Part No. 314754-C Rev 00
March 2003

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Passport 8000 Series Switch Software Release 3.3.2

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

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

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

Trademarks

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

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

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

The asterisk after a name denotes a trademarked item.

Contents

Introduction

These release notes for the Nortel Networks* 8000 Series Switch Software Release 3.3.2 describe the new hardware and software features introduced in this release, the bugs fixed in this software release, and known issues that exist in this software release.

A list of related publications can be found on page 104. The 8000 Switch Series Software Release 3.3.2 documentation suite can be found on the Nortel Networks technical documentation Web site, www.nortelnetworks.com/documentation.

The software in release 3.3.2 supports all current Passport 8100 and 8600 modules, although certain features are available only for the 8600 modules.

In addition, this software release supports the Web Switching Module (WSM) running version WebOS 10.0 code on the 8000 Series Switch.

This document contains information about the following topics:

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

New hardware

This section describes the new hardware introduced with Passport 8000 Series Switch Software Release 3.3.2.

1000BASE-T GBIC

- The 1000BASE-T GBIC (P/N Finisar FCM-8520-3) is specified for a distance of 100 meters over Category-5 unshielded twisted pair (UTP) cable.The 1000BASE-T GBIC is qualified for operation in the Passport 8608GB (DS1404015), 8608GBE (DS1404038), 8608GBM (DS1404059), 8632TXE (DS1404024) and 8632TXM (DS1404055)

Note: The 1000BASE-T GBIC is currently not available directly from Nortel Networks. Please contact an authorized Finisar retailer for this hardware.

- The 8608GB (DS1404015), 8608GBE (DS1404038) and 8608GBM (DS1404059) may support up to six (6) 1000BASE-T GBICs per module. The 8632TXE (DS1404024) and 8632TXM (DS1404055) may support up to two (2) 1000BASE-T GBICs per module.

Limitations

- The 1000BASE-T GBIC qualified with Release 3.3.2 (Finisar p/n FCM-8520-3) does not support auto-negotiation. By default, GBICs inserted into the Passport 8608GB/GBE/GBM and 8632TXE/TXM are set for Autonegotiation= “True.” You must disable autonegotiation prior to operation of the 1000BASE-T GBIC.

- The 1000BASE-T GBIC qualified with Release 3.3.2 (Finisar p/n FCM-8520-3) is not supported in a single MLT group if there is a mix of GBICs supporting autonegotiation and GBICs not supporting autonegotiation. Nortel qualified GBICs currently supporting auto-negotiation include SX (AA1419001), LX (AA1419002), XD (AA1419003), ZX (AA1419004) and CWDM (AA1419017 through AA1419024).

8624FXE

- The 8624FXE has been qualified to interoperate with 50/125 micron multimode fiber (MMF) optic cable.
- The following specifications apply for 50/125 micron MMF cable.
    - Wavelength: 1300nm
    - Distance: 4264 ft (1.3km)
    - Optical budget: -17 dBm to -8.5 dBM
    - Transmitter Characteristics: Minimum Optical Transmit Power: -22.5dBm
    - Maximum Optical Transmit Power: -14 dBm
    - Average Receiver Sensitivity: -31 dBm

Note: The use of 50/125 micron MMF cable is not release dependent. Therefore use of 50/125 micron MMF cable is qualified with the 8624FXE as well as the discontinued 8624FX with any Passport 8600 release version.

- The specifications for the 62.5/125 micron MMF on the 8624FXE remain unchanged. Please refer to *Installing Passport 8600 Switch Modules* for additional information.

New software features: Stacked VLANs (SVLANs)

This section describes Stacked VLAN (SVLAN) concepts, and how to configure the feature using CLI.

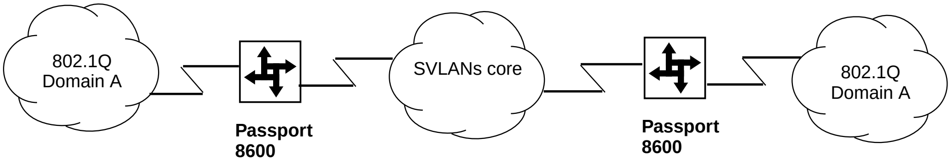
Note: In release 3.3.2, SVLANs are configurable only with the CLI. The Device Manager implementation will be available in Passport 8000 Switch Series Software Release 3.5.

SVLAN concepts

Note: This information applies to Passport 8600 modules only.

An SVLAN transparently tunnels packets through an SVLAN domain by adding an additional 4-byte header to each packet. The additionally tagged packets may already have an IEEE 802.1Q tag, but it is not required. Figure 1 shows a basic SVLAN model using Passport 8600 switches.

Figure 1 SVLAN



Spanning tree packets are also transparently bridged through an SVLAN domain. Routing cannot be enabled on an SVLAN port. SVLAN user-to-network interface (UNI) ports are VLAN unaware and classify any traffic into the SVLAN which is configured on the port. SVLAN network-to-network interface (NNI) ports connect SVLAN switches together and support multiple SVLAN and VLANs per port.

Note: You can enable SVLANs on all ports. If the port belongs to an MLT, however, you should perform all of the SVLAN configuration at the MLT level.

SVLAN specifications

SVLANs provide the following features:

- VLAN transparency for IEEE 802.1Q tagged or untagged traffic through service provider core networks
- A solution to VLAN scalability issues by allowing you to summarize customer VLANs into core SVLANs
- Use layered architecture to improve scalability
- Spanning tree bridge protocol data unit (BPDU) transparency for customer UNI ports

SVLAN rules

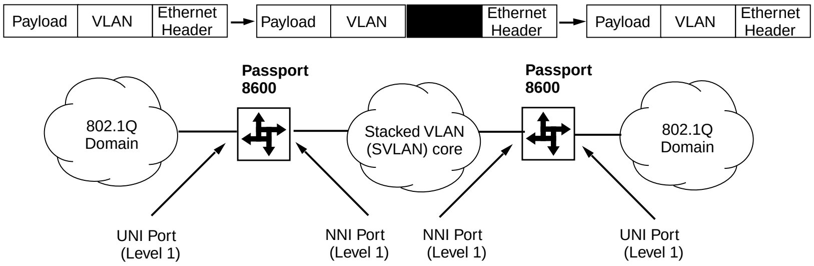
SVLANs operate under the following basic set of rules:

- IP filters are not supported on SVLAN.
- To apply QoS to SVLAN, use the per VLAN QoS option.
- On a SVLAN NNI port, regular VLANs are not supported; therefore, SVLAN switches cannot be managed in-band. An out-of-band or parallel network is recommended for management of the devices
- When creating an SVLAN spanning tree group, the tagged BPDU address of the spanning tree group should be different from the standardized BDPU MAC address.
- The SVLAN is created with the UNI and NNI ports.
- An SVLAN cannot span multiple spanning tree groups; that is, the ports in the SVLAN must all be within one spanning tree group. Spanning tree groups IDs can range in value from 1 to 64.
- To propagate user BPDUs transparently across the network, the BPDU MAC Address of the SLVAN spanning tree group must be the same across all switches on which it is configured and it must be set to a value other than the standardized BPDU MAC addresses (01:80:c2:00:00:00 - 01:80:c2:00:00:0f).
- SVLANs cannot have routing enabled
- SVLAN UNI and NNI ports are applicable on a per Octapid basis. All ports on a Octapid can either be normal ports or SVLAN NNI/UNI ports. Please refer to “Appendix A: Tap and OctaPID assignment” on page 107 for more details.

Levels

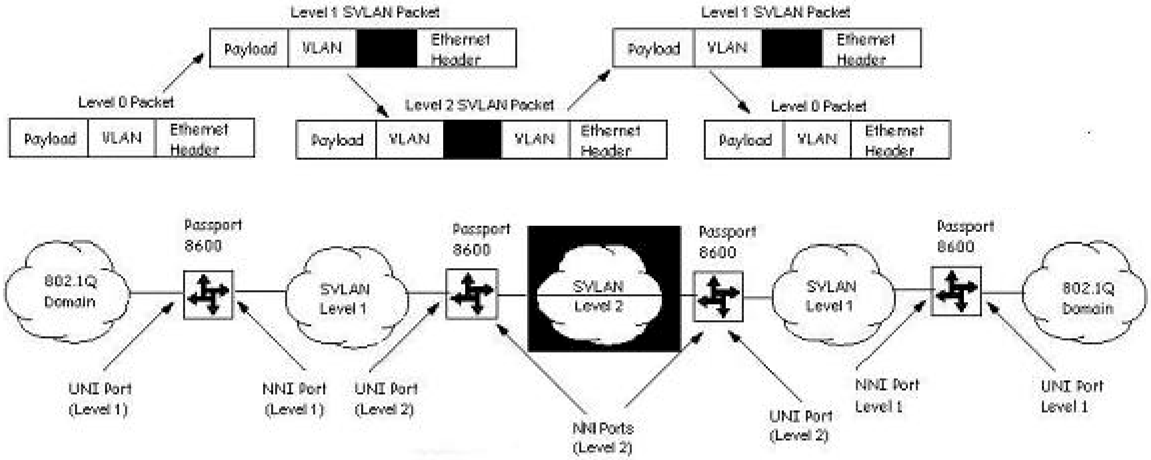
You can stack SVLANs in a hierarchical fashion to achieve greater VLAN scalability. An SVLAN level defines the hierarchy for the operating switch. When configuring the switch, you must specify only one level at a time. Figure 2 shows a one layer SVLAN, while Figure 3 shows two layers.

Figure 2 One layer SVLAN



10683BEA

Figure 3 Two layer SVLAN



SVLAN tags are added onto SVLAN NNI ports and removed on SVLAN UNI ports. You must configure UNI ports on both ends of the tunnel at the same level. Since SVLAN switching is MAC-addressed based, the normal issues of VLAN switching apply.

- If you build SVLAN networks with multiple levels, the network MAC addresses you specify must all be unique.
- Independent VLAN learning is only applicable within SVLAN, not the VLAN context.
- SVLANs are aggregated into a next level so duplicate MAC addresses on different ports will trigger the loop detection function, which will disable an SVLAN on a port.

Note: The Spanning Tree Protocol (STP) is not supported in a SVLAN network with multiple levels. It is supported for single level SVLAN networks only.

UNI, NNI, and normal ports

The ports in the switch can be configured as SVLAN user-to-network interface (UNI), SVLAN network-to-network interface (NNI), or normal.

Note: You must change the switch level to 1 or above before you configure SVLAN UNI or NNI ports.

You must configure the ports to which you want to provide VLAN transparency as UNI ports. UNI ports can only belong to one SVLAN. When you configure a UNI port in the CLI, the tagged-frames-discard parameter is automatically enabled.

NNI ports interconnect the switches in the core network, drop untagged frames on ingress, and insert the SVLAN tag at the egress. NNI ports can belong to multiple SVLANs and also to regular (port- and protocol-based) VLANs. An NNI port sends SVLAN tagged frames. When you configure an NNI port in the CLI, the untagged-frames-discard parameter is automatically enabled.

- If a Spanning Tree Group (STG) contains both UNI and NNI ports, you should delete standardized MAC addresses used for BPDUs.
- The UNI and NNI ports are kept in SVLAN type STG.
- All of the ports in the MLT should have the same port type (normal/UNI/NNI).
- Large frame support is automatically enabled on UNI/NNI ports.

When you change the SVLAN port type from normal to UNI/NNI, all the affected ports are removed from the configured STGs and VLANs. Similarly, when you change the SVLAN port type from UNI/NNI to normal, all the affected ports are removed from the configured STGs and VLANs and added to the default STG and default VLAN.

➡ **Note:** The affected ports are all the ports in the Octapid. See "Appendix A: Tap and OctaPID assignment" on page 107.

➡ **Note:** An NNI port belonging to default VLAN and default STG is not saved across reboots. To avoid this, do not configure an NNI port under default VLAN/STG.

Configuring SVLANs using the CLI

The SVLAN protocol transparently transports packets through an SVLAN domain by adding an additional 4-byte header to each packet.

For more information about SVLAN concepts and terminology, see "SVLAN concepts" on page 10.

Follow these steps to create an SVLAN using the CLI:

➡ **Note:** You must follow these steps in sequence to configure an SVLAN.

1 Set the SVLAN switch level to a 1 or above.

For more information, see "Setting the ether-type and switch level."

2 Configure UNI and NNI ports.

For more information, see "Setting the SVLAN port type."

3 Create a STG of type SVLAN and set the tagged BPDU address as different from the standardized BPDU.

For more information, see "Creating an SVLAN STG."

4 Add UNI or NNI ports to the STG.

For more information, see “Adding UNI or NNI ports to the STG.”

5 Create VLAN of type SVLAN within the STG created in Step 3 and add ports to it.

For more information, see “Creating an SVLAN.”

Setting the ether-type and switch level

To set the ether-type and switch level, use the following commands:

`config svlan ether-type level <value> <ethertype>` (sets the ether-type)

`config svlan level <value>` (sets the switch level)

For SVLAN configurations, you must set the switch level to 1 or above.

The **`config svlan`** command includes the following parameters:

config svlan followed by:	
info	Displays current configuration information for an SVLAN (Figure 4).

config svlan followed by:	
`ether-type [level <value>]<ethertype>`	Sets an SVLAN tag for a specified level. *<value>* is an integer value in the range of 0 to 7 *<ethertype>* 8 default values which correspond to switch levels as follows: • Level 0 — 0x8100 • Level 1 — 0x8020 • Level 2 — 0x8030 • Level 3 — 0x8040 • Level 4 — 0x8050 • Level 5 — 0x8060 • Level 6 — 0x8070 • Level 7 — 0x8080
`level <value>`	Allows you to specify the switch level associated with this SVLAN. • *<value>* is an integer value in the range of 0 to 7. Level 0 (normal port): 802.1Q frames are classified into port-based VLANs. Level 1-7: any frame type is transparently switched and an additional Ether type 4 bytes is added. The default level is 0.

Figure 4 shows the **`config svlan info`** command output.

Figure 4 config svlan info command output

```
Passport-8610:5/config/svlan# ether-type level 1 0x8022
Passport-8610:5/config/svlan# level 2
Passport-8610:5/config/svlan# info

Sub-Context:clear config dump monitor show test trace wsm
Current Context:

        LEVEL ETHER-TYPE
        0     0x8100
        1     0x8022
        2     0x8030
        3     0x8040
        4     0x8050
        5     0x8060
        6     0x8070
        7     0x8080

        Active-Level = 2
```

Showing ether-type and switch level information

To display SVLAN ether-type and level information, use the following commands:

`show svlan info ether-type` (displays ether-types)

`show svlan info active-level` (displays active-levels)

Figure 5 shows sample output for the **`show svlan info ether-type`** command, while Figure 6 shows output for the **`show svlan info active-level`** command.

Figure 5 show svlan info ether-type command output

```
Passport-8610:5/show/svlan/info# ether-type
==============================================================
                           Stacked Vlan Ether Type
==============================================================
LEVEL ETHER-TYPE
--------------------------------------------------------------
0     0x8100
1     0x8022
2     0x8030
3     0x8040
4     0x8050
5     0x8060
6     0x8070
7     0x8080
```

Figure 6 show svlan info level command output

```
Passport-8610:5/show/slvan/info# active-level
Active-Level = 2
```

Setting the SVLAN port type

You must set the SVLAN port type to SVLAN UNI or SVLAN NNI.

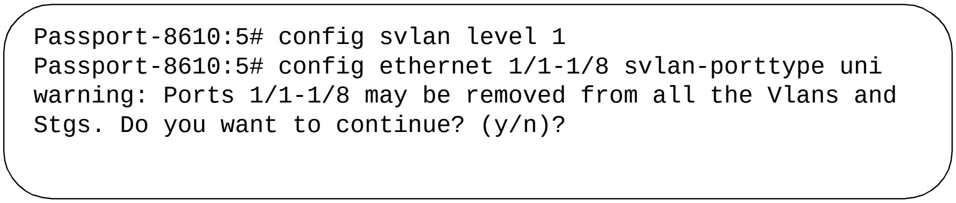
To set the SVLAN port type, use the following command:

`config ethernet <`*`ports`*`> svlan-porttype <`*`uni|nni`*`>`

Note: You must specify all of the ports within an octapid as the same port type (normal, uni, nni). See "Appendix A: Tap and OctaPID assignment" on page 107.

You will see the warning shown in Figure 7.

Figure 7 SVLAN-porttype warning



```
Passport-8610:5# config svlan level 1
Passport-8610:5# config ethernet 1/1-1/8 svlan-porttype uni
warning: Ports 1/1-1/8 may be removed from all the Vlans and
Stgs. Do you want to continue? (y/n)?
```

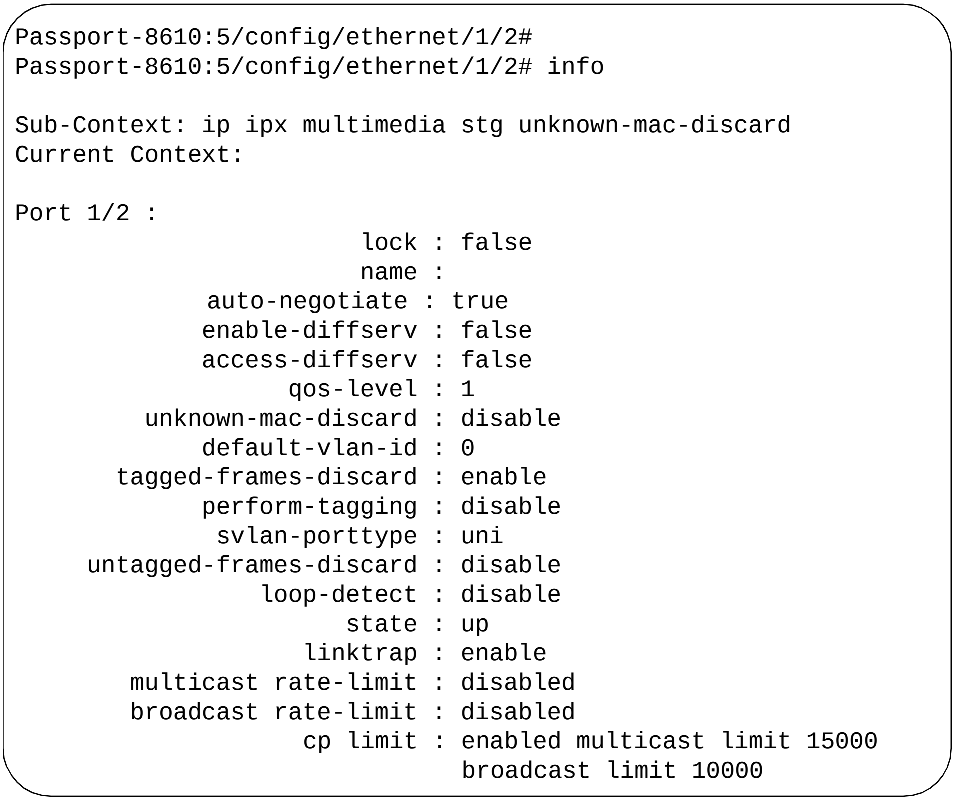
When you configure a UNI port in the CLI, the tagged-frames-discard parameter is automatically enabled. Similarly, when you configure an NNI port in the CLI, the untagged-frames-discard parameter is automatically enabled.

The **config ethernet <ports>** command includes the following parameters:

config ethernet <*ports*> followed by:	
info	Displays the current port settings (Figure 8).
svlan-porttype <*normal*|*uni*|*nni*>	Sets the port type for the svlan to normal, user-to-network interface (uni), or network-to-network interface (nni). The default is normal.

Figure 8 shows sample output for the **config ethernet <*ports*> info** command.

Figure 8 config ethernet <ports> info command output



```
Passport-8610:5/config/ethernet/1/2#
Passport-8610:5/config/ethernet/1/2# info

Sub-Context: ip ipx multimedia stg unknown-mac-discard
Current Context:

Port 1/2 :
                        lock : false
                        name :
             auto-negotiate : true
             enable-diffserv : false
             access-diffserv : false
                   qos-level : 1
         unknown-mac-discard : disable
             default-vlan-id : 0
       tagged-frames-discard : enable
             perform-tagging : disable
              svlan-porttype : uni
     untagged-frames-discard : disable
                 loop-detect : disable
                       state : up
                    linktrap : enable
        multicast rate-limit : disabled
        broadcast rate-limit : disabled
                    cp limit : enabled multicast limit 15000
                               broadcast limit 10000
```

Creating an SVLAN STG

To set a tagged BPDU address different from the standardized BPDU address and create an SVLAN STG, use the following commands:

`config stg <sid> create mac <value> type <value>`

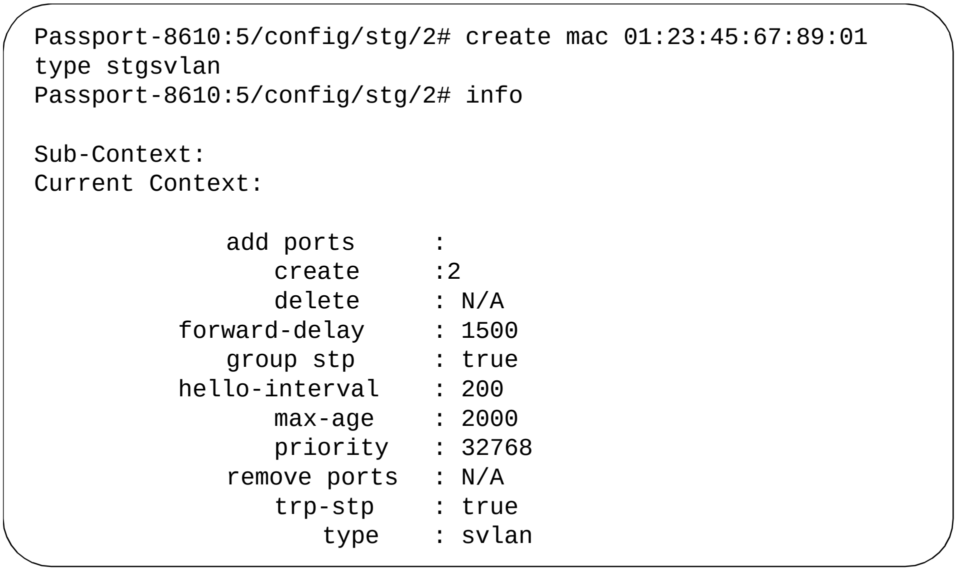
The **`config stg <sid>`** command configures parameters for a specified spanning tree group. The required parameter **`<sid>`** (spanning tree group ID) is from 1 to 64.

The **config stg <*sid*>** command includes the following parameters:

config stg <*sid*> followed by:	
create [<*ports*>] [vlan <*value*>] [mac <*value*>] [type <stgnormal|stgsvlan>]	Creates a new spanning tree group. • <*ports*> specifies one or more ports. • vlan <*value*> is the VLAN ID. If a VLAN spans multiple switches, it must be within the same STG across all switches. • mac <*value*> is the MAC address. • type <stgnormal|stgsvlan> sets the spanning tree group to normal or SVLAN.

Figure 9 shows sample output for the **config stg info** command

Figure 9 config stg info command output



```
Passport-8610:5/config/stg/2# create mac 01:23:45:67:89:01
type stgsvlan
Passport-8610:5/config/stg/2# info

Sub-Context:
Current Context:

             add ports      :
                create      :2
                delete      : N/A
          forward-delay     : 1500
             group stp      : true
          hello-interval    : 200
                max-age     : 2000
                priority    : 32768
             remove ports   : N/A
                trp-stp     : true
                   type     : svlan
```

Adding UNI or NNI ports to the STG

To add UNI or NNI ports to the STG, use the following command:

`config stg <sid> add ports <ports>`

The **config stg <*sid*>** command configures parameters for a specified spanning tree group. The required parameter **<*sid*>** (spanning tree group ID) is from 1 to 64.

The **config stg <*sid*>** command includes the following options:

config stg <*sid*> followed by:	
add ports <*ports*>	Adds ports to a spanning tree group. *ports* specifies one or more ports.

Figure 10 shows sample output for the **config stg <sid> info** command.

Figure 10 config stg <sid> info command output

```
Passport-8610:5/config/stg/2# add ports 1/1-1/8
Passport-8610:5/config/stg/2# info

Sub-Context:
Current Context:

             add ports      :1/1-1/8
                create      :2
                delete      : N/A
          forward-delay     : 1500
             group stp      : true
          hello-interval    : 200
                max-age     : 2000
                priority    : 32768
             remove ports   : N/A
                trp-stp     : true
                   type     : svlan
```

Creating an SVLAN

To create a VLAN of type SVLAN, use the following command:

```
config vlan <vid> create bysvlan <sid>
```

This command allows you to specify the type of VLAN. The required parameter `vid` is the VLAN ID (from 1 to 4094). VLAN 1 is the default VLAN.

This command includes the following parameters:

config vlan <*vid*> create followed by:	
bysvlan <*sid*> [name <*value*>] [color <*value*>]	Creates an SVLAN. • *sid* is spanning tree ID 1 to 64. • name <*value*> is the name of the VLAN from 0 to 20 characters. • color <*value*> is the color of the VLAN (0 to 32). The color attribute is used by Optivity software to display the VLAN. This command is available only for the Passport 8600.

Figure 11 shows sample output for the **config vlan info** command

Figure 11 config vlan info command output

```
Passport-8610:5/config/vlan/2# create bysvlan 2 name SVLAN2
color 11
Passport-8610:5/config/vlan/2# info

Sub-Context: create-fdb-entry fdb-filter fdb-static ip ipx
ports scrmac static-mcastmac
Current Context:

                action      : N/A
                add-mlt     :
                agetime     : 0
                delete      : N/A
                qoslevel    : 1
                name        : SVLAN2
```

Configuration example

This configuration example uses all the commands required to create an SVLAN.

Note: You must enter the commands in sequence.

```
Passport-8610co:5/config# svlan level 3
Passport-8610co:5/config# ethernet 1/1-1/8 svlan-porttype uni
Passport-8610co:5/config# stg 7 create mac 01:90:c2:00:00:00 type
stgsvlan
Passport-8610co:5/config# vlan 1476 create bysvlan 7 name matt
color 11

Passport-8610co:5/config# stg 7 add ports 1/1-1/8
```

File names for this release

Table 1 describes the Passport 8000 Series software release 3.3.2 software files and the hardware they support:

Table 1 8000 Release 3.3.2 software files and associated hardware

Module or file type	File name	Mapping file (if applicable)
8000 Series files		N/A
Boot image	p80b3320.img	N/A
Main image	p80a3320.img	N/A
MIB file	p80a3320.mib	N/A
8600 only		N/A
8672ATME and 8672ATMM modules	p80t3320.dld	N/A
8683POSE and 8683POSM module	p80p3320.dld	N/A
8100 only	p80e3320.dld	N/A

Table 1 8000 Release 3.3.2 software files and associated hardware (continued)

Module or file type	File name	Mapping file (if applicable)
Encryption files (8690/8691, 8190)		N/A
3DES encryption file. This special image file is required for Secure SHell (SSH). For instructions on downloading this file, see "Downloading the DES and 3DES encryption images" on page 43.	p80c3320.img	N/A
DES encryption file. This special image file is required for SNMPv3. For instructions on downloading this file, see "Downloading the DES and 3DES encryption images" on page 43.	p80c3320.des	N/A
Web Switching Module files to upgrade to WebOS software version 10.0.27.0.	**Mapping file name** p80w3320.img p80w3320.boot p80w3320.mp	**WSM file name** <wsm100270_bin.img> <wsm100270_boot.img> <wsm100270_mp.img>

Caution: Read first before upgrading to release 3.3.2

Before upgrading to 8000 Switch Series Software Release 3.3.2, take special note of the following cautionary messages:

- The configuration file generated with software release 3.3.2 contains options that are not backward compatible with software release 3.0.x, 3.1.x, or 3.2.x. Loading a 3.3.2.0 configuration file on a 3.0.x, 3.1.x, or 3.2.x run-time image generates errors and causes the image to abort loading the configuration file.
- Before executing any copy command (that uses the TFTP protocol), be aware that if there is any failure (TFTP server not available, TFTP Time Out, etc.), the file on the flash (or the PCMCIA) is deleted if the name of this file is the same as the one that you specified in the copy command. For example:

  ```
  8610:5> copy 111.111.1.11:p80a3320.img /flash/
  p80a3320.img
  ```

  If the server is not available, or if the file on the server does not exist, the p80a3320.img file will be deleted on the flash (if previously existing). In order to preserve the original file, you can either rename or make a backup copy of this file on the PCMCIA or flash before you begin the copy process. (Q00433556)

- 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 one of the following CLI commands:

```
copy /flash/<config filename> /pcmcia/<config
filename.old>
```

```
copy /flash/<config filename> /flash/<config
filename.old>
```

```
copy /flash/<config filename> <remote device IP
address>:<config filename.old>
```

where the remote device IP address is the device to which you want to copy the file.

Note: Before upgrading the boot flash, Nortel Networks recommends that you copy the boot image and the software image to a local switch using one of the sets of CLI commands below:

To copy from PCMCIA to flash:

- **`copy /pcmcia/p80b3320.img /flash/p80b3320.img`**
- **`copy /pcmcia/p80a3320.img /flash/p80a3320.img`**

To copy the from TFTP server to flash:

- **`copy <tftpserver IP address>:p80b3320.img /flash/p80b3320.img`**
- **`copy <tftpserver IP address>:p80a3320.img /flash/p80a3320.img`**

After a successful copy of the boot image and software image, use the CLI command **boot /flash/p80b3320.img** at the switch prompt to boot your switch with the boot image.

- Nortel Networks recommends having a copy of the boot.cfg file in the /flash directory. During bootup, if the /flash/boot.cfg file is not present, and if there is a PCMCIA card present, the 8000 Series switch will search for the file /pcmcia/boot.cfg. If a PCMCIA card is not present, or if the file /pcmcia/boot.cfg is not present, the 8000 Series switch will boot using the default boot-configuration settings. (Q00484865, Q00530115)

Caution: If using a PCMCIA card manufactured by Sandisk, the 8000 Series switch may not be able to access the /pcmcia/boot.cfg file during boot-up. This limitation has only been observed during boot-up. No limitation has been observed when accessing the Sandisk(*) device after boot-up.

Upgrading to Release 3.3.2

Caution: Prior to upgrading your software, see “Caution: Read first before upgrading to release 3.3.2” on page 25.

This section describes how to upgrade to 8000 Switch Series Software Release 3.3.2, and includes the following topics:

Upgrading the 8000 boot flash image

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

```
Loading p80b3320.img with tftp from 10.10.10.10...
<<711284
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<
<<<
to 1189500 (1189500)
Starting at 0x10000...

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

File p80b3320b013.rom found in loaded image
File size: 658504 bytes
Number of flash sectors to be programmed: 6

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

Press <Return> to stop monitor upgrade....
erased 6 sectors of bootflash
programmed bootflash
Verifying new BOOTFLASH Image...
658504 matches, 0 mismatches

Update complete!

Press return to reboot

Copyright (c) 2003 Nortel Networks, Inc.
CPU Slot 5:    PPC 740 Map B
Version:       3.3.2.0
Creation Time: Feb  6 2003, 17:21:44
Hardware Time: FEB 06 2003, 17:19:11 UTC
Memory Size:   0x08000000
Start Type:    cold
/flash/  - Volume is OK

Loaded boot configuration from file /flash/boot.cfg

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

monitor#
```

Note: Press return to go to monitor mode, otherwise, the switch will boot with the previous release.

Upgrading the software image on a non-redundant 8600 CPU

Caution: Prior to upgrading your software, see "Caution: Read first before upgrading to release 3.3.2" on page 25.

- To copy the configuration file currently used by the switch in memory, *at the switch prompt*, use the following command:

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

- To copy the configuration file specified by the boot.cfg file, use the following command:

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

  where:

  device is flash or PCMCIA.

- To upgrade the 8600 switch CPU with the version 3.3.2 software image:

  a Make sure the image file p80a3320.img is successfully copied to the flash. To ensure the image is successfully copied, boot the image from the Passport prompt using the CLI command **`boot /flash/p80a3320.img`**.

  b If the image successfully boots, modify the boot.cfg file using the CLI command **`config bootconfig choice primary image-file /flash/p80a3320.img`**.

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

  ```
  save bootconfig
  ```

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

Caution: The configuration file generated with software release 3.3.2 contains options that are not backward compatible with software release 3.0.x, 3.1.x, or 3.2.x. Loading a 3.3.2 configuration file on a 3.0.x, 3.1.x, or 3.2.x run-time image generates errors and causes the image to abort loading the configuration file.

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

Note: Hitless upgrade from 3.2.x to 3.3.2 is not supported.
Note: Before upgrading in HA mode, be sure your `ha-cpu` and `savetostandby` flags are set to `true` (enabled). To check if flags are set to `true`, use the CLI command **`config boot flags info`**.

To upgrade from 3.2.x to 3.3.2 in HA mode, follow these steps (dependent on your new image location).

1 Telnet to the master CPU or connect to the console port of the master CPU.

2 Load the 3.3.2 image to the flash of the master and the standby CPU.

For the master CPU, at the prompt, use the CLI command:

```
➔ copy <tftpserver IP address>:p80a3320.img /flash/
p80a3320.img
```

For the standby CPU, at the prompt, use the CLI command:

```
➔ copy /flash/p80a3320.img peer:/flash/p80a3320.img
```

3 Load the new boot monitor image to both the flash of both the CPUs.

For the master CPU, at the prompt, use the CLI command:

```
➔ copy <tftpserver IP address>:p80b3320.img /flash/
p80b3320.img
```

For the standby CPU, at the prompt, use the CLI command:

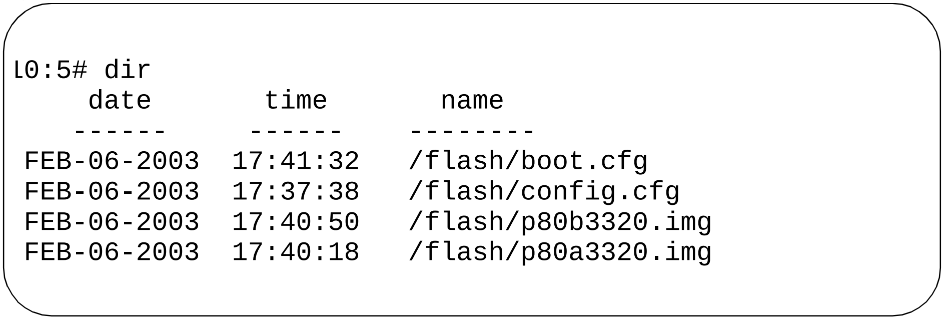
```
➔ copy /flash/p80b3320.img peer:/flash/p80b33200.img
```

4 Verify that the software has been copied to the master and the standby CPU (Figure 12 and Figure 13).

For the master CPU, at the prompt, use the CLI command:

➔ **`dir`**

Figure 12 Sample dir command output



```
L0:5# dir
    date        time        name
   ------      ------     --------
FEB-06-2003  17:41:32   /flash/boot.cfg
FEB-06-2003  17:37:38   /flash/config.cfg
FEB-06-2003  17:40:50   /flash/p80b3320.img
FEB-06-2003  17:40:18   /flash/p80a3320.img
```

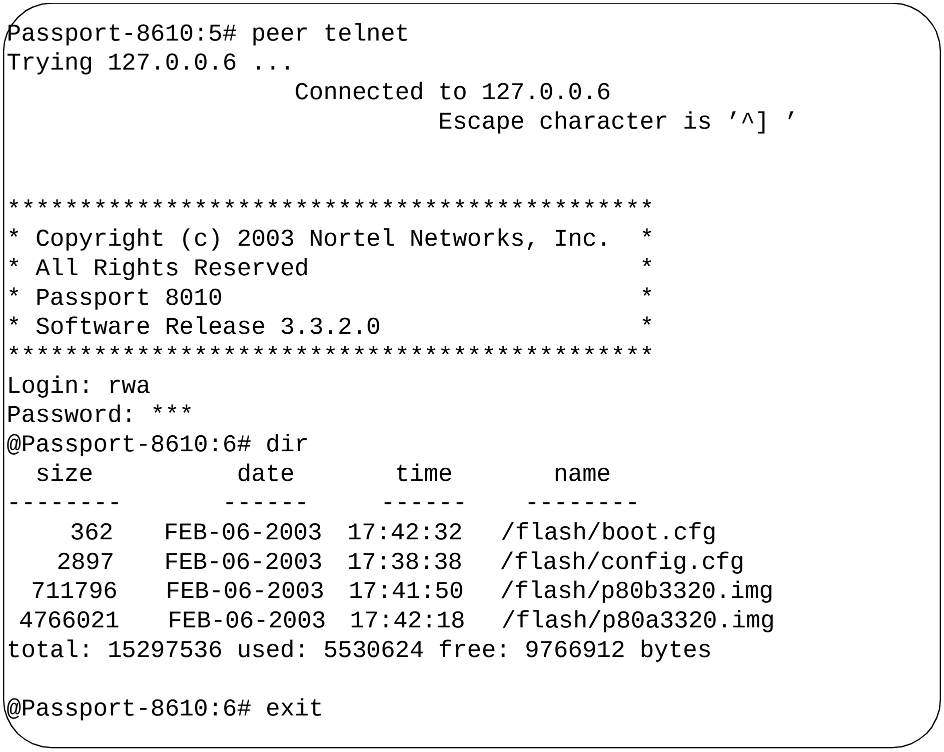
For the standby CPU, at the prompt, use the CLI command:

➔ **`peer telnet`**

Note: When connected to a CPU, the easiest way to connect to a redundant CPU is through the `peer telnet` command.

5 After you are connected, log in and execute the `dir CLI` command.

Figure 13 Sample peer telnet command output



```
Passport-8610:5# peer telnet
Trying 127.0.0.6 ...
                    Connected to 127.0.0.6
                              Escape character is '^] '


*********************************************
* Copyright (c) 2003 Nortel Networks, Inc.  *
* All Rights Reserved                       *
* Passport 8010                             *
* Software Release 3.3.2.0                  *
*********************************************
Login: rwa
Password: ***
@Passport-8610:6# dir
  size          date       time       name
--------       ------     ------    --------
     362    FEB-06-2003  17:42:32   /flash/boot.cfg
    2897    FEB-06-2003  17:38:38   /flash/config.cfg
  711796    FEB-06-2003  17:41:50   /flash/p80b3320.img
 4766021    FEB-06-2003  17:42:18   /flash/p80a3320.img
total: 15297536 used: 5530624 free: 9766912 bytes

@Passport-8610:6# exit
```

6 On the master CPU, at the prompt, set the primary image choice to the new image file (this will automatically synchronize to the standby CPU in HA-mode) using the CLI command:

➔ **`config bootconfig choice primary image-file /flash/p80a3320.img`** (*if the software image is stored on the flash*)

or

`config bootconfig choice primary image-file <tftp-server IP address>:p80a3320.img` (*if the software image is stored on the TFTP server*)

7 On the master CPU, at the prompt, save the boot configuration and run-time configuration (the configurations are automatically saved to the standby CPU in HA-Mode) using the CLI commands:

➔
```
save bootconfig
save config
```

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

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

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

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

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

For the standby CPU, at the prompt, use the CLI command:

➔ ->**peer telnet**

->**boot /flash/p80b3320.img** (*if the software image is stored on the flash*)

or

->**boot <tftp-server IP address>:p80b3320.img** (*if the software image is stored on the TFTP server*)

For the master CPU, at the prompt, use the CLI command:

➔ ->**boot /flash/p80b3320.img** (*if the software images is stored on the flash*)

or

->**boot <tftp-server IP address>:p80b3320.img** (*if the software image is stored on the TFTP server*):

Warning: Do not wait for the standby CPU to complete the boot process before booting the master CPU. This results in different images on each CPU. While in HA-mode, booting the master CPU and the standby CPU with different software images can cause the standby CPU to crash. For example, if the CPU master is using the 3.3.2.0 image and the standby CPU is booted with a 3.2.x image you will see multiple error messages on the console and the standby CPU will reboot. Nortel Networks does not support different software versions, for example 3.2.2 and 3.3.2, on the master and standby CPU. (Q00471745)

Note: In order to boot from a TFTP server, follow steps 1, 5, 6, and 7and follow the CLI examples for use with a TFTP server.

Caution: The configuration file generated with software release 3.3.2 contains options that are not backward compatible with software release 3.0.x, 3.1.x, or 3.2.x. Loading a 3.3.2 configuration file on a 3.0.x, 3.1.x, or 3.2.x run-time image generates errors and causes the image to abort loading the configuration file.

Upgrading the 8600 redundant CPU remotely (non-HA mode)

To upgrade the 8600 redundant CPU remotely, follow these steps:

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

   ```
   save config
   ```

   ```
   save bootconfig
   ```

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

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

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

3. Verify flash capacity before downloading the files.

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

   ```
   copy <tftp server ip address>:p80a3320.img /flash/
   p80a3320.img
   ```

   ```
   copy <tftp server ip address>:p80b3320.img /flash/
   p80b3320.img
   ```

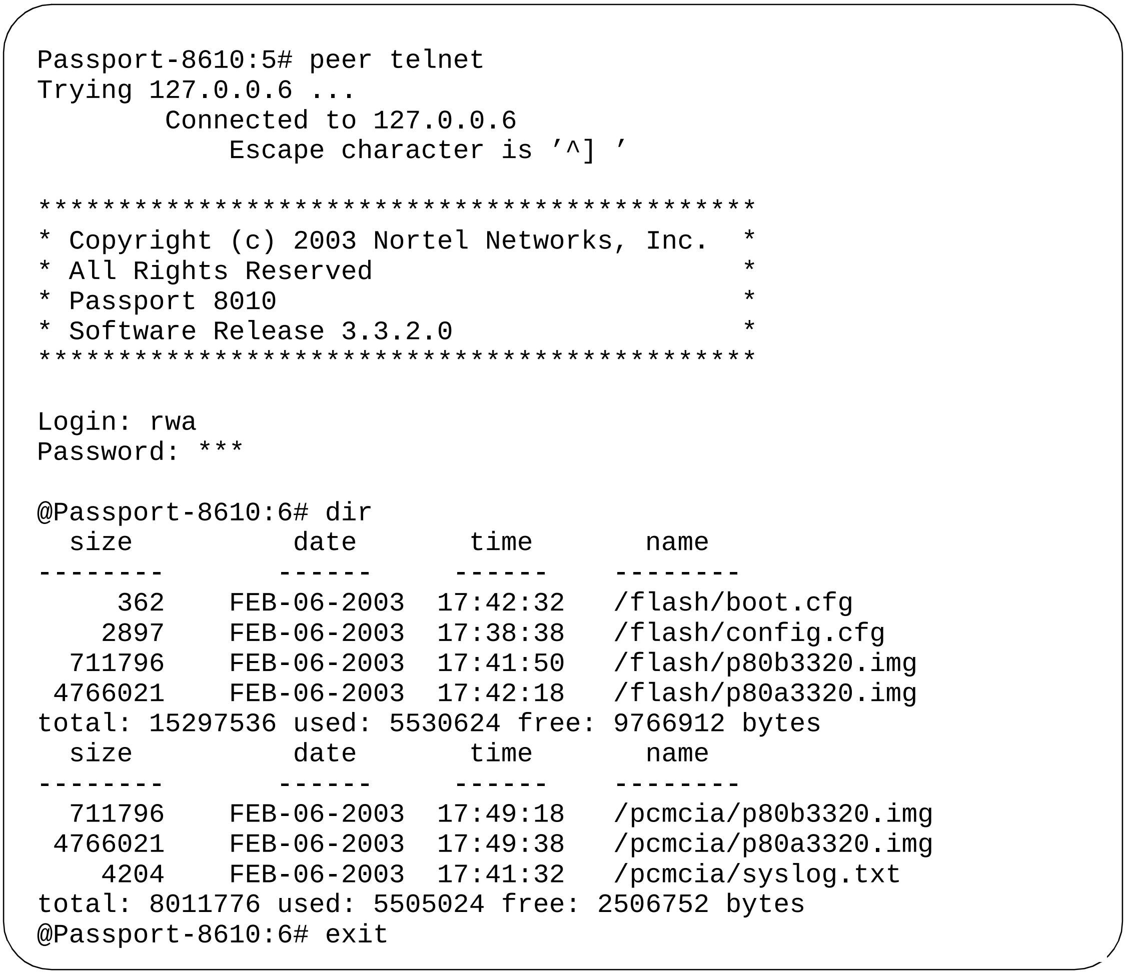
5. Copy the new software to the standby CPU using the CLI commands:

   ```
   copy /flash/p80a3320.img peer:/flash/p80a3320.img
   ```

   ```
   copy /flash/p80b3320.img peer:/flash/p80b3320.img
   ```

6. Log in to the standby CPU to verify that the software has been copied properly and exit the CPU as shown in Figure 14.

Figure 14 Sample login to verify software copy process



```
Passport-8610:5# peer telnet
Trying 127.0.0.6 ...
        Connected to 127.0.0.6
            Escape character is '^] '

*********************************************
* Copyright (c) 2003 Nortel Networks, Inc.  *
* All Rights Reserved                       *
* Passport 8010                             *
* Software Release 3.3.2.0                  *
*********************************************


Login: rwa
Password: ***

@Passport-8610:6# dir
  size          date       time       name
--------       ------     ------    --------
     362    FEB-06-2003  17:42:32   /flash/boot.cfg
    2897    FEB-06-2003  17:38:38   /flash/config.cfg
  711796    FEB-06-2003  17:41:50   /flash/p80b3320.img
 4766021    FEB-06-2003  17:42:18   /flash/p80a3320.img
total: 15297536 used: 5530624 free: 9766912 bytes
  size          date       time       name
--------       ------     ------    --------
  711796    FEB-06-2003  17:49:18   /pcmcia/p80b3320.img
 4766021    FEB-06-2003  17:49:38   /pcmcia/p80a3320.img
    4204    FEB-06-2003  17:41:32   /pcmcia/syslog.txt
total: 8011776 used: 5505024 free: 2506752 bytes
@Passport-8610:6# exit
```

7 From the master CPU, change your `bootconfig choice primary-image` file to the new run-time image file and save the **`boot.cfg`** file on both CPUs as shown in Figure 15.

Figure 15 Sample primary save bootconfig change and save

```
Passport-8610:5# config bootconfig choice primary image-file
                 /flash/p80a3320.img
Passport-8610:5#
Passport-8610:5# save bootconfig
Save to standby file /flash/boot.cfg successful.
Save bootconfig to file /flash/boot.cfg successful.
Passport-8610:5#
```

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

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

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

For the standby CPU, at the prompt, use the CLI command:

➔ ->**peer telnet**

->**boot /flash/p80b3320.img** (*if the software image is stored on the flash*)

or

->**boot <tftp-server IP address>:p80b3320.img** (*if the software image is stored on the TFTP server*)

For the master CPU, at the prompt, use the CLI command:

->boot /flash/p80b3320.img (*if the software image is stored on the flash*)

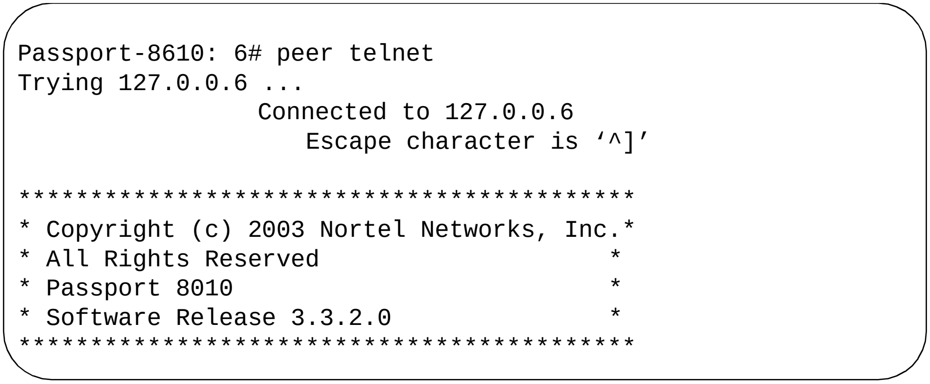
or

->boot <tftp-server IP address>:p80b3320.img (*if the software image is stored on the TFTP server).*

Warning: If you wait for the standby CPU to come up before booting the master CPU, when the standby CPU comes up, multiple error messages will display. **Nortel Networks does not support configurations that contain a master CPU and the slave CPU with different software image versions.**

9 Telnet back to the standby CPU after a few seconds to verify that the new image is running. The run-time image is shown in the Nortel Network banner displayed before the login prompt, as shown in Figure 16.

Figure 16 Sample login banner



```
Passport-8610: 6# peer telnet
Trying 127.0.0.6 ...
                 Connected to 127.0.0.6
                    Escape character is ‘^]’

*******************************************
* Copyright (c) 2003 Nortel Networks, Inc.*
* All Rights Reserved                     *
* Passport 8010                           *
* Software Release 3.3.2.0                *
*******************************************
```

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

Note: If the standby CPU is not running the new software version, you need to either repeat the procedures if the CPU allows you to log in or you may have to access the console port on the standby CPU to stop at the boot monitor and fix the problem. Most common failures are caused by improperly typing the image file name in the bootconfig file or because the software is not present on the flash on the standby CPU. Using the console port to stop at the boot monitor allows you to re-enter the bootconfig choice primary information if it has been improperly typed in and verify that the software is present on the flash of the standby CPU. If the software is not present on the standby CPU, you may have to copy it from the master CPU to a PCMCIA card on the master and then move the PCMCIA card to the standby CPU. You can then either copy it to the flash or change the bootconfig choice primary to use the PCMCIA card.

Upgrading the Web Switching Module image

This section describes how to upgrade the Web Switching Module image. Table 2 describes the Passport 8000 Series software and Web Switching Module WebOS software compatibility.

Table 2 Passport 8000 Series software and WebOS software compatibility

Passport software version	WebOs software version
3.1.3	9.0.25
3.2.1	9.0.25, 9.0.41
3.2.2	9.0.41 and up
3.3	10.0.27
3.3.2	10.0.27

⛔ **Caution:** For all new installations and upgrades, Nortel Networks recommends upgrading the Web Switching Module software before upgrading the 8600 series software.

Caution: Before upgrading to software release 3.3.X check the `WSM#/boot/cur.` If your maintenance kernel is lower than `10.0.27` then you must perform a serial upgrade on the Web Switching Module before upgrading the chassis code. This approach replaces the maintenance kernel as well as the runnable image, which resolves any upgrade issues from 3.1.3 to 3.3.x.

Use the **`copy`** CLI command to download the new firmware image file from a TFTP server to the Web Switching Module. Information about TFTPing to the Web Switching Module can be found in TFTP server to the Web Switching Module, p. 51, *Installing the Web Switching Module for the 8000 Series Switch*, (part number 314969-A).

As noted in the release notes, the procedures for a SERIAL/BINARY upgrade can be found in Appendix A, Performing a serial download, p. 63, *Installing the Web Switching Module for the 8000 Series Switch* (part number 314969-A).

To upgrade the Web Switching Module firmware image to WebOS 10.0.27.0:

1 Use the **`copy`** command to download the new firmware image file from a TFTP server to the Web Switching Module.

In the following example, the file, *wsm100270_mp.img* is copied to the Web Switching Module in slot 8, and is saved as the boot image, image1.

a

```
copy <tftpserver IP address>:wsm100270_mp.img /
<device>/image1
```

where:

`device` is wsm/8

b Set the boot image:

```
wsm setboot 8 image1
```

c Reset the Web Switching Module to boot with the new image:

```
wsm wsmreset 8
```

To upgrade the Web Switching Module binary firmware image to WebOS 10.0.27:

- Refer to Appendix A, Performing a serial download, p. 63, *Installing the Web Switching Module for the 8000 Series Switch* (part number 314969-A).

To upgrade the Web Switching Module boot image to WebOS 10.0.27:

- Refer to Extensions to copy command, p. 49, *Installing the Web Switching Module for the 8000 series switch* (part number 314969-A).

Note: In the `copy` command, make sure the file extension for the `<srcfile>` and `<destfile>` parameters is *boot*.

For a thorough discussion on Installing and Configuring the Web Switching Module, see *Installing the Web Switching Module for the 8000 Series Switch* (part number 314969-A) and *Using Device Manager to Configure the Web Switching Module* (part number 314995-A).

Downloading the DES and 3DES encryption images

In 8000 Series Switch Software Release 3.3.2, the following encryption protocols are supported

— 3DES for SSH (Secure SHell) version 1 and 2

— DES for SNMPv3

Note: Refer to the read me document, *Important Security Information for the 8000 Series Switch*, part number 314497-A which describes how to quickly disable non-secure security protocols and configure your selected security feature(s), or the document, *Configuring and Managing Security*, part number 314724-A, which provides detailed information about configuring security in your network.

Note: To protect the integrity of your switch, you cannot use Device Manager to change the passwords after a software image upgrade. Use the CLI to change your passwords.

The SSH server and SNMPv3 will not function properly without the use of the 3DES or DES (respectively) encryption algorithms to scramble the data. However, due to export restrictions Nortel Networks cannot bundle the encryption algorithms into the Passport 8000 Series switch software image, and a separate image must be downloaded.

To download the 8000 DES or 3DES encryption image:

1 Go to the Nortel Networks, Customer Support Web site at the following URL:

http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp

2 Login with your Nortel Networks user name and password.

3 Select the Product Line.

4 From the pull down menu, select the product line.

a Click “Passport 8600 Routing Switch” and click Save.

5 Select the file image to download.

a Click `Passport 8000 [DES|3DES] v3.3.2.0`.

b Complete the questionnaire that is presented.

Approval is required before receiving the encryption code.

6 Download and save the image file.

3DES for SSH

7 Copy the *p80c3320.img* image file to the Passport 8000 Series switch CPU:

a Execute the CLI command **`copy <tftpserver IP address>:p80c3320.img /<device>/p80c3320.img`**

where

`device` is flash or PCMCIA.

b Load the encryption image into memory using the command:

```
config load-module [DES|3DES] <filename>
```

where

`filename` is `/<device>/p80c3320.img`

(for example **`config load-module 3DES /flash/p80c3320.img`**)

DES for SNMPv3

To use SNMPv3 for DES, in Step 7, replace the filename p80c3320.img with the filename p80c3320.des.

8 Save your configuration.

Installing Device Manager

The 8000 Switch Series software release 3.3.2 is supported with Device Manager version 5.5.6. When installing Device Manager version 5.5.6, please note the following:

- For proper operation of the context-sensitive online Help in Device Manager, you need at least the following release versions of Internet Explorer or Netscape Navigator:
  - Internet Explorer 5.0 or later
  - Netscape Navigator 4.7—6.0
- Upgrade your Java Run-time Environment (JRE) to version 1.3.1.

Refer to Device Manager on page 70 in the Known limitations and considerations in this release section of these release notes for considerations or limitations with the Device Manager software.

For complete instructions to install Device Manager, refer to *Getting Started with the 8000 Series Management Software.*

When you install Device Manager in a Windows environment, the default directory is C:\Program Files\JDM.

When you start Device Manager in a UNIX environment, enter one of the following commands:

- The **./JDM** command to open Device Manager without specifying a device
- The ***./JDM a.b.c.d*** command to open Device Manager and the device at the IP address specified by *a.b.c.d*

Supported software and hardware capabilities

This section describes supported software and hardware capabilities in 8000 Series Switch Software Release 3.3.2, and contains the following topics:

Topic	Page
Supported software capabilities	46
Non-supported software capabilities	49
Non-supported hardware capabilities	49
Limitations between WSM & Alteon 180 Series Stackable Switches	50

Supported software capabilities

Table 3 lists the current values for supported capabilities in the 8000 Series Software Release 3.3.2. These capabilities are enhanced in subsequent software releases.

Note: The capabilities described in Table 3 are supported as individual protocols.

Table 3 Supported capabilities in the Passport 8000 Series switch (Release 3.3.2)

Feature	**Maximum number supported**
Hardware forwarding records	Non-E and E-modules: 25,000 M modules: 125,838[1]
10 GE	This release ***does not*** support the combination of the following features with the 10 GE LAN/WAN module: • IPX routing • SMLT • External MLT (Nortel Networks recommends that you use a layer 3 protocol for resiliency, for example, OSPF associated to Equal Cost MultiPath (ECMP)) • Egress port mirroring
VLANs	Passport 8100 switch: 2013 Passport 8600 switch: 1980
IP subnet-based VLANs (8600 only)	Non-E and E-modules: 200 M modules: 800
IP interfaces (8600 switch only)	500
BGP forwarding routes	• Maximum of 20,000 forwarding routes with the non-E modules and E modules • Maximum of 119,000 forwarding routes with the M Modules
BGP peers	10
RIP routes (8600 switch only)	2,500
OSPF areas per switch (8600 switch only)	5
OSPF adjacencies per switch (Passport 8600 switch only)	80
OSPF routes (8600 switch only)	Non-E and E-modules: 15,000 M modules: 20,000
DVMRP routes (8600 switch only)	2,500
DVMRP interfaces (8600 switch only)	500
DVMRP neighbors (8600 switch only)	512
PIM interfaces (8600 switch only)	500
Multicast source subnet trees (Passport 8600 switch only)	500
Multicast (S, G) records—PIM: IPMC	500
Multicast (S, G) records—PIM:	500

Table 3 Supported capabilities in the Passport 8000 Series switch (Release 3.3.2) (continued)

Feature	Maximum number supported
Multicast (S, G) records—DVMRP	1,980
IPX interfaces (Passport 8600 switch only)	100
IPX RIP routes (Passport 8600 switch only)	5,000
IPX SAP entries (Passport 8600 switch only)	7,500
VRRP interfaces (Passport 8600 switch only)	255
Spanning Tree Groups	Passport 8100 switch: 1 Passport 8600 switch: 25[2]
MLT groups[3]	Passport 8100 switch: 6 Passport 8600 switch: 32
Ports per MLT	Passport 8100 switch: 4 Passport 8600 switch: 8

[1] The number of records available, with all the record reservation fields set to zero. See *Platform and System Management* (part number 315545-A) for more information about the record reservation feature.

[2] Nortel Networks supports ONLY 25 STGs in this release. Although you can configure up to 64 STGs (63 with the Web Switching Module), configurations including more than 25 STGs are **not** supported. If you need to configure more than 25 STGs, please contact your Nortel Networks Customer Support representative for more information about the support of this feature.

[3] The MLT feature is statically compliant with the 802.3ad standard (no support of LACP).

Table 4 lists the current values for supported capabilities for the Web Switching Module in release 3.3.2. These capabilities are enhanced in subsequent software releases.

Table 4 Current supported capabilities in the Web Switching Module (release 3.3.2)

Feature	Maximum number supported
Ethernet 1000BASE-SX or 10/100BASE-T ports (or any combination that equals four ports)	4
IP interfaces per module	255
RIP routes per module	1024
Spanning tree group	15
Virtual Matrix Architecture	yes
IP Routing	yes
IP Routing Interfaces	256

Table 4 Current supported capabilities in the Web Switching Module (release 3.3.2) (continued)

Feature	**Maximum number supported**
MLT groups	4
Ports/Trunk per MLT	4
VLANs	246
Port Mirroring	yes
Filters	2048
Quality of Service (filter IP ToS)	yes
SNMP Private MIB	yes
Chassis support: The Web Switching Module is supported in the 8006, 8010, 8010co chassis, and as of release 3.3, supported in the 8003 chassis.	

For more information about Web Switching Module supported capabilities, see *Installing the Web Switching Module for the 8000 Series Switch* (part number 314969-A).

Non-supported software capabilities

Device Manager version 5.5.6 and beyond no longer provides support for the Passport 8100 1.x software code. (Q00481346)

Non-supported hardware capabilities

- 1000baseT GBICs are not supported by the Passport 8100 modules.
- Passport 8000 Series software release 3.2.0 and later does not support configurations of Passport 8100 modules and Passport 8600 modules simultaneously within the same chassis.
- The Web Switching Module is not supported in the Passport 8100 switch or in 8100 module configurations.
- The Passport 8003 chassis does not support Passport 8100 switch modules. (Q00045908)
- When used with 8690SF modules, M-Modules support a maximum of 25,000 hardware forwarding records only.

Limitations between WSM & Alteon 180 Series Stackable Switches

The Web Switching Module WebOS software implementation for STP over MLT has been modified in Passport 8000 Series Software Release 3.3 and WebOS 10.0.27.0 to make it fully compatible with Nortel Passport 8600 series switches. Note that if you trunk the Web Switching Module with Alteon Stackable 180 series switches, STP must be disabled on either the Web Switching Module or the Alteon Stackables to avoid incorrect STP operation.

Web Switching Module configuration and initialization

This section describes the Web Switching Module default software configuration considerations and the initialization process events summary.

Caution: A serial download is mandatory for all new Web Switching Modules. The serial download must occur before the chassis is upgraded.

Web Switching Module default software configuration considerations

For a thorough discussion on Installing and Configuring the Web Switching Module, see *Installing the Web Switching Module for the 8000 Series Switch* (part number 314969-B), *Using Device Manager to Configure the Web Switching Module* (part number 314995-A), and *Network Design Guidelines and Implementation Notes* (part number 313197-B).

For Web Switching Module known limitations and considerations in the Passport 8600 environment, see “Web Switching Module” on page 81.

Web Switching Module initialization process events summary:

This section summarizes the stages and automatic assignment of BFM port membership in Passport 8600 VLANs when a Web Switching Module is inserted in a Passport 8600 chassis.

The following example demonstrates this process with the Web Switching Module installed in slot 2 of a Passport 8010 Chassis with the factory default configuration. In the default configuration, a Passport 8600 has one VLAN, VLAN 1 in Spanning Tree group 1 (STG 1).

When a Web Switching Module is inserted in the Passport 8600 chassis the following events take place:

1 A syslog notification is generated, notifying insertion of a new Web Switching Module in the Passport 8600 chassis. To view the notification, enter the following CLI command:

```
Passport-8610:5# more /pcmcia/syslog.txt
```

```
[09/05/02 18:57:47] Card inserted: Slot=2 Type=ALTEON WSM
[09/05/02 18:57:47] Initializing ALTEON WSM in slot #2...
[09/05/02 18:57:48] 2k card up(CardNum=2 AdminStatus=1
OperStatus=1)
[09/05/02 18:58:17] Link Up(2/1)
[09/05/02 18:58:17] Link Up(2/2)
[09/05/02 18:58:17] Link Up(2/3)
[09/05/02 18:58:17] Link Up(2/4)
```

2 Links on four Web Switching Module BFM ports are activated. This example shows the activation process on BFM ports 2/1-2/4 when a Web Switching Module is inserted in Slot 2. The Passport 8600 uses four gigabit links (2 MLTs) through a backplane for connectivity to an Alteon Web Switching Module running WebOS 10.0 software code.

3 If you execute the **`wsm info`** CLI command, you will notice that the Web Switching Module's status is in `booting` state during its initialization and that the image status is reported as `undefined` while the WebOS 10.0 software is booting:

```
Passport-8610:5# wsm info
Card Info :
Slot# Mgmt IP FrontType BackType Status     Image Severity Version
     Assigned
   3     No  ALTEON_WSM     BFM4 Booting undefined   0   10.0.27.0

Passport-8610:5#
```

4 The Web Switching Module internal management VLAN 4093 is created in the Passport 8600 when a Web Switching Module is inserted in one of the slots. VLAN 4093 is automatically deleted when a Web Switching Module is removed from Passport 8600. VLAN 4093 is used by the Passport 8600 to manage the Web Switching Module. VLAN 4093 is a port-based VLAN and uses the highest available STG ID available in the Passport 8600. For example, in Passport 8600 Release 3.3, VLAN 4093 uses STG ID 64 (Spanning Tree Group ID). VLAN 4093 and STG 64 parameters on a Passport 8600 cannot be modified. For more information on VLAN 4093, see *Installing the Web Switching Module for the 8000 Series Switch* (part number 314969-A)

5 The Passport 8600 searches for two available MLT IDs to create the Web Switching Module's dynamic MLTs. This search starts with the highest available MLT ID and continues to the lowest ID.

For example, in Passport release 3.3, there are 32 possible MLT IDs available [`mlt id {1..32}`]. Figure 17 displays the CLI output reflecting MLT ID 32 and 31, the dynamic MLTs created with the default configuration.

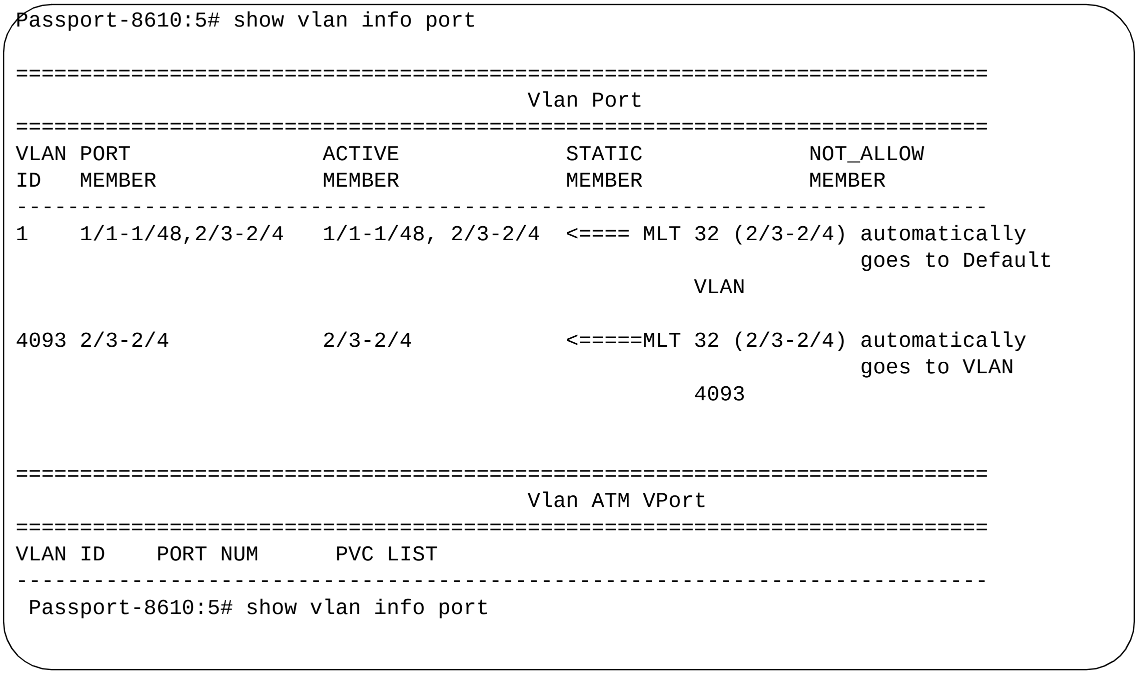
Figure 17 show mlt info sample command output

```
 Passport-8610:5# show mlt info

============================================================================
                                        Mlt Info
============================================================================
                     PORT   SVLAN  MLT   MLT      PORT     VLAN    MULTICAST
MLTID IFINDEX NAME   TYPE  TYPE  ADMIN CURRENT  MEMBERS   IDS    DISTRIBUTION
----------------------------------------------------------------------------
----
31  4126   MLT-31   trunk  normal norm  norm    2/1-2/2           disable
32  4127   MLT-32    trunk  normal norm  norm    2/3-2/4    4093 1  disable

 Passport-8610:5#
```

Note that MLT 32, the higher MLT ID, is assigned to the default VLAN (VLAN 1) and Web Switching Module management VLAN 4093, the lower MLT ID is user-configurable and is not assigned by default to any VLAN or spanning tree group.

The `show vlan info port` sample display output in Figure 18, displays the VLAN associations in the Passport 8600 after inserting the Web Switching Module.

Figure 18 show vlan info port sample command output



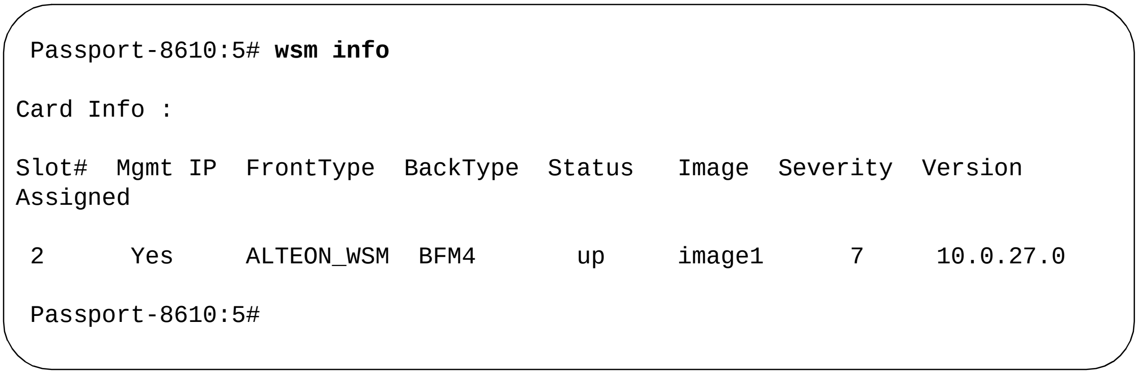
```
Passport-8610:5# show vlan info port

============================================================================
                                        Vlan Port
============================================================================
VLAN PORT               ACTIVE             STATIC             NOT_ALLOW
ID   MEMBER             MEMBER             MEMBER             MEMBER
----------------------------------------------------------------------------
1    1/1-1/48,2/3-2/4   1/1-1/48, 2/3-2/4  <==== MLT 32 (2/3-2/4) automatically
                                                                  goes to Default
                                                     VLAN

4093 2/3-2/4            2/3-2/4            <=====MLT 32 (2/3-2/4) automatically
                                                                  goes to VLAN
                                                     4093


============================================================================
                                        Vlan ATM VPort
============================================================================
VLAN ID    PORT NUM      PVC LIST
----------------------------------------------------------------------------
 Passport-8610:5# show vlan info port
```

6 When the Web Switching Module completes the initialization process, the following syslog message is automatically generated:

```
[09/05/02 19:09:01] WSM initialization completed - Slot 2
```

7 Verify that the Web Switching Module is operational by executing the `wsm info` CLI command. The Web Switching Module's status should be `UP` and the version output should display the correct WebOS software version (Figure 19).

Figure 19 wsm info sample command output



```
 Passport-8610:5# wsm info

Card Info :

Slot#  Mgmt IP  FrontType  BackType  Status   Image  Severity  Version
Assigned

 2      Yes     ALTEON_WSM  BFM4       up     image1      7     10.0.27.0

 Passport-8610:5#
```

The Web Switching Module will remain in a booting state if the WebOS software version is not compatible with the Passport 8600 software version. Use the software compatibility matrix to ensure that the Web Switching Module software is compatible with Passport 8600 software. For more information about the WebOS software and the necessary mapping files, see “8000 Release 3.3.2 software files and associated hardware” on page 24.

Caution: If a wrong software image is loaded in the Web Switching Module, you may need to use the maintenance port to serial download the correct WebOS software image. The maintenance port is a DIN-8 connector. You can connect to the Web Switching Module with this port. A DB-9 to DIN-8 serial cable is provided.

Documentation corrections and additions

This section describes documentation corrections or documentation that has not yet been added to the larger documentation suite. This information is in addition to the documentation corrections and additions defined in the *Release Notes for the Passport 8000 Series Switch Software Release 3.3* (part number 314754-A).

Documentation additions

This section describes information that is not yet documented in the manuals provided with your software or hardware.

Filters

For IPSEC traffic to successfully pass a port with default action drop, it is required to create traffic filters allowing:

- Protocol 17 (UDP)
- Source and destination port 500
- Protocol 50 (ESP)
- Protocol 51 (AH)

An example configuration is shown below:

```
ip traffic-filter create source
src-ip 61.88.131.13/255.255.255.255 dst-ip 0.0.0.0/0.0.0.0
id 4
ip traffic-filter filter 4 action mode forward
ip traffic-filter filter 4 match protocol ipsec_esp
ip traffic-filter create source
src-ip 61.88.131.13/255.255.255.255
dst-ip 0.0.0.0/0.0.0.0 id 5
ip traffic-filter filter 5 action mode forward
ip traffic-filter filter 5 action statistic enable
ip traffic-filter filter 5 action tcp-connect enable
ip traffic-filter filter 5 match protocol ipsec_ah
ip traffic-filter create source
src-ip 61.88.131.13/255.255.255.255
dst-ip 0.0.0.0/0.0.0.0 id 6
ip traffic-filter filter 6 action mode forward
ip traffic-filter filter 6 action statistic enable
ip traffic-filter filter 6 match dst-port 500
dst-optionequal
ip traffic-filter filter 6 match src-port 500 src-option
equal
ip traffic-filter filter 6 match protocol udp
ip traffic-filter set 300 create name "internet"
ip traffic-filter set 300 add-filter 4
ip traffic-filter set 300 add-filter 5
ip traffic-filter set 300 add-filter 6
ethernet 4/8 ip traffic-filter create
ethernet 4/8 ip traffic-filter add set 300
ethernet 4/8 ip traffic-filter default-action drop
ethernet 4/8 ip traffic-filter enable
```

Configuring IP Routing Operations (314720-A)

- A new CLI command has been introduced, **`config ethernet (slot/port) high-secure`**. When enabled, the Passport 8600 routing switch will drop all packets with a source IP address of 255.255.255.255, 0.0.0.0, Class D, and Class E addresses. (Q00288340-02)

Configuring and Managing Security (314724-A)

A new parameter `access-strict` has been added to the CLI access policy tree. This parameter, if set to **true**, grants access to the configured level only. This will allow access policies to be created to allow only `read only` or only `read write` access. An example of the format of this command is below:

`config sys access-policy policy access-strict [true/false]`
(The default value of `access-strict` is false)

If `access-strict` is `false`, the access-policy will operate as before. A configured access level of `ro` will grant access to `ro` and above access levels. If `access-strict` is `true`, a configured access level of `ro` will grant access to only `ro` access level.

(Q00520275-04)

Platform and System Management (315545-A)

A new option, `file`, has been added to the CLI command `config bootconfig flags debug-config <true|false|`**`file`**`>` which allows you to specify a file. This new flag logs all the output to the file on the PCMCIA under the filename `debugconfig.txt`.

If this flag is set to `true`, configuration errors are displayed to the console port. If this flag is set to `false`, nothing is displayed. If this flag is set to `file`, the output will be logged to a file on the PCMCIA with the name `debugconfig.txt`.

To view the `debugconfig.txt` file, use the CLI command **`edit pcmcia debugconfig.txt`**

Before setting the `file` option, be sure that the PCMCIA card is not near its capacity. If the `debug-config flag` is set to `file` and it is necessary to downgrade the software, the flag will need to be set back to `true` or `false`.

(Q00462041-01)

Documentation corrections

Configuring IP Routing Operations (314720-A)

Configuring directed broadcast on a brouter port

A directed broadcast is a frame sent to the broadcast address of a specific subnet. Disabling the routing of directed broadcasts protects networks and their hosts from possible denial of service (DOS) attacks. However, since there are some applications that rely on directed broadcasts for proper operation, make certain that directed broadcasts are not used on your network prior to disabling them.

The **`config ethernet <slot/port> ip directed-broadcast`** command allows you to enable or disable the routing of directed broadcast. This option will only affect brouter ports.

➡ **Note:** The CPU does not receive a copy of routed directed broadcast packets and, therefore, does not respond to a subnet broadcast ping sent from a remote subnet. A subnet broadcast ping sent from a local subnet (and not routed) is received by the CPU, and the CPU responds.

The **`config ethernet <slot/port> ip directed-broadcast`** command includes the following options:

`config ethernet <slot/port> ip directed-broadcast` followed by:	
`info`	Displays the current forwarding setting.
`disable`	Disables the routing of directed broadcasts on the specified brouter port or ports.
`enable`	Enables the routing of directed broadcasts on the specified brouter port or ports. This is the default setting.

Configuring directed broadcast on a VLAN

A directed broadcast is a frame sent to the broadcast address of a specific subnet. Disabling the routing of directed broadcasts protects networks and their hosts from possible denial of service (DOS) attacks. However, since there are some applications that rely on directed broadcasts for proper operation, make certain that directed broadcasts are not used on your network prior to disabling them.

The **`config ethernet <vlanID> ip directed-broadcast`** command allows you to enable or disable routing of directed broadcast. This option only affects how an ingress directed broadcast packet from a remote subnet is handled.

Note: The CPU does not receive a copy of routed directed broadcast packets and, therefore, does not respond to a subnet broadcast ping sent from a remote subnet. A subnet broadcast ping sent from a local subnet (and not routed) is received by the CPU, and the CPU responds.

The **`config ethernet <vlanID> ip directed-broadcast`** command includes the following options:

`config ethernet <vlanID> ip directed-broadcast` followed by:	
`info`	Displays the current forwarding setting.
`disable`	Disables the routing of directed broadcasts on the specified brouter port or ports.
`enable`	Enables the routing of directed broadcasts on the specified brouter port or ports. This is the default setting.

Using the 10 Gigabit Ethernet Modules: 8681XLR and 8681XLW (315893-A)

The *Using the 10 Gigabit Ethernet Modules: 8681XLR and 8681XLW* (part number 315893-A) book, in Figure 7 on page 43, incorrectly displays “none” as a configurable parameter for support framing type.

Bugs fixed in this release

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

Platform

- A check is now performed to prevent the Passport 8100 switch from learning a broadcast source MAC address. (Q00248798-02)
- Performing a `change directory` operation on the flash through FTP no longer causes flash corruption when the command is performed more than 22 times. (Q00564272)
- Connectivity is now maintained on 8108GB ports when autonegotiation is disabled and the primary bus master is removed. (Q00535545-01)
- Traffic is now properly recovered on 8116FX ports that are disabled and then re-enabled. (Q00470100-03)
- Outgoing telnet sessions are now terminated properly when the source telnet into the switch is terminated. (Q00500315-02)
- The MIB file has been modified so that it no longer contains any object descriptors longer than 64 characters. This is in compliance with RFC 1902-SNMPv2-SMI, Section 3.1. (Q00545287-02)
- RWA (read-write-all) access is now required to view community strings. (Q00470515-04)
- Syslog hosts now receive the syslog if they are enabled, and will not receive it if they are disabled, independent of their order in the syslog host listing. (Q00485569-02)

- A warm start trap is now generated when the primary CPU fails over to the standby CPU. When the standby CPU becomes the primary, it generates the trap, as well as the following message in the log file: `Cpu switch over, standby in slot # <slot no.> has become master`. (Q00459756-01)
- It is now possible to copy files between master and standby CPUs without enabling the TFTPD flag. TFTP file transfer from an external TFTP client still requires the TFTPD flag to be enabled. (Q00604900)

Switch management

Select a topic:

Topic	Page
General	62
Device Manager	63
CLI	63
Port mirroring	64

General

- The traffic flow on MLT/SMLT/IST links is determined by the hardware algorithm in real time dependent on how many ports are active and the source/destination addresses of the packets transmitted. It is possible that the packet streams may traverse through different links of an MLT trunk when there are changes to the link state on one of the individual links of the MLT trunk. This behavior does not affect the end to end delivery of a data stream between systems. This is the normal behavior of link aggregation. (Q00288535)
- Tagged ports can now be successfully configured with a `default-vlan-id` set to `0` using the CLI or Device Manager, and this setting is now maintained across a reboot. (Q00485733)
- Issuing the **`show log file`** CLI command now displays only the log messages after the system reset. This avoids system problems when displaying larger (larger than 10MB) log files. (Q00484994-02)
- The character `"` is not allowed as part of any CLI or Device Manager string input. (Q00541574-01)

Device Manager

- Device Manager now requires `read-write` access and above to modify QoS settings. (Q00510143-03)
- The object/field `ifLastChange` under the Device Manager Edit menu correctly reflects the port operational state changes made through the CLI or Device Manager. (Q00551688, Q00551733-01)

CLI

- DVMRP route policies can now be configured with a maximum string length of 64 characters in the CLI and Device Manager. (Q00572865)
- CLI `show ip dhcp-relay` counters now display all of the dhcp-relay enabled interfaces. (Q00536028-01)
- Log messages referring to slot 5 and slot 6 in an 8003 3-slot chassis have been removed. (Q00509354-03)
- The CLI command **`show ip mroute next-hop`** now properly displays the status as pruned for those streams pruned by a downstream switch. (Q00494559-01)
- Changing the password more than twenty-one times using the CLI, no longer results in flash corruption. (Q00526417-02)
- On a Passport 8100, all MAC addresses are properly displayed when you execute the **`show vlan fdb-entry`** CLI command. Previously, only MAC addresses that started with 00:xx were displayed. (Q00561539)

SNMP

- The following SNMP v1 traps now use the proper format: SMLT link down, SMLT link up, SMLT IST link down, SMLT IST link up, and Password change. (Q00587526-01)
- SNMP traps with a destination of a loopback address or the management port IP address are now properly dropped. (Q00471269-03)
- `sysUpTime` SNMP v2 traps are now sent with the correct format. (Q00554345-01)
- A Passport 8600 routing switch running software version 3.3.2.0 returns correct values for the SNMP GetNext requests of the ifTable and rcPortTable. (Q00568468)

SMLT

- In a Square SMLT topology, if the last SMLT link is removed and reconnected while the SMLT link is UP on the peer, the fdb-entries are now learned properly and we no longer have connectivity issues. (Q00590125)

Port mirroring

The Passport 8100 switch can now be configured for all port mirroring modes: RX, TX and both. (Q00520880-02)

Security

- SSH parameters now properly load from the configuration file on a Passport 8600 when the `sshd` flag is enabled. (Q00513370-01)
- Authentication traps are now only sent if the `config sys set sendtrap` flag is set to `true`. (Q00526713-02)
- The file name for the 3DES encryption image is now limited to a length of 99 characters. (Q00552391-01)

Hardware

GBICs

GBIC modules with administratively disabled port(s) no longer result in GBIC recognition issues upon GBIC insertion or removal. (Q00502473-03, Q00505066-01)

Management port

- The management port now supports RADIUS protocol. Refer to your RADIUS documentation for a list of supported RADIUS servers. (Q00318032-03)
- The management port IP address can be reset back to the default IP address without any errors. (Q00576336-01)

8672ATM/ATME module

- ATM port LEDs now operate properly when the link has been administratively set to down. (Q00471033-02)

- On a Passport 8672ATM module, a port is now brought down with F5OAM failure on the last PVC of the port. (Q00505713-02)
- When an 8672ATM module is removed and re-inserted, the F5OAM status is renegotiated for all the F5OAM enabled PVCs on the ATM ports. This will avoid ATM ports from coming up when all F50AM enabled PVCs are down during re-insertion of the module. (Q00554022-02)
- Modification of ATM port parameters will no longer result in traffic loss when over 200 PVCs are configured. (Q00522216-01, Q00544052-01)

Filters and bandwidth control

- DSCP bits can be modified only when `translate-dscp` of the traffic profile is set to `true`. (Q00539793-01)
- Modifying either the DSCP or p-bit for a filter results in both values being changed based on the mapping in the QoS Ingress table. If both the DSCP and the p-bit are modified, then for global filters the P-bit has higher precedence, while for traffic (src/dst) filters the DSCP will have the higher precedence. A warning message is now displayed if the values do not match. (Q00225567-02)
- Traffic filters with a non-zero source/destination port and the ignore option configured now operate properly. (Q00468327-03)

Layer 2 switching

High Availability mode

- Syslog configurations are now properly synched when HA-CPU mode is enabled, and the settings are preserved across an HA-CPU failover. (Q00568730-01)

MLT

- When 8608GB ports are added to an MLT, port parameters such as autonegotiation and speed are now set to default values. (Q00537386-01, Q00563608)

VLANs

- Source MAC VLANs can now pass directed broadcast traffic. This requires a system filter (created automatically) which is not available in High Performance mode. (Q00465843-01)
- Ports configured with default action drop and with an ARP protocol VLAN now correctly process bridged ARP traffic when an IP address is configured on the VLAN. (Q00503231-02)
- A VLAN configuration is now restored correctly across reboots when the VLAN contains both the Web Switching Module and non-Web Switching Module ports. (Q00493619-02)

IP unicast

ARP

- Discarded ARP records for the next-hop of a static route with a nonlocal-next-hop set are now removed when that next-hop is reachable through a dynamic route. (Q00527165-02)
- The Next Hop Forward Filter configuration no longer causes connectivity problems when ARPs age out. (Q00486312-02)

OSPF

- NSSA ABR routers now automatically act as an ASBR. (Q00474283-01, Q00539259-02)
- Configuring an OSPF interface in a specific area no longer inappropriately displays the error message: `Error: consistency check failed - ospf interface area-id conflicts with configure range`. (Q00516523-02)
- Changes in the `config ip route preference` to make OSPF_E2 (ASE External type-2) more preferred over OSPF_E1 (ASE External type-1) now take effect. (Q00512072-03)

RIP

The RIP holddown timer now operates properly. (Q00476501-01)

VRRP

- VRRP State Transition Trap log messages now contain slot/port for brouter ports and VLAN ID for VLANs. (Q00522473-02)
- VRRP transitions from backup to master now delay becoming master for three times the hello interval. (Q00582030)
- Setting the VRRP hold down timer to a non-zero value no longer causes continuous VRRP transitions. (Q00575128)
- VRRP sessions are not impacted when saving a large configuration file with more than 100 vrids. (Q00558551)

IP multicast

Multicast packets configured with a less than 2 second time to live (TTL) are no longer routed, and a prune is sent to the sender. (Q00524063-01)

IPX routing

When an IPX local route goes down and that same network is learned as a RIP route, IPX forwarding is no longer impacted. (Q00484550-02)

Known limitations and considerations in this release

This section describes issues and limitations known to exist in this software release. The section includes the following topics:

Topic	Page
Platform	68
Switch management	69
Hardware	77
Layer 2 switching	83
VLANs	83
Filters and bandwidth control	87
IP unicast	90

Platform

- To avoid disk cache errors or disk read failures before a CPU switchover (except for hot-standby), execute the CLI command `pcmcia-stop` before removing the PCMCIA card. (Q00527228)
- When you change the bootconfig flag 8100-mode from `false` to `true` (8600 to 8100), you may see error messages and the switch may reset. Nortel Networks recommends that you modify the `boot.cfg` file manually, offline, transfer the file to the switch, and reboot the switch. (Q00278145)
- After FTPing a host image to a switch, errors may generate and the image may be deleted from the flash. If this occurs, recopy the files. (Q00502846)
- When viewing a prefix list using the `config ip prefix-list 1 info` CLI command, the list continues to generate without page breaks even if the `config cli more true` command is configured. (Q00516265)
- Upon bootup or after a CPU failover, the error message `ERROR Task=tChasServ RTC update on standby CPU failed!` may appear. It has no negative impact on your switch. (Q00527144)
- In rare cases where there is a power outage between 3-5 seconds, you may see a connection loss between the master and the standby CPU. (Q00415626)
- When hotswapping modules in an 8000 Series Chassis, wait for at least 30-45 seconds before reinserting the same module or a different module. Failure to wait this amount of time could result in the module not initializing. (Q00428915)
- Data packets will be sent to the CPU for an ICMP redirect error condition unless the `icmp-redirect-msg` feature is disabled. (Q00084232) (Passport 8600)
- During periods of high CPU activity, do not globally disable routing protocols or flush routing tables. These actions could cause the CPU to prioritize these commands rather than network control packet processing. (Q00024204, Q00024060) (Passport 8600)
- RADIUS configurations using the Passport 8100 are not supported with HA-mode in this release. (Q00157512)

Switch management

Select a topic:

General

- Nortel Networks recommends that you not mix GBICs with different settings (specifically autonegotiation) in an MLT group. Because the configuration is based on the first port of the MLT, a configuration including a mix of SX and 1000BASE-T GBICs would fail if the first port has the autonegotiation set. 1000BASE-T GBICs do not support autonegotiation (Q00596318).
- The link flap detection feature now properly utilizes the configured time interval. (Q00500313-02)
- It appears you can select DS3 framing types for an OC-3/OC-12 port that cannot be used. If you select an incorrect framing type, an error message is generated. (Q00502251)
- Syslog and Trap Log may not capture all log session messages for the Web Switching Module. (Q00423460)
- You cannot copy files to the standby CPU if the primary CPU does not have enough disk space. If you attempt to do so, the following error message is generated: `Error: Insufficient disk space: Required xxxxxxxx Free xxxx`. (Q00340408)
- The CLI command **`save standby`** supports the configuration file, but it does not support trace or log files. (Q00418553)

- On a Passport 8100 Series switch, the Management port on the Passport 8190SM module does not participate in the Autotopology™ algorithm for network management software. You must enter the IP address of each Passport 8100 switch as a seed address to have the topology of that switch discovered by the network management software.
  (Q00023301)
- On a Passport 8000 Series switch, in rare cases, it is possible for a port to become disabled during switch startup if traffic is ingressing during the module initialization.

  To workaround this issue, stop the traffic ingressing on the module and either reseat the module or reboot the switch. (Q00044113) (Passport 8100/8600)
- Device Manager and the CLI incorrectly allow you to configure a large IPX tick value (up to 2147483647). The actual maximum tick value that can be used is 65535. Do not enter a value higher than this. (Q00538449, Q00538439)

Device Manager

- Device Manager does not properly call the correct help files when accessing help in the Security > SNMP path. You can still find this information through the table of contents in the help files. (Q00534761)
- With HA enabled, you cannot edit multiple 10 GE LAN/WAN module ports using Device Manager. (Q00535353)
- In the OSPF tab (VLAN > IP > OSPF), you cannot change the HelloInterval and RtrDeadInterval and apply the changes at the same time; if you attempt to do so, the error message `rcIpConfOspfHelloInterval.2101: Router dead-interval must be a multiple of the hello interval` is displayed. To workaround this issue, first configure the RtrDeadInterval and apply the change, then configure the HelloInterval and apply the change. (Q00533862)
- Device Manager does not properly display all fields in the IP multicast Next Hop table. To workaround this issue, use the CLI command `show ip mroute# next-hop`. (Q00531492)

- The maximum number of enabled mirrored ports supported is 383. Because the software processes enable/disable requests sequentially, if you attempt to enable mirrored ports and the error message `rcDiagMirrorByPortEnable.35:maxOfMirroringPortAllowedExceed` displays, it is because the disabled ports have not yet been recognized. To workaround this issue, first disable your selected mirrored ports and apply the action prior to enabling new mirrored ports. (Q00089459)
- In Device Manager, when a peer group is applied to a peer when the peer is created, the inbound route policy is not correctly added to the peer. To work around this issue, reapply the peer group to the peer and the inbound policy will be set correctly. (Q00517676)
- Device Manager uses the default settings of the Java application launcher when it is launched. These default fits most operations, but in large configurations you may need to increase the default heap size setting in Device Manager from 64MB to 128MB (-Xmx128m) to avoid display issues or error messages, for example, `java.lang.OutOfMemoryError`. (Q00487953)
- In various protocols, Device Manager incorrectly allows you to set the SetAsPath Mode to tag. The set tag feature is not supported in this release. (Q00502166, Q00502162)
- Multicast Flow Distribution is not supported in this release. However, Device Manager online help may display help for this feature. (Q00527800)
- Device Manager incorrectly displays the IPX network number in the ATM 1483 ELAN tab. You can view the correct IPX network numbers in the CLI using the commands **`show port inf atm 1483`** or **`config atm <port> pvc 1483 mux inf`**. (Q00523934)
- You cannot enable or configure the Web Switching Module Web responder using Device Manager. To enable and configure the Web responder, use the CLI commands **`cfg sys http`** and **`cfg sys wport`** (Q00432920)
- You cannot configure Bootp parameters for the Web Switching Module using Device Manager. To work around this issue, use the CLI or the Web Switching Module Element Manager software. (Q00432092)
- Device Manager incorrectly displays information for the IP address of default VLAN4093 using the following two paths: IP Routing > DVMRP> Interfaces and IP Routing > PIM > Interfaces. (Q00248618)

- Device Manager allows you to create an authentication-key for simple authentication longer than the 8-character maximum (IP Routing > OSPF > Interface). To work around this issue, enter only an 8 character string as your authentication key. (Q00418387)
- When a brouter port exists in a VLAN, you cannot create a IP-based VLAN in Device Manager (VLAN > STG > Insert (VLAN).

  To workaround this issue, create this VLAN type using the following CLI commands:

  ```
  config vlan <vlan id>
  config vlan <vlan id> create byprotocol <sid> ip
  config vlan <vlan id> info
  ```

  (Q00416781)
- Device Manager does not automatically assign a default VLAN name (as is the case when you use the CLI). (Q00224955)
- You can configure an IP address with an invalid broadcast address using Device Manager. (Q00224945)
- In Device Manager, if you create a trunk MLT with multiple byport VLAN IDs selected, the resulting MLT will have only one VLAN in its VLAN IDs list. You have to reenter any missing VLAN IDs in the MLT dialog box. (Q00207960-01)
- Device Manager will not allow you to select a Gigabit port on a Passport 8616SX and a GBIC SX port on a Passport 8632TX module simultaneously. Therefore, you are unable to graph the ports. You can only select ports of a similar type for editing/graphing purposes. For example, you can select ATM OC3 and ATM OC12 simultaneously. (Q00041550) (Passport 8632TX only)
- In a Solaris environment, if you hold the left mouse button and drag the cursor back and forth between cascade menus, Device Manager quits and displays an error message. This is a Java Runtime Environment issue. (Q00031469) (Passport 8100/8600)
- When you create a static route using a host IP address and mask, a `No such Instance` error message may be displayed the first time you try to view the static route. If you refresh the display, the table displays the correct information. (Q00044192) (Passport 8600)
- Device Manager displays the administrative configuration of the Management port, but not the operational status. To see the current operational status of the Management port, use this CLI command:

`config bootconfig net mgmt info`

(Q00035754)

- When you add multiple global filter sets to a port using Device Manager, the following error message may be displayed:

  ```
  rcIpFilterPortFilterList:172 apply duplicated global
  filter to port
  ```

  When you refresh the display, the operation continues properly. (Q00038808)

CLI

- The CLI command `config ether <slot/port>-<slot/port>` does not support configurations containing the 10 GE LAN/WAN module. (Q00480621)
- The bridge entry for OC-3 and OC-12 links are not reported correctly in the `sh ports stats info stg exten` CLI command output. (Q00342977)
- When you save a configuration file with the CLI command **`save config file <filename>`**, and `<filename>` is a duplicate of the filename in flash, a warning message is not displayed that this operation will overwrite the exiting file in the flash. (Q00418380)
- On a Passport 8600 Series switch, no CLI commands exist to configure the Device Manager equivalent of “Manual Edit” or “MAC Learning Entry.” (Q00047767) (Passport 8600)
- On a Passport 8000 Series switch, the **`show sys topology`** CLI command displays the wrong value for the port/slot of the management port. (Q00048170) (Passport 8100/8600)
- On a Passport 8000 Series switch, the **`clear port stats`** CLI command does not clear STG and OSPF port statistics. (Q00043777)

Web management

- The Web Management Interface does not support performing lexicographic ordering with Instance-ID's equal to or larger than 2^32, for example, 4, 294, 967, 295. (Q00478480)
- The Web management interface incorrectly displays fields for unsupported features in Passport 8000 Switch Series Software Release 3.3. (Q00537594)

- There is no online help support built into the Web management interface for 3.3 features. If you try to open an unsupported feature, the following error message will display:

  ```
  Tftp Error
  ```

  ```
  The file in the specified tftp server could not be
  retrieved.Please check if the path and the tftp server
  address are correct.
  ```

  ```
  click here for help on configuring help file path </
  help_configure.html>
  ```

Management port

- You can change, but not delete, the 869x CPU net management IP address in the run-time mode. To delete the CPU net management IP address, reboot the 869x CPU to boot monitor mode. In the boot monitor mode you can delete the CPU management IP address by inputting the following IP address, `net mgmt ip 0.0.0.0/0 cpu-slot <cpu slot #>` (Q00453989)
- In redundant CPU switch configurations, if you are changing the master CPU management IP address, the CLI may display the error message `Master IP should be in same subnet as Standby IP`. To change the Master CPU management IP address, reboot the Master CPU to boot monitor mode. In the boot monitor change/delete the CPU management IP. Save the boot.cfg on the master and then save to the standby. (Q00454983)

RMON

- When there are several RMON alarms and running MIBwalks on the master CPU, although there is no impact to network traffic, the slave CPU console may get the following error message:

  ```
  Can’t open directory /pcmcia
  S_dosFsLib_FILE_NOT_FOUND
  ```

  (Q00083161)
- On a Passport 8600 switch, you may need to set the RMON memory size to 250K if the 250K default is not reallocated after a system reboot. (Q00041986)

- The Passport 8600 switch CLI incorrectly allows RMON History and Etherstats to be configured for ATM and POS ports, even though this functionality is not supported for ATM and POS. (Q00041025) (Passport 8600)

SNMP

- Passport 8000 Switch Series Software Release 3.3.2 is not fully compliant with SNMPv3 RFCs: 2572, 2573, and 2574:
  - The agent does not properly handles unknown `contextEngineID` values. (Q00486049)
  - After sending a SET on a new instance of `vacmAccessReadViewName` with a value with the `vacmAccessStatus` excluded, the agent does not return an inconsistent name, value, or an error. (Q00486966)
  - The agent does not properly implement transitions of the `vacmSecurityToGroupStatus` object from the `notReady` state. (Q00486800)
  - The agent does not properly implement transitions of the `vacmSecurityToGroupStatus` object from the non-existent state. (Q00486811)
  - The agent does not increment `snmpUnknownPDUHandlers` after receiving malformed ASN1 packets. (Q00486105)
  - The agent doesn't return the expected error when creating a row without a `VacmGrName`. (Q00486792)

Security

- The boot flag setting for block-snmp (`config bootconfig flags block-snmp`) and the runtime config SSH secure (`config sys set ssh enable <true/false/secure>`) both modify the block-snmp boot flag. If enabling SSH secure, the block-snmp boot flag will be modified to `true` and the change will take effect after reboot. To set the block-snmp boot flag to `false`, SSH secure mode should first be disabled. (Q00540689)
- If there are SSHv1 clients (both Unix and PC) connected to the switch and SSH is disabled the following error messages will display before the logout message:

  ```
  SwitchC:5# [09/24/02 13:41:16] ERROR Task=sshdSession
  Write failed: S_iosLib_INVALID_FILE_DESCRIPTOR
  ```

  (Q00528007)
- For security purposes, if you fail to login correctly on the master CPU in three consecutive instances, the CPU will lock for 60 seconds. If fail to login correctly on the slave CPU in three consecutive instances, the CPU fails to recover from the lockup. To resolve this issue, do one of the following:
  - — Reseat the slave CPU
  - — Boot the slave from a different client
  - — Configure the slave CPU to be the master CPU

  (Q00246377)
- The 8600 does not generate a log message when a RSA key is manually generated. This is not the case with DSA, where a message indicating that a key has been generated, is issued by the switch. (Q00252543)

Hardware

Select a topic

General

- 8608 Gigabit ports may not initialize if there is a 5112 firewall connected to any of the ports. This same issue may occur if there is a port connected to other Alteon products such as the Alteon 184 or 180e. To workaround this issue, disable auto negotiation on the Gigabit ports of both the Passport and the Alteon switch prior to a reboot. (Q00538075)
- If you bring up a HA-CPU enabled switch with 8672 ATM/ATME/ATMM, 8683POS/POSE/POSM modules, or Web Switching Module in the chassis, the modules will be brought offline. 8672 ATM/ATME/ATMM or 8683POS/POSE/POSM, and the Web Switching Module are not supported in HA-mode. (Q00421847, Q00233322, Q00157482)
- The CLI command `show vlan info all` does not display IGMP output. (Q00278240) (Passport 8100)
- CPU I/O operations errors may be generated when a PCMCIA module is near 100% capacity. (Q00088823)
- Under certain network conditions, error task messages may be generated with references to the RAR with resulting error codes. Below is a list of error task messages and a few examples of RAR (RaptAru Records) error codes:

  ```
  ERROR Task=tMainTask rcIpAddRoute: rarAddIpRoute failed
  with <error code>
  ```

  ```
  ERROR Task=tMainTask rcIpVlanUp rarAddArp failed with
  Status <error code>
  ```

  ```
  ERROR Task=tMainTask rcIpSuperNetAddRoute: rarAddIpRoute
  failed with <error code>
  ```

```
ERROR Task=tMainTask rcIpAddRoute: rcIpAddArp failed with
<error code>
```

```
ERROR Task=tMainTask rcIpModifyNextHop: rarReplaceIpRoute
failed with <error code>
```

Below is a list of the RAR error codes:

RAR_DUPLICATE	-100	Duplicate Record
RAR_INCONSISTANT	-101	Inconsistent Record between CPU and Hardware
RAR_TABLE_FULL	-102	Record Table full
RAR_MGID_INUSE	-103	MGID (Multicast Group ID) already used
RAR_INVALID_MGID	-104	Invalid MGID (Multicast Group ID)
RAR_INVALID_PORT	-105	Invalid Port
RAR_MGID_NOT_INUSE	-106	MGID not used
RAR_INVALID_PARAMETER	-107	Invalid Parameter
RAR_RECORD_NOT_FOUND	-108	Record Not Found
RAR_WRITE_FAILED	-109	The writing of a Record has failed
RAR_ARP_NOT_FOUND	-110	The ARP has not been found
RAR_ARP_NOT_ROUTER	-111	The ARP is not corresponding to a Router
RAR_NON_ZERO_REFERENCE_COUNT	-112	
RAR_TOO_MANY_EQUAL_COST_PATHS	-113	

(Q00416517)

Passport 8672 ATM/ATMM module

- Although you can configure higher VPI numbers than those supported PVCs specified below (without a warning or error message displaying), these higher numbers do not function properly.

Interface	VPI Bits	Available PVCs
OC12	1	1.3323 and below
OC12	2	3.1259 and below
OC12	3	7.251 and below
OC12	4-8	all available
OC3	1	1.251 and below
OC3	2-6	all available
DS3	1	0.2047 and below
DS3	2	1.1023 and below
DS3	3	3.511 and below
DS3	4	7.255 and below
DS3	5	15.127 and below
DS3	6	31.63 and below
DS3	7	63.31 and below

  (Q00536665)

- Nortel Networks strongly recommends that you do not hot swap any other module-type during an insertion/de-insertion of an ATM module, and that you wait at least 30 seconds (corresponding to the ATM initialization boot time) before making any change in the hardware configuration of your chassis. (Q00483414)
- If a DS3 ATM MDA is not seated properly on the ATM module baseboard, DS3 port status, port administrative status and port LED status may appear in an “up” states, however, the PVCs may remain in a down state.

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

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

b. Create a VLAN under this STG group.

c. Add ATM ports to this STG and VLAN.

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

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

f. Create an ELAN by executing the CLI command `config atm slot#/port# pvc 1483 bridged create vlan# 0.1`.

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

(Q00539342)

- When you soft reset your switch, ATM I/O modules does not properly drop its link during the booting state. (Q00499717)
- By default, on STG ports, change detection is enabled on all ports. You are unable to disable this parameter on DS3 ports. (Q00526054)
- The CLI incorrectly allows you to assign a traffic filter on a DS3 port, even though ATM does not support DiffServ. (Q00526070)
- When the `InArpsendinterval` variable is configured, requests are sent out the port at a frequency double the configured value. (Q00495092)
- Links on switches connected to an 8672 ATM/ATMM module will continue to receive a signal from the module even when it is administratively disabled through the CLI or Device Manager. The 8672 ATM/ATMM module LED will display amber (as it should when disabled). However, the LED for the port on the ATM MDA will remain green as if the module were still enabled. (Q00471085-01)
- If you have the F5-OAM Request feature enabled, and you recycle the chassis (power on/power off), intermittently, the LOOPBACK REPLY SENT field of the `show ports info atm f5` CLI command output will not be updated. A chassis `reset` will not restore this information.

  To workaround this issue, perform another chassis recycle procedure. Note, this behavior has no effect on the behavior of F5-OAM Loopback request/reply mechanism. (Q00432989)

Passport 8683POS module

When a POS port is administratively disabled and then administratively enabled, STP is disabled or enabled according to the BCP state. So, if BCP is enabled and STP is disabled, STP will become enabled because BCP was enabled. In this case, you will need to manually disable STP. (Q00281408)

Web Switching Module

- With firewall load balancing (FWLB) in a configuration containing four Web Switching Modules, persistence binding using Secure Socket layer session ID on service https does not function properly. This does not affect other persistence binding settings, for example, clientID/cookie settings and FWLB operations. (Q00535591)
- Setting a NULL password for a Web Switching Module username is not supported. If a NULL password is set for a username, the username will not be authenticated at the Web Switching Module maintenance port, though a connection to the Web Switching Module can be made through the Passport CLI using the command `wsm connect`. (Q00532908)
- The 8000 Series CLI command save `config` creates or updates the wsmtrunk.bin in flash if a Web Switching Module is present in Passport 8600 chassis. If the Web Switching Module is removed from the 8600 chassis and wsmtrunk.bin is present in the flash, the command `save config` updates the wsmtrunk.bin present in the flash. If you delete the wsmtrunk.bin file present in the flash and a Web Switching Module is inserted in Passport 8600 chassis, the Web Switching Module configurations for VLAN and MLT are reset to the factory default. For more information about the wsmtrunk.bin file, see *Installing the Web Switching Module for the 8000 Series Switch* (part number 314969-A). (Q00520252)
- If a Web Switching Module is present in a Passport 8600 chassis and MLTs are created dynamically for the Web Switching Module, these MLTs are not allowed to be set to SMLT. For both CLI and JDM operation, the MLT is verified before it is set to SMLT. In Device Manager, if a MLT is the Web Switching Module MLT, then the `mltType` is not allowed to be set to SMLT. (Q00227876)
- There error message `ERROR Task=WsmPreConfigTask wsmAddVlanToTrunk: Consistency check failed` is displayed if there is an inconsistency in the wsmtrunk.bin file and the Passport 8600 configuration file. In the Passport 8600, information for the assignment of VLANs to dynamic MLT connections for the Web Switching Module is

stored in wsmtrunk.bin file. If the operation for adding MLT to a VLAN during Web Switching Module initialization process fails, the above error message is displayed in Passport 8600 CLI. To correct this issue, the wsmtrunk.bin can be deleted and re-created using the CLI command `save config`. Note that the information stored in the wsmtrunk.bin file will be lost if the file is deleted and the Passport 8600/Web Switching Module is rebooted. (Q00497469)

- If a policy-based VLAN is configured on a Passport 8600 and Web Switching Module BFM ports are added into the Not_Allow member list in that VLAN, in the case where a Web Switching Module is relocated to a new slot in the Passport 8600 chassis, the BFM ports will not display in the Not_Allow member column after the Web Switching Module is rebooted. Functionality of the VLAN is not affected as these ports do not participate in the VLAN as active members. (Q00527151)
- When using four Web Switching Modules in one Passport 8600 chassis (8010) with a Firewall Load Balancing (FWLB) configuration, removing one of the firewall connections on the clean side may result in a display of incorrect information about the reference port in the Web Switching Module forwarding table. The displayed information is corrected in a short time period (usually within 5 minutes), and has no effect on the Web Switching Modules' FWLB operation. (Q00522296)
- A wsmtrunk.bin file is not portable from one Web Switching Module to another. A configuration saved in a wsmtrunk.bin file is bound with the Switch Mac Address of the Web Switching Module. If a Web Switching Module is replaced with a new Web Switching Module in the same slot, dynamic MLT configuration return to the default settings. See *Installing the Web Switching Module for the 8000 Series Switch*, (part number 314969-A) for the procedure to replace a WSM Module and restore your configuration. (Q00458795)
- When a Web Switching Module is reset using the `/wsm/wsmreset` CLI command, the last software version that the Web Switching Module used to reboot incorrectly displays while the Web Switching Module is in a booting state. (Q00469612)

10 GE LAN/WAN module

- In rare cases, after disabling and then reenabling a 10GE LAN module port (manual action, reboot, or link flap), the link cannot initialize or there may be a delay of a few seconds before the link does initialize. Bouncing the port through the CLI or using Device Manager resolves this issue. (Q00486214)
- FDB filter entries may be removed if the 10 GE LAN/WAN module is hot-swapped. If you have FDB filters and you need to hot-swap your 10 GE LAN/WAN module, power down the switch, swap the modules, and then power up the switch. (Q00532602)
- The STP standard (802.1D) does not specify any pathcost calculation for a 10 GE LAN/WAN interface. Nortel Networks recommends that you keep the value of the STG priority for a port to as low a value as possible (which should guarantee that this port is active after the STP calculation). While the default value is typically 128, it is recommended that you use a value equal to or less than 10. (Q00259692)

Note: Refer to *Using the 10 Gigabit Ethernet Modules: 8681XLR and 8681XLW* (part number 315893-A) for more information about concepts, limitations and considerations when configuring your 10 GE LAN/WAN module.

Layer 2 switching

Select a topic

General

- You can incorrectly create, modify, and delete access policies when you are logged into the CLI as a layer 2 user. (Q00338574)
- You can incorrectly assign or remove an IP address on a VLAN when you are logged into the CLI as a layer 2 user. This issue does not apply to assigning or removing IP addresses on a port. (Q00337907)

High availability (HA) mode

- RMON configurations are not synchronized in HA mode. (Q00535146)
- Brouter port configurations are not supported in HA mode. (Q00532910)
- Trace auto-enable parameters are not synced in HA mode. (Q00505814)
- No error message is displayed if you do not have matching software versions on the primary and secondary CPU and are in HA mode. (Q00248522)
- When you configure a CPU for HA-CPU in the absence of a standby or a slave CPU, you will *not* receive a warning message that indicates that the standby or slave CPU is not available. In addition, HA-CPU is not disabled automatically. (Q00246794)
- The robust value may incorrectly display in the `show ip igmp mrdisc-nei` CLI output on the receiving switch. The incorrect value is then copied to the standby CPU. This value is for informational purposes only and does not affect the operation of your switch. (Q00536682, Q00537245)
- When you remove your standby CPU with an older version of software code with HA-CPU enabled, and then install your CPU with Passport 8000 Series Switch Software Release 3.3 installed without HA-CPU enabled, HA-CPU will not be enabled during the synchronization process. Therefore, the standby CPU will remain in a disabled state and the master CPU will remain in the initialization state. (Q00469480, Q00283033)
- When a Passport 8600 chassis is configured with factory default settings, and then HA-CPU is enabled, the save-to-standby feature is also enabled. After disabling HA-CPU, and rebooting the switch, the savetostandby feature remains enabled. (Q00468677)

- When the HA-CPU flag is enabled, the `verify-config` flag is automatically set to `false`. This allows you to load a layer 3 configuration in HA-mode. If the flag was set to `true` (which is the default value) the switch would fail to load the configuration when it is booted. With release 3.3, HA (High Availability) has the ability to support some layer 3 configurations (static routes/ARP entries) and if the verify-config flag is set to `true`, loading of the configuration stops at the first error. (Q00108384)
- After a failover (HA enabled), wait until the message `syncing is complete` is displayed on the console prior to replacing a GBIC in a Passport 8608GB or Passport 8632TXE to avoid port types not being recognized. (Q00157375)
- After a failover (HA enabled), if the new master CPU does not complete table synchronization prior to another failover, the new master CPU will reboot. (Q00157504)

MLT/SMLT

This section describes MLT and SMLT behavior with specific protocols.

General

- On a Passport 8600 switch, a port added to an MLT does not automatically assume the DiffServ properties of the MLT. You must manually configure the correct DiffServ settings for the port. (Q00428992) (Passport 8600)
- On a Passport 8600 Series switch, the **`monitor mlt stats interface`** CLI command displays an invalid value for utilization percentage. (Q00043890) (Passport 8600)

SMLT and Spanning Tree

Spanning Tree is not supported on SMLT/IST ports. (Q00303475)

SMLT and VRRP

This section describes SMLT and VRRP behavior with specific protocols.

- The VRRP virtual IP address and the VLAN IP address cannot be the same when backup-master is enabled.

VLANs

- Nortel Networks recommends that you not save a configuration that includes an IP protocol-based VLAN without an assigned port. If you have another IP protocol-based VLAN configured, and that second VLAN has ports, the first IP Protocol-based VLAN, if it has a lower ID, will have the ports assigned after the reboot. You should remove the IP protocol-based VLAN from the configuration before saving the configuration file. (Q00494125-01)
- The IN and OUT FLOWCNTRL port statistics are no longer displayed under show port stat interface main for Passport 8608 modules. This statistic is not accurate for these modules and has been suppressed from the CLI output. The FLOWCNTRL statistics can also be seen in Device Manager under Graph > Port, but the numbers are inaccurate for the 8608 modules. (Q00470266-02)

STP

- Disabling STP at the port level is not dynamic. The BDPUs are still received and processed as if the port has STP enabled, even though the port state shows that STP is disabled. The change takes effect only after a state transition occurs on the port whereby the BDPU received on the port is not processed. (Q00323156)

Filters and bandwidth control

This section describes the known filters and bandwidth issues and limitations that exist in this release, and includes the following topics:

Filters

Table 5 describes considerations for IP filters.

Table 5 IP filter considerations

Filter type	Number
Filter IDs (any type)	1..3071 (including global and source/dest filters)
Global filters	8 per RAPTARU (group of 8 10/100 ports or 1 Gig port)
Filters set IDs (any type)	128
Global filters set IDs	1..100 (range)
Source/Dest Filter set IDs	300..1000 (range)
Number of filters per set	32 (maximum)
Number of sets per port (any type)	32 (maximum)
Number of filters per port	1024 (maximum) (32 * 32)

- You must delete all multimedia streams prior to deleting the associated device. (Q00535647)
- Zero-mask source-type IP filters are not effective for incoming source IP addresses for which an IP route or ARP or a matching non-zero-mask subnet IP source/destination filter does not exist (Q00528807)

- If a destination filter is set to drop a local bridged traffic, the ingress traffic sent to an end device will not be dropped (you have to use global filters to realize this function), but the traffic sent to IP interface of the VLAN (CPU) will be dropped. But if the traffic is a “traceroute” packet sent to the CPU, it won't be dropped (the CPU replies to the originator with an ICMP TTL expired message). (Q00464627)
- The maximum number of multimedia filters you can configure is one multimedia filter enabled per port and two multimedia filters enabled per system. If you attempt to configure more than the specified limit, an error message will display. (Q00501427)
- Modification of DSCP values using global filters if the destination address is 0.0.0.0 is not supported on E-modules. (Q00427253, Q00509096)
- A protocol port number is not used as a match criterion if an IP address is specified for a Multimedia Device (Q00477434)
- When viewing IP traffic filter statistics, the rcFilterInOctets, rcIpFilterInPackets, and rcIpFilterRateLimitDiscardPacketsCounter may not be consistent between the MIB variable and the CLI. Both sources are correct. The difference is due to the MIB variable using a 32-bit counter and the CLI using a 64-bit counter. Device Manager does not have access to the IP traffic filter statistics. (Q00247020)
- On a Passport 8600 switch, to create a static MAC filter, if the MAC address to be used in the filter was learned dynamically, you must flush the forwarding database (fdb) first. (Q00024659)
- On a Passport 8600 switch, an fdb-filter may be displayed for VLANs which it is not assigned to. This issue is with the display only and does not affect functionality. (Q00041001)
- On a Passport 8600 switch, you must apply filters individually to each port in an MLT. (Q00043648, Q00045276-01)
- On a Passport 8600 switch, when you use the **`show vlan info all`** CLI command to display fdb-filters, each filter is displayed a number of times equal to the total number of VLANs on the switch. (Q00043780)

QoS

- The `translate-dscp` flag does not work for profiles. If applied to a filter, the profile in and out DSCP settings will override the filter settings even if translate-dscp is disabled. (Q00539793)
- A value of `000000` in InProfile or OutProfile changes the DSCP field of the packets. (Q00085495)
- On a Passport 8600 switch, when you route without filters, the bits in the DiffServMatchDscpReserved field are not preserved unless traffic is forwarded through a filter. (Q00024228)

DiffServ

- On a Passport 8600 switch, under normal conditions, global filters can modify the DSCP value if you have enabled the `dscp` parameter for the **`config ip traffic-filter filter modify`** CLI command or the `DiffServModifyDscpEnable` parameter on the IP Routing > Filter > Insert tab in Device Manager. The port QoS, VLAN QoS, or MAC QoS settings should also modify the DSCP value if one of these QoS levels is greater than the DSCP value specified by the filter (QoS level-to-DSCP mapping table). In this release, the port QoS and VLAN QoS do not override the DSCP value specified in the filter. To override the filter DSCP value, you must use the MAC QoS level. In Device Manager, set the QoS level for a MAC address using the Forwarding tab (reached by choosing VLAN > VLANs > Bridging). Enter a value in the QosLevel field. (Q00040984) (Passport 8600)
- User-defined DiffServ settings are not retained when you hotswap an I/O module.To reinstate your user-defined settings, either reconfigure the DiffServ settings for that I/O module or reboot the switch. (Q00421191)

Rate limiting

- On a Passport 8000 Series switch, broadcast traffic is rate limited at the multicast value if no value is configured for broadcast. (Q00042995)

Unknown MAC discard

- On a Passport 8600 switch, enabling the Unknown MAC Discard feature on a port does not flush existing MAC addresses from the FDB table. You must flush the table manually. (Q00039672)

IP unicast

Select a topic:

General

- If you are using VLAN 4093 and you have an assigned IP address, the IP address will work, but it will not display in the IP routing table. (Q00525239)
- When you configure more than 256 VLANs with an assigned IP address in a SMLT configuration with the last VLAN configured with VRRP, and the switch with the highest VRRP priority receives an ARP from the sender with the same IP address, the following message will appear on the console: `ERROR Task=tMainTask portGetPortNum: invalid physical port`. You must use a separate dedicated IP address for VRRP.(Q00487614)

- Interrupting a RSH session (^CTRL-C) may result in CPU lockup. An established telnet session will remain active if no CLI commands are executed. Any attempt to create a telnet/rsh/ssh session will fail. (Q00426337)

IP policies

Creating and editing a route policy

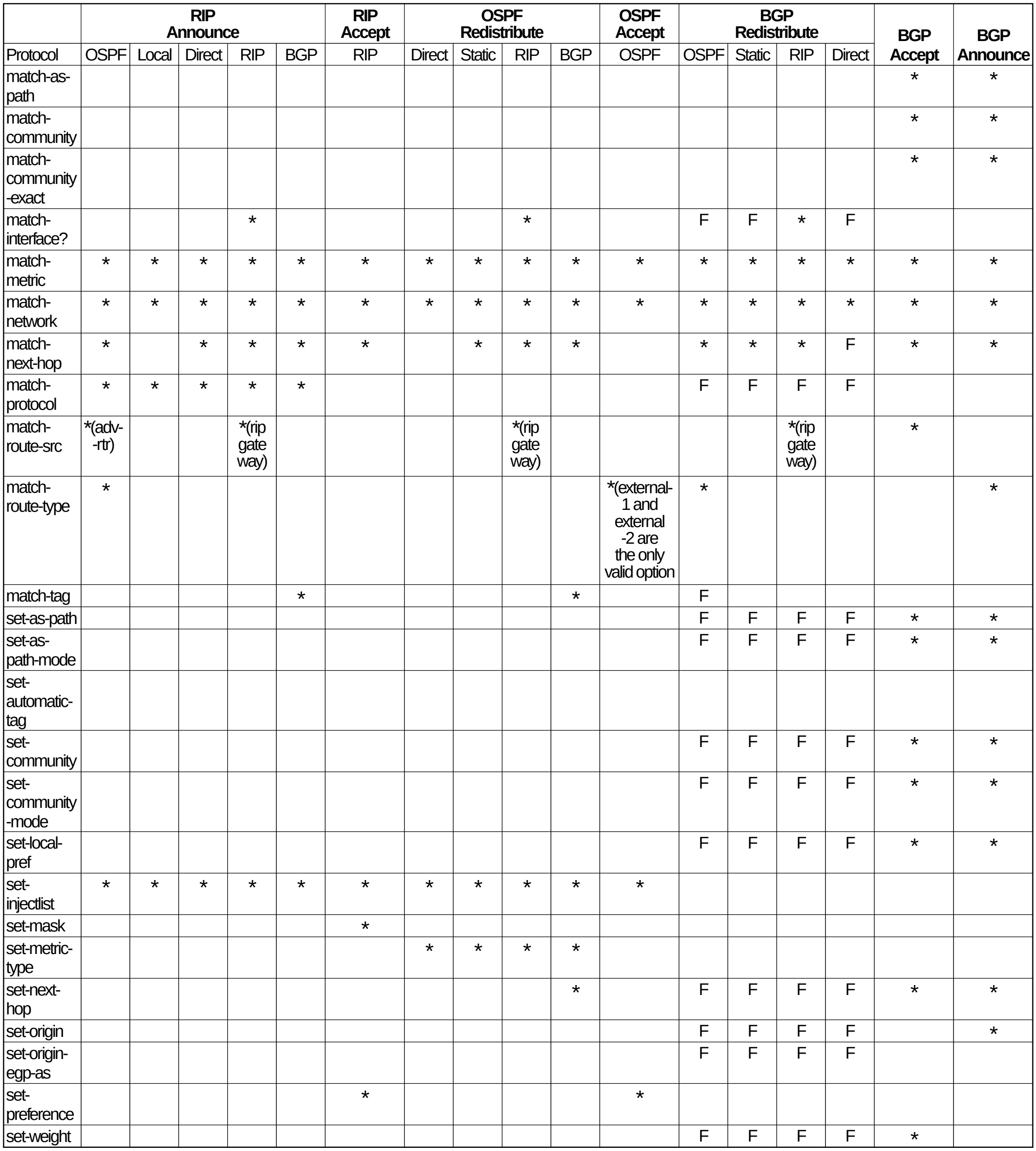
When you create a route-policy using Device Manager, you have the option of selecting the ID number. When you create a route-policy using the CLI, the route-policy ID is automatically generated.

You can configure route policies to be used for In, Out, and Redistribute purposes by all protocols.

Figure 20 reflects the accept and announce policies for RIP, OSPF, and BGP protocols. It also reflects which matching criteria are applicable for a certain routing policy.

For more information about IP routing policies, see *Configuring IP Routing Operations* (part number 314720-A).

Figure 20 Protocol Route Policy table



	RIP Announce					RIP Accept	OSPF Redistribute				OSPF Accept	BGP Redistribute				BGP Accept	BGP Announce
Protocol	OSPF	Local	Direct	RIP	BGP	RIP	Direct	Static	RIP	BGP	OSPF	OSPF	Static	RIP	Direct		
match-as-path																*	*
match-community																*	*
match-community-exact																*	*
match-interface?				*					*			F	F	*	F		
match-metric	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
match-network	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
match-next-hop	*		*	*	*	*		*	*	*		*	*	*	F	*	*
match-protocol	*	*	*	*	*							F	F	F	F		
match-route-src	*(adv-rtr)			*(rip gateway)					*(rip gateway)					*(rip gateway)		*	
match-route-type	*										*(external-1 and external-2 are the only valid option	*					*
match-tag					*					*		F					
set-as-path												F	F	F	F	*	*
set-as-path-mode												F	F	F	F	*	*
set-automatic-tag																	
set-community												F	F	F	F	*	*
set-community-mode												F	F	F	F	*	*
set-local-pref												F	F	F	F	*	*
set-injectlist	*	*	*	*	*	*	*	*	*	*	*						
set-mask						*											
set-metric-type							*	*	*	*							
set-next-hop										*		F	F	F	F	*	*
set-origin												F	F	F	F		*
set-origin-egp-as												F	F	F	F		
set-preference						*					*						
set-weight												F	F	F	F	*	

F = Support in a future release * = currently supported

10762EA

- Immediately after a conversion from Passport software release 3.1, the IP policy prefix index is shown as 1001, 1002, 2001, 2002, etc.

  To work around this issue, reboot with a converted Passport 3.2 configuration and the policy prefix index returns to 1,2,3, etc. (Q00093453)

BGP

Caution: Care should be taken when executing the `admin state enable | disable` CLI command. As there is no disable/enable commands under the `config ip bgp neighbor` tree, if you execute the `admin state enable | disable` command at this point, you will access local BGP disable and consequently, disable BGP. Instead, use the `admin-state enable or disable` command. (Q00137838)

- In this release, the invalid router ID statistics are not incremented correctly for BGP neighbor statistics in Device Manager and the CLI. (Q00507638)
- Even though Device Manager and the CLI contain options to enable the automatic tagging feature in BGP, this feature is not supported in this release. Enabling this tag has no effect. (Q00502170)
- Device Manager does not properly display the cluster IDs for BGP routes. You can view BGP route cluster IDs using the CLI command `show ip bgp route`. (Q00525859)
- Whenever a route policy is applied to a BGP peer, a message is incorrectly prompted on the console to bounce BGP for route policy to take effect. This message should be prompted while working in a telnet session. (Q00516654, Q00510171)
- The BGP command `config ip bgp redistribute direct` is not in compliance with the CLI nomenclature and should be `config ip bgp redistribute` **`local`**. This will be fixed in a future release. (Q00528995)
- To avoid route rejections from a peer, before performing any route-policy configuration within BGP, be sure to always enable the protocol prior to making configuration changes. This does not apply to global route policy configurations which can be configured at anytime. (Q00533820)
- When changing your route reflector configuration in BGP using the CLI command `config ip bgp route-reflector`, it is necessary to next disable and then reenable BGP for the changes to take effect. (Q00532889))

- Do not use Device Manager to enable policies if BGP policies are configured. BGP into OSPF redistribution is supported only from the command line interface, not Device Manager. For example, use the CLI command `config ip ospf redistribute bgp apply`. (Q00531897)
- Replacing static routes with the set-inject-list CLI command, does not work properly with BGP. To work around this issue:

  a To summarize the routes that are locally originated and are being redistributed to BGP, for example, direct and static, enter the CLI command `config ip bgp auto-summary enable`.

  b Apply your changes using the CLI command `config ip bgp red static apply`.

  (Q00522821)
- The Web Management interface does not correctly display BGP route preferences (Layer3 > IP> Route Preference). (Q00517857)
- A route while being injected by network command can get metric information from redistribute if it is being injected by network and redistribute both. (Q00526957)
- BGP allows any name to be used as a peer group name. This can generate confusion when using names that are also CLI command. Nortel Networks recommends that you avoid using CLI commands as peer group names. (Q00487979)
- When disabling IP forwarding, BGP will maintain its neighbors and also exchange route information. Be sure to disable BGP when disabling IP forwarding to prevent black holes. (Q00518921)
- An invalid error message is displayed when you delete a nonexistent route policy. (Q00504510)
- Aggregation should not occur when routes have different MEDs or Next Hops. (Q00252393)
- Device Manager and the CLI incorrectly allow you to enter a value of 0 in the `local-as` field when configuring BGP. The correct range of values for this parameter are from 1 to 65535. Entering a value of 0 will prevent you from being able to globally enable BGP. (Q00471894)
- Arranging the path attributes in ascending order, which is an optional optimization, is not supported in this release.(Q00176871)

DHCP/UDP

You can configure up to 16 UDP forwarding list IDs. Device Manager incorrectly displays the range of allowed IDs as 1...100 but the CLI displays the correct range of allowed IDs as 1...1000. (Q00322145)

OSPF

- In a mixed vendor environment, you may need to set the 8600s OSPF default `RtrDeadInterval` from the factory default to 40 seconds. (Q00138349-01)
- A condition may occur in which when a large number of VLANs are configured with OSPF, the buffer may temporarily exceed buffer space. In this case, the following error message will display: `IP ERROR ipPktOut: can’t copy frame buffer!`. To work around this issue, reduce the number of broadcast OSPF interfaces so that there is least one broadcast OSPF interface per area, with the total not exceeding 96. The remainder can be used as passive OSPF interfaces. (Q00521156)
- If you delete an OSPF interface configured for simple authentication, and then reconfigure the interface, the authentication values from the original interface authentication-key are retained along with non-specified characters. (Q00422614)
- After you delete an OSPF interface, the OSPF interface configuration remains in the memory. This issue occurs even if you save your configuration after deleting the OSPF interface and resetting the switch. However, functionality is not affected as the OSPF interfaces are recreated in an administratively disabled state. They will remain disabled unless you manually change their state. In addition, if you delete the IP address corresponding to the deleted OSPF interface, the remaining stored information regarding the OSPF interface is deleted. (Q00419072)
- For clarification, when reading OSPF statistics, the **`show ip ospf area`** CLI command displays the number of intra area SPF runs per area, and the **`show ip ospf stats`** CLI command displays the total number of SPF runs including intra, inter and AS external SPF runs. (Q00419224)
- On a Passport 8600 module, virtual link information is not saved if the auto-virtual feature is enabled. If you want to save your virtual link configuration, first disable the auto-virtual feature and then configure the virtual link information statically. (Q00072039, Q00072038)

- On a Passport 8600 switch, OSPF statistics are not available on a port or ports that belong to a VLAN. When graphing one port, the OSPF tab in Device Manager is unavailable. When graphing a brouter port or multiple ports, the OSPF tab is available. (Q00041794).

RIP

- RIP timeout values are not displayed in the `sho ip rip info` CLI command display output. This information can be retrieved in the display output of the **`config ip rip info`** CLI command. (Q00469135)
- When configuring a RIP announce policy, the match protocol field can have the values any or local, ospf, rip, static, or a combination of these values. When you apply the policy a search is made for a match of the configured field with the protocol through which the route is learned. This field is used only for RIP announce policies, and otherwise ignored. (Q00510250-02)

VRRP

- Ping packet larger than 1472 bytes will fail to reach a VRRP IP address. (Q00498626-02)
- The VRRP transition log message displays the incorrect VLAN ID for VRRP configured on a VLAN. However, for VRRP on brouter ports, the VRRP transition log message displays the correct slot/port value. (Q00522473)
- When SNMP trap receivers are created and the IP address is not reachable, the switch sends the cppCheckVrrpMaster to the CPU. This packet will continue to resend to the CPU until the trap receiver address is removed. (Q00297197-01)
- VRRP transition may occur when any I/O module is removed from the chassis. This transition is seen only in the log file, showing the VRRP transition from backup to master and then again to backup. This VRRP transition should not cause any data loss. (Q00519363)
- VRRP incorrectly allows you to create multiple VRRP interfaces sharing the same VRID. (Q00510996)
- VRRP hotstandby (with WebOS software version 10.0.27.0) is not supported in this release. (Q00249554)
- The VRRP virtual IP address and the VLAN IP address cannot be the same when backup-master is enabled.
- The VRRP preempt hold-down timer feature is not supported in this release. (Q00287299)

IP multicast

Select a topic:

General

- If you have two Passport 8600 switches connected through an MLT, with IP multicast flowing between both switches, you must enable/disable multicast on both switches (IGMP or DVMRP). If you do not, multicast traffic loops may occur. (Q00146547)
- An interface in a prune pending state will send join messages to the upstream source. Therefore, upstream routers in the same VLAN will take longer to prune an (S,G) entry in a forwarding state. The time to prune will vary with the number of routers in the spanning VLAN. (Q00154810)
- When using the Multicast Router Discovery protocol on a Passport 8100/8600 connected to other devices implementing this protocol, there could be interoperability issues given that the Passport 8600 implementation sends multicast router discovery messages to the 224.0.0.2 address (all routers address) based on the fact that early drafts did not define this destination address. Newer drafts (http://ietf.org/internet-drafts/draft-ietf-idmr-igmp-mrdisc-08.txt), define the destination address as the all hosts address of 224.0.0.1 and devices implementing Multicast Router Discovery protocol based on the latest drafts will not interoperate with the Passport 8100/8600, unless they are able to send and receive Multicast Router Discovery messages using the 224.0.0.2 address. (Q00309216)
- In this release, the flush group feature is supported only for IGMP snooping. (Q00428284)
- In this release, the flush sender feature is supported only for IGMP snooping. (Q00254719, Q00254720, Q00391515)

- Multicast routing with PIM and DVMRP enabled is not supported on the edge switch of a Triangle SMLT configuration. In addition, IP multicast routing is not supported on SMLT square and cross configurations. See *Network Design Guidelines & Implementation Notes* (part number 313197-B) for a detailed discussion on these subjects. (Q00080536) (Passport 8600)
- However, IGMP Snooping is supported and queries for a given VLAN must be placed on one switch only. (Q00072438, Q00075866) (Passport 8600)
- On a Passport 8000 Series switch, IP multicast traffic is not distributed across MLT links; however, failover between links is supported. (Q00020899, (Q00091731) (Passport 8100)
- On a Passport 8600 switch, you must configure the IGMP Query Interval with a value higher than 5 to prevent the switch from dropping some multicast traffic. (Q00021069, Q00025086)
- In a configuration containing non-E modules, when a Passport 8600 switch receives an IP multicast packet with a TTL of 1, the packet is sent to the CPU and dropped. To prevent this problem, make sure the originating application uses a hop count large enough to enable the multicast streams to travel the network and reach all destinations without reaching a TTL of 1.

  When two Passport 8600 switches are involved, you can also prevent the switch from unnecessarily receiving and dropping egressing multicast traffic with a TTL of 1 by setting the TTL threshold on the neighboring switches. In Device Manager, choose IP Routing > Multicast > Interface and set the TTL to 2 so the switch will drop all packets with a TTL less than 2. After you change the TTL value, disable DVMRP and reenable it again to activate the change. (Q00022968, Q00023583)

IGMP

- In the Web management interface, in the IGMP sender table, the `TPort` field doesn't display the active ports. (Q00519999)
- The Web management interface does not display the correct time in the IGMP Cache table. (Q00520033)
- In the Web management interface, the IGMP group table may not display all active IGMP groups. (Q00519947)
- The CLI displays the incorrect count for total igmp static receivers and unique groups if you interrupt the display. However, if you allow the display to continue until finished processing, the correct counts are displayed. (Q00522292)

- In the Web management interface, although IGMPv3 is not supported in this release, some CLI commands may display for this feature. (Q00520033)
- On a Passport 8600 Series switch, using a static querier port or changing a querier port in IGMP Snoop when the number of multicast streams is high, may cause occasional multicast traffic delays or interruptions. It may result in multicast data loss for a short period of time. (Q00041423) (Passport 8600)
- On a Passport 8000 Series switch, IGMP Snoop static entries (such as static group receivers and static group not allowed to join ports) configured for a port are not removed when the module containing that port is removed from the chassis. These static entries are still displayed as valid. This issue does not affect the operation of the switch or the configuration file when saved. (Q00042216)

DVMRP

- The interface in the mroute route table always displays the interface connected to the upstream, regardless of whether it is a bridged or a routed session. (Q00421696)
- When you first globally enable DVMRP on the switch, a 30 second timer routine initializes the DVMRP protocol (e.g., static source group table). During this initialization period, the CLI output for the command `show ip dvmrp info` will display global DVMRP settings as disabled, and the `config ip dvmrp info` output will display “enabled.” This is a known behavior of global DVMRP initialization. (Q00209708)
- Changing the subnet mask configuration for DVMRP interfaces may cause network instability if the interface has DVMRP enabled. In order to avoid this issue, disable DVMRP on both sides of the interface before making subnet mask configuration changes. DVMRP can be reenabled after the change is performed. (Q00078084, Q00087301, Q00087305)

PIM

- The following PIM CLI commands are not supported in this release:

  ```
  — config vlan <vid> ip pim candbsr
                 enable preference <value>
                 disable
                 info
  — config ether <slot/port> ip pim candbsr
                 enable preference <value>
                 disable
                  info
  ```

  (Q00527810)

- Static RP cannot be enabled or configured on a switch in a mixed mode of Candidate RP and Static RP switches, if a switch needs to learn a RP-set and has a unicast route to reach the BSR through this switch.

  Example configuration 1

  ```
  Sw3 (BSR) - Sw4 (Candidate RP)
  |
  |
  Sw2 (cannot be configured as static RP)
  |
  |
    Sw1 (PIM enabled, needs to learn RP-set through Sw2)
  ```

  Example configuration 2

  ```
  Sw3 (BSR) - Sw4 (Candidate RP)
  | /
  | Sw5


  | Sw5
   / (cannot be configured as a static RP)
   |   Sw6
   |  /
  ```

- `Sw1` (PIM enabled, does have a route to BSR through Sw5, but shortest path route to BSR is through Sw2). (Q00474113)
- To avoid multicast data loss, the MBR needs to be the last switch to be activated in a multicast domain that contain both PIM and DVMRP configurations. For any reason, if the DVMRP interface to MBR is reset, re-activate the MBR *after* DVMRP becomes stable. (Q00529109)
- You cannot configure a static RP-only switch with a local RP when other switches in the domain are configured with candidate RPs. (Q00474120)
- Additional (S,G) join ports may occur if there is an extended VLAN with multiple ports. While only one port receives the (S,G) join, the other ports receive the (*, G) Join. Traffic is then forwarded to the extra join ports but is discarded at downstream switches. (Q00093461)
- On a VLAN spanning more than 2 switches, `SPT path joins` are received on one port of the spanning VLAN. The messages on the VLAN port on which RP-to-source prune messages are received will not be properly pruned and will stay in a prune pending state (because of overriding joins received on the port in the SPT path). (Q00421566)
- Non-DR switch receives double traffic when a receiver is connected to a non-DR switch and the unicast route (shortest path) towards the source is not through a DR switch. Both non-DR and DR switches create (*,G) and (S,G) records. (Q00086744, Q00283015)
- Device Manager does not have a tab that displays the active PIM RPs. For diagnostic purposes, you may need to know which active IGMP group is mapped to each active RP.

  This information is available by executing the **`show ip pim active-rp`** CLI command. (Q00084832) (Passport 8600)
- Multicast streams do not load share across ECMP paths. Even though you may have enabled multiple paths and multiple receivers, PIM selects only one path from the source to the receiver. (Q00018858)
- When the non-RP source switch is the same as the receiver switch, while the RPT and SPT paths are different, record leaks occur on switches along the RPT between the source and the RP. This condition diminishes when the traffic stops and receivers are no longer present.
  (Q00160428, Q00322236, and Q00250460)

MBR

- In a network configured with a MBR connecting a PIM domain to a DVMRP domain, when the OSPF metric (cost) on the path changes dynamically in the PIM domain, the new metric is not updated by the MBR in the DVMRP domain. (Q00124030)
- With MBR enabled, if you disable PIM and enable DVMRP, and then disable DVMRP and reenable PIM, PIM neighbors are not processed correctly. To work around this issue, whenever you reconfigure a PIM interface to a DVMRP interface, make sure the MBR flag is set to disabled (unchecked). After making your configuration changes, re-enable MBR. (Q00101793)
- Nortel Network recommends the configuration of MBR to comply with the following guideline:
  - Connect PIM and DVMRP domains using one link or MLT.
  - Use MBR to connect one PIM domain to one DVMRP domain, without any extended VLANs.
  - Configure the RP for the PIM domain on the MBR switch.
  - Additionally, note that if the DVMRP interface is dropped or goes down, MBR may need to be disabled and then re-enabled after DVMRP is back up and stabilized.

  This configuration is simple and easy to troubleshoot.

  (Q00500409, Q00529109)
- Nortel Networks does not support a configuration in which receivers are directly connected to the MBR. (Q00526230)
- The DVMRP VLAN on the MBR cannot be extended to more than one switch in the DVMRP domain. (Q00129285, Q00138346)
- Multicast traffic cannot flow from a DVMRP domain to another DVMRP domain if they are connected through a MBR. (Q00155058)
- When connecting PIM and DVMRP domains with MBR, care should be taken so that the cost for IP routes learned for PIM does not exceed 31 in order to route properly in the DVMRP domain. (Q00155066)
- In a redundant MBR configuration, the VLANs connecting the DVMRP domain to the PIM domain cannot span the two MBR switches. (Q00094681, Q00094710, Q00103589)

IPX routing

- You cannot configure IPX RIP timers globally using Device Manager (IPX Routing > IPX). To configure global IPX RIP timers, use the CLI command **`config ipx rip`**. (Q00432141)
- In networks where OSPF, RIPv2, VRRP, SMLT, and IPX are running, IPX traffic receives the lowest priority. As a result, IPX control traffic, such as IPX SAPs, may get dropped prior to IP traffic under heavy traffic conditions. (Q00429241)
- On a Passport 8600 switch, when there are more than 2000 entries for IPX routes, IPX services, or IPX destination services, CPU utilization goes up to 100% when Device Manager is used to view this information. Network connectivity is not affected while you are viewing this information. (Q00033565)
- When you remove an IPX VLAN from a MLT, the IPX route table entries are not updated for a maximum of 60 seconds or until you flush the routes. (Q00023971, Q00023976)
- The Passport 8600 switch does not answer an IPX ping to its own interfaces. You can determine the status of the interface using the **`show ipx stats <IPX-network-number>`** CLI command. (Q00022802)
- On a Passport 8600 switch, the minimum setting for the max-route value is 1500. (Q00024074)

Related publications

For more information about the Passport 8000 Series switch, refer to the following publications:

Important information and reference

- *Important information about your hardware and supporting software release compatibility* (part number 314937-B)
- *Read Me for Security* (part number 314997-A)
- *Network Design Guidelines & Implementation Notes* (part number 313197-B)

Hardware books

- *Installing and Maintaining the 8000 Series Chassis and Components* (part number 316314-A)

Hardware upgrade and replacement manuals

- *Installing 8600 Switch Modules* (part number 312749-C)
- *Installing 8100 Switch Modules* (part number 312750-B)
- *Installing the Breaker Interface Panel for the 8010co Chassis* (part number 312755-D)
- *Installing a DC Power Supply in an 8000 Series Switch* (part number 313070-C)
- *Installing a AC Power Supply in an 8000 Series Switch* (part number 312751-C)
- *Installing a Fan Tray in an 8000 Series Switch* (part number 312752-B)
- *Installing Gigabit Interface Converters (GBICs)* (part number 312865-A)
- *Replacing an Air Filter in the 8010co Chassis* (part number 313592-C)
- *Installing Media Dependent Adapters (MDAs)* (part number 302403-G)
- *Installing CWDM Gigabit Interface Converters (GBICs)* (part number 212256-B)
- *Installing Media Dependent Adapters for the 8672ATME and 8672ATMM Modules* (part number 313071-B)

- *Installing Media Dependent Adapters for the 8683POSM Module* (part number 313072-B)
- *Installing the Web Switch Module for the 8000 Series Switch* (part number 314969-A)

Module using guides

- *Using the 8672ATME and 8672ATMM Modules* (part number 209195-C)
- *Using the 8683POSM Module* (part number 209564-B)
- *Using the 10 Gigabit Ethernet Modules: 8681XLR and 8681XLW* (part number 315893-A)

Software books

- *Platform and System Management* (part number 315545-A)
- *Configuring and Managing Security* (part number 314724-A)
- *Getting Started with the Management Software* (part number 313189-B)
- *Configuring IP Routing Operations* (part number 314720-A)
- *Configuring IP Multicast Routing Protocols* (part number 314719-A)
- *Configuring BGP Services* (part number 314721-A)
- *Configuring IPX Routing Operations* (part number 314722-A)
- *Configuring Network Management and Diagnostics* (part number 314723-A)
- *Configuring Layer 2 Operations: VLANs, Spanning Tree, Multilink Trunking (part number 314725-A)*
- *Configuring the Web Switch Module with Device Manager* (part number 314995-A)
- *(Alteon) WebOS Switch Software 10.0 Application Guide* (part number 212777-A)
- *(Alteon) WebOS Switch Software 10.0 Command Reference* (part number part number 212778-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 one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

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://www130.nortelnetworks.com/cgi-bin/eserv/common/essContactUs.jsp URL.

Appendix A: Tap and OctaPID assignment

The switch fabric in the 8600 modules has nine switching taps, one for each of the eight I/O slots (1 to 4 and 7 to 10) and one for the CPU slots (5 and 6). Taps 0-7 map to the eight I/O slots and can support up to eight OctaPIDs. Each OctaPID can support up to eight ports.

In the Passport 8600 module, a physical port number is 10 bits long and has the following format:

```
9   6 5   3 2   0
+-----+----+----+
|     |    |    |
+-----+----+----+
```

bits 9–6: Tap number (0–15)

bits 5–3: OctaPID number (0–7)

bits 2-0: MAC port number (0-7)

The Tap number bits and the OctaPID number bits combined (bits 9–3) are usually referred to as the OctaPID ID.

Table 1 lists the module types that are currently available, along with the associated OctaPID ID assignments for each module.

Table 1 Available module types and OctapPID ID assignments

Module type	Port type	OctaPID ID assignment
8608GBE and 8608GBM Modules	1000BASE-SX (GBIC)	Table 2 next
	1000BASE-LX (GBIC)	
	1000BASE-ZX (GBIC)	
	1000BASE-XD (GBIC)	
	1000BASE-TX (GBIC)	
8608GTE and 8608GTM Modules	1000BASE-T	Table 2 next
8608SXE Module	1000BASE-SX	Table 2 next
8616SXE Module	1000BASE-SX	Table 3 on page 109

Table 1 Available module types and OctapPID ID assignments (continued)

Module type	Port type	OctaPID ID assignment
8624FXE Module	100BASE-FX	Table 4 on page 109
8632TXE and 8632TXM Modules	10BASE-T/100BASE-TX	Table 5 on page 109
	1000BASE-SX (GBIC)	
	1000BASE-LX (GBIC)	
	1000BASE-ZX (GBIC)	
	1000BASE-XD (GBIC)	
	1000BASE- TX (GBIC)	
8648TXE and 8648TXM Modules	10/100 Mb/s	Table 6 on page 110
8672ATME and 8672ATMM Modules	OC-3c MDA	Table 7 on page 110
	OC-12c MDA	
	DS3	
8681XLR Module	10GBASE-LR	Table 8 on page 111
8681XLW Module	10GBASE-LW	Table 9 on page 111
8683POSM Module	OC-3c MDA	Table 10 on page 112
	OC-12c MDA	

Table 2 describes the OctaPID ID and port assignments for the 8608GBE, Passport 8608GBM, 8608GTE, 8608GTM, and 8608SXE modules.

Table 2 8608GBE/8608GBM/8608GTE/8608GTM, and 8608SXE modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	Port 2
OctaPID ID: 2	Port 3
OctaPID ID: 3	Port 4
OctaPID ID: 4	Port 5
OctaPID ID: 5	Port 6
OctaPID ID: 6	Port 7
OctaPID ID: 7	Port 8

Table 3 describes the OctaPID ID and port assignments for the 8616SXE Module.

Table 3 8616SXE module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 and 2
OctaPID ID: 1	Ports 3 and 4
OctaPID ID: 2	Ports 5 and 6
OctaPID ID: 3	Ports 7 and 8
OctaPID ID: 4	Ports 9 and 10
OctaPID ID: 5	Ports 11 and 12
OctaPID ID: 6	Ports 13 and 14
OctaPID ID: 7	Ports 15 and 16

Table 4 describes the OctaPID ID and port assignments for the 8624FXE Module.

Table 4 8624FXE module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24

Table 5 describes the OctaPID ID and port assignments for the 8632TXE and 8632TXM Modules.

Table 5 8632TXE and 8632TZM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24
-	-
-	-
OctaPID ID: 5	Ports 25 through 32

Table 5 8632TXE and 8632TZM modules (continued)

OctaPID ID assignment	**Port assignment**
OctaPID ID: 6	Port 33 (GBIC port)
OctaPID ID: 7	Port 34 (GBIC port)

Table 6 describes the OctaPID ID and port assignments for the 8648TXE and 8648TXM Modules.

Table 6 8648TXE and 8648TXM modules

OctaPID ID assignment	**Port assignment**
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24
-	-
-	-
OctaPID ID: 5	Ports 25 through 32
OctaPID ID: 6	Port 33 through 40
OctaPID ID: 7	Port 41 through 48

Table 7 describes the OctaPID ID and port assignments for the 8672ATME and 8672ATMM Modules.

Table 7 8672ATME and 8672ATMM modules

OctaPID ID assignment	**Port assignment**
OctaPID ID: 0	• Ports 1 through 4 (with OC-3c MDA) • Port 1 (with OC-12c MDA) • Ports 1 through 2 (with DS-3 MDA)
OctaPID ID: 1	• Ports 5 through 8 (with OC-3c MDA) • Port 5 (with OC-12c MDA) • Ports 5 through 6 (with DS-3 MDA)
OctaPID ID: 2	Not used

Table 8 describes the OctaPID ID and port assignments for the 8681XLR Module.

Table 8 8681XLR module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	
OctaPID ID: 2	
OctaPID ID: 3	
OctaPID ID: 4	
OctaPID ID: 5	
OctaPID ID: 6	
OctaPID ID: 7	

Table 9 describes the OctaPID ID and port assignments for the 8681XLW Module.

Table 9 8681XLW module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	
OctaPID ID: 2	
OctaPID ID: 3	
OctaPID ID: 4	
OctaPID ID: 5	
OctaPID ID: 6	
OctaPID ID: 7	

Table 10 describes the OctaPID ID and port assignments for the 8683POSM Module.

Table 10 8683POSM module

OctaPID ID assignment	**Port assignment**
OctaPID ID: 0	• Ports 1 and 2 (with OC-3c MDA) • Port 1 (with OC-12c MDA)
OctaPID ID: 1	• Ports 3 and 4 (with OC-3c MDA) • Port 3 (with OC-12c MDA)
OctaPID ID: 2	• Ports 5 and 6 (with OC-3c MDA) • Port 5 (with OC-12c MDA)