Part No. 316811-B Rev 00
May 2004

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Passport 8300 Series Switch Software Release 2.0.0.1

316811-B REV 00

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.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

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 switch software release 2.0.0.1 describe the hardware and software and any known issues that exist in this release. They are based on REL2.0.0.1 and Java Device Manager (JDM) 577.

A list of related publications can be found on page 32. The Passport 8300 switch software release 2.0.0.1 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/documentation. For more information, see the "Reading path" on page 31.

The following topics are discussed in this document:

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

Passport 8300 hardware

Table 1 describes the Passport 8300 hardware in this release.

Table 1 Passport 8300 hardware

New hardware	Module part number	Where to find information	Document part number
Passport 8310 (10-slot PoE chassis)	DS1402007	Installing and Maintaining the Passport 8306 and 8310 Chassis	316795-A
Passport 8301 AC Power Supply	DS1405A14	Installing an AC Power Supply in the Passport 8300 Series Chassis	316797-A
Passport 8393SF CPU module	DS1404076	Installing Passport 8300 Switch Modules	316796-A
Passport 8348TX 48p line module	DS1404077	Installing Passport 8300 Switch Modules	316796-A
Passport 8348TX-PWR 48p PoE module	DS1404078	Installing Passport 8300 Switch Modules	316796-A
Passport 8324GTX 24p line module	DS1404079	Installing Passport 8300 Switch Modules	316796-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.

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.

Features supported in this release

The Passport 8300 is a Layer 2/3 switch designed to support the requirements of converged networks. Its hardware and software capabilities provide the PoE, quality of service, and feature set to enable voice over IP, video and multimedia applications.

This section provides a list of the Passport 8300 switch software release 2.0.0.1 software features.

- Virtual cable tester
- Eight hardware-based queues
- 802.3af PoE
- 802.1Q
- Link Aggregation and Distributed Link Aggregation (MLT and DMLT)
- Utilize existing chassis- installed base upgrade
- Uplinks are switch fabric based to maximize copper connections
- IGMP snooping with IGMP v1/v2 and IGMP proxy and multicast access control
- Port mirroring
- Multiple Spanning Tree Group (STG) support
- Policing and Shaping
- QoS support with Diffserv and 802.1p

- Static Routes
- SNMPv1/v2/v3
- ASCII configuration file
- Real-time event log
- SysLog and SMP support
- Radius authentication/accounting
- FTP/TFTP Support
- NNCLI (support both current CLI and NNCLI)
- 802.1x (EAP)

Supported software and hardware capabilities

Table 2 lists the known limits for REL2.0.0.1 and JDM 577 of the Passport 8300 switch software. These capabilities will be enhanced in subsequent software releases.

Table 2 Supported capabilities in the Passport 8300 Series switch (Release 2.0.0.1)

Feature	**Maximum number supported**
By port VLANs	Up to 4,000 VLANs. 200 have been tested and are officially supported in release 2.0.0.1
Protocol-based VLANs	12 records, 50 VLANs maximum
IP interfaces	Up to 500 IP interfaces. 200 have been tested and are officially supported in release 2.0.0.1
Spanning Tree Groups	64
Link 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.
Number of Ports in a Link Aggregation Group	4
Dynamic ARPs	2500
Local next hops	500
Static routes	1000
IGMP Maximum number of unique groups	 1800

The Passport 8300 supports VLAN IDs from 1- 4000. The default is 1- 2000. However, when the *vid-max4k* flag is set to true, you can configure VLAN IDs in the range of 1 and 4000.

Note that when the *vid-max4k* flag is enabled, you need to follow these guidelines if you have IGMP snooping enabled on VLANs. These will help avoid any issues that may result in improper broadcast and multicast handling:

- If snooping has to be enabled on VLANs, first create ALL the VLANs, and then enable IGMP snooping.
- If you need to create additional VLANs, follow these instruction:
  - While the flag is enabled, first disable IGMP snooping on the existing VLANs
  - Add the new VLANs
  - Then, enable IGMP snooping on the VLANs where you wish it enabled.

➡ **Note:** Subnet-based VLANs and Jumbo Frames are not supported in Release 2.0.0.1. 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 60 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*.

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 3 shows the number of records that each specified protocol VLAN takes.

Table 3 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

Protocol	Number configurable	Actual number of records per VLAN
ipxEthernet2	6	2
appleTalk	3	4
decLAT	12	1
decOther	1	9
sna802.2	12	1
snaEthernet2	12	1
netBios	12	1
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.

JDM installation

JDM installation procedures are now standardized across all platforms. In addition, the required Java Runtime Environment (JRE) (version 1.3.1) is now part of the JDM installation package and does not require a separate installation. The bundled JRE will be used with this JDM only and should not affect other JAVA applications on the same system.

For Solaris, please note that certain OS patches are required for JDM/JRE to function properly. Please consult SUN to install the appropriate OS patches before launching JDM. For complete information on how to install and use Java Device Manager in this release, refer to *Installing and Using Device Manager* (part number 316808-A)

Documentation corrections and additions

- In the online help, *LastMembQueryIntvl* is referenced in the IP Routing > IGMP > Interface tab. This parameter is not supported in the Passport 8300 switch and has been removed from the JDM interface.
- The Virtual Cable Tester (VCT) test warning box and the Refresh button are *not* described in the online help. For the complete procedure for testing a single port or multiple ports using the VCT, see *Using Device Manager Diagnostic Tools*.

Known limitations and considerations in this release

The following topics describe issues known to exist in the Passport 8300 Series switch Beta 2.0 release and include the following topics:

Hardware and platform

- 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. 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. To prevent this, you must save your configuration following the new module insertion. (Q00848027)
- • A save config to standby operation may fail. The way you perform this operation (i.e., via the JDM, command line, or with the boot flag) determines the failure indication you receive. Either a confirmation message, such as `saved to standb`y, fails to appear, or an error is produced.

  If this happens, you should power-cycle the Passport 8300. To work around the problem, you can copy the file directly to the standby CPU. For example, if slot 5 is the master and slot 6 the secondary, you enter the following:

  ```
  copy config.cfg 127.0.1.6:/flash/config.cfg
  ```

  (Q00885275)
- Access policies are not dynamically applied to the standby CPU. In order for access policy changes to take effect, the standby CPU must be rebooted. (Q00864800)
- If the serial console speed is not set to 9600 baud, the proper characters will not display at boot time (i.e., the transition from PowerBoot to boot monitor loader). (Q00747777)
- If both CPUs are stopped at the boot monitor prompt, the Passport 8300 may fail if you exit from both boot monitor prompts almost at the same time. (Q00827090)
- An SNMP trap is not generated when an invalid user attempts to access the standby CPU. (Q00855540)
- 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 switch reset 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)

- You cannot use the disable slot function on the standby CPU. No error message displays if you execute the corresponding command or perform the JDM action. (Q00894433)
- During a reset, if you need to break out and go to a Boot Monitor prompt, you do so by pressing *return* as indicated in the following procedure:

```
Copyright (c) 2004 Nortel Networks, Inc.
CPU Slot 6: PPC 750Cxe
Version: 2.0.0.1/110
Creation Time: MAR 18 2004, 20:45:33
Hardware Time: MAR 23 2004, 20:36:15 UTC
Memory Size: 0x08000000
Start Type: cold
ti1410cscHandler -- Card Insertion
Loaded boot configuration from file /flash/boot.cfg
Attaching network interface lo0... done.

Press <Return> to stop auto-boot...
```

— Be sure to press *return* at this point.

```
monitor#
monitor#
monitor#
monitor#
monitor# boot
Loading /flash/p83a2001b110.img ... 5518464 to 21848256
(21848256)
Starting at 0x10000...
Init DTLB/ITLB for block translation, enable MMU
Enabling Instruction/Data Address translation in MSR
Init exception vectors starting at address: 0x00000100
Enable L1-Icache
Enable L1-Dcache
Enable L2-Cache
Check for AutoBoot....
Autoboot enabled...
```

— Do not press *enter* after `AutoBoot enabled` because this is not the boot monitor.

```
01s
```

— Do not press *enter* here either since this is also not for the boot monitor.

— Note that if you press *enter* in any of the two previous instances, the switch stops booting at the `PowerBoot` prompt. (Power Boot is a mode used by technical support only). If so, the switch displays the following:

```
Break by console keypress, autoboot aborted-<<

<< PowerBoot Version-3.6 for PowerPMC-240NV1 >>

<< (c) 2002 by FORCE COMPUTERS >>

PowerBoot>
```

— If the Passport 8300 is at the `PowerBoot>` prompt, you need to type **`reset`** and press *enter* as shown in order to exit from this mode and allow the switch to continue booting properly.

```
PowerBoot>reset
```

Caution: Do *not* attempt to type any command other than **`reset`** at the `PowerBoot>` prompt since it may result in permanent flash corruption.

(Q00895098)

- Be aware that the *daylight-saving-time true* flag is not functional in the Passport 8300. You can change the time manually if necessary. (Q00893764)
- 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 you delete files from flash, be aware that wild card file specification is unpredictable as far as which file names will match. Be sure that you specify full file names when performing flash file operations. (Q00896307)

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)
- When you enter **`show ip route info`** in the CLI, be aware that the total number of routes that displays may not be accurate. (Q00830558)
- 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)
- In the CLI, **`config eth`** *<port>* **`filter modify`** *<acg>* is not supported. The **`modify`** option produces the following error message and the command has no effect:

  ```
  modify operation FAIL
  ```

You should instead use **conf eth** *<port>* **filter delete** followed by **conf eth** *<port>* **filter create** *<acg>*. (Q00863954)

➡ **Note:** When **show sys sw** is entered in the CLI and NNCLI, the downloadable image version is displayed. For example with any line module in slot 1, you see the following output:

```
Slot#1: file /flash/p83r2000.dld version 2.0.0.1/011
```

You can ignore the number 011 at the end of the string.

- 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)
- Be aware that the Passport 8300 does not support **config vlan** *<vid>* **action all**. Unexpected behavior may result when using this command. (Q00885402)
- In the CLI and NNCLI, **monitor** references the ATM and POS interfaces. Neither of these options are supported in the Passport 8300. (Q00884069)
- In the CLI and NNCLI, be aware that the Passport 8300 does not support **trace route-policy**. (Q00884051)

NNCLI

- 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)
- When you enter **filter acl**, the help information that appears in the NNCLI does not show decimal and hex input in the list of available options. (Q00859926)

- You cannot display the autolearned 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 JDM. (Q00869924 and Q00876361)
- In some instances, **`show tech-support`** in the NNCLI displays incorrect LastRuntimeConfigSource information. This is particularly true when both the primary and backup configurations produce errors during loading. To obtain reliable LastRuntimeConfigSource information, access Edit > Chassis > Boot Config in the JDM, or enter **`show sys sw`** in the CLI. (Q00868853)
- If the primary and specified backup configuration files fail to load, no indication of a load failure is provided in either case. (Q00868848)
- The current running status of the management port (speed, duplex etc.) cannot be displayed from the NNCLI. It can be displayed in the JDM using the Edit > Port > Interface tab, or in the CLI using **`config bootconfig net mgmt info`**. (Q00842478)
- In the NNCLI, **`filter access-list`** *`<number>`* **`protocol`** *`<value>`* **`udp le tcp`** does not work. Use the JDM to configure this instead. (Q00815353)
- In the NNCLI, **`boot host tftp-timeout`** prompts you for a hexadecimal entry. However, the system only accepts and displays decimal 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)
- The NNCLI help for **`framing`** interface/port displays *`sonet`* and *`sdh`* as valid options. The Passport 8300 does not support either of these options. (Q00876411)
- When adding static multicast entries using **`vlan static`** *`<vid>`* **`add-mlt`**, the NNCLI help indicates that the valid MLT range is between 1- 16. This is incorrect. The actual range is between 1- 31. (Q00883943)
- 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, **`monitor`** references the ATM and POS interfaces. Neither of these options are supported in the Passport 8300. (Q00884069)
- 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 JDM. Note that you can configure the *dst-port* field in the NNCLI with the range and mask operators. (Q00901990)

JDM

- The p-to-dscp table is not available in JDM. However, it is available in the CLI and NNCLI. (Q00834504)
- When using JDM, 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 JDM operates normally. (Q00793639)
- Be aware that JDM may timeout when performing operations with trace level 3 turned on. (Q00851125)
- If trace is enabled, especially in a case where verbose is being configured, you may experience JDM timeouts. You cannot avoid this problem completely. You can minimize it, however, by increasing the JDM 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 JDM using the VLAN > Mac Learning >VlanMacLearning dialog boxes. (Q00802165)
- Be aware that JDM may timeout after converting MAC entries and refreshing the AMT 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 JDM 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 JDM:

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

In a UNIX environment:

1 Go to the directory where JDM is installed.

2 Enter the following command to launch JDM:

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

Note: 256m is the memory size you plan to use. The default value is 64MB. You may assign the proper size based on your system environment. (Q00862945).

- In JDM, 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 JDM, 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 JDM 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 JDM 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)
- You cannot use JDM to set the *remark-dscp* and *remark-user-priority* fields in an existing ACE with the traffic type already set to routed. As a workaround, you should use the CLI to perform this operation instead. (Q00891752)

- JDM permits you to set *all* as the traffic type with both the *remark-dscp* and *remark-user-priority* fields in an existing ACE. This is not valid since only the routed and bridged traffic types are supported on the Passport 8300 with both fields set. (Q00891759)
- In JDM, the DSCP to CoS Map table is missing the column specifying the DSCP value. This option is available in the CLI and NNCLI. (Q00780367)

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)

- 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 need 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)

- 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)
- If you wish to delete a QoS policy, it is recommended that you use the CLI. JDM does not automatically clean up ACE records that may be using that policy, while the CLI performs this operation automatically. (Q00896616)

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)
- When creating an ACE, you cannot specify the traffic-types *tagged* or *untagged* unless you have defined either *ether-type* or *user-priority* in the Access-Template. (Q00798469)
- 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)
- In the CLI and NNCLI, filter statistics do not display using **`show filter acl stat`** if the filter mode equals deny- even if mirror or redirect is not configured. (Q00862407 and Q00858970)
- When you configure ACL filters, the allowed VLAN ID range displays as 1-4095. Only values between 1- 4000 are valid, however, and in the case of values between 2001- 4000, only when the *vid-max4k* flag is set to true. (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

- Be aware that running VCT tests on an active port interrupts traffic. JDM does not ask for confirmation before initiating a VCT test. (Q00860941)
- After running a VCT test on an MLT port, you must manually disable/ re-enable the port once the test is finished. (Q00865582)
- 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)
- It is recommended that you avoid using operators like ne, ge, le in the range of MAC addresses. These are large fields (6 bytes) and they expand internally and require many filter resources. (Q00777592)
- 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)
- The 802.1x feature only supports one MAC per port. The 8300 switch puts a port into force-unauthorized state if it sees more than one MAC on that EAPoL-aware port (i.e. admin-status = auto). To put the port back into a VLAN, you must set the EAPoL admin-status to force-authorized.
- 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)
- A save config operation is not support through RSH in the Passport 8300 switch. (Q00897629)

- 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)

- 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.

  It is recommended that you return to the default log setting (log level 1) after capturing the required log messages since having the log level set to 0 may result in issues at boot or failover time. If this happens, you need to reset the switch with log level 1.(Q00886136)

Reading path

This section lists the documentation specific to the Passport 8300 switch platform. To find the most up-to-date 8300 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 8300 Ethernet 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.

Important information

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

Chassis and module installation

- *Installing and Maintaining the Passport 8306 and 8310 Chassis* (part number 316795-A)
- *Installing Passport 8300 Switch Modules* (part number 316796-A)
- *Installing the Passport 8300 AC Power Supply* (part number 316797-A)

- *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-A
Passport 8300 Power Considerations	317223-A
Installing Passport 8300 Switch Modules	316796-A
Installing the Passport 8300 AC Power Supply	317797-A
Installing a Fan Tray in a Passport 8300 Series Chassis	318034-A
Installing GBIC and Gigabit SFP Transceivers	316342-A
Installing and Using Device Manager	316808-A
Getting Started	316799-A
Using Device Manager Diagnostic Tools	317359-A
Configuring PoE	317337-A

Reference and Configuration Guides

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

Configuring IP Routing and Multicast Operations using Device Manager	317338-A
Configuring IP Routing and Multicast Operations using the NNCLI and CLI	316800-A
Configuring QoS and IP Filters using the NNCLI	316801-A
Configuring QoS and IP Filters using the CLI	317339-A
Configuring QoS and IP Filters using Device Manager	317340-A
Configuring Network Management using the NNCLI, CLI, and Device Manager	316803-A
Configuring and Managing Security using the NNCLI and CLI	316804-A
Configuring and Managing Security using Device Manager	317346-A
Configuring VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI	316805-A
Configuring VLANs, Spanning Tree, and Static Link Aggregation using the CLI	317347-A
Configuring VLANs, Spanning Tree, and Static Link Aggregation using Device Manager	317348-A
System Messaging Platform Reference Guide	316806-A
Network Design Guidelines	316809-A
NNCLI Command Line Reference for the Passport 8300 Series Switch	316810-A
CLI Command Line Reference for the Passport 8300 Series Switch	317360-A

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.