



Nortel Ethernet Routing Switch 8300 Series

Nortel Ethernet Routing Switch 8300 Release Notes - Software Release 3.0

Document status: Standard
Document version: 02.01
Document date: 28 September 2006

Copyright © 2004-2006, Nortel Networks
All Rights Reserved.

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.

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

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

2. **Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.
3. **Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The 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 3.0 Release Notes	7
Introduction	7
File names for this release	8
Ensuring Device Manager Online Help displays correctly	9
Upgrading the switch to Release 3.0 software	10
Before upgrading the switch from a previous release	10
Note about DLD files	11
Upgrade procedures	12
New Ethernet Routing Switch 8300 hardware	13
8348GB module	13
New software features in this release	13
Platform	14
Reliability/Resiliency	16
Supported software and hardware capabilities	19
Supported Standards (IEEE, RFCs and others)	21
Ethernet Routing Switch 8010/8006 chassis support	25
Supported SFPs	25
Hot-removal/hot-insertion of Ethernet Routing Switch 8300 modules	27
Hot-removal of master CPU	27
Problems resolved in this release	28
Known limitations and considerations in this release	31
Reading path	44
Important information	44
Chassis and module installation	44
Related publications	44
Hard-copy technical manuals	46
How to get help	47

Ethernet Routing Switch 8300 Release 3.0 Release Notes

Introduction

These release notes for the Nortel* Ethernet Routing Switch 8300 (formerly known as Passport 8300) Software Release 3.0 describe the hardware and software and any known issues that exist in this release. They are based on Ethernet Routing Switch 8300 Software Release 3.0 and Java Device Manager (Device Manager) 6.0.2.0.

A list of related publications can be found on "[Reading path](#)" (page 44). The Ethernet Routing Switch 8300 Software Release 3.0 documentation suite can be found on the documentation CD included with your software or on the Nortel technical documentation Web site, www.nortel.com/support. For more information, see the "[Reading path](#)" (page 44).

The following topics are discussed in this document:

Topic
"File names for this release" (page 8)
"Upgrading the switch to Release 3.0 software" (page 10)
"New Ethernet Routing Switch 8300 hardware" (page 13)
"New software features in this release" (page 13)
"Supported software and hardware capabilities" (page 19)
"Problems resolved in this release" (page 28)
"Known limitations and considerations in this release" (page 31)
"Reading path" (page 44)
"Hard-copy technical manuals" (page 46)
"How to get help" (page 47)

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 3.0 software files and the hardware they support.

Ethernet Routing Switch 8300 Software Release 3.0 files and associated hardware

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	p83b3000.img	1074451
Run-time image	Flash, PCMCIA, or TFTP. The Ethernet Routing Switch 8300 image.	p83a3000.img	6816131
Input/output modules download file	Flash 8300 I/O Module Image	p83r3000.dld	2229928
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	p83f3000.img	230786
Software licensing file Note: Refer to "Accessing the License file" in <i>Nortel Ethernet Routing Switch 8300 Upgrades - Software Release 3.0</i> (NN46200-400) for details on how to access and configure the license file.	Flash, PCMCIA or TFTP Note: Needed to activate advance features (OSPF, VRRP and SMLT)	license.dat	varies

Ethernet Routing Switch files			
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.	p83a3000.mib.zip p83a3000.mib	486570 3044950
md5 checksum file	Flash or PCMCIA. MD5 checksums of all release 3.0.0 software files	p83a3000.md5	477
SNMP encryption file (required for SNMPv3)	Flash or PCMCIA Note: Available only on the Nortel web site www.nortel.com/support	p83c3000.aes	26960
3DES encryption file (required for SSH)	Flash or PCMCIA Note: Available only on the Nortel web site www.nortel.com/support	p83c3000.img	55976

JDM Images			
Solaris for SPARC image	Device manager software image	jdm_6020_solaris_sp arc.sh	167069058
Microsoft Windows image	Device manager software image	jdm_6020.exe	141559337
Linux image	Device manager software image	jdm_6020_linux.sh	167658882
HP Unix image	Device manager software image	jdm_6020_hpux_pa-r isc.sh	182404482

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 making a context call to on-product Help, perform the following procedure once before requesting 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 Explorer** in the Rendering Engine area of the window.
7. Click **OK** to close the Options - Site Controls window.

Upgrading the switch to Release 3.0 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 3.0, you must do the following:

- Consult *Important Security Information for the 8300 Series Switch* (216512-C) 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 3.0* (NN46200-400).
- Take special note of the following cautionary messages:
 - The configuration file generated with software release 3.0 contains options that are not backward-compatible with software release 2.3.x or earlier. Loading a 3.0.0.0 configuration file on a 2.3.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:

```
copy 111.111.1.11:p83a3000.img /flash/p83a3000.img
```

If the server is not available, or if the file on the server does not exist, the p83a3000.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**

Make sure your files are copied correctly to the flash. Nortel recommends that the MD5 checksum be used. Refer to "MD5 Command" in Nortel Ethernet Routing Switch 8300 Upgrades - Software Release 3.0 (NN46200-400).

- When installing files on the onboard flash or PCMCIA, ensure that you 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.

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 will not be downloaded to the I/O boards.

- On boot up, if a DLD file is not configured in boot.cfg, the CP code will search 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 will search 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 will be loaded.
```



CAUTION

Do not interrupt the DLD download once it has started or failure could occur.

—End—

Upgrade procedures

Refer to *Nortel Ethernet Routing Switch 8300 Upgrades - Software Release 3.0 (NN46200-400)* for the detailed procedures to upgrade the switch.

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

New Ethernet Routing Switch 8300 hardware

This section describes the new Ethernet Routing Switch 8300 Release 3.0 hardware.

New hardware	Module part number	Where to find information
"8348GB module" (page 13) 48-port 1000BASE-SFP	DS1404095-E5	<i>Nortel Ethernet Routing Switch 8300 Installation - Modules (NN46200-305)</i>

8348GB module

The 8348GB module provides 48 1000BASE-X (SFP) ports. You can use the ports on the SFPs to make riser connections, server attachments, or interswitch links. The 8348GB module supports standards-based 1000 Mb/s.

Note 1: The 8348GB module requires Release 3.0.0 or later versions of the software to operate in a Ethernet Routing Switch 8300 switch.

Note 2: LLDP-enabled 8348GB port is capable of sending a Shutdown LLDPDU message before shutting down when administratively disabled.

For more information regarding the 8348GB 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)*
- *Important Information for the 8300 Series Switch Modules (216511-E)*

New software features in this release

This section describes the new software features for the Ethernet Routing Switch 8300 Software Release 3.0.

Feature	Description
Platform	
"EAP support on tagged ports" (page 14)	New feature
"SNMP service support in access policy" (page 14)	New feature

Feature	Description
Platform	
"Software Licensing" (page 15)	New feature introduced in 3.0
"Jumbo Frames" (page 15)	New feature introduced in 3.0

Reliability/Resiliency	
"SMLT/SLT with Ping Snoop" (page 16)	New feature introduced in 3.0
"OSPFv2 (RFC 1850)" (page 17)	New feature introduced in 3.0
"VRRP (RFC 2787)" (page 18)	New feature introduced in 3.0

Security	
"Nortel Secure Network Access" (page 18)	Merged with the 2.2.8 release with added support of the 48 10/100/ 1000 and 48 Gig SFP modules

Convergence	
"802.1AB (LLDP)" (page 19)	New feature introduced in 3.0

Platform

EAP support on tagged ports

The Ethernet Routing Switch 8300 implements Extensible Authentication Protocol (EAP) for authenticating devices connected to access (untagged) ports. This feature extends the support for EAP to tagged ports. With IP phones implementing 802.1x supplicant, it is required to support tagged frames coming from the IP phone.

This feature allows the user to enable EAP on tagged ports. The enhancement also provides guest VLAN support and multiple clients per port, on tagged ports. The Guest VLAN feature allows the users connected on the port with EAP enabled to have guest network access on the switch until they are authenticated. With multi-host feature enabled, more than one client can be connected on an EAP enabled port. Each of these clients has to be authenticated in order to gain network access on the switch.

SNMP service support in access policy

The access policy feature in Ethernet Routing Switch 8300 determines the access level for the users connecting to the switch with different services like FTP, TFTP, Telnet, rlogin etc. The system access-policy feature is based on the access-levels and the network address of the user. It covers services like TFTP, HTTP, SSH, rlogin, SNMP. However with SNMP-v3

engine, the community names do not map on to an access-level but the access privileges are determined only through the VACM (Variable Access Control Model) configuration.

The new enhancement allows the user to specify groups for the SNMP access policy which enables SNMP to be covered under the access policy services. Since the access restriction is based on groups defined through the VACM model, the synchronization will be made using the snmp-v3 VACM configuration. This feature enables the administrator to bind these groups along with the security level to an access-policy..

Software Licensing

You will now need to access the software license file to activate advanced features such as OSPF, VRRP and SMLT. For more information on software licensing, refer to *Nortel Ethernet Routing Switch 8300 Upgrades - Software Release 3.0 (NN46200-400)* and *Nortel Ethernet Routing Switch 8300 Configuration - Platform Operations (NN46200-602)*.

Jumbo Frames

This release introduces the use of Jumbo Frames, the purpose of which is to support Data Frames with sizes up to 10,240 bytes.

Note: The following limitations apply to this feature:

- Only boards with Gigabit Ethernet ports can support jumbo frames.
- QoS does not work for frame sizes that exceed 9000.
- Traffic rate only supports up to 95 percent of the load
- Jumbo frames that cascade through multiple 8348GTX ports (from one switch through another) may experience some packet loss
- Mixed traffic comprising of Jumbo frames and small frames on the same link may drop some small frames that are less than 128 bytes

	8393SF	8324GTX	8324FX	8348TX/ 8348TXP WR	8348GTX/ 8348GTXP WR	8348GB
8393SF	Supported	Supported	Not Supported	Not Supported	Supported (with some limitations)	Supported
8324GTX	Supported	Supported	Not Supported	Not Supported	Supported (with some limitations)	Supported
8324FX	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

	8393SF	8324GTX	8324FX	8348TX/ 8348TXP WR	8348GTX/ 8348GTXP WR	8348GB
8348TX/ 8348TX-P WR	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
8348GTX/ 8348GTX- PWR	Supported (with some limitations)	Supported (with some limitations)	Not Supported	Not Supported	Supported (with some limitations)	Supported (with some limitations)
8348GB	Supported	Supported	Not Supported	Not Supported	Supported (with some limitations)	Supported

For more information on Jumbo Frames, refer to *Nortel Ethernet Routing Switch 8300 Configuration - Platform Operations* (NN46200-602).

Reliability/Resiliency

SMLT/SLT with Ping Snoop

The Split Multi-Link Trunking (SMLT) and the Single port SMLT (SLT) allows the Ethernet Routing Switch 8300 to deliver increased available bandwidth, dramatically increasing network availability and resiliency designed for unified communications architecture.

SMLT Network resiliency is the most basic requirement when implementing a converged network. The network needs to be available to be able to support the applications whose ultimate promise is increasing the bottom line. The Ethernet Routing Switch 8300 addresses resiliency at multiple levels for maximum coverage. At the hardware level, the Ethernet Routing Switch 8300 provides hot swappable modules including fan trays and N+1 power supplies. The Ethernet Routing Switch 8300 software ensures resiliency for the network core with industry-leading features like Split Multi-Link Trunking (SMLT) and VRRP Active/Active.

Connectivity within the network often relies on trunks or groups of ports connecting disparate areas of the network. The resiliency of these trunks can mean the difference between a highly available network and a network plagued with outages and crippling delays. Multi-Link Trunking support allows up to four ports to be grouped into a single trunk, providing increased bandwidth and resilient connections. Split Multi-Link Trunking combines the increased bandwidth of MLT with industry-leading resiliency. SMLT allows desktop or access switches to be dual homed/connected to Ethernet Routing Switch 8300s in the network core and have all links active. This innovative technology delivers a solution that provides increased bandwidth as well as sub-second failover.

SLT Single port SMLT (SLT) lets you configure a split multi-link trunk using a single port per Ethernet Routing Switch 8300. SLT behaves just like an MLT-based SMLT and can coexist with SMLTs in the same system. SLT lets you scale the number of split multilink trunks on a switch to a maximum number of available ports.

Up to 399 SLT are supported in this Ethernet Routing Switch 8300 release. The maximum number of SLT depends on the number of ports in the entire 8300 system. For more information on these features, refer to the following documents:

- *Nortel Ethernet Routing Switch 8300 Configuration - VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI* (NN46200-504)
- *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)

Ping Snoop The Ping-Snoop feature is a diagnostics utility used for troubleshooting MLT/ SMLT networks.

For more information on the Ping Snoop feature, refer to *Nortel Ethernet Routing Switch 8300 Performance Management — Diagnostics Tools using NNCLI and CLI* (NN46200-700) and *Nortel Ethernet Routing Switch 8300 Performance Management — Diagnostics Tools using Device Manager* (NN46200-702).

OSPFv2 (RFC 1850)

The Open Shortest Path First (OSPF) protocol is an interior gateway protocol (IGP) intended for use in large networks. Using a link state algorithm, OSPF exchanges routing information between routers in an autonomous system. Routers synchronize their topological databases. After the routers are synchronized and the routing tables built, routers flood the topology information only in response to some topological change. For OSPF, the “best” path to a destination is the path that offers the least-cost metric delay. In OSPF, cost metrics are configurable, allowing users to specify preferred paths.

Routers keep a table of “reachability information” containing a list of networks and routers. The table is maintained with current information via a regular exchange of hello packets. OSPF is a link-state protocol. A router running a link-state protocol periodically tests the status of the physical connection to each of its neighbor routers and sends this information to its other neighbors. A link-state protocol does not require each router to send its entire routing table to its neighbors. Instead, each OSPF router floods only link-state change information throughout the autonomous system

(or area, if the AS is divided into areas). This process is referred to as the synchronization of the routers' topological databases. With the link information, each router builds a shortest-path tree with itself as the root of the tree. It then can identify the shortest path from itself to each destination and build its routing table.

With the support of OSPF, Redistribution Policies have been updated to include direct, static, RIP and OSPF.

For more information about this feature, refer to 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)*

VRRP (RFC 2787)

Nortel Ethernet Routing Switch 8300 is now fully compliant with the latest Virtual Router Redundancy Protocol (VRRP) implementation (including the standard VRRP MIB support).

For more information about VRRP, 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)*

Security

Nortel Secure Network Access The Nortel Secure Network Access (NSNA) Manager is a solution where the edge devices (ERS 55xx/ERS8300) and the Nortel Secure Network Access Switch (NSNAS) will work in coordination to authenticate and give access of network resource to a user. NSNAS is a special device, which can serve multiple edge devices in a network and maintains user profile and authentication state. NSNAS can be the proxy agent for the DNS as well as a relay agent for the DHCP. NSNAS will also talk to Radius at the back end.

With the 3.0 release, Nortel ERS 8300 supports NSNA Release 1.1 on every module – including the latest high density gig copper – 48 10/100/1000 – as well as the new 3.0 module – 48 SFP ports.

For a complete description of the Nortel Secure Network Access solution, please refer to 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)*

Convergence

802.1AB (LLDP) This new protocol, defined by IEEE as LLDP or Link Layer Discovery Protocol is used for topology discovery and capability advertising between networking devices (end stations like IP phones included) connected together:

- Identifying interconnection points
- Populating the physical topology and device discovery MIBS

The information distributed using this protocol is stored by the different stations – including PCs, IP Phones, switches, routers or any interconnection device – in a standard Management Information Base (MIB), making it possible for the information to be accessed by a network management system or application (NMS).

Switches like the 8300 can act based on the information received – typically assign the Voice VLAN when a port is connected to an IP phone.

For more information on 802.1AB, refer to *Nortel Ethernet Routing Switch 8300 Configuration - Platform Operations* (NN46200-602).

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 3.0 and JDM 6.0.2.0 of the Ethernet Routing Switch 8300 Series software. These capabilities will be enhanced in subsequent software releases.

Feature	Maximum number supported
VLANs	Up to 2047 VLANs; 200 have been tested and are officially supported in Release 3.0 Note: The range of valid ID numbers is greater than the maximum number of supported VLANs. The range for VLAN IDs is 1- 4000.

Feature	Maximum number supported
Protocol-based VLANs ARP records	12 records, 50 VLANs maximum 2500
IP interfaces	Up to 512 IP interfaces; 200 have been tested and are officially supported in Release 3.0
Local next hops	500
Static routes	1000
Spanning Tree groups	Up to 64; groups 1 through 25 have been tested and are officially supported in Release 3.0
Aggregation groups <ul style="list-style-type: none"> 802.3ad static aggregation groups 	31 <ul style="list-style-type: none"> 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
Ports per aggregation group Note: All the ports MUST be of the same type (no mix of technology is supported)	4
IGMP maximum number of unique groups	1500
RIP scaling	<ul style="list-style-type: none"> 8 routed VLANs 750 RIP routes 500 ARP entries 1500 MAC entries 8 STGs
EAPoL 802.1x supplicants	Up to 3072 supplicants; 128 have been tested and are officially supported in Release 3.0

Feature	Maximum number supported
RADIUS MAC centralization clients	Up to 3072 clients; 64 have been tested and are officially supported in Release 3.0
OSPF	<ul style="list-style-type: none"> • 5 Areas • 80 Adjacencies • 4000 Routes
SMLT/SLT	SMLT=31 SLT=399
VRRP	128 instances
LLDP 802.ab	384 neighbors

Note: Jumbo Frames are supported in Release 3.0. You can now use the `mtu` command in the NNCLI Global configuration mode.

Supported Standards (IEEE, RFCs and others)

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

Supported Standards	
802.1ab	IEEE 802.1ab
802.3 CSMA/CD Ethernet ISO/IEC 8802	ISO/IEC 8802.3
802.3i 10BaseT	ISO/IEC 8802.3
802.3u 100BaseT	ISO/IEC 8802.3
802.3z	Gigabit Ethernet
802.3ab	Gigabit Ethernet 1000Base T 4 pair Cat5 UTP
802.1q and 802.1p	VLAN tagging and prioritization
802.3x	Flow Control
802.1d	MAC bridge/spanning tree protocol
802.1X	EAPOL

Supported IPv4 standards	
RFC 768	UDP protocol
RFC 783	TFTP protocol
RFC 791	IP protocol
RFC 792	ICMP protocol

Supported IPv4 standards	
RFC 793	TCP protocol
RFC 826	ARP protocol
RFC 854	Telnet protocol
RFC 903	Reverse ARP protocol
RFC 1058	RIPv1 protocol
RFC1112	IGMPv1 protocol
RFC1541/1542, updated by RFC2131	Bootp/DHCP protocols
RFC1812	Router requirements
RFC1866	HTMLv2 protocol
RFC 2068	Hypertext Transfer Protocol
RFC 2138/2139	RADIUS Authentication/RADIUS Accounting
RFC 2326	IGMPv2 protocol
RFC 1850	OSPFv2 protocol
RFC 2787	VRRP (Virtual Router Redundancy Protocol)
RFC2353	RIPv2 protocol
RFC2819	RMON (Remote Monitoring) Alarms, Events, Statistics & Groups

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 will contain 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

Standard MIB name	RFC	File name
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: 8300 supports Alarms, Events, Statistics & History	RFC1757/RFC2819	rfc1757.mib
OSPF Version 2 Management Information Base	RFC1850	rfc1850.mib
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

Standard MIB name	RFC	File name
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

Proprietary MIB name	File name
Rapid City MIB	rapid_city.mib
SynOptics Root 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 4096 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 1024 to 4096. For more information about this kit, see *Adding MAC Addresses to the Passport 8000 Series Chassis (212486-B)*.
2. The Ethernet Routing Switch 8300 switch fabric modules (8393SF) 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.

Supported SFPs

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

SFP order number	SFP type	Wavelength
AA1419013	LC type 1000BASE-SX	550m
AA1419014	MT-RJ type 1000BASE-SX	550m
AA1419015	LC type 1000BASE-LX	5Km

SFP order number	SFP type	Wavelength
AA1419025	1470nm/Gray 1000BASE CWDM	40Km
AA1419026	1490nm/Violet 1000BASE CWDM	40Km
AA1419027	1510nm/Blue 1000BASE CWDM	40Km
AA1419028	1530nm/Green 1000BASE CWDM	40Km
AA1419029	1550nm/Yellow 1000BASE CWDM	40Km
AA1419030	1570nm/Orange 1000BASE CWDM	40Km
AA1419031	1590nm/Red 1000BASE CWDM	40Km
AA1419032	1610nm/Brown 1000BASE CWDM	40Km
AA1419034	1490nm/Violet 1000BASE CWDM	70Km
AA1419035	1510nm/Blue 1000BASE CWDM	70Km
AA1419036	1530nm/Green 1000BASE CWDM	70Km
AA1419037	1550nm/Yellow 1000BASE CWDM	70Km
AA1419038	1570nm/Orange 1000BASE CWDM	70Km
AA1419039	1590nm/Red 1000BASE CWDM	70Km
AA1419040	1610nm/Brown 1000BASE CWDM	70Km
AA1419043	RJ-45 Type 1000BASE-T	100m

SFP order number	SFP type	Wavelength
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	100m
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	100m

For detailed information about SFPs, refer to *Installing SFP and XFP Transceivers and GBICs* (318034-D).

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 8393 SF module for management, add a virtual IP address. The virtual IP address will allow 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 re-insert 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 will not contain the removed CPU configuration. You will then need to reconfigure the CPU ports.

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

Problems resolved in this release

"[Problems resolved, by type of issue](#)" (page 28) describes issues that have been fixed since the 8300 Series Release 2.3 in the following categories:

Topic
Platform
Device Manager
NNCLI
Layer 2
Miscellaneous

CR reference	Description
SOFTWARE	
Platform	
Q01313950	The EAP port state can now be set to force-auth from either force-unauth or auto when EAP is disabled globally.
Q01326368	An EAP enabled tagged port now moves 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 disabled state of the syslog host is retained.
Q01343042-02	Simultaneous link state changes on multiple ports are now logged properly.

CR reference	Description
SOFTWARE	
Platform	
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 now matches the incoming packets.
Q01374779-01	Configuring a syslog host with a severity level of INFO no longer causes system instability.
Q01243757 Q01232899	STP now converges properly after CPU failover.
Q01201638/ Q01201638-01	The RSA key generated when SSH is enabled, will no longer be printed on the CLI.
Q01237128	The allocated power for PoE no longer shows a negative value.
Q01189519	The port utilization values are now calculated properly by including the Preamble and Inter-Frame Gap.
Q01254489	Changes to NTP interval now takes effect from the next synchronization cycle. Also changes to NTP interval will take effect properly across reboot.
Q01193827	The 8348TX and 8348TXPoE modules no longer erroneously report InternalMacReceiveErrors upon toggling the link state.
Q01234950-01	The maximum configurable value for RADIUS server retry time is now 20 seconds.
Q01226753 Q01226761-01	Non EAP Clients can now be authenticated successfully when multiple Radius servers are configured.
Q01265501	CPU utilization values are now calculated correctly on an Ethernet Routing Switch 8300.
Q01282637	If an ACE is configured with both Acelid and Precedence set to the same value, the precedence value of an ACE no longer sets to the default value after reboot.
Q01237567-01	On an Ethernet Routing Switch 8300, traffic from the management port will no longer be forwarded to the internal network.
Q01311357	VRRP Hello packets can sometimes be delayed by up to 8 seconds.
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.
Device Manager	
Q01349008	In the JDM and LLDP, AddrPortsTxEnable port numbers are off by one. Workaround: The correct display is available using the CLI.
NNCLI	
Q01405645	Removal of group access from the V3 VACM table is not preserved after reboot.

CR reference	Description
SOFTWARE	
Platform	
LAYER 2	
Q01386745	A conflict between arp table and MAC table intermittently occurred.
Q01397092	When flapping the route protocol within a VLAN with broadcast rate limiting configured, the VLAN which enabled RIP/OSPF sometimes did not transfer broadcast data. Workaround: Avoid route protocol flapping in conjunction with broadcast rate limiting
Q01386733	Learned MAC entries aged out before the configured aging time is reached.
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	Access policies can only be configured by users with RWA access level.
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	The default access policy can no longer be deleted.
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.

CR reference	Description
SOFTWARE	
Platform	
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. Workaround: Ignore error messages.
Q01384936	The save config verbose sometimes caused a delay in configuring the load SNMP V3 section. Workaround: Do not do a save config in the verbose mode
Q01398967	On one occasion, an error message: HAL WARNING NPAL_AddNHToCreateBulkList:, appeared indicated that it could not allocate the next hop.
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: 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: Keep 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: Keep Transmit Delay at 3000 or less.

Known limitations and considerations in this release

This section describes issues known to exist in the 8300 Series Software Release 3.0 in the following categories:


Topic
HARDWARE
SOFTWARE
CLI
NNCLI
Device Manager
Layer 2
QoS
Multicast
Bandwidth management

Topic
Security
Miscellaneous

CR reference	Description
HARDWARE	
Q01398031	Attempting to do a 8348GB hotswap disables udpforwarding.
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.
Q01420932	When using two ERS 8300s with two OSPF-enabled interfaces between them, forming OSPF adjacencies, do not set the transit delay to more than 900. Setting the transit delay greater than 900 in this instance will cause the neighbor state to remain in ExchangeStart and not continue on.Q01420932
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.
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	Port Mirroring modifies the transmitted LLDP packets.
Q01439225	The area aggregate will not work if modified or deleted without first disabling or enabling OSPF.
Q01060954	Doing an MIB-walk and performing a trace level 25 3 or 4 on the console causes SNMP to timeout.
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 ARPs.

CR reference	Description
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. Workaround: Monitor the traffic on either the same IO board or a different board that is not an 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. Workaround: Configure SMLT links on I/O modules. In a dual CPU configuration IST links should also be configured on I/O modules. In a single CPU configuration IST links may be configured on the CPU module.
Q01369125	When a large number of very small packets follows the jumbo frames between two 8348GTX modules, packets loss occurs on the 8348GTX with the Jumbo Frame enable command. Workaround: Avoid topology configurations that exacerbate this issue (for example, VOIP and Jumbo Frame Servers transiting the same link).
Q01370912	When a large number of very small packets follow the jumbo frames between two 8348GTX modules, low performance occurs under mixed size traffic with the JF enable Workaround: Avoid topology configurations that exacerbate this issue (for example, VOIP and Jumbo Frame Servers transiting the same link).
Q01399835	When a large number of very small packets follow the jumbo frames between two 8348GTX or 8348GB modules, the QoS does not work when packets size > 9000 Workaround: Avoid topology configurations that exacerbate this issue (for example, VOIP and Jumbo Frame Servers transiting the same link).
Q01370691	When the mirrored port is on a module other than 8348GB or 8348GTX and the analyzer port is on the 8348GB or 8348GTX module, the egress mirroring adds a VLAN tag. Workaround: When mirroring packets, both mirrored and monitoring ports must be on same module.
Q01219890	LogtoPcmcia configurations are not saved across reboots when set to FALSE in the PCMCIA.
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.
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.
Q01040803	On devices with IP interfaces (IP-enabled VLANs), you cannot change the management IP address back to default (0.0.0.0/0) using config bootconfig net mgmt. You can make this change only from the monitor prompt during boot or if the device does not have IP-enabled VLANs.

CR reference	Description
<p>Q00904970 Q00861897</p>	<p>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..</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p> <p>The message shows either 127.0.1.5 or 127.0.1.6 depending on the slot the master is in. If this message is not displayed on the master while booting or inserting a second CPU, the hang problem results from the standby's inability to check the master's software version. To recover in the cleanest possible way, 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.</p>
<p>Q00896569</p>	<p>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.</p>
<p>Q00885154</p>	<p>Check both the IP ARP and FDB tables if the following message displays: HAL WARNING NPAL_CreateNhld: could not create next hop x.x.x.x, Status x</p> <p>The message indicates that either the FDB or ARP limits have been exceeded.</p>

CR reference	Description
Q00862905	If egress counter statistics are attached to an MLT port and a VLAN ID has been assigned to those statistics, remove the statistics before performing any negative operations on that MLT. Negative operations include such items as removing and reinserting the module, and link down and link up. Otherwise, the port will be removed from the MLT and the only way to add it back is to first remove the statistics.
Q00853775	Do not use a virtual interface index, such as an MLT group or VLAN, when gathering statistics or error information. If you wish to monitor such an interface, use the appropriate physical port(s) index.
Q00851722	Be aware that changing CP limit settings on a single port belonging to an MLT does not change the settings for the other ports in the MLT. You need to make the change for all the ports belonging to that MLT.
Q00848027	<p>If you remove a module and intend to replace it with a different module type, the new module comes up with a default configuration.</p> <div style="border: 1px solid black; padding: 5px;">  <p>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.</p> </div>
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	
Q01334778	There is no way to display VLAN interface OSPF statistics in CLI even though device manager allows you to do so. Workaround: Use the show ip ospf stats [mismatch] [detail] command to display the OSPF interface state.
Q01153279 Q01153288	There are grammar and spelling errors in the descriptions for various RIP commands and options. Refer to <i>Nortel Ethernet Routing Switch 8300 Configuration - IP Routing and Multicast Operations using the NNCLI and CLI (NN46200-500)</i> for the correct descriptions.
Q01145231	The command <code>save config verbose</code> causes a 0.0.0.0 mgmt-virt-address to be saved.

CR reference	Description
Q00957081	When a file is being copied to the flash, CPU utilization may show as 100% during the copy.
Q00876505 Q0855057	When you enter <code>show ports error, ospf [<ports>]</code> displays in the CLI help as one of the available options. The Ethernet Routing Switch 8300 does not support this option.
Q00876390	When you enter some commands under <code>config sys access-policy policy <number> service, ssh</code> 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.
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.
Q00876423	Jumbo Frames is supported in Release 3.0 but you must use the bootconfig flags <code>jumboframe</code> command in the NNCLI Global configuration mode to enable Jumbo Frame support on the chassis.
Q01153279 Q01153288	There are grammar and spelling errors in the descriptions for various RIP commands and options. Refer to <i>Nortel Ethernet Routing Switch 8300 Configuration - IP Routing and Multicast Operations using the NNCLI and CLI (NN46200-500)</i> for the correct descriptions.
Q01010343	In the NNCLI, the command <code>eapol re-authenticate</code> 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 <code>show interfaces vlan autolearn</code> , it does not provide an option to specify a port.
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 <code>config sys access-policy enable false</code> command. In NNCLI use the <code>access-policy disable</code> 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.
Q00862945	Be aware that the Device Manager may time out after converting MAC entries and refreshing the Allowed MAC table.

CR reference	Description
Q00851125 Q00831569 Q00831575	If trace is enabled, you may experience Device Manager timeouts. You cannot avoid this problem completely. You can minimize it, however, by increasing the Device Manager timeout interval.
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.
Q00793639	When using the Device Manager, the hourglass pointer may appear unexpectedly directly over the column headers. If you move the mouse to areas where the tabs for functions exist, the hourglass does not appear and the Device Manager operates normally.
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.
Layer 2	
Q01436928	The 8348GB port sends out a Shutdown LLDPDU message when disabled administratively
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 Workaround: Reconnect the MLT groups in a smooth flow and avoid overlapping them.
Q01386746	The MAC table intermittently does not age out.
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.

CR reference	Description																				
Q00883592	<p>If you create an IP VLAN that belongs to a subnet represented by an existing static route, the following error message may display:</p> <pre>IP ERROR rcIpModifyNextHop: Arp pointer is NULL for route: x.x.x.x mask: x.x.x.x</pre> <p>The new local route should take over as the best route in the route table. If so, you can ignore this error.</p>																				
Q00867919	<p>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.</p>																				
Q00860990	<p>If you remove a module that has associated static FDB or FDB-filter entries, the CLI command <code>show vlan info all</code> 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.</p>																				
Q00841632	<p>If you delete selected ports bound to multicast MAC filtering and then source the configuration (<code>source config.cfg</code>), 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.</p>																				
Q00806545	<p>For byProtocol VLANs, a certain number of "protocol-type" values are restricted (invalid), because the preconfigured VLAN types (IP/IPX/AppleTalk) already use these values.</p> <p>The table below lists the currently restricted hex values for preconfigured VLAN protocol types.</p> <table border="1" data-bbox="523 1388 1323 1822"> <thead> <tr> <th data-bbox="523 1388 999 1440">Protocol type</th> <th data-bbox="999 1388 1323 1440">Hex value</th> </tr> </thead> <tbody> <tr> <td data-bbox="523 1440 999 1482">XNS</td> <td data-bbox="999 1440 1323 1482">0600</td> </tr> <tr> <td data-bbox="523 1482 999 1524">IP</td> <td data-bbox="999 1482 1323 1524">0800</td> </tr> <tr> <td data-bbox="523 1524 999 1566">BANYAN VINES</td> <td data-bbox="999 1524 1323 1566">0BAD</td> </tr> <tr> <td data-bbox="523 1566 999 1608">DEC LAT</td> <td data-bbox="999 1566 1323 1608">6004</td> </tr> <tr> <td data-bbox="523 1608 999 1650">RARP</td> <td data-bbox="999 1608 1323 1650">8035</td> </tr> <tr> <td data-bbox="523 1650 999 1692">SNA Ethernet2</td> <td data-bbox="999 1650 1323 1692">80D5</td> </tr> <tr> <td data-bbox="523 1692 999 1734">AppleTalk</td> <td data-bbox="999 1692 1323 1734">809B, 80F3</td> </tr> <tr> <td data-bbox="523 1734 999 1776">IPv6</td> <td data-bbox="999 1734 1323 1776">86DD</td> </tr> <tr> <td data-bbox="523 1776 999 1818">IPX Ethernet2, IPX SNAP</td> <td data-bbox="999 1776 1323 1818">8137, 8138</td> </tr> </tbody> </table>	Protocol type	Hex value	XNS	0600	IP	0800	BANYAN VINES	0BAD	DEC LAT	6004	RARP	8035	SNA Ethernet2	80D5	AppleTalk	809B, 80F3	IPv6	86DD	IPX Ethernet2, IPX SNAP	8137, 8138
Protocol type	Hex value																				
XNS	0600																				
IP	0800																				
BANYAN VINES	0BAD																				
DEC LAT	6004																				
RARP	8035																				
SNA Ethernet2	80D5																				
AppleTalk	809B, 80F3																				
IPv6	86DD																				
IPX Ethernet2, IPX SNAP	8137, 8138																				

CR reference	Description																
	<p>The table below lists additional protocol types, from the IANA Protocol Types listing (http://www.iana.org/assignments/ethernet-numbers), whose hex values are restricted:</p> <table border="1" data-bbox="523 478 1321 831"> <thead> <tr> <th data-bbox="523 478 1002 531">Protocol type</th> <th data-bbox="1002 478 1321 531">Hex value</th> </tr> </thead> <tbody> <tr> <td data-bbox="523 531 1002 573">BANYAN VINES Loopback</td> <td data-bbox="1002 531 1321 573">0BAE</td> </tr> <tr> <td data-bbox="523 573 1002 615">BANYAN VINES Echo</td> <td data-bbox="1002 573 1321 615">0BAF</td> </tr> <tr> <td data-bbox="523 615 1002 657">DEC unassigned</td> <td data-bbox="1002 615 1321 657">8039-803C</td> </tr> <tr> <td data-bbox="523 657 1002 699">DEC Ethernet Encryption</td> <td data-bbox="1002 657 1321 699">803D</td> </tr> <tr> <td data-bbox="523 699 1002 741">DEC unassigned</td> <td data-bbox="1002 699 1321 741">803E</td> </tr> <tr> <td data-bbox="523 741 1002 783">DEC LAN Traffic Monitor</td> <td data-bbox="1002 741 1321 783">803F</td> </tr> <tr> <td data-bbox="523 783 1002 825">DEC unassigned</td> <td data-bbox="1002 783 1321 825">8040-8042</td> </tr> </tbody> </table>	Protocol type	Hex value	BANYAN VINES Loopback	0BAE	BANYAN VINES Echo	0BAF	DEC unassigned	8039-803C	DEC Ethernet Encryption	803D	DEC unassigned	803E	DEC LAN Traffic Monitor	803F	DEC unassigned	8040-8042
Protocol type	Hex value																
BANYAN VINES Loopback	0BAE																
BANYAN VINES Echo	0BAF																
DEC unassigned	8039-803C																
DEC Ethernet Encryption	803D																
DEC unassigned	803E																
DEC LAN Traffic Monitor	803F																
DEC unassigned	8040-8042																
Q00802887	<p>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.</p>																
QoS																	
Q01407039	<p>When the port mirror is enabled, the normal egress traffic and the mirrored traffic have the same precedence.</p>																
Q01256112	<p>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.</p> <p>Note: There are eight hardware priority queues. By default, all queues are configured to use DWRR1 scheduling group. Nortel does not recommend that users change a higher priority queue to use DWRR0 while the lower priority queues still use DWRR1. This change will cause improper operation of hardware scheduling.</p>																
Multicast																	
Q00889744	<p>IGMP static receivers are not supported in the Ethernet Routing Switch 8300.</p>																
Q00843934	<p>Traffic filters for IGMP join and leave packets are not effective if the port belongs to one or more IGMP interfaces.</p>																

CR reference	Description
Q00841340	Rate limiting configured on an inactive MLT port will not be effective for the traffic flowing over that MLT.
Q00810524	When performing broadcast/multicast rate limiting on an ingress port, if the bandwidth of the egress ports is significantly less than that of the ingress ports (e.g., 1G -> 100M or 100M -> 10M), then the egress ports may drop even more than requested. This occurs only when the ingress burst rate is greater than the egress ports.
Q00804941	Rate limiting will become less accurate with frame sizes larger than 64 bytes. The minimum effective rate limiting on 10Mbps is 6%. 10Mbps rate limiting is done in blocks of 6%.
Q00791636	In the NNCLI and CLI, <code>show ip igmp interface</code> 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.
Q00788415	The Ethernet Routing Switch 8300 does not drop joins from a client whose IP address matches the VLAN IP itself.
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.
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.
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. Workaround: 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)
Q01407654	When using the <code>show nsna client</code> command, some IP addresses are not listed as part of the NSNA client or the SNAS server even though they are registered.
Q01399831	Clearing filter statistics results in corrupted filter statistics. Workaround: Reboot switch to correct the filter statistics.
Q01378041	When default NSNA filters are modified on 8348GTX ports, IPC PCL filter error messages are generated on the switch console. Workaround: Nortel recommends that modifications be done before NSNA is globally enabled or ignore error messages as they will stop once NSNA filter modifications are completed.

CR reference	Description
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: <pre>QOS ERROR gtcCreateTcEntry: Failed, status = 20</pre> <p>Should this happen, you need to delete one filter stat instance or policer before adding another.</p>
Q00813681	When using <code>config qos egress-counter-set</code> , the NNCLI does not allow you to configure a VLAN, even though <code>VLAN</code> appears to be a valid command option. As a workaround, configure without specifying a VLAN to ensure that the egress counters are created properly.
Q00803181	Be aware that you can configure different filter remarking values for ports within an MLT.
Q00799518	Filter counter/stats do not work when you use remark-user-priority for DiffServ remarking.
Q00797808 Q00797811 Q00806856	Partial masking of Access-Template fields is not supported. For example, Access-Template Src Mac field defined as <code>00:00:00:ff:ff:ff</code> 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 <code>show filter access-list statistics</code> 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.

CR reference	Description
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 <code>show qos egress-stats</code> .
Q00783230 Q00783234	The Policing remarking feature does not work when you use <code>remark-user-priority</code> 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.
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.
Security	
Q01435536	In the CLI and NNCLI, the EAPOL session is not terminated when the VLAN with authenticated client is deleted
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.

CR reference	Description
Q01017469- 01	When you create a user in SNMPv3 by entering the command <code>config snmp-v3 usm Manager md5 pass</code> and you remove the initial password by entering the command <code>config snmp-v3 usm delete initial</code> , you must enter the command <code>auth Manager old-pass pass new-pass pass</code> to make it work.
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.
Miscellaneous	
Q01393096	While doing a Windows tracert (tracert utility) command from PC1 to PC2 with the 8348GTX between them, the traceroute times-out on the first hop (8300 ip address) but is able to reach the destination ip address and shows the tracert as complete. The destination ip address can be pinged successfully including the interface on the 8348GTX.
Q01314902	Some IP multicast streams may flood all ports when IGMP snooping was enabled.
Q01354262	When the ping snoop feature is edited via JDM, information in CLI does not change. Note: The Ping Snoop feature is only supported via CLI & NNCLI
Q01424477	Although ping-virtual-address is enabled by default, the feature does not work until the VRRP interface is created and then globally disabled or 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 <code>save config</code> success message may follow a failure message. Recovery: Check flash to ensure sufficient free space and then re do the save config.
Q01395019	Using SNMPv3, the switch intermittently resets due to the use of the JDM with a .des file from a previous release. Workaround: When running Device Manager, use the .aes file distributed with this release.
Q01386755	The panic ring buffer overflows intermittently. This may occur during startup in a fully populated chassis. The system will recover without user intervention.
Q01227117	Creation of a non-zero length prefix for SNMPv3 cannot be allowed for group-access entry because non-zero length prefixes are not supported. Also, the switch cannot be accessed with non-zero length prefixes.

CR reference	Description
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. As a 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 three minutes 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).

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 ["Hard-copy technical manuals"](#) (page 46).

Important information

- *Important Information for the 8300 Series Switch Modules (216511-C)*
- *Read Me First for the Ethernet Routing Switch 8310 Chassis (318192-C)*
- *Important Security Information for the 8300 Series Switch (216512-B)*
- *Important Notice for the 8000 Series Switch PCMCIA Card (318844-A)*

Chassis and module installation

- *Installing a Fan Tray in an Ethernet Routing Switch 8300 Series Chassis (316798-B)*
- *Installing the Ethernet Routing Switch 8300 AC Power Supply (316797-C)*
- *Installing and Maintaining the Ethernet Routing Switch 8306 and 8310 Chassis (316795-C)*
- *Nortel Ethernet Routing Switch 8300 Installation - Modules (NN46200-305)*
- *Installing GBIC and Gigabit SFP Transceivers (318034-A)*

Related publications

This section describes common documentation related to 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.

- *Adding MAC Addresses to the Passport 8000 Series Chassis (212486-B)*
- *Configuring Power over Ethernet (317337-C)*
- *Getting Started (316799-C)*
- *Installing a Fan Tray in an Ethernet Routing Switch 8300 Series Chassis (316798-B)*
- *Installing the Ethernet Routing Switch 8300 AC Power Supply (316797-C)*
- *Installing and Maintaining the Ethernet Routing Switch 8306 and 8310 Chassis (316795-C)*
- *Installing and Using Device Manager (316808-C)*
- *Nortel Ethernet Routing Switch 8300 Installation - Modules (NN46200-305)*
- *Installing GBIC and Gigabit SFP Transceivers (318034-A)*
- *Nortel Ethernet Routing Switch 8300 Planning - Power Considerations (NN46200-511)*
- *Nortel Ethernet Routing Switch 8300 Upgrades - Software Release 3.0 (NN46200-400)*
- *Using Device Manager Diagnostic Tools (317359-C)*

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 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)*

- *Configuring Network Management using the NNCLI, CLI, and Device Manager (316803-C)*
- *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)*
- *Using NNCLI and CLI Diagnostic Tools (317222-B)*

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 www.nortel.com/support.

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 opens.
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—

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

How to get help

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 for assistance.

If you purchased a Nortel service program, contact Nortel Technical Support. To obtain contact information online, go to the www.nortel.com/contactus web page and click Technical Support.

Information about the Nortel Technical Solutions Centers is available from the www.nortel.com/callus web page.

An Express Routing Code (ERC) is available for many Nortel 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 the ERC for your product or service, go to the www.nortel.com/erc web page.

Nortel Ethernet Routing Switch 8300 Series

Nortel Ethernet Routing Switch 8300 Release Notes - Software Release 3.0

Copyright © 2004-2006, Nortel Networks
All Rights Reserved.

Publication: NN46200-401
Document status: Standard
Document version: 02.01
Document date: 28 September 2006

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.

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

