the eap.ini file in the SBR's " Radius\Service" directory to accommodate the authentication paradigm.
3. Update 5 files for the SBR server:

   — The main dictionary (radius.dct). This file must be edited to contain an entry of parameters from the newly created Passport dictionary.

   — A private dictionary (pprt8300.dct). This file, which is specific to the Passport 8300 switch, must be generated. It will be sourced and used by (dictiona.dcm) and (vendor.ini).

   — The vendor.ini file. This file must contain an entry for the Passport 8300 in order for the file to acknowledge the model/type during the client configuration.

   — The account.ini file. This file must contain the CLI Command = entry.

   — The eap.ini file for SBR Ver4.0 and above for EAP authentication.

   Specifically, you must make the following configuration changes for the SBR server:

   a Add the following lines in files radius.dct and pprt8300.dct:

   ```
   ATTRIBUTE Access-Priority 26 [vid=1584 type1=192
   len1=+2 data=integer]
   VALUE Access-Priority None-Access 0
   VALUE Access-Priority Read-Only-Access 1
   VALUE Access-Priority L1-Read-Write-Access 2
   VALUE Access-Priority L2-Read-Write-Access 3
   VALUE Access-Priority L3-Read-Write-Access 4
   ```

```
VALUE Access-Priority Read-Write-Access 5
VALUE Access-Priority Read-Write-All-Access 6
ATTRIBUTE Cli-Command 26 [vid=1584 type1=193 len1=+2
data=string]
```

Note: The value in the type1 field must match the vendor-specific authentication attribute value.

b Add the following lines in vendor.ini:

```
vendor-product = Nortel Passport 8300
dictionary = pprt8300
ignore-ports = no
port-number-usage = per-port-type
help-id = 0
```

c Add the following entry to the account.ini file:

```
Cli-Command=
```

d In the account.ini file, make sure that the following lines are present:

```
vendor-product = Nortel Passport 8300
dictionary = pprt8300
ignore-ports = no
port-number-usage = per-port-type
help-id = 0
```

e To enable EAP authentication, for the SBR Server Version 4.0 and above, uncomment the line in the eap.ini file.

f Save changes and restart the server to activate the changes.

(Q00947764)

Problems resolved in this release

The following topics describe issues that have been fixed since the Passport 8300 Series switch release 2.0 and include the following topics:

Hardware and platform

- The save config to standby operation no longer fails. (Q00885275)
- An SNMP trap is now generated when an invalid user attempts to access the standby CPU. (Q00855540)
- You can now use the disable slot function on the standby CPU. (Q00894433)
- The *daylight-saving-time true* flag is now functional in the Passport 8300. (Q00893764)
- A save config operation is now supported through RSH in the Passport 8300 switch. (Q00897629)

CLI

- When you enter **`show ip route info`** in the CLI, the total number of routes displayed is now accurate. (Q00830558)
- In the CLI, **`config eth`** *`<port>`* **`filter modify`** *`<acg>`* is now supported. (Q00863954)
- The Passport 8300 now supports **`config vlan`** *`<vid>`* **`action all`**. (Q00885402)

- In the CLI and NNCLI, **`monitor`** no longer references the ATM and POS interfaces. Neither of these options is supported in the Passport 8300. (Q00884069)

NNCLI

- When you enter **`filter acl`**, the help information that appears in the NNCLI now shows decimal and hex input in the list of available options. (Q00859926)
- **`show tech-support`** in the NNCLI now correctly displays LastRuntimeConfigSource information. (Q00868853)
- If the primary and specified backup configuration files fail to load, an indication of a load failure is now provided. (Q00868848)
- In the NNCLI, **`filter access-list`** *`<number>`* **`protocol`** *`<value>`* **`udp le tcp`** now works. (Q00815353)
- In the NNCLI, **`boot host tftp-timeout`** prompts you for a hexadecimal entry. The system now accepts and displays both decimal and hexadecimal values. The range of acceptable values in both the CLI and NNCLI is listed as 1–2147483647. Note that the accepted values are only 1–120. (Q00876473)
- When adding static multicast entries using **`vlan static`** *`<vid>`* **`add-mlt`**, the NNCLI help no longer incorrectly indicates that the valid MLT range is 1–16 but shows the correct range of 1–31. (Q00883943)

Device Manager

- You can now use Device Manager to set the *remark-dscp* and *remark-user-priority* fields in an existing ACE with the traffic type already set to routed. (Q00891752)
- Device Manager no longer permits you to set *all* as the traffic type with both the *remark-dscp* and *remark-user-priority* fields in an existing ACE. (Q00891759)

QoS

- When the MAC address is learned initially, it is assigned the QoS level in the FDB table. In order for the newly configured QoS level to be effective, one of the following events needs to take place:

a The MAC addresses must age out in the FDB table and the new, learned MAC address is assigned to the newly configured QoS level

or

b The FDB table is flushed using **`config vlan x fdb-entry flush`**

or

c The update-dynamic-mac-qos-level on the port is enabled using **`config ethernet 1/1 qos update-dynamic-mac-qos-level enable`** (Q00743087)

- When you delete a QoS policy, Device Manager now does automatically clean up ACE records that may be using that policy. (Q00896616)

Filters

- When creating an ACE, you can now specify the traffic-types *tagged* or *untagged* even if you have not defined either *ether-type* or *user-priority* in the Access-Template. (Q00798469)
- Filters can now be applied to ports from the CPU module. (Q00858970)

VCT

- Be aware that running VCT tests on an active port interrupts traffic. CLI and Device Manager now both ask for a confirmation before this feature is enabled. (Q00860941)
- After running a VCT test on an MLT port, you no longer need to manually disable/re-enable the port once the test is finished. (Q00865582)

Miscellaneous

- On the Passport 8300 switch, the default setting for logging is log level 1 (WARNING level and higher) which does not log messages under the INFORMATIONAL category. If the log level INFORMATIONAL (log level 0) is required, you can turn it on using the **`config log level 0`** command.

  You do not need to return to the default log setting (log level 1) after capturing the required log messages. Having the log level set to 0 no longer results in issues at boot or failover time. (Q00886136)

Known limitations and considerations in this release

The following topics describe issues known to exist in the Passport 8300 Series switch Software Release 2.1 and include the following topics:

Hardware and platform

- If you boot the Passport 8300 with no configuration file and then try to source a configuration file that contains RMON alarms, you can experience a number of instances of the following error message:

  ```
  SNMP WARNING RMON not init before RmonAlarmCreate
  ```

  The RMON configuration messages appear if RMON is not enabled. Alternatively, if RMON is enabled, then the RMON task initialization is delayed. Use **`show rmon info`** to check if RMON is enabled, and reconfigure the RMON alarms and events. (Q01026909)

- Operations over FTP may be slow. It may take several minutes for flash writes for larger files. Do not attempt to abort FTP operations since it may cause flash corruption. (Q00841620)

- If you remove a module and intend to replace it with a different module type, the new module comes up with a default configuration.

Caution: If you do not save the configuration after inserting this module, the next time you reboot the switch, the entire switch comes up with a default configuration.

(Q00848027)

- If a login fails after three attempts when using the console port on a standby CPU, the console port locks. In order to access the CPU, you must use Telnet. A reset of the standby CPU is required to unlock the console port. (Q00885284)
- You cannot re-initialize the management port IP address to 0.0.0.0 from run-time. You can only perform this operation at the console from monitor mode. (Q00883620)
- On devices with IP interfaces and IP-enabled VLANs, you cannot change the management IP address back to default (0.0.0.0/0). You can make this change only from the monitor prompt during boot or if the device does not have IP-enabled VLANs. (Q01040803)
- In a redundant CPU configuration, if both the *savetostandby* and *factorydefault* boot flags are set to true and the box is rebooted, the *factorydefault* flag on the secondary CPU comes up as true, even though the factory default value should be false. You should manually adjust this flag. The flags on the primary CPU are set correctly after the boot. (Q00896569)
- When an image file is copied to the switch using the **`copy`** command, two messages display on the console if the command completes successfully:

  The first message confirms completion of the image data transfer through TFTP:

  ```
  File [source file-path] - xxxx bytes successfully
  transferred
  ```

  The second message confirms that the image has been saved to flash:

  ```
  File [source file-path] - successfully written
  ```

  If the second message does not display, then the file has not been successfully written to flash. (Q01033494)

- File transfer from switch to host workstation can be slow with the **`copy`** command or TFTP client. You will not experience this problem with FTP. In this case, Nortel recommends that you use FTP, or execute a TFTP client on remote host workstation and use the GET operation. (Q001035465)
- After you set the dst-mac's ace-op parameter to a value other than *`any`* and *`eq`* in Device Manager, and then create an ACG, ports cannot be assigned to the ACG.

  The following are examples of the kinds of error messages that display:

  ```
  8310-41:6/config/filter/access-list/1# config ether 4/
  7 filter create 1
  Error Handler:Gen lib error code: 5
  Error Handler:the unit is: 24 and the device: 24
  Error: Port = 4/7, Acl Port create operation FAIL
  ```

  ```
  8310-41:6/config/filter/access-list/1# config ether 4/
  5 filter create 1
  Error Handler:Gen lib error code: 5
  Error Handler:the unit is: 24 and the device: 24
  Error: Port = 4/5, Acl Port create operation FAIL
  ```

  If you change the dst-mac's ace-op to *`eq`*, ports can be added without error messages. (Q00777592)
- You may experience a delay of up to 10 seconds before the login prompt displays in a Telnet session. (Q00972634)
- A copper SFP installed in an 8393 SFP port will only support 1000 Mbps speed. Therefore, it cannot be connected to any device that only supports speeds of 100 Mbps or 10 Mbps (Q00988540)
- The 8302AC power supply requires V2.1 software in order for the system to recognize it properly. If the system has a version of software prior to V2.1 and is booted with the 8302AC power supply in place, PoE will not be available.

CLI

- As it appears in the CLI, the maximum value of the committed and peak burst rate is misleading. The Passport 8300 switch shows only a fixed maximum value of 65535, which does not change based on the configuration. The actual maximum value is calculated from the committed and peak information rates. (Q00765155)

- If you enter **`show filter access-list statistics`** in the CLI when ACE MatchCountMode is disabled, an error message should appear indicating that the feature is not enabled. Currently, the console shows all 0 counters without any traffic or warning messages. (Q00787044)
- The *`ospf [<ports>]`* option under **`show ports error`** is not supported on the Passport 8300 switch. (Q00855057)
- The agetime that displays under **`show vlan info advance`** actually applies to dynamic VLAN membership. In the Passport 8300 switch, dynamic VLAN membership is not supported, so this agetime always appears as 0. Note that this differs from the FDB aging timer. To verify aging time, enter **`info`** under **`config vlan`** *<vid>* **`fdb-entry`**. (Q00827920)
- The **`config bootconfig flags nocheck-sw-version`** command is used for internal troubleshooting purposes only. Its default is false. As a result, the syntax check command **`config bootconfig flags ?`** does not show the nocheck-sw-version.

  To display the current value of nocheck-sw-version, enter the **`config bootconfig flags info`** command. This is also true in the boot monitor mode minus the **`config bootconfig`** portion of the command syntax. (Q00861897)
- The CLI encrypted passwords contain an invalid username called NNCLI. (For security purposes, the file name is not included.) (Q00860779)
- When you enter some commands under **`config sys access-policy policy`** *<number>* **`service`**, *`ssh`* appears in the CLI help as one of the available services. The Passport 8300 does not support this option. (Q00876390)
- When you enter **`show ports error`**, **`ospf`** *[<ports>]* displays in the CLI help as one of the available options. The Passport 8300 does not support this option. (Q00876505)
- In the CLI and NNCLI, be aware that the Passport 8300 does not support **`trace route-policy`**. (Q00884051)
- If the **`show logging file`** command is typed after the logging file has been deleted, the following message displays:

  ```
  can't seek to EOF & BOF <logfile path name> errno:3670026
  S_dosFsLib_INVALID_PARAMETER
  ```

  This indicates that the file cannot be found.

The same error occurs whenever a log message should have been written, but the log file was no longer present on the system. A new log file is created after the error occurs. (Q01026921)

- When a file is being copied to the flash, CPU utilization may show as 100% during the copy. (Q00957081)
- You cannot perform more than one configuration file save at a time. If a second configuration file save is initiated from a separate Telnet session while a file save is in progress, the second operation fails. The following messages display:

  ```
  Another show or save in progress. Please try the command
  later.
  malloc: 0x3d0002
  S_objLib_OBJ_UNAVAILABLE
  Save boot to file <filename> failed.
  ```
  (Q01029311)

- If PCMCIA logging is enabled and the remaining space in the /pcmcia directory is less than the required minimum, the following error message will repeat on the CLI:

  ```
  CPU6 [11/17/04 03:41:01] SW INFO free space 8192 bytes is
  less than minimum 102400 bytes

  CPU6 [11/17/04 03:41:01] SW INFO Logging to PCMCIA
  stopped
  ```
  (Q01029341)

- If you attempt to copy a file to the /pcmcia directory after a previously installed PCMCIA card has been removed, the following message displays, to indicate that the operation failed:

  ```
  Can't open directory "/pcmcia".
  ```

  A number of error codes, starting with a hex number and the `(tShell):`, follow. Ignore these messages. (Q01012518)

NNCLI

- You cannot use the commands `ls` and `directory` while in the NNCLI. Instead, you must use the `dir` command. (CR Q01036158).
- When using RADIUS, no accounting data is sent when you use the NNCLI. Only start/stops are sent. (Q00836588)

- When sourcing a configuration file, even with **`verify config`** enabled, no error message will be generated if a configuration file fails to load due to errors. (Q00799673)
- You cannot display the auto-learned MAC for a specific port in the NNCLI. Instead, it only shows the number of MACs learned. When you enter **`show interfaces vlan autolearn`**, it does not provide an option to specify a port. (Q00816522)
- Be aware that in **Interface Config** mode, **`ip igmp last-member-query-int`** *`<value>`* will have no effect on the Passport 8300 switch. This parameter is not supported. (Q00867884)
- You cannot disable an access-policy in the NNCLI. However, you can still delete it. You can disable access policies from Device Manager. (Q00869924 and Q00876361)
- The current running status of the management port (speed, duplex, etc.) cannot be displayed from the NNCLI. It can be displayed in the Device Manager using the Edit > Port > Interface tab, or in the CLI using **`config bootconfig net mgmt info`**. (Q00842478)
- The NNCLI help for **`no radius-server`** displays *`cli`*, *`snmp`*, and *`eapol`* as valid options. In the Passport 8300, *`snmp`* is not a valid option here. (Q00883983)
- In the NNCLI and CLI, be aware that the Passport 8300 does not support **`trace route-policy`**. (Q00884051)
- In the NNCLI, the *src-port-pair* field is **not** set when you use the range and mask operators. Instead, you can configure this field using the CLI and Device Manager. Note that you can configure the *dst-port* field in the NNCLI with the range and mask operators. (Q00901990)
- In the NNCLI, the command **`eapol re-authenticate`** displays some garbage characters along with the EAP authentication messages. (Q01010343)
- When configuring DHCP Relay for the first time on the Passport 8300 switch, a `save config` is required when using the NNCLI. DHCP Relay will not work until you enter `save config`. (Q01028334)

Device Manager

- The p-to-dscp table is not available in Device Manager. However, it is available in the CLI and NNCLI. (Q00834504)

- When using Device Manager, the hourglass pointer may appear unexpectedly directly over the column headers. If you move the mouse to areas where the tabs for functions exist, the hourglass does not appear and Device Manager operates normally. (Q00793639)
- Be aware that Device Manager may time out when performing operations with trace level 3 turned on. (Q00851125)
- If trace is enabled, you may experience Device Manager timeouts. You cannot avoid this problem completely. You can minimize it, however, by increasing the Device Manager timeout interval. (Q00831569 and Q00831575)
- You cannot convert a MAC auto-learned entry to manual via the CLI and NNCLI. You can only do so via the Device Manager using the VLAN > Mac Learning >VlanMacLearning dialog boxes. (Q00802165)
- Be aware that Device Manager may time out after converting MAC entries and refreshing the Allowed MAC table. You can prevent this problem by increasing the runtime memory allocation size. To do so:

  In a Windows environment:

1. Open a command prompt.
2. Go to the directory where Device Manager is installed.

   For example, if the install directory is C:/Program Files/JDM, in the Command prompt window, type:

   ```
   cd \Program Files\JDM
   ```

3. Enter the following command to launch Device Manager:

   ```
   .\jre\bin\java - Xmx256m- DEMPATH=. -jar .\jdm.jar
   ```

In a UNIX environment:

1. Go to the directory where Device Manager is installed.
2. Enter the following command to launch Device Manager:

```
./jre/bin/java -Xmx256m -DEMPATH=. -jar ./jdm.jar
```

> **Note:** 256 MB is the memory size you plan to use. The default value is 64 MB. You may assign the proper size based on your system environment.

(Q00862945)

- In Device Manager, select VLAN > MAC Learning > Auto Learn > and choose Auto Learn Action (default if none). Highlight a MAC entry and click Apply to convert the entry to manual. Once you do so, it is recommended that you refrain from clicking Apply for these same entries again. Also, be sure to exit this menu following the first apply. (Q00867972)
- When viewing the results under the VLAN tab for Bridge > Forwarding, you may see *unknown:6* displayed for MACs. This is a MAC discard record. (Q00867889)
- Using Device Manager, when you perform an internal loopback test on Passport 8393 data ports (e.g., 5/7 and 5/8), be aware that the operating speed is inaccurate. It indicates 100Mbps, while the CLI shows a value of 0. (Q00870918)
- When you select multiple ports in Device Manager using Edit > Port, the following options are not available: STG, Rate Limiting, or TxQueue. Also, the Dual tab is invalid. When you select a single port, all valid options are available. (Q00870966)
- In Device Manager, when MLT ports are highlighted under the EAPoL tab, the Port Initialize and Port Reauthenticate fields show Unknown:0. This has no affect on EAPoL operation. You can still set the action to true and apply it. (Q00887001)
- In Device Manager, the DSCP to CoS Map table is missing the column specifying the DSCP value. This option is available in the CLI and NNCLI. (Q00780367)

- The Passport 8300 switch displays the following error message when you attempt to configure Guest VLAN in a spanning tree group in Device Manager:

  ```
  rcEapPortGuestVlanEnable.298: The specified operation is
  not allowed
  ```

  The error message is incorrect and misleading. It should read as follows:

  ```
  "Port does not belong to the STG of the Guest Vlan"
  ```

  (Q01024579)

Security

- When you create a user in SNMPv3 by entering the command **`config snmp-v3 usm Manager md5 pass`** and you remove the initial password by entering the command **`config snmp-v3 usm delete initial`**, you must enter the command **`auth Manager old-pass pass new-pass pass`** to make it work. (Q01017469-01)
- The Passport 8300 switch does not meet the following requirements for 802.1x authentication related to the RADIUS authentication:
  - The switch does not return NAS-Port-Type or Called-Station-Id (port MAC address) in authentication requests.
  - The PP8300 switch does not return NAS-Port-Type, Called-Station-Id, or Calling-Station-Id (user MAC address) in accounting requests.

  Full support for these options will be provided in a subsequent release. (Q01032071)

- In rare cases, when the command **`config ethernet <slot/port> eapol`** is entered, the console on the Passport 8300 switch displays the following error message:

  ```
  IoWrite sendto failed : bufSize = 123,
  pRemote = 0x2f50e7fe, pLocal = 0x0
  snmpIoWrite sendto failed : bufSize = 123,
  pRemote = 0x2f50e7fe, pLocal = 0x0
  ```

  (Q01026930)

- Enabling port mirroring on an EAP-enabled port causes authentication failures. (Q01021626)

- Session time values displayed for terminated and unauthenticated sessions in `Multi-host Session Stats` are incorrect. Values displayed for *Session-Id* and *User-name* are also incorrect for some sessions. (Q01042958, Q01042890)
- Up to 8 non-EAP MACs can get through an EAP port when the value of the *`max-non-eap-clients`* parameter is decreased from a previously set value. (Q01040742)
- When EAP is enabled on a port, the port also needs to be configured as multihost if N+1 authorized users will be accessing the port. Otherwise, when the N+1 user accesses the port, EAP port status is changed to force-unauthorized and all currently authorized users are dropped. (Q01038051)

Layer 2 VLANs

- For byProtocol VLANs, a certain number of 'protocol-type' values are restricted (Invalid), because the preconfigured VLAN types (IP/IPX/AppleTalk) already use these values.

  Table 6 lists the currently restricted hex values for preconfigured VLAN protocol types.

Table 6 Restricted protocol-type values (current)

Protocol type	**Hex value**
XNS	0600
IP	0800
BANYAN VINES	0BAD
DEC LAT	6004
RARP	8035
SNA Ethernet2	80D5
AppleTalk	809B, 80F3
IPv6	86DD
IPX Ethernet2, IPX SNAP	8137, 8138

Table 7 lists additional protocol types, from the IANA Protocol Types listing (http://www.iana.org/assignments/ethernet-numbers), whose hex values are restricted:

Table 7 Restricted protocol-type values (additional)

Protocol type	**Hex value**
BANYAN VINES Loopback	0BAE
BANYAN VINES Echo	0BAF
DEC unassigned	8039-803C
DEC Ethernet Encryption	803D
DEC unassigned	803E
DEC LAN Traffic Monitor	803F
DEC unassigned	8040-8042

(Q00806545)

- Device Manager incorrectly allows you to violate the rule that a port cannot belong to more than one user-defined protocol-based VLAN with the same PID. To avoid violating this rule, add ports to VLANs one at a time, and click the Apply button after every addition. (Q01045465)
- CLI and NNCLI help text does not indicate that you can use decimal as well as hex input for the user-defined PID when configuring user-defined protocol-based VLANs. (Q01041504)

PoE

- Current Passport 8300 software does not support a modular automatic power pruning function. When the total Available Power for allocation is 0 and an additional PoE module is inserted, the additional module will not receive any PoE power even if it is configured with Critical Priority. You must manually admin disable a selected PoE module in order to release the power to the higher priority module. (Q00961155)
- Device Manager reports an incorrect amount of PoE power for an installed 8302 Power Supply. The actual amount of power is half what the Device Manager indicates. (Q01039044)

QoS

- When using **config qos egress-counter-set**, the NNCLI does not allow you to configure a VLAN, even though VLAN appears to be a valid command option. As a workaround, configure without specifying a VLAN to ensure that the egress counters are created properly. (Q00813681)
- 802.1p bits are unchanged at egress if ingress traffic is tagged with override enable. (Q00697474)
- The 802.1p bit is not overwritten for untrusted Layer 2 ports. You can use filters to perform the same functions. (Q00697474)
- There is no provision in the Passport 8300 switch Layer 2 commands to look up the DSCP value based on the .p bit. (Q00788755)
- In some configurations, egress counters for multicast traffic show the counter values for unicast traffic when a port belongs to a protocol-based VLAN. In such instances, these counters are not shown under the unicast counter values. (Q00785950)
- A common pool of 128 records exists for both policies (policers) and filter stats. If this pool is exhausted and an additional record is requested, an error message like the following appears:

  ```
  QOS ERROR gtcmCreateTcEntry: Failed, status = 20
  ```

  Should this happen, you need to delete a filter stat instance or policer before adding another. (Q00831460).
- Be aware that QoS shaping does not perform correctly at lower rates. There is a 10-20% variation in the actual traffic rate as compared with the configured rate. (Q00730427)
- In the Passport 8300, the VLAN QoS level is only supported on protocol-based VLANs. (Q00755441)
- When you poll statistics for the QoS egress-counter-set, counters are reset to zero. You cannot gather a cumulative number of packets over a period of time using this feature if you execute **show qos egress-stats**. (Q00783246)
- No statistics are available for traffic shaping. (Q00785991)
- If a traffic policy is applied on multiple ports, these ports should belong to the same FPI. If the policy is applied across multiple I/O cards and multiple ports, the peak information rate/committed information rate (PIR/CIR) is not guaranteed. (Q00840339)
- DiffServ and policing share the same table for DiffServ remarking and policing. (Q00777622)

- The Policing remarking feature does not work when you use remark-user-priority for DiffServ remarking. (Q00783230 and Q00783234)
- Filter counter/stats do not work when you use remark-user-priority for DiffServ remarking. (Q00799518)
- Disabling the p-bit override does not change a learned FDB entry's QoS level. (Q00802732)
- Be aware that you can configure different filter remarking values for ports within an MLT. (Q00803181)

Filters

- You can apply fdb-filters to ports but they act only on VLANs. For example, if you assign an fdb-filter to a port in a VLAN, all ports in that VLAN will act on the filter. If the port to which the fdb-filter is assigned is disabled or goes down unexpectedly, the filter remains in effect for all other ports in the VLAN. (Q00785103)
- Partial masking of Access-Template fields are not supported. For example, Access-Template Src Mac field defined as *00:00:00:ff:ff:ff* is not a supported configuration. (Q00797808, Q00797811, Q00806856)
- If you remove a module that has associated static FDB or FDB-filter entries, the CLI command **show vlan info all** shows information for ports that are no longer present. This is a display issue only and does not affect the operation of the Passport 8300 switch. (Q00860990)
- It is recommended that you keep ACL names to 15 characters or less. Longer ACL names cause a mis-alignment of fields when displaying the ACL. In addition, an ACL with a traffic type other than routed, bridged, or all also causes a field mis-alignment. (Q00826795)
- The VLAN ID range 1–4000 is supported under VLAN configuration for data traffic. The remainder of the VLAN ID range that displays is reserved for network control traffic. Do not configure filters to match the reserved VLAN ID range. (Q00879816)

Multicast/broadcast rate limiting

- Rate limiting will become less accurate with frame sizes larger then 64 bytes. (Q00804941)
- The minimal effective rate limiting on 10Mbps is 6%. 10Mbps rate limiting is done in blocks of 6%. (Q00804941)

- When performing broadcast/multicast rate limiting on an ingress port, if the bandwidth of the egress ports is significantly less than that of the ingress ports (e.g., 1G -> 100M or 100M -> 10M), then the egress ports may drop even more than requested. This occurs only when the ingress burst rate is greater than the egress ports. (Q00810524)
- Rate limiting configured on an inactive MLT port will not be effective for the traffic flowing over that MLT. (Q00841340)

VCT

- If VCT test results show a normal status, you should ignore the values displayed in the PairErrLength field. They are not applicable. (Q00745966)
- When you enable the VCT test, the PHY waits a fixed amount of time before sending out the TDR test pulse. This is to ensure that the link is broken and that the link partner is not sending 10/100/1000Mbps traffic.

  As soon as the VCT test is finished, the PHY automatically resumes normal operation. This means that auto-negotiation starts again and the link is established. (Q00755304)
- The Passport 8300 switch displays an invalid test result when the port is connected to a 100BASE-T hub or a test port. (Q00757309)

Unknown MAC discard

- The autolearned MAC entry does not get re-learned after a conversion to manual entry and deletion until the FDB entry ages out. When you convert, you delete the manually-entered MAC entry in the unknown MAC discard table. However, the FDB entry itself is not deleted. (Q00802887)
- When you use the unknown MAC discard feature on a given port, the first ARP request for an address, including those to be discarded, is processed. This does not impact feature operation and all packets matching the entries to be discarded will not be forwarded by the Passport 8300 and discarded as expected. (Q00867919)

IGMP

- If a client sends an IGMP report with a source address from a different subnet than the VLAN’s subnet, the Passport 8300 accepts these joins. (Q00810854)

- Traffic filters for IGMP join and leave packets are not effective if the port belongs to one or more IGMP interfaces. (Q00843934)
- On an IGMP snoop device, the sender is available only if the traffic is unregistered. In other words, no receiver exists locally on the device. Otherwise, sender information will not be available on a snoop device. (Q00737617)
- The Passport 8300 switch does not drop joins from a client whose IP address matches the VLAN IP itself. (Q00788415)
- In the NNCLI and CLI, **`show ip igmp interface`** displays the IGMP snoop interfaces. Those interfaces that are not IGMP-enabled are shown as inactive if the interface is IP-enabled, or was previously IGMP snoop enabled. (Q00791636)
- IGMP static receivers are not supported in the Passport 8300. (Q00889737, Q00889777, and Q00889744)

Miscellaneous

- The ICMP response time is not reported correctly when a ping to a subnet broadcast command is issued from the Passport 8300 switch. (Q00788580)
- You should ONLY use **`dos-format`** to format the PCMIA card and **`format-flash`** to format the flash. If you use these commands on the wrong target, it may damage your flash. (Q00830458)
- Do not use a virtual interface index, such as an MLT group or VLAN, when gathering statistics or error information. If you wish to monitor such an interface, use the appropriate physical port(s) index. (Q00853775)
- The Passport 8300 switch provides limited support for Web management. It provides information for viewing purposes only. It is recommended that you do *not* use Web management for operational network management purposes. (Q00802594, Q00803154), Q00803806, Q00837041, and Q00837034)
- Should you delete selected ports bound to multicast MAC filtering and then source the configuration (**`source config.cfg`**), the deleted ports do not get restored as originally configured. The reason for this is that the MAC is already learned before you source the configuration. Thus, the port does not get added to the MAC. (Q00841632)
- When you first activate unknown MAC discard, it causes the Auto-learn mode on that port to stop functioning. (Q00784962)

- If egress counter statistics are attached to an MLT port and a VLAN ID has been assigned to those statistics, you should ensure that the statistics are removed before performing any negative operations on that MLT. Negative operations include such items as removing and reinserting the module and link down and link up. Otherwise, the port will be removed from the MLT and the only way to add it back is to first remove the statistics. (Q00862905)
- Be aware that the access level feature for SNMP access policies does not work correctly. If you wish to configure SNMP security beyond community strings and/or SNMPv3, it is recommended that you use the boot flag *block-snmp* to prevent all SNMP transactions. (Q00863759)
- To disable RADIUS accounting, you must disable RADIUS globally as well as disabling RADIUS accounting. Disabling the RADIUS feature alone does not stop accounting. (Q00862936)
- Be aware that changing CP limit settings on a single port belonging to an MLT does not change the settings for the other ports in the MLT. You need to make the change for all the ports belonging to that MLT. (Q00851722)
- The CP limit ability to shut down a port is reduced when more than four ports are in the same VLAN. (Q00850119)
- If you enable port mirroring on a tagged interface, the mirrored packets will not contain the 802.1Q header. (Q00773426)
- Note that tagging and EAP are mutually exclusive. If you enable EAP on a port, using auto or force-authorize, you cannot enable tagging on the port and vice-versa. (Q00819777)
- If you configure a port shaper on an output port and multiple flows with different priorities are egressing through this port, one flow can monopolize the entire bandwidth up to the shaper rate configured on that port. As a workaround, it is recommended that you use shaper on a per-queue basis. (Q00784096)
- Port error stats display a column labelled *FCS Error*s. This count includes FCS, CRC, and align errors. (Q00846062)
- SNMPv3 notification is not supported in v2.0.0.1 of the Passport 8300. (Q00820269)
- The FTP password also applies to TFTP. (Q00876457)
- If you create an IP VLAN that belongs to a subnet represented by an existing static route, the following error message may display:

  ```
  IP ERROR rcIpModifyNextHop: Arp pointer is NULL for
  route: x.x.x.x mask: x.x.x.x
  ```

The new local route should take over as the best route in the route table. If so, you can ignore this error. (Q00883592)

- Check both the IP ARP and FDB tables if the following message displays:

  ```
  HAL WARNING NPAL_CreateNhId: could not create next hop
  x.x.x.x, Status x
  ```

  It indicates that either the FDB or ARP limits have been exceeded. (Q00885154)

- When creating user-defined, protocol-based VLANs, with non-default optional parameters, such as name, color, and encapsulation, the protocol ID defined by the user is not saved in the configuration file. (Q00889957)
- If you enable fast-start on a port that is added or removed from an MLT, fast-start will become disabled on that port. As a result, you must re-enable fast-start on that port. (Q00890827)
- If you create multiple port mirroring entries where different *rx* ports configured, disabled entries cannot be saved unless the port mirroring index number is lower than the index number of the enabled entry. Note that you cannot enable more than one *rx* port at any given time. (Q00896254)
- You cannot configure an IP protocol-based VLAN and an ARP-based VLAN on the same port using the user-defined VLAN protocol type 0x0806. (Q00892593)
- Operations like adding or removing ports on an MLT, or changing STP configuration on the MLT while traffic is flowing will result in data loss. For unicast traffic, the data loss lasts for 20- 30 seconds. For multicast traffic, it may last for 2 to 3 minutes depending upon the IGMP configuration. (Q00897494)
- The *nocheck-sw-version* flag, dedicated for use by Nortel Networks customer support engineers, is available on the Passport 8300. If this flag is changed, it will disable all image consistency checks. The default value of this flag is set to false. You should ensure that this flag remains at its default value and is not changed.

  The flag not only determines whether local images match, but also determines if a master CPU will respond to software version queries from a standby CPU. If the flag is set to true on the master and a standby CPU is present at boot or is later inserted with its flag set to false, the standby boot process hangs with no error as it tries to query the master for software versions.

Since it is impossible to check the condition of the flag on the hung standby CPU, the only way to determine whether this is happening is to see if a software version query message displays on the master. If the following message is observed on the master console or log (if the log level is set to INFO), the hang problem is caused by something other than the *nocheck-sw-version* flag state.

```
CPU6 [05/12/04 10:44:53] SW INFO Software version query
from 127.0.1.5 version 2.0.0.1/011, running 2.0.0.1/011
```

The message shows either 127.0.1.5 or 127.0.1.6 depending on the slot the master is in. If this message is not displayed on the master while booting or inserting a second CPU, the hang problem results from the standby's inability to check the master's software version. To recover in the cleanest possible way, it is recommended that you reboot the Passport 8300 switch, exit to monitor mode, and set the flag to its default value (false) on both CPUs. If that is too intrusive, setting the flag to false on the master and then resetting the secondary should cause the secondary to finish booting up. (Q00904970)

Reading path

This section lists the documentation specific to the Passport 8300 switch platform. To find the most up-to-date 8300 document, go to the www.nortelnetworks.com URL. Click Support & Training, select Technical Support, and then select Technical Documentation. Find the product for which you need documentation.

Follow these steps on the Browse product support tab:

1. In the Select from Product Families drop-down list, select Passport: Passport 8000 Ethernet Switch Series.
2. In the ...choose a product... list, select Ethernet Routing Switch 8300.
3. In the ...get the content... list, select **Documentation** and then click Go.

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.

Important information

- *Important Information for the 8300 Series Switch* (part number 216511-B)
- *Read Me First for the Passport 8300 Chassis* (part number 318192-B)
- *Important Notice for the Passport 8300 Ethernet Switch* (part number 316802-B)
- *Important Security Information for the 8300 Series Switch* (part number 216512-A)
- *Important Notice for the 8300 Series Switch PCMCIA Card* (part number 208703-F)

Chassis and module installation

- *Installing and Maintaining the Passport 8306 and 8310 Chassis* (part number 316795-B)
- *Installing Passport 8300 Switch Modules* (part number 316796-B)
- *Installing the Passport 8300 AC Power Supply* (part number 316797-B)
- *Installing a Fan Tray in a Passport 8300 Series Chassis* (part number 316798-A)
- *Installing GBICs and Gigabit SFP Transceivers* (part number 318034-A)

Related publications

This section describes common documentation related to the Passport 8300 switch.

Installation and User Guides

These guides provide instructions for installing the chassis and its components, installing and getting started with the Device Manager software, and configuring various protocols on the Passport 8300 switch.

Adding MAC Addresses to the 8000 Series Chassis	212486-B
Installing and Maintaining the Passport 8306 and 8310 Chassis	316795-B
Installing Passport 8300 Switch Modules	316796-B
Installing the Passport 8300 AC Power Supply	316797-B
Installing a Fan Tray in a Passport 8300 Series Chassis	316798-A
Passport 8300 Power Considerations	317223-B
Getting Started	316799-B
Installing and Using Device Manager	316808-B
Configuring PoE	317337-B
Using Device Manager Diagnostic Tools	317359-A
Installing GBIC and Gigabit SFP Transceivers	318034-A

Reference and Configuration Guides

These guides provide reference and configuration information for the Passport 8300 switch.

Configuring IP Routing and Multicast Operations using the NNCLI and CLI	316800-A
Configuring QoS and Filters using the NNCLI	316801-A
Configuring Network Management using the NNCLI, CLI, and Device Manager	316803-B

Configuring and Managing Security using the NNCLI and CLI	316804-B
Configuring VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI	316805-B
Network Design Guidelines	316809-B
System Messaging Platform Reference Guide	316806-B
NNCLI Command Line Reference for the Passport 8300 Series Switch	316810-B
Using NNCLI and CLI Diagnostic Tools	317222-A
Configuring IP Routing and Multicast Operations using Device Manager	317338-A
Configuring QoS and Filters using the CLI	317339-A
Configuring QoS and Filters using Device Manager	317340-A
Configuring and Managing Security using Device Manager	317346-B
Configuring VLANs, Spanning Tree, and Static Link Aggregation using the CLI	317347-B
Configuring VLANs, Spanning Tree, and Static Link Aggregation using Device Manager	317348-B
Managing Platform Operations using Device Manager	317350-B
CLI Command Line Reference for the Passport 8300 Series Switch	317360-B

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com URL. Click Support & Training, select Technical Support, and then select Technical Documentation. 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 www.nortelnetworks.com. Click Support & Training and select 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.

From the Technical Support page you can also get an Express Routing Code (ERC) 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.