Nortel Ethernet Routing Switch 8300

Release Notes - Software Release 4.0

NN46200-401 (316811-J Rev 04)

Document status: Standard
Document version: 03.04
Document date: 22 February 2008

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.

Trademarks

*Nortel, the Nortel Networks logo and the Globemark are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

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

The asterisk after a name denotes a trademarked item.

Statement of conditions

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

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

Nortel Networks software license agreement

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

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

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

include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

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

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

4. **General**

   a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

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

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

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

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

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

Contents

Ethernet Routing Switch 8300 Release 4.0 Release Notes 7
Introduction 7
File names for this release 8
Ensuring Device Manager Online Help displays correctly 9
Upgrading the switch to Release 4.0 software 10
Before upgrading the switch from a previous release 10
Note about DLD files 11
Upgrading an advanced software license 12
New Ethernet Routing Switch 8300 hardware 13
8308XL module 14
8394SF module 14
New software features in this release 14
IP routing 15
Multicast 16
Platform 19
Security 21
Supported software and hardware capabilities 22
Supported Standards (IEEE, RFCs and others) 23
Ethernet Routing Switch 8010/8006 chassis support 29
Supported SFPs 30
Supported XFPs 31
Hot-removal/hot-insertion of Ethernet Routing Switch 8300 modules 32
Hot-removal of master CPU 32
Problems resolved in this release 33
Known limitations and considerations in this release 38
Reading path 49
Important information 50
Chassis and module installation 50
Related publications 50
Hard-copy technical manuals 52
How to get help 52
Getting help from the Nortel web site 52
Getting help over the phone from a Nortel Solutions Center 53

Getting help from a specialist using an Express Routing Code 53
Getting help through a Nortel distributor or reseller 53

Ethernet Routing Switch 8300 Release 4.0 Release Notes

Introduction

These release notes for the Nortel* Ethernet Routing Switch 8300 (formerly known as Passport 8300) Software Release 4.0 describe the hardware and software and any known issues that exist in this release. They are based on Ethernet Routing Switch 8300 Software Release 4.0 and Java Device Manager (Device Manager) 6.0.7.0.

A list of related publications can be found on "Reading path" (page 44). The Ethernet Routing Switch 8300 Software Release 4.0 documentation suite can be found on the documentation CD included with your software or on the Nortel technical documentation Web site, . For more information, see the .

Topic
"File names for this release" (page 8)
"Upgrading the switch to Release 4.0 software" (page 10)
"Upgrading an advanced software license" (page 12)
"New Ethernet Routing Switch 8300 hardware" (page 13)
"New software features in this release" (page 14)
"Supported software and hardware capabilities" (page 22)
"Problems resolved in this release" (page 33)
"Known limitations and considerations in this release" (page 38)
"Reading path" (page 49)
"Hard-copy technical manuals" (page 52)
"How to get help" (page 52)

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

File names for this release

This section describes the Ethernet Routing Switch 8300 Software Release 4.0 software files and the hardware they support.

Module or file type	Location/Description	File name	Size in bytes
Boot configuration file	Configuration file for the boot firmware	boot.cfg	n/a
Configuration file	Configuration file for the runtime image	config.cfg	n/a

Ethernet Routing Switch files			
Boot monitor image	Flash, PCMCIA, or TFTP. CPU and switch fabric boot firmware for the Ethernet Routing Switch 8300	p83b4000.img	1082932
Run-time image	Flash, PCMCIA, or TFTP. The Ethernet Routing Switch 8300 image.	p83a4000.img	6925800
Input/output modules download file	Flash 8300 I/O Module Image	p83r4000.dld	2286048
Pre-boot monitor image	Flash or PCMCIA ***Note:*** This pre-boot image file is only required to be loaded when upgrading from software release 2.0.0.1 and the pre-boot image version is below Release 3.7.	p83f4000.img	230786
Software licensing file ***Note:*** For more information about how to access and configure the license file, see *Nortel Ethernet Routing Switch 8300 Upgrades — Software Release 4.0* (NN46200-400).	Flash, PCMCIA or TFTP ***Note:*** Needed to activate advance features (OSPF, VRRP, SMLT, SLPP, and PIM)	license.dat	varies

MIB zip file (includes private MIB)	This compressed .mib file contains a file named “manifest”, which contains a list of the MIBs supported by the switch, including the private MIBs.	p83a4000.mib.zip p83a4000.mib	498466 3129565
md5 checksum file	Flash or PCMCIA. MD5 checksums of all release 4.0.0 software files	p83a4000.md5	524
SNMP encryption file (required for SNMPv3)	Flash or PCMCIA ***Note:*** Available only on the Nortel web site www.nortel.com/support	p83c4000.aes	26960
3DES encryption file (required for SSH)	Flash or PCMCIA ***Note:*** Available only on the Nortel web site www.nortel.com/support	p83c4000.img	52424

JDM Images			
Solaris for SPARC image	Device manager software image	jdm_6070_solaris_sparc.sh	178413011
Microsoft Windows and Microsoft Vista image	Device manager software image	jdm_6070.exe	168000623
Linux image	Device manager software image	jdm_6070_linux.sh	173563347

Ensuring Device Manager Online Help displays correctly

Nortel supports the following two browsers for Java Device Manager Online Help:

- Netscape
- Internet Explorer

If you use Netscape as your Web browser, to ensure that the topics and table of contents display correctly when you make a context call to on-product Help, perform the following procedure once before you request Help on a topic:

1. Start the Netscape browser.

2. From the Tools menu, select **Options** (An Options window opens.)
3. In the Security and Privacy panel of the Options window, click **Site Controls**. (An Options - Site Controls window opens.)
4. Ensure that the **Site List** tab is selected.
5. Select **Local Files** in the Master Settings area of the window.
6. Select **Internet Explore**r in the Rendering Engine area of the window.
7. Click **OK** to close the Options - Site Controls window.

Upgrading the switch to Release 4.0 software

This section discusses issues related to the upgrading of the Ethernet Routing Switch 8300 to the current software.

Before upgrading the switch from a previous release

Before upgrading to Ethernet Routing Switch 8300 Software Release 4.0 you must do the following:

- Consult *Ethernet Routing Switch 8300 Important Notice — Administration and Security* (NN46200-601) for security-related issues.
- Read the entire upgrade procedure before attempting to upgrade the software on the switch. The upgrade procedure causes interruption of normal switch operation. Refer to *Nortel Ethernet Routing Switch 8300 Upgrades — Software Release 4.0* (NN46200-400).
- Take special note of the following cautionary messages:
  - The configuration file generated with software release 4.0 contains options that are not backward-compatible with software release 3.0.x or earlier. Loading a 4.0.0.0 configuration file on a 3.0.x or earlier 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 (including TFTP server not available, or TFTP Time Out), then 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:

    If the server is not available, or if the **`copy 111.111.1.11:p83a4000.img /flash/p83a4000.img`** file on the server does not exist, the p83a4000.img file is deleted on the flash (if previously existing). 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.

CAUTION
Ensure your files are copied correctly to the flash. Nortel recommends that you use the MD5 checksum. Refer to "MD5 Command" in Nortel Ethernet Routing Switch 8300 Upgrades — Software Release 4.0 (NN46200-400).

— When you install files on the onboard flash or PCMCIA, verify flash capacity before downloading the files.

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

copy/<device>/<config filename> <tftpServerIPAddr>:<config filename.old>

where device can be PCMCIA or flash.

— Nortel recommends that you have 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 8300 Series switch searches for the file /pcmcia/boot.cfg. If a PCMCIA card is not present, or if the file /pcmcia/boot.cfg is not present, then the 8300 Series switch boots using the default boot-configuration settings.

CAUTION
If you are using a PCMCIA card manufactured by SanDisk, the 8300 Series switch may be unable to access the /pcmcia/boot.cfg file during bootup. This limitation has only been observed during bootup. No limitation has been observed when accessing the SanDisk device after bootup.

— In NNCLI mode, if you use a configuration file from a previous release, the configuration loading process can fail. This failure is because the functionality of the **end** command is redefined in Software Release 4.0.

Note about DLD files

When the boot configuration is saved in runtime, the current bootp DLD image names are saved in the boot.cfg file. If you load a new image without removing the bootp DLD entry references from the boot.cfg, then the new version of the file is not downloaded to the I/O boards.

- On boot up, if a DLD file is not configured in boot.cfg, the CP code searches for a DLD file with the following file name:

p83r<stream name><version>.dld

The stream name and version must match the CP image being initialized. If this file is found, its checksum is verified and it is downloaded to the I/O boards. If the boot configuration is saved, this is the DLD file name saved in boot.cfg.

- If the CP does not find this DLD file name in its flash, it searches for the following default file name:

  p83r<stream name>.dld

  Only the stream name must match the CP image being initialized. If this file is found, its checksum is verified and it is downloaded to the I/O boards. If the boot configuration is saved, this is the DLD file name saved in boot.cfg.

To make the system boot from the default DLD files, first clear the DLD file references made by boot.cfg:

Step	Action
1	Enter the boot monitor.
2	Enter the following command: **bootp image default** This clears the DLD file entries so that the new version of **p83r<stream name><version>.dld** or **p83r<stream name>.dld** is loaded.

CAUTION
Do not interrupt the DLD download after it has started or failure can occur.

—End—

Upgrading an advanced software license

Follow the steps in this procedure to upgrade your current advanced software license for 4.0:

Procedure steps:

Step	Action
1	Open www.nortellicensing.com. The Nortel Electronic Licensing portal appears.
2	Click on **License Bank** (Upper left navigation). The Log in to License Bank dialog box appears.
3	In the **License Bank Name** box, type your license bank name.
4	In the **License Bank Password** box, type your license bank password. Your license bank screen appears.
5	In the Used column of Your License Bank, click the **Details** button. The License Bank Details dialog box appears.
6	In the **License or License File** box, click the file name (license_0823.dat). A file download dialog box appears.
7	Click **Save**.
8	Reinstall the license. For information about how to install the license, see *Nortel Ethernet Routing Switch 8300 Configuration — Platform Operations* (NN46200-602).

—End—

New Ethernet Routing Switch 8300 hardware

This section describes the new Ethernet Routing Switch 8300 Release 4.0 hardware.

New hardware	Module part number	Where to find information
"8308XL module" (page 14)	DS1404100-E6	*Nortel Ethernet Routing Switch 8300 Installation — Modules* (NN46200-305)
"8394SF module" (page 14)	DS1404099-E5	*Nortel Ethernet Routing Switch 8300 Installation — Modules* (NN46200-305)

8308XL module

The 8308XL I/O module provides eight ports for installing 10 Gigabit Ethernet XFP pluggable transceivers. The 10GBASE-X ports on this module are LAN capable and operate in full-duplex mode.

For more information about the 8308XL module, refer to the following documents:

- *Nortel Ethernet Routing Switch 8300 Installation — Modules* (NN46200-305)
- *Nortel Ethernet Routing Switch 8300 Planning — Power Considerations* (NN46200-511)
- *Nortel Ethernet Routing Switch 8300 Important Notice — 8300 Series Modules* (NN46200-603)

8394SF module

The 8394SF Switch Fabric/CPU module with 2-port 10GBASE-X XFP slots, provides two ports for installing 10 Gigabit Ethernet small form factor-pluggable (XFP) transceivers. The 10GBASE-X port operates in full-duplex mode.

For more information about the 8394SF module, refer to the following documents:

- *Nortel Ethernet Routing Switch 8300 Installation — Modules* (NN46200-305)
- *Nortel Ethernet Routing Switch 8300 Planning — Power Considerations* (NN46200-511)
- *Nortel Ethernet Routing Switch 8300 Important Notice — 8300 Series Modules* (NN46200-603)

New software features in this release

This section describes the new software features for the Ethernet Routing Switch 8300 Software Release 4.0.

Feature	Description
IP routing	
"Multihoming" (page 16)	New feature introduced in 4.0

Feature	Description
Multicast	
"Layer 2 Internet Group Management Protocol snoop querier" (page 16)	New feature introduced in 4.0

Multicast	
"Multicast access control feature" (page 16)	Feature enhanced in 4.0
"Multicast flow distribution over MLT" (page 17)	New feature introduced in 4.0
"Multicast Stream Limitation" (page 17)	New feature introduced in 4.0
"Protocol Independent Multicast passive interfaces" (page 17)	New feature introduced in 4.0
"Protocol Independent Multicast-Sparse Mode" (page 18)	New feature introduced in 4.0
"Protocol Independent Multicast-Split MultiLink Trunking " (page 18)	New feature introduced in 4.0
"Static source groups" (page 18)	New feature introduced in 4.0
"Static rendezvous point router" (page 19)	New feature introduced in 4.0

Platform	
"8 port MLT/SMLT support" (page 19)	Feature updated in 4.0
"Microsoft Network Load Balancing Support" (page 20)	New feature introduced in 4.0
"Port auto-recovery" (page 20)	New feature introduced in 4.0
"Simple Loop Prevention Protocol" (page 20)	New feature introduced in 4.0

Security	
"Nortel Secure Network Access 1.5" (page 21)	Feature updated in 4.0

IP routing

The Nortel Ethernet Routing Switch 8300 Software Release 4.0 supports the following IP routing features:

Multihoming

With the multihoming feature, the Ethernet Routing Switch 8300 can support clients or servers that have multiple IP addresses associated with a single MAC address. Multihomed hosts can be connected to port-based, policy-based, and IP subnet-based VLANs. The IP addresses associated with a single MAC address on a host must be in the same IP subnet.

For more information about multihoming, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Multicast

The Nortel Ethernet Routing Switch 8300 Software Release 4.0 supports the following multicast features:

Layer 2 Internet Group Management Protocol snoop querier

In the 4.0 release, the Nortel Ethernet Routing Switch 8300 supports the Layer 2 Internet Group Management Protocol (IGMP) snoop querier. With this feature, a snoop VLAN can send out IGMP query messages.

For more information about Layer 2 IGMP snoop querier, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Multicast access control feature

You can configure an IP multicast-enabled VLAN with an access control policy that consists of several IP multicast groups.

In the 4.0 release, the Nortel Ethernet Routing Switch 8300 supports six types of multicast access control policies:

- deny-tx
- deny-rx
- deny-both
- allow-only-tx
- allow-only-rx
- allow-only-both

For more information about the Multicast access control feature, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Multicast flow distribution over MLT

Multicast flow distribution over MultiLink Trunking (MLT) is a mechanism that uses all the MLT (Trunk Group) ports to distribute multicast data traffic. This mechanism simplifies the data traffic distribution over an MLT because instead of distributing the traffic load evenly on the links of an MLT, it distributes the streams of multicast data traffic over the ports of an MLT. As a result, this feature distributes the load on different ports of the multilink trunk and (whenever possible) achieves an even distribution of the streams. In applications like TV distribution, multicast flow distribution is particularly important, because the bandwidth requirements can be substantial when a large number of TV streams are used.

For more information about multicast flow distribution over MLT, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Multicast Stream Limitation

You can configure the multicast stream limitation feature to limit the number of multicast groups that can join a VLAN. By limiting the number of concurrent multicast streams, a service provider can, for example, protect the bandwidth on a specific interface and control access to multicast streams.

For more information about Multicast Stream Limitation, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Protocol Independent Multicast passive interfaces

A passive interface drops all Protocol Independent Multicast (PIM) control traffic, thereby reducing the load on the system. This feature is useful when you have a high number of PIM interfaces and these interfaces are connected to end-users, not to other switches.

For more information about PIM passive interfaces, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Protocol Independent Multicast-Sparse Mode

Protocol Independent Multicast-Sparse Mode (PIM-SM), as defined in RFC 2362, supports multicast groups spread out across large areas of a company or the Internet. Unlike dense mode protocols, such as Distance Vector Multicast Routing Protocol (DVMRP), that initially flood multicast traffic to all routers over an entire internetwork, PIM-SM sends multicast traffic to only routers that specifically joined a multicast group. This technique reduces traffic flow over wide area network (WAN) links and overhead costs for processing unwanted multicast packets.

For more information about PIM-SM, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Protocol Independent Multicast-Split MultiLink Trunking

Software Release 4.0 supports IP Multicast routing with Split MultiLink Trunking (SMLT) by building a virtual switch that represents the two switches of the split multilink trunk core. When the switches are running PIM-SM in the core, they need to exchange protocol related updates as part of the interswitch trunking (IST) protocol. IST hides the fact that the edge switch is attached to two physical switches.

Release 4.0 supports only triangular SMLT topology with PIM-SM. This release does not support a square SMLT or a partial mesh square SMLT with PIM-SM.

For more information about PIM-SMLT, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Static source groups

You can use static source groups (or static mroutes) to configure static source-group entries in the PIM-SM multicast routing table. PIM cannot prune these entries from the distribution tree; even if there are no receivers

for the group, the multicast stream for a static source-group entry stays active. Static forwarding entries are never pruned. When they are no longer needed, you manually delete them.

Static source groups ensure that the multicast route (mroute) records remain in the distribution tree. When receivers join the group, there is no delay in receiving multicast data because there is no need to graft onto the group or start a join process in the case of PIM. No delay is essential for applications where the multicast data must be sent to a receiver as soon as the receiver joins the group, for example, when a switch delivers TV channels to receivers. When the receiver turns the channel, which is equivalent to joining a group, the receiver can view the channel immediately.

For more information about static source groups, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Switch Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Static rendezvous point router

This feature avoids the process of selecting an active rendezvous point (RP) from the list of candidate RPs and dynamically learning about RPs through the BSR mechanism. Static RP-enabled switches cannot learn about RPs through the BSR because the switch loses all dynamically-learned BSR information and ignores BSR messages. When you configure static RP entries, the switch adds them to the RP-set as if they were learned through the BSR.

For more information about static rendezvous point router, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Platform

The Nortel Ethernet Routing Switch 8300 Software Release 4.0 supports the following platform features:

8 port MLT/SMLT support

The Ethernet Routing Switch 8300 supports eight ports for each aggregation group. All ports in a link aggregation group must be of the same media type and have the same speed and duplex settings.

For more information about port auto-recovery, see the following documents:

- *Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI* (NN46200-504)
- *Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (NN46200-509)
- *Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the Device Manager* (NN46200-510)

Microsoft Network Load Balancing Support

Microsoft Network Load Balancing Support (NLBS) is a clustering technology that Microsoft includes in the Windows 2000 Advanced Server and Datacenter Server operating systems. NLBS increases the scalability and availability of TCP- and IP-based services such as Web, Terminal Services, virtual private networking, and streaming media servers.

For more information about NLBS, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)

Port auto-recovery

The port auto-recovery feature can automatically enable a port that is shut down by SLPP, CP-limit or Link Flap Detect. When a port with auto-recovery enabled, is operationally shut down by SLPP or CP-limit, the port is enabled within a specific, configurable time delay.

For more information about port auto-recovery, see the following documents:

- *Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI* (NN46200-504)
- *Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (NN46200-509)
- *Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the Device Manager* (NN46200-510)

Simple Loop Prevention Protocol

Use Simple Loop Prevention Protocol (SLPP) at the edge of a network to prevent loops in a Split MultiLink Trunking (SMLT) network if you are not using Spanning Tree. Although SLPP is focused on SMLT networks, it also works with other configurations. Logical loops can occur in SMLT networks for the following reasons:

- Misconfigurations (for example, when SMLT client devices are erroneously directly connected together).

- MLT is not operating correctly (for example, when a switch is connected to the network using the default configuration without any MLT settings).
- Problems occur with the edge switch (for example, when MLT or some other form of link aggregation is not working).

For more information about SLPP, see the following documents:

- *Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI* (NN46200-504)
- *Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (NN46200-509)
- *Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the Device Manager* (NN46200-510)

Security

The Nortel Ethernet Routing Switch 8300 Software Release 4.0 supports the following security features:

Nortel Secure Network Access 1.5

Nortel Secure Network Access (NSNA) 1.5 is a protective framework that addresses endpoint security and enforces policy compliance. The framework completely secures the network from endpoint vulnerability and delivers endpoint security by enabling only trusted, role-based access privileges premised on the security level of the device, end user identity, and session context. NSNA enforces policy compliance, such as Sarbanes-Oxley and COBIT, ensuring that the required anti-virus applications or software patches are installed before users are granted network access.

For more information about NSNA 1.5, see the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration — Security using the NNCLI and CLI*(NN46200-503)
- *Nortel Ethernet Routing Switch 8300 Configuration — Security using Device Manager* (NN46200-508)

New commands and Syslog messages

For complete listings of all commands and system messages, see:

- *Nortel Ethernet Routing Switch 8300 Command Reference - CLI* (NN46200-513)
- *Nortel Ethernet Routing Switch 8300 Command Reference NNCLI*(NN46200-306)
- *Nortel Ethernet Routing Switch 8300 Fault Management - System Messaging Platform Reference*(NN46200-701)

Supported software and hardware capabilities

This section lists the known limits for the Ethernet Routing Switch 8300 Software Release 4.0 and JDM 6.0.7.0 of the Ethernet Routing Switch 8300 Series software. These capabilities will be enhanced in subsequent software releases.

Feature	Maximum number supported	
Media Access Control (MAC)/forwarding data bases (FDB) Entries	Up to 16 000	
Address Resolution Protocol (ARP) Entries	Up to 2 994	
Spanning Tree Groups (STG)	Up to 64	
VLANs	By-Port up to 500 IP Based By-Port up to 1 972 non-IP Based By-Protocol up to 500 IP Based By-Protocol up to 1 972 non IP Based Maximum number of VLAN IDs 4 096	
MultiLink Trunk (MLT) Groups Split Multilink Trunking (SMLT) Groups Max Number of Links per MLT/SMLT/interswitch trunking (IST) group	Up to 31 Up to 30 with 1 IST group 8	***Note:*** • For 8348TX, 8348TX-PWR and 8324FX ports, you can use only Link Aggregation Groups 1-7. • For 8348GB, 8324GTX, 8348GTX and 8348GTX-PWR ports and 8393SF, you can use Link Aggregation Groups 1-31.
Internet Protocol (IP) Interfaces	Up to 500–1 024 desired	
Static Routes	Up to 500	
Routing Information Protocol (RIP)	Up to 200 RIP Neighbors Up to 1 000 RIP Routes	
Open Shortest Path First (OSPF) OSPF combination	Up to 6 OSPF areas Up to 200 OSPF neighbors Up to 8 000 OSPF routes 3 Areas/ 10 Adjacencies/ 8 000Routes 5 Areas/ 80 Adjacencies/ 6 000 Routes 6 Areas/ 32 Adjacencies/ 4 000 Routes	
Virtual Router Redundancy Protocol (VRRP) Instances	Up to 256	

Feature	Maximum number supported
Internet Group Management Protocol (IGMP) Snoop	Maximum number of IGMP Interfaces: 500 Maximum number of IGMP clients: 1 500 Maximum number of IGMP clients with unique multicast groups: 1 026 IGMP Joins/sec: 200 IGMP Leaves/sec: 200
Protocol Independent Multicast (PIM)	Up to 128 PIM neighbors Up to 1 024 (Source, Group) pairs
Extensible Authentication Protocol over LAN (EAPoL) 802.1X supplicants	Up to 8 supplicants per port
Remote Access Dial-in User Service (RADIUS) Media Access Control (MAC) centralization clients	Up to 8 supplicants per port
Link Layer Discovery Protocol (LLDP) Neighbors	Up to 384
IP Filters	
ACL	Up to 512 (IP or non-IP based)
ACT	With one ACL, up to 34 (IP or non-IP based)
ACE	With one ACL and one ACT, up to 128 (IP or non-IP based)
ACG	With one ACL, one ACT and one ACE, up to 1 024 (IP or non-IP based)

Supported Standards (IEEE, RFCs and others)

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

Supported Standards	
802.1D	MAC Bridges (Spanning Tree Protocol)
802.1p	Traffic Class Expediting
802.1Q	Virtual LANs
802.1X	Port-Based Network Access Control (Extensible Authentication Protocol)

Supported Standards	
802.1AB	Station and Media Access Control Connectivity Discovery (LLDP)
802.3	10BASE-T (ISO/IEC 8802-3, Clause 14)
802.3u	100BASE-T (ISO/IEC 8802-3, Clause 25)
802.3u	Auto-Negotiation on Twisted Pair (ISO/IEC 8802-3, Clause 28)
802.3x	100Mb/s Full Duplex Operation
802.3z	Gigabit Ethernet (1000BASE-X)
802.3ab	1000BASE-T
802.3ae	10Gb/s Ethernet (10GBASE-X)

Supported IPv4 standards	
RFC 768	User Datagram Protocol (UDP)
RFC 783	Trivial File Transfer Protocol (TFTP) v2
RFC 791	IP
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol (TCP)
RFC 826	Ethernet Address Resolution Protocol
RFC 854	Telnet protocol
RFC 903	Reverse ARP
RFC 1058	RIP

Supported IPv4 standards	
RFC1112	Host Extensions for IP Multicasting
RFC1157	Simple Network Management Protocol (SNMP)
RFC1213	TCP/IP Management Information Base (MIB)-II
RFC1493	Bridge MIB
RFC1541	Dynamic Host Configuration Protocol (DHCP)
RFC1542	Bootstrap Protocol (Clarifications and Extensions)
RFC1591	Domain Name System
RFC1757	Remote Network Monitoring
RFC1812	IPv4 Router Requirements
RFC1850	OSPFv2 MIB
RFC1866	HyperText Markup Language v2
RFC 2068	Hypertext Transfer Protocol (HTTP) v1.1
RFC 2138	RADIUS Authentication
RFC2139	RADIUS Accounting
RFC 2328	OSPFv2
RFC 2236	IGMPv2
RFC2338	VRRP
RFC 2362	Protocol Independent Multicast-Sparse Mode (PIM-SM)
RFC2453	RIPv2

Supported IPv4 standards	
RFC2474	Differentiated Services in IPv4 and IPv6
RFC2475	Differentiated Services
RFC2570	Simple Network Management Protocol (SNMP)v3
RFC2571	SNMP Frameworks
RFC2572	SNMP Message Processing and Dispatching
RFC2573	SNMPv3 Applications
RFC2574	SNMPv3 User-based Security Model (USM)
RFC2575	SNMPv3 View-based Access Control Model (VACM)
RFC2576	SNMP Coexistence of v1, v2, & v3 of Internet Network Management Framework
RFC2597	Assured Forwarding per hop behavior (PHB) Group
RFC2598	Expedited Forwarding PHB
RFC2665	Ethernet MIB
RFC2737	Entity MIBv2
RFC2787	VRRP MIB
RFC 2819	Remote Monitoring (RMON) MIB
RFC2863	Interfaces Group MIB

The Ethernet Routing Switch 8300 is an SNMPv1/v2/v2c/v3 agent with Industry Standard MIBs, as well as private MIB extensions, which ensures compatibility with existing network management tools.

These MIBs are provided with different versions of code. Consult the Nortel website where a file named mib.zip contains all these MIBs, and a special file named manifest for the order of the MIB compilation.

Standard MIB name	IEEE	File name
802.1ab	802.1ab	ieee8021ab.mib ieee8021ab1x.mib ieee8021ab3x.mib ieee8021abMed.mib
EaPoL (802.1X)	802.1X	ieee8021x.mib

Standard MIB name	RFC	File name
IANA Interface type	n/a	iana_if_type.mib
SMI	RFC1155	rfc1155.mib
SNMP	RFC1157	rfc1157.mib
MIB for network management of TCP/IP based Internet MIBs	RFC 1213	rfc1213.mib
A convention for defining traps for use with SNMP	RFC 1215	rfc1215.mib
RIP version 2 MIB extensions	RFC1389	rfc1389.mib
Definitions of Managed Objects for Bridges	RFC1493	rfc1493.mib
Evolution of the Interface Groups for MIB2	RFC1573	rfc1573.mib
Definitions of Managed Objects for the Ethernet-like Interface types	RFC1643	rfc1643.mib
Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2	RFC1657	rfc1657.mib
RIP version 2 MIB extensions	RFC1724	rfc1724.mib
Remote Network Monitoring Management Information Base (RMON) ***Note:*** Ethernet Routing Switch 8300 supports Alarms, Events, Statistics and History.	RFC1757/RFC2819	rfc1757.mib
OSPF Version 2 Management Information Base	RFC1850	rfc1850.mib

Standard MIB name	RFC	File name
Management Information Base of the Simple Network Management Protocol (SNMPv2)	RFC1907	rfc1907.mib
Remote Network Monitoring Management Information Base (RMON) version 2 using SMIv2	RFC2021	rfc2021.mib
IP Forwarding Table MIB	RFC2096	rfc2096.mib
The Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
An Architecture for Describing SNMP Management Frameworks	RFC2571	rfc2571.mib
Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	RFC2572	rfc2572.mib
SNMP Applications	RFC2573	rfc2573.mib
User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)	RFC2574	rfc2574.mib
Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	RFC2576	rfc2576.mib
Definitions of Managed Object for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN extensions	RFC2674	rfc2674.mib
Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
The Interface Group MIB	RFC2863	rfc2863.mib
Internet Group Management Protocol MIB	RFC2933	rfc2933.mib
The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP Used-based Security Model	RFC3826	rfc3826.mib
VRRP (Virtual Router Redundancy Protocol)	RFC2787	rfc2787.mib

Supported Standards	
Rapid City MIB	rapid_city.mib
Rapid City MIB	synro.mib
Other SynOptics definitions	s5114roo.mib
Other SynOptics definitions	s5tcs112.mib
Other SynOptics definitions	s5emt103.mib
Nortel IGMP MIB	rfc_igmp.mib
Nortel VRRP MIB	vrrp_rcc.mib
Nortel MIB definitions	wf_com.mib
OSPF Version 2 Management Information Base-Nortel	rfc1850t_rcc.mib

Ethernet Routing Switch 8010/8006 chassis support

You can use Ethernet Routing Switch 8300 modules with the Ethernet Routing Switch 8010 and 8006 chassis. The following requirements must be adhered to:

1. The Ethernet Routing switch 8010 and 8006 chassis must support up to 16 000 media access control (MAC) addresses to be used with Ethernet Routing Switch 8300 modules. Upgrade kit (DS1411015) upgrades the number of supported MAC addresses on the chassis from 1 024 to 16 000. For more information about this kit, see *Nortel Ethernet Routing Switch 8300 Installation — MAC Addresses* (NN46200-600).
2. The Ethernet Routing Switch 8300 switch fabric modules (8393SF or 8394SF) are limited to one switch fabric per Ethernet Routing Switch 8010 or Ethernet Routing Switch 8006 chassis. This single switch fabric in the 8010 or 8006 chassis can be in either slot 5 or 6. Dual switch fabric modules in these chassis are not supported. Only Ethernet Routing Switch 8310 and 8306 (10-slot and 6-slot PoE chassis) support dual switch fabric configurations.
3. The Ethernet Routing Switch 8010 and 8006 chassis do not support Power over Ethernet (PoE) capabilities on the PoE module. Therefore, the PoE feature is not available in these chassis.

Note:

1. You can use the Ethernet Routing Switch 8348TX-PWR or the 8348GTX-PWR module in the 8010 or 8006 chassis. Be aware, however, that when the 8348TX-PWR or the 8348GTX-PWR module is operating in the 8010 or 8006 chassis, it operates without the PoE function being available.

2. In an 8010 or 8006 chassis, you cannot mix Ethernet Routing Switch 8300 modules with Ethernet Routing Switch 8600 or 8100 modules.
3. The 8003 chassis is not supported.
4. The 8393SF module supports all existing modules and the new IO module.
5. The new 8394SF module supports all existing IO modules and the new 8308XL module.
6. A single chassis supports the 8393SF and 8394SF modules only during the software and hardware upgrades.

Supported SFPs

This section lists the transceivers supported by the Ethernet Routing Switch 8300.

SFP order number	SFP type	Reach
AA1419013	LC type 1000BASE-SX	Up to 550 m
AA1419014	MT-RJ type 1000BASE-SX	Up to 550 m
AA1419015	LC type 1000BASE-LX	Up to 5 km
AA1419025	1470nm/Gray 1000BASE CWDM	Up to 40 km
AA1419026	1490nm/Viole t 1000BASE CWDM	Up to 40 km
AA1419027	1510nm/Blue 1000BASE CWDM	Up to 40 km
AA1419028	1530nm/Green 1000BASE CWDM	Up to 40 km
AA1419029	1550nm/Yellow 1000BASE CWDM	Up to 40 km
AA1419030	1570nm/Orange 1000BASE CWDM	Up to 40 km
AA1419031	1590nm/Red 1000BASE CWDM	Up to 40 km
AA1419032	1610nm/Brown 1000BASE CWDM	Up to 40 km
AA1419034	1490nm/Violet 1000BASE CWDM	Up to 70 km

SFP order number	SFP type	Reach
AA1419035	1510nm/Blue 1000BASE CWDM	Up to 70 km
AA1419036	1530nm/Green 1000BASE CWDM	Up to 70 km
AA1419037	1550nm/Yellow 1000BASE CWDM	Up to 70 km
AA1419038	1570nm/Orange 1000BASE CWDM	Up to 70 km
AA1419039	1590nm/Red 1000BASE CWDM	Up to 70 km
AA1419040	1610nm/Brown 1000BASE CWDM	Up to 70 km
AA1419043	RJ-45 Type 1000BASE-T	Up to 100 m
AA1419069 ***Note:*** Release 3.0 is required for recognition of this SFP.	1-port 1000BASE-BX Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1310nm Wavelength. Must be paired with AA1419070	Up to 10 km
AA1419070 ***Note:*** Release 3.0 is required for recognition of this SFP.	1-port 1000BASE-BX Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1490nm Wavelength. Must be paired with AA1419069	Up to 10 km

For detailed information about SFPs, refer to *Nortel Ethernet Routing Switch 8300 Installation — SFPs and XFPs* (NN46200-307)

Supported XFPs

XFPs are hot-swappable input/output enhancement components designed for use with Nortel products to allow 10 Gigabit Ethernet ports to link with other 10 Gigabit Ethernet ports. Digital diagnostic monitoring (DDM) provides real-time access to device operating parameters. All XFPs come with DDM capability.

All Nortel XFPs use LC connectors to provide precision keying, low interface losses, and space savings.

Table 1 "XFP models" (page 32) lists and describes the Nortel XFP models:

Table 1
XFP models

Model number	Product name	Description
10GBASE-SR	AA1403005-E5	850 nanometers (nm). The range is up to • 22 m using 62.5 micrometer (µm), 160 megaHertz times km (MHz-km) MMF • 33 m using 62.5 µm, 200 MHz-km MMF • 66 m using 62.5 µm, 500 MHz-km MMF • 82 m using 50 µm, 500 MHz-km MMF • 82 m using 50 µm, 500 MHz-km MMF :
10GBASE-LR/LW	AA1403001-E5	1 310 nm SMF. The range is up to 10 km.
10GBASE-ER/EW	AA1403003-E5	1 550 nm SMF. The range is up to 40 km.
10GBASE-ZR/ZW	AA1403006-E5	1 550 nm SMF. The range is up to 80 km.

Hot-removal/hot-insertion of Ethernet Routing Switch 8300 modules

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

Hot-removal of master CPU

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

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

Step	Action
1	Use the save to standby option to automatically save both the boot and the configuration files to both CPUs (master and standby).
2	If you are using the out-of-band Ethernet port of the 8393SF or 8394SF module for management, add a virtual IP address. The virtual IP address allows access to the master CPU whether the master CPU is slot 5 or slot 6.
3	Perform a soft reset on the master CPU to cause failover to occur.
4	Wait until the new master comes up and the old master becomes the standby.
5	Remove the standby CPU. If you need to reinsert this CPU, you must wait at least 60 seconds.

—End—

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

To avoid this issue, back up the existing configuration file before saving any configuration. After you insert the removed CPU, you can then reboot the switch with the backup configuration file to restore the configuration. For more information about warm standby, see *Nortel Ethernet Routing Switch 8300 Planning and Engineering Network Design Guidelines* (NN46200-200).

Problems resolved in this release

This section describes issues that have been fixed since the 8300 Series Release 2.3 in the following categories:

Topic
HARDWARE
SOFTWARE
Platform
CLI
Device Manager

Topic
NNCLI
Layer 2
Multicast
Security
Miscellaneous

CR reference	Description
HARDWARE	
Q01412542	Error messages may appear in the console terminal when inserting a 8348GB module into the chassis.
Q01391245	In a fully populated chassis, when using copper SFP's in the standby CPU, resetting the standby CPU may cause the CPU to produce I2C write errors on the console. The system recovers without any impairment.
Q01400659	If a hot insertion of a PoE board occurs during a CPU boot cycle, the PoE terminates with a hardware error message after reboot.
Q01399804	8348GB is allowing link up before the module and system is able to forward.
Q01399823	CPU removal does not time out the peer L2 connection.
SOFTWARE	
Platform	
Q01264094	If CLI Log (clilog.txt) file exceeds the PCMCIA capacity, an endless scrolling of INFO message occurs until enough space is cleared on the PCMCIA.
Q01368963	Egress traffic cannot be mirrored when attempting to do so on an 8348GB or 8348GTX and monitoring the traffic on a different 8348GB or 8348GTX.
Q01360780	When SMLT attempts to re-establish its original data path during the recovery phase, traffic loss (6-7s) occurs on one of the core switches.
Q00851722	Changing CP limit settings on a single port belonging to an MLT does not change the settings for the other ports in the MLT.
Q01313950	The EAP port state cannot be set to force-auth from either force-unauth or auto when EAP is disabled globally.
Q01326368	An EAP enabled tagged port does not move from the guest VLAN to the authenticate VLAN after successful authentication.
Q01296753	In CLI mode, when a syslog host is in disabled state and the Ethernet Routing Switch 8300 switch is rebooted in NNCLI mode, the state of the syslog host changes to enable.
Q01343042-02	Assertion fails if simultaneous link state changes on multiple ports.

CR reference	Description
Q01322891-01	When the VLAN ID and the TCP/UDP destination port are selected and 12 other octets are configured for a PCL template, the TCP/UDP destination port cannot match the incoming packets.
Q01374779-01	Configuring a syslog host with a severity level of INFO causes system instability.
Q01243757 Q01232899	STP does not converge properly after CPU failover.
Q01201638/ Q01201638-01	See RSA key on the CLI during generating when SSH is enabled.
Q01237128	The allocated power for PoE is a negative value.
Q01189519	The port-utilization calculation takes data-bytes only into account with Preamble and Inter-Frame Gap excluded.
Q01254489	Changes to NTP interval cannot take effect if NTP is already running or system reboot.
Q01193827	The 8348TX and 8348TXPoE modules erroneously report InternalMacReceiveErrors upon toggling the link state.
Q01234950-01	The maximum configurable value for RADIUS server retry time is 10 seconds is too short.
Q01226753 Q01226761-01	Only first Radius server works although multiple servers are configured. EAP Clients authenticate fail if first one is unreachable.
Q01265501	CPU utilization value calculates wrongly.
Q01282637	If an ACE is configured with both AceId and Precedence set to the same value, the precedence value of an ACE is set to the default value after reboot.
Q01237567-01	Traffic from the management port is forwarded to the internal network.
Q01311357	VRRP Hello packets can sometimes be delayed by up to 8 seconds.
Q01678479	LLDP dot3 neighbor PoE powerMDIEnable and PowerPairControlable will not be updated by the received LLDP packet.
Q01691584	The 8348GTX and 8348GTX-PWR modules crash when you delete port mirror with traffic flow.
Q01616478	83R4B45: The memory is depleted after loading the B045 image and may cause a switch crash.**Workaround:** Nortel recommends that, if you have a large-scaled environment, do not run the Jumbo Frame feature with the 8393 and 128M RAM.
CLI	
Q00876505 Q00855057	When you enter show ports error, ospf [<ports>] displays in the CLI help as one of the available options. The Ethernet Routing Switch 8300 does not support this option.

CR reference	Description
Q00876390	When you enter some commands under **`config sys access-policy policy <number> service, ssh`** appears in the CLI help as one of the available services. Although the Ethernet Routing Switch 8300 supports SSH v1/v2, the Ethernet Routing Switch 8300 does not support this option in this release.
Q01657836	The 10G port is UP on the CLI, but the Rx LED is in orange if RX power doesn't meet the threshold.
Device Manager	
Q01445326	Device Manager loses connection to ERS 8300 when the access policy is globally enabled before an access policy for the SNMP v3 group is provisioned in the Access Policies SNMP groups table. **Workaround**: Disable the access policy function first to recovery if this provisioning was not done initially. In CLI use the **`config sys access-policy enable false`** command. In NNCLI use the **`access-policy disable`** command.
Q01434476	A management IP address can be assigned an existing VLAN IP address via Device Manager but not in the CLI/NNCLI. **Workaround:** Ensure IP address does not conflict before completing the management IP assignment.
Q01349008	In the JDM and LLDP, AddrPortsTxEnable port numbers are off by one. Workaround: The correct display is available using the CLI.
NNCLI	
Q01451184	When the ping snoop feature is enabled and an interface is pinged, the ICMP reply does not appear on the telnet screen.
Q01441874	Syslog host state becomes true after rebooting in NNCLI.
Q01405645	Removal of group access from the V3 VACM table is not preserved after reboot.
Layer 2	
Q01416621-01	Using the **`show vlan info port`** command in CLI brings up incomplete output information (some assigned ports to the VLAN are missing from the output). This occurs when the name of the configured VLAN exceeds 14 characters with many ports assigned to that VLAN.
Q01369756	The 8300 MLT trunk port does not come up after overlapping the links
Q01397092	LAN which enabled RIP/OSPF could not transfer broadcast data' with ' VLAN which enabled RIP/OSPF could not transfer broadcast data.
Q01386733	Learned MAC entries aged out before the configured aging time is reached.

CR reference	Description

Q00883592	If you create an IP VLAN that belongs to a subnet represented by an existing static route, the following error message may display:
	
	`IP ERROR rcIpModifyNextHop:  Arp pointer is NULL for route:`
	`x.x.x.x mask:  x.x.x.x`
	
	The new local route should take over as the best route in the route table. If so, you can ignore this error.

Multicast	
Q00763045	IGMP MRDISC is supported on the Ethernet Routing Switch 8300, but there may be interoperability issues with other 8000 series switches. In an SMLT setup, the switch should find only one mrouter on its MLT link.
Q00843934	Using IP traffic filter, user is not be able to deny IGMP join or IGMP leave messages.
Security	
Q01435536	In the CLI and NNCLI, the EAPOL session is not terminated when the VLAN with authenticated client is deleted
Q01017469- 01	When you create a user in SNMPv3 by entering the command **`config snmp-v3 usm Manager md5 pass`** and you remove the initial password by entering the command **`config snmp-v3 usm delete initial`**, you must enter the command **`auth Manager old-pass pass new-pass pass`** to make it work.
Miscellaneous	
Q01438382	When applying a filter to a fiber port with layer 4 protocol parameters, the access list does not work on the trunk ports.
Q01281360	When an access policy with SSH service enabled exists, the configured value of accesslevel is now applied to SSH users accessing the switch with RSA/DSA public key authentication.
Q01325130	*RW* user is able to configure access-policies which should not be allowed.
Q01305174	The access policy usage counters are now updated properly when telnetting to the peer CPU module on a ERS 8300 switch with dual CPU modules.
Q01381069	The show sys access-policy snmp-group-info command now displays the snmp groups without causing switch instability.
Q01158832-02	There will no longer be an issue of CPU utilization going higher while processing SNMP packets.
Q01200901-01	Added a condition check when we try deleting the default-access policy with the submit.

CR reference	Description
Q01200902-01	Access policy can now be created from Device Manager without enabling any service.
Q01304306	On Ethernet Routing Switch 8300, the last entry in the access policy list will no longer be lost after reboot
Q01183804-01 Q01295814	Ethernet Routing Switch 8300 now displays a message when user connection is established or disconnected via FTP
Q01250458	Setting the SSH mode to Secure through Device Manager will no longer cause any system instability.
Q01205411-01	RIP version can now be configured as rip1 via NNCLI.
Q01265965	Ethernet Routing Switch 8300 no longer displays a warning message when a circuitless IP interface with 32 bit mask is deleted
Q01148215-01	Ethernet Routing Switch 8300 no longer allows route-discovery parameters to be set for a non-routable VLAN.
Q01388357	Deleted SNMPv3 default entries were recreated after reboot Workaround: Delete default entries after reboot.
Q01384959	Error messages sometimes occurred during configuration loads in the area of the V3 Group Membership.
Q01384936	The save config verbose sometimes caused a delay in configuring the load SNMP V3 section.
Q01400506	When the Transmit Delay was set to the maximum of 3600 and then during device time-out, LSA 5 packets did not flood if a cable is removed and reinserted. **Workaround:** Nortel recommends that you keep Transmit Delay at 3000 or less.
Q01400519	When the Transmit Delay was set to the maximum of 3600, then during device time-out, LSA5 packets cleared when applying RedistributeApply. **Workaround:** Nortel recommends that you keep the Transmit Delay at 3000 or less.
Q01400530	When the Transmit Delay was set to the maximum of 3600, then during device time-out, LSA5 packets cleared when changing LSA external type. **Workaround:** Nortel recommends that you keep the Transmit Delay at 3000 or less.
Q01424477	Although ping-virtual-address is enabled by default, the feature does not work until the VRRP interface is created and then globally disabled/enabled.

Known limitations and considerations in this release

This section describes issues known to exist in the 8300 Series Software Release 4.0 in the following categories:

Topic
HARDWARE
SOFTWARE
Platform
CLI
NNCLI
Device Manager
Layer 2
QoS
Multicast
Bandwidth management
OSPF
Security
Miscellaneous

CR reference	Description
HARDWARE	
Q00961155	Current Ethernet Routing Switch 8300 software does not support a modular automatic power pruning function. When the total Available Power for allocation is 0 and an additional PoE module is inserted, the additional module will not receive any PoE power even if it is configured with Critical Priority. You must manually admin disable a selected PoE module in order to release the power to the higher priority module.
SOFTWARE	
Platform	
Q01356776	If you use the port mirroring feature while monitoring LLDP packets, the mirrored packets can miss four bytes from ethertype and chassis ID TLV.
Q01439225	The area aggregate will not work if modified or deleted without first disabling or enabling OSPF. OSPF configurations. **Workaround:** If an area aggregate entry is created or modified dynamically, Nortel recommends that you disable and then reenable global OSPF.
Q01403458	Tracing of LLDP task 68 above level 1 to the console blocks Telnet, SNMP, and transmission and reception of LLDP frames, Ping responses and the ability to respond to ARP **Workaround:** If trace level 68 is needed for debugging purposes, Nortel recommends that you run only level 1.
Q01370912	While sending traffic at line rate, a small frame loss can be seen if jumbo frame is enabled. Therefore when this feature is enabled, Nortel recommends not to send traffic from the servers or clients at port line rate.

CR reference	Description
Q01399835	When a large number of very small packets follow the jumbo frames between two 8348GTX or 8348GB modules, packets that are larger than 9000 bytes cannot be prioritized through QOS. **Workaround:** Avoid topology configurations that exacerbate this issue (for example, VOIP and Jumbo Frame Servers transiting the same link).
Q01370691	When running port mirroring, Nortel recommends to have both mirroring and mirrored ports on the same type of IO modules. Otherwise the traffic analyzer may see a 4 byte tag on untagged packets.
Q00803154 Q00803806	The Ethernet Routing Switch 8300 provides limited support for Web management. It provides information for viewing purposes only. Nortel recommends that you do not use Web management for operational network management purposes.
Q01040803	If changing management IP address for the switch, Nortel recommends to do the operation from monitor prompt. Changing it from the command line interface, user may experience some inconsistent behavior.
Q00904970 Q00861897	The **`config bootconfig flags nocheck-sw-version [true|false]`** command is internal use only for troubleshooting purpose. The default value is false. The nocheck-sw-version flag, utilized only during redundant CPU upgrade procedures, is available on the Ethernet Routing Switch 8300. If this flag is changed, it will disable all image consistency checks. The default value of this flag is set to false. Ensure that this flag remains at its default value and is not to be changed except as indicated in the redundant CPU upgrade procedure. To display the current value of nocheck-sw-version, enter the config bootconfig flags info command. This is also true in the boot monitor mode minus the config bootconfig portion of the command syntax. The flag not only determines whether local images match, but also determines if a master CPU will respond to software version queries from a standby CPU. If the flag is set to true on the master and a standby CPU is present at boot or is later inserted with its flag set to false, the standby boot process hangs with no error as it tries to query the master for software versions. Since it is impossible to check the condition of the flag on the hung standby CPU, the only way to determine whether this is happening is to see if a software version query message displays on the master. If the following message is observed on the master console or log (if the log level is set to INFO), the hang problem is caused by something other than the nocheck-sw-version flag state. CPU6 [05/12/04 10:44:53] SW INFO Software version query from 127.0.1.5 version 2.0.0.1/011, running 2.0.0.1/011 The message shows either 127.0.1.5 or 127.0.1.6 depending on the slot the master is in. If this message is not displayed on the master while booting or inserting a second CPU, the hang problem results from the

CR reference	Description
	standby's inability to check the master's software version. To recover in the cleanest possible way, Nortel recommends that you reboot the Ethernet Routing Switch 8300, exit to monitor mode, and set the flag to its default value (false) on both CPUs. If that is too intrusive, setting the flag to false on the master and then resetting the secondary should cause the secondary to finish booting up.
Q00896569	In a redundant CPU configuration, if both the savetostandby and factorydefault boot flags are set to true and the box is rebooted, the factorydefault flag on the secondary CPU comes up as true, even though the factory default value should be false. You should manually adjust this flag. The flags on the primary CPU are set correctly after the boot.
Q00885154	Check both the IP ARP and FDB tables if the following message displays: HAL WARNING NPAL_CreateNhId: could not create next hop x.x.x.x, Status x The message indicates that either the FDB or ARP limits have been exceeded.
Q00851722	When the CP rate limit feature is required on MLT ports, the must configure the rate on all MLT ports manually.
Q01542964	Some ports of 8324GTX will not count LLDP and SONMP into statistics, because of hardware limitations
Q01678495	During a hotswap and hot insertion, LLDP-tx-tlv dot1, dot3 and MED may experience some issues.
Q00788580	The ICMP response time is not reported correctly when a ping to a subnet broadcast command is issued from the Ethernet Routing Switch 8300.
Q00757309	The Ethernet Routing Switch 8300 displays an invalid test result when the port is connected to a 100BASE-T hub or a test port.
Q00755304	When you enable the VCT test, the PHY waits a fixed amount of time before sending out the TDR test pulse. This is to ensure that the link is broken and that the link partner is not sending 10/100/1000Mbps traffic. As soon as the VCT test is finished, the PHY automatically resumes normal operation. This means that auto-negotiation starts again and the link is established. CLI Nortel Ethernet Routing Switch 8300 Series Nortel Ethernet Routing Switch 8300 Release Notes - Software Release 4.0 NN46200-401 03.01 Draft 4.0 5 August 2007 Copyright © 2004-2007, Nortel Networks .

CR reference	Description
Q00848027	If you remove a module and intend to replace it with a different module type, the new module comes up with a default configuration.  **CAUTION** If you do not save the configuration after inserting this module, the next time you reboot the switch, the entire switch comes up with a default configuration. Nortel recommends that you must save your configuration after you insert a new module.
Q01353799	In some rare instances, the deleted host-route displayed in the routing table
Q01389780	The ARP table sometimes did not update with high scaling and traffic.
Q01692535	The pd_detect_type is displayed differently between CLI/NNCLI with JDM, when the POE oper state is off. The CLI/NNCLI is showing the current status, and the JDM is showing the current configuration.
CLI	
Q00957081	When a file is being copied to the flash, 8393SF CPU utilization may show as 100% during the copy.
NNCLI	
Q01010343	In the NNCLI, the command **`eapol re-authenticate`** displays some garbage characters along with the EAP authentication messages.
Q00816522	You cannot display the auto-learned MAC for a specific port in the NNCLI. Instead, it only shows the number of MACs learned. When you enter **`show interfaces vlan autolearn`**, it does not provide an option to specify a port.
Device Manager	
Q00851125	When trace level 3 is turned on, JDM may time out
Q00834504	The p-to-dscp table is not available in the Device Manager. However, it is available in the CLI and NNCLI.
Q00802165	You cannot convert a MAC auto-learned entry to manual via the CLI and NNCLI. You can only do so via the Device Manager using the VLAN > Mac Learning > VlanMacLearning dialog boxes.
Q00780367	In the Device Manager, the DSCP to CoS Map table is missing the column specifying the DSCP value. This option is available in the CLI and NNCLI.
Q01523005	When sending traffic with high speed, there is possibility that the packets count exceeds the up limit of the counter and cause some Policy Statistics not showing out in JDM.
Layer 2	

CR reference	Description
Q01436928	Unlike other IO modules, 8348GB card sends out a shutdown LLDP PDU before it goes down when administratively disabled. This was an added functionality in this module only. Port sends out a Shutdown LLDPDU message when disabled administratively.
Q01041504	You can use decimal as well as hex input for the user-defined PID when configuring user-defined protocol-based VLANs. CLI and NNCLI help text does not indicate that you can use both.
Q00897494	Operations like adding or removing ports on an MLT, or changing STP configuration on the MLT while traffic is flowing, will result in data loss. For unicast traffic, the data loss lasts for 20–30 seconds. For multicast traffic, it may last for 2–3 minutes depending upon the IGMP configuration.
Q00892593	You cannot configure an IP protocol-based VLAN and an ARP-based VLAN on the same port using the user-defined VLAN protocol type 0x0806.
Q00867919	When you use the unknown MAC discard feature on a given port, the first ARP request for an address, including those to be discarded, is processed. This does not impact feature operation. All packets matching the entries to be discarded will not be forwarded by the Ethernet Routing Switch 8300 but will be discarded as expected.
Q00860990	If you remove a module that has associated static FDB or FDB-filter entries, the CLI command **`show vlan info all`** shows information for ports that are no longer present. This is a display issue only and does not affect the operation of the Ethernet Routing Switch 8300.
Q00841632	If you delete selected ports bound to multicast MAC filtering and then source the configuration (**`source config.cfg`**), the deleted ports do not get restored as originally configured. The reason for this is that the MAC is already learned before you source the configuration. Thus, the port does not get added to the MAC.
Q00802887	The autolearned MAC entry does not get re-learned after a conversion to manual entry and deletion until the FDB entry ages out. When you convert, you delete the manually entered MAC entry in the unknown MAC discard table. However, the FDB entry itself is not deleted.
QoS	
Q01407039	When the port mirror is enabled, the normal egress traffic and the mirrored traffic have the same precedence.

CR reference	Description
Q01256112	When two different Scheduling groups are used, traffic flow is not expected. For example, if we are egressing traffic from two 8348GTX-PWR Gigabit ports into one 8348GTX-PWR Gigabit port and the two transmit streams have a QoS level of 3 and 4, if level 3 and 4 have the same scheduling group (say both are dwrr1,dwrr0 or strict priority), then traffic arrives as expected. However, if we change level 3 to DWRR1 and level 4 to DWRR0, the highest priority traffic always has less drops even though it is in a lower scheduling group i.e, 4 has a higher priority even though it has lower scheduling group. There are 8 hardware priority queues. By default, all queues are configured to use DWRR1 scheduling group. It is not recommend that the user change a higher priority queue to use DWRR0 while the lower priority queues still use DWRR1
Q01691602	The Qos egress counter set works abnormally if you add the same port multiple times and then delete it.
Q01691582	The QoS egress counter can configure more than 2 sets on 1 pp of 8308 but sets 3 and 4 cannot work.
Q01654805	On I/O cards based on Value Blade architecture, the qos-shaper setting is per PP based, not per port based
Q01597266	Pathcost will be kept once this port is up and will not change back to default when this port is down again.
Q01513779	ERS 8300 has limited support for policy that is configured with 'Remark-Drop-Precedence' option. In certain IO modules, this functionality is not supported.
Q01576676	When policing traffic, be aware that remark-cos behavior can be different between older and newer modules.
Q01576683	When policing traffic, be aware that remark UP and DSCP behavior can be different between older and newer modules
Multicast	
Q00889744	IGMP static receivers are not supported in the Ethernet Routing Switch 8300.
Q00804941	Rate limiting will become less accurate with frame sizes larger than 64 bytes.
Q00791636	In the NNCLI and CLI, **`show ip igmp interface`** displays the IGMP snoop interfaces. Those interfaces that are not IGMP-enabled are shown as inactive if the interface is IP-enabled, or was previously IGMP snoop enabled.
Q00737617	On an IGMP snoop device, the sender is available only if the traffic is unregistered. In other words, no receiver exists locally on the device. Otherwise, sender information will not be available on a snoop device.
Q01689040	When the remote IST is down, the local SMLT will show SMLT status after 30 seconds to prevent a possible loop.

CR reference	Description
Q01595453	The user cannot flush FDB entries learned on an MLT by flushing MAC on an MLT member.
Q01536016	When running IGMP Snooping in a multicast square SMLT, if one of the IST trunk fails, traffic can be lost and will only recover when the IST trunk comes back up.
Q01548125	Multicast group IP cannot map to the same MAC address as reserved multicast IP. Nortel recommends not to use a multicast group for user traffic for which the MAC address of that multicast IP is mapped to a reserved multicast address.
Q01659446	When IGMP snooping is enabled, NLB multicast mode may flood multicast traffic.
Q01749866	From NNCLI, you will not be able to configure a PIM BSR on a circuitless IP (CLIP). However from regular CLI, you should be able to perform this operation.
Note: The Ethernet Routing Switch 8300 Software Release 4.0 does not support sub-second failover on switch recovery in a Multicast SMLT (MSMLT) environment.	
Bandwidth management	
Q01421840	When connecting a pc behind a i2004 phone and connecting the phone to the 8300 dynamic NSNA port, it takes about 5-20 minutes for the phone to obtain an IP address and indefinitely for the status to be registered. Nortel recommends that you disconnect your pc from the phone (the phone quickly gets an IP and is registered), then reconnect the pc to the phone port (the pc will then obtain a red VLAN IP)
Q01399831	After invoking clear filter statistics command, the stat sometimes show erroneous values.
Q00879816	The VLAN ID range 1–4000 is supported under VLAN configuration for data traffic. The remainder of the VLAN ID range that displays is reserved for network control traffic. Do not configure filters to match the reserved VLAN ID range.
Q00840339	If a traffic policy is applied on multiple ports, these ports should belong to the same FPI. If the policy is applied across multiple I/O modules and multiple ports, the peak information rate/committed information rate (PIR/CIR) is not guaranteed.
Q00831460	A common pool of 128 records exists for both policies (policers) and filter stats. If this pool is exhausted and an additional record is requested, an error message like the following appears: `QOS ERROR gtcmCreateTcEntry:  Failed, status = 20` Should this happen, you need to delete one filter stat instance or policer before adding another.

CR reference	Description
Q00803181	Be aware that you can configure different filter remarking values for ports within an MLT. Nortel recommends configuring the same remarking values across all ports in MLT.
Q00799518	While using remark-user-priority, filter counters and stats may show invalid values.
Q00797808 Q00806856	Partial masking of Access-Template fields is not supported. For example, Access-Template Src Mac field defined as **`00:00:00:ff:ff:ff`** is not a supported configuration.
Q00788755	There is no provision in the Ethernet Routing Switch 8300 Layer 2 commands to look up the DSCP value based on the .p bit.
Q00787044	If you enter **`show filter access-list statistics`** in the CLI when ACE MatchCountMode is disabled, an error message should appear indicating that the feature is not enabled. Currently, the console shows all 0 counters without any traffic or warning messages.
Q00785991	No statistics are available for traffic shaping.
Q00785950	In some configurations, egress counters for multicast traffic show the counter values for unicast traffic when a port belongs to a protocol-based VLAN. In such instances, these counters are not shown under the unicast counter values.
Q00785103	You can apply fdb-filters to ports but they act only on VLANs. For example, if you assign an fdb-filter to a port in a VLAN, all ports in that VLAN will act on the filter. If the port to which the fdb-filter is assigned is disabled or goes down unexpectedly, the filter remains in effect for all other ports in the VLAN.
Q00783246	When you poll statistics for the QoS egress-counter-set, counters are reset to zero. You cannot gather a cumulative number of packets over a period of time using this feature if you execute **`show qos egress-stats`**.
Q00783230 Q00783234	The Policing remarking feature does not work when you use **`remark-user-priority`** for DiffServ remarking.
Q00777622	DiffServ and policing share the same table for DiffServ remarking and policing.
Q00765155	As it appears in the CLI, the maximum value of the committed and peak burst rate is misleading. The Ethernet Routing Switch 8300 shows only a fixed maximum value of 65535, which does not change based on the configuration. The actual maximum value is calculated from the committed and peak information rates.
Q00755441	In the Ethernet Routing Switch 8300, the VLAN QoS level is only supported on protocol-based VLANs.
Q00730427	Be aware that QoS shaping does not perform correctly at lower rates. There is a 10–20% variation in the actual traffic rate as compared with the configured rate.

CR reference	Description
Q00697474	802.1p bits are unchanged at egress if ingress traffic is tagged with override enable. The 802.1p bit is not overwritten for untrusted Layer 2 ports. You can use filters to perform the same functions.
OSPF	
Q01420932	When using two ERS 8300s with two OSPF-enabled interfaces between them, forming OSPF adjacencies, Nortel recommends that you set the transit delay timer to 900 or less. If you set the transit delay higher than 900, the neighbors can get stuck.
Security	
Q01271108	The RADIUS accounting UDP port configuration change cannot be saved. The default port for RADIUS accounting is 1813, which works for all the current RADIUS servers and is the port to use according to RFC's. After a reboot or config source, the port returns to the default of 1813.
Q01054364	Once a user has established a SSH session to an Ethernet Routing Switch 8300, the switch will return an error message when the user attempts to Telnet from the switch to another device.
Q00862936	To disable RADIUS accounting, you must disable RADIUS globally as well as disabling RADIUS accounting. Disabling the RADIUS feature alone does not stop accounting.
Q00819777	Note that tagging and EAP are mutually exclusive. If you enable EAP on a port, using auto or force-authorize, you cannot enable tagging on the port, and vice versa.
Q01379140	Extensive DHCP spoof can cause SSCP to disconnect. User can prevent this problem by adding QOS policy on NSNA filter.
Q01755998	When NSNA is enabled with default filters created for the user, the DHCP request could not be forwarded to CPU as expected. **Workaround:** Nortel recommends the following two options: **Option 1** Manually change the configuration file by replacing the `bootpstrap` with `bootpd-dhcp` in the NSNA default filters. For example: **Procedure steps:** 1. Change **`filter acl 1 ace 1 port dst-port bootpstrap`** to **`filter acl 1 ace 1 port dst-port bootpd-dhcp`** 2. Change **`filter acl 3 ace 1 port dst-port bootpstrap`** to **`filter acl 3 ace 1 port dst-port bootpd-dhcp`** 3. Change **`filter acl 5 ace 1 port dst-port bootpstrap`** to **`filter acl 5 ace 1 port dst-port bootpd-dhcp`** 4. Save the file in the text editor. 5. Reboot the switch with the changed config file.

CR reference	Description

	Option 2
	Modify the NSNA default filters by using either of the following procedures:
	• ***CLI***
	Modify the NSNA default filters in the CLI.
	Procedure steps
	1. Disable NSNA by using the following command:
	`config nsna state disable`
	2. Delete the NSNA default access control groups (ACG) by using the following commands:
	`config filter acg 210 delete`
	`config filter acg 220 delete`
	`config filter acg 230 delete`
	3. Modify the default filters by using the following commands:
	`config filter acl 1 ace 1 port dst-port bootpd-dhcp`
	`config filter acl 3 ace 1 port dst-port bootpd-dhcp`
	`config filter acl 5 ace 1 port dst-port bootpd-dhcp`
	4. Recreate the ACGs for NSNA by using the following commands:
	`filter acg 210 create 1,2 acg-name "red-filter"`
	`filter acg 220 create 3,4 acg-name "yellow-filter"`
	`filter acg 230 create 5,6 acg-name "green-filter"`
	5. Reenable NSNA by using the following command:
	`config nsna state enable`
	• ***NNCLI***
	Modify the NSNA default filters in the NNCLI.
	Procedure steps
	1. Disable NSNA by using the following command from the Global configuration mode:
	`no nsna enable`
	2. Delete the NSNA default ACGs by using the following commands from the Global configuration mode:
	`no filter acg 210`
	`no filter acg 220`
	`no filter acg 230`

CR reference	Description

	3. Modify the default filters by using the following commands from the Global configuration mode:
	`filter acl 1 port 1 dst-port bootpd-dhcp`
	`filter acl 3 port 1 dst-port bootpd-dhcp`
	`filter acl 5 port 1 dst-port bootpd-dhcp`
	4. Recreate the ACGs for NSNA by using the following commands from the Global configuration mode:
	`filter acg 210 1,2 acg-name "red-filter"`
	`filter acg 220 3,4 acg-name "yellow-filter"`
	`filter acg 230 5,6 acg-name "green-filter"`
	5. Reenable NSNA by using the following command from the Global configuration mode:
	`nsna enable`

Miscellaneous	
Q01314902	Some IP multicast streams may flood all ports when IGMP snooping was enabled.
Q01140665	BGP only fields that are not applicable to RIP under the CLI Route Policies node are being displayed and need to be hidden or removed.
Q01131665	A `save config` success message may follow a failure message. **Recovery:** Check flash to ensure sufficient free space and then re do the save config.
Q00784096	If you configure a port shaper on an output port and multiple flows with different priorities are egressing through this port, one flow can monopolize the entire bandwidth up to the shaper rate configured on that port. **Workaround:** Nortel recommends that you use shaper on a per-queue basis.
Q00773426	If you enable port mirroring on a tagged interface, the mirrored packets will not contain the 802.1Q header.
Q01221206	48 port 10/100/1000 8348GTX & 8348GTX-PWR module hardware takes approximately 90 seconds per board during initial DLD upload to come online. Online is defined as the start of the module insert to completion and system message stating "HW INFO Finished insertion for slot x" of config load (default config).
Q01398967	On one occasion, an error message: HAL WARNING NPAL_AddNHToCreateBulkList:, appeared indicated that it could not allocate the next hop.

Reading path

This section lists the documentation specific to the Ethernet Routing Switch 8300 platform. For information on finding and accessing up-to-date documentation, see

Important information

- *Nortel Ethernet Routing Switch 8300 Important Notice — 8300 Series Modules* (NN46200-603)
- *Read Me First for the Ethernet Routing Switch 8310 Chassis* (318192-C)
- *Nortel Ethernet Routing Switch 8300 Important Notice — Administration and Security* (NN46200-601)

Chassis and module installation

- *Nortel Ethernet Routing Switch 8300 Installation — Fan Tray* (NN46200-302)
- *Nortel Ethernet Routing Switch 8300 Installation — AC Power Supply* (NN46200-301)
- *Nortel Ethernet Routing Switch 8300 Installation — Chassis Installation and Maintenance* (NN46200-304)
- *Nortel Ethernet Routing Switch 8300 Installation — Modules (NN46200-305)*
- *Nortel Ethernet Routing Switch 8300 Installation — SFPs and XFPs* (NN46200-307)

Related publications

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

Installation and User Guides

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

- *Nortel Ethernet Routing Switch 8300 Installation — MAC Addresses* (NN46200-600)
- *Nortel Ethernet Routing Switch 8300 Configuration — Power over Ethernet* (NN46200-512)
- *Nortel Ethernet Routing Switch 8300 Installation and Commissioning — Quick Start* (NN46200-100)
- *Nortel Ethernet Routing Switch 8300 Installation — Fan Tray* (NN46200-302)
- *Nortel Ethernet Routing Switch 8300 Installation — AC Power Supply* (NN46200-302)

- *Nortel Ethernet Routing Switch 8300 Installation — Chassis Installation and Maintenance* (NN46200-304)
- *Nortel Ethernet Routing Switch 8300 Fundamentals — Using Device Manager* (NN46200-508)
- *Nortel Ethernet Routing Switch 8300 Installation — Modules* (NN46200-305)
- *Nortel Ethernet Routing Switch 8300 Installation — SFPs and XFPs* (NN46200-307)
- *Nortel Ethernet Routing Switch 8300 Planning — Power Considerations* (NN46200-511)
- *Nortel Ethernet Routing Switch 8300 Upgrades — Software Release 4.0* (NN46200-400)
- *Nortel Ethernet Routing Switch 8300 — Troubleshooting* (NN46200-704)

Reference and Configuration Guides

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

- *Nortel Ethernet Routing Switch 8300 Command Reference — CLI* (NN46200-513)
- *Nortel Ethernet Routing Switch 8300 Command Reference — NNCLI* (NN46200-306)
- *Nortel Ethernet Routing Switch 8300 Configuration — Security using Device Manager* (NN46200-508)
- *Nortel Ethernet Routing Switch 8300 Configuration — Security using the NNCLI and CLI* (NN46200-503)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using Device Manager* (NN46200-505)
- *Nortel Ethernet Routing Switch 8300 Configuration — IP Routing and Multicast Operations using the NNCLI and CLI* (NN46200-500)
- *Nortel Ethernet Routing Switch 8300 Configuration — Network Management using NNCLI, CLI, and Device Manager* (NN46200-502)
- *Nortel Ethernet Routing Switch 8300 Configuration — QoS and Filter using the CLI* (NN46200-506)
- *Nortel Ethernet Routing Switch 8300 Configuration — QoS and Filter using Device Manager* (NN46200-507)
- *Nortel Ethernet Routing Switch 8300 Configuration — QoS and Filter using the NNCLI* (NN46200-501)
- *Nortel Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (NN46200-509)

- *Nortel Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using Device Manager* (NN46200-510)
- *Nortel Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI* (NN46200-504)
- *Nortel Ethernet Routing Switch 8300 Configuration — Platform Operations* (NN46200-602)
- *Nortel Ethernet Routing Switch 8300 Planning and Engineering Network Design Guidelines* (NN46200-200)
- *Nortel Ethernet Routing Switch 8300 Command Reference — NNCLI* (NN46200-306)
- *Nortel Ethernet Routing Switch 8300 Fault Management — System Messaging Platform Reference* (NN46200-701)
- *Nortel Ethernet Routing Switch 8300 — Troubleshooting* (NN46200-704)

Hard-copy technical manuals

You can download current versions of technical documentation for your Ethernet Routing Switch 8300 from the Nortel customer support web site at

If, for any reason, you cannot find a specific document, use the Search function:

Step	Action
1	Click **Search** at the top right-hand side of the web page. The **Search** page appears.
2	Ensure the **Support** tab is selected.
3	Enter the title or part number of the document in the **Search** field.
4	Click **Search**.

—End—

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site: www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region: www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to: www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Nortel Ethernet Routing Switch 8300

Release Notes - Software Release 4.0

Publication: NN46200-401
Document status: Standard
Document version: 03.04
Document date: 22 February 2008

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback

Sourced in Canada and the United States of America.

The information in this document is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering or manufacturing may warrant.