Part No. 316811-D
June 2005

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Ethernet Routing Switch 8300 Software Release 2.2

NORTEL

Nortel Networks Inc. software license agreement

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

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

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

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

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The 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

Introduction

These release notes for the Nortel* Ethernet Routing Switch 8300 (formerly known as Passport 8300) Software Release 2.2 describe the hardware and software and any known issues that exist in this release. They are based on Ethernet Routing Switch 8300 Software Release 2.2 and Java Device Manager (Device Manager) 5.9.2.0.

A list of related publications can be found on page 52. The Ethernet Routing Switch 8300 Software Release 2.2 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" on page 52.

The following topics are discussed in this document:

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

File names for this release

Table 1 describes the Ethernet Routing Switch 8300 Software Release 2.2 software files and the hardware they support.

Table 1 Ethernet Routing Switch 8300 Software Release 2.2 files and associated hardware

Module or file type	Description	File name	File size (bytes)
Boot monitor image	CPU and switch fabric firmware for the Ethernet Routing Switch 8300. Supported on Ethernet Routing Switch 8393SF modules	p83b2200.img	1071565
Runtime image	The Ethernet Routing Switch 8300 image. Supported on Ethernet Routing Switch 8393SF modules	p83a2200.img	5795216
Pre-boot monitor image	Pre-boot monitor image	p83f2200.img	230786
MIB (private)	Ethernet Routing Switch 8300 private MIB	p83a2200.mib	2035197
MIB zip file	Ethernet Routing Switch 8300 MIB	p83a2200.mib.zip	322157
md5 checksum file	md5 checksums of all Release 2.2 software files	p83a2200.md5	477
Input/output modules download file	Supported on Ethernet Routing Switch 8348TX, 8348TX-PWR, 8324FX, and 8324GTX	p83r2200.dld	1664168
Encryption module for SNMPv3 (includes DES encryption capabilities) **Note:** Available only on the Nortel web site (www.nortel.com/support)	Supported on the Ethernet Routing Switch 8393SF modules	p83c2200.des	8638
Encryption module for SSH (includes 3DES encryption capabilities) **Note:** Available only on the Nortel web site (www.nortel.com/support)	Supported on the Ethernet Routing Switch 8393SF modules	p83c2200.img	52424

Table 1 Ethernet Routing Switch 8300 Software Release 2.2 files and associated hardware

Module or file type	Description	File name	File size (bytes)
Java Device Manager software image for Windows (Version 5.9.2.0)	Device Manager software image for Windows NT, Windows XP, Windows 2003, Windows 2000	jdm_5920.exe	110977058
Java Device Manager software image for UNIX (Version 5.9.2.0)	Device Manager software image for Solaris	jdm_5920_solaris_sparc.sh	129097258
	Device Manager software image for HP-UX	jdm_5920_hpux_pa-risc.sh	157998634
Java Device Manager software image for Linux (Version 5.9.2.0)	Device Manager software image for Linux	jdm_5920_linux.sh	131522090
Readme file	Device Manager readme file	readme_v5.9.2.0.txt	3295

Upgrading the switch to Release 2.2 software

Before upgrading the switch from a previous release

Before upgrading to Ethernet Routing Switch 8300 Software Release 2.2, take special note of the following cautionary messages.

- The configuration file generated with Ethernet Routing Switch 8300 Software Release 2.2 software may contain options that are not backward compatible with any prior release.
- After you upgrade your Ethernet Routing Switch 8300 series software, make sure you save the configuration file.
- When installing files on the on-board flash or PCMCIA, make sure that you verify flash capacity before downloading the files.
- As a precaution, before you upgrade or downgrade your switch software, make a copy of the switch configuration file specified in the boot.cfg file using the following CLI command:

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

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

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:

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.
   (CR Q01086305, Q01148710)

Upgrade procedures

Refer to *Upgrading to Ethernet Routing Switch 8300 Software Release 2.2* (318769-C) 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

Table 2 describes the new Ethernet Routing Switch 8300 hardware in this release.

Table 2 New Ethernet Routing Switch 8300 hardware

New hardware	Module part number	Where to find information
8324FX (24-port 100FX) module	DS1404098	*Installing Ethernet Routing Switch 8300 Series Modules* (316796-C)

8324FX module

The 8324FX module provides 24 100BASE-FX ports requiring MT-RJ connectors. The module is non-blocking. Each 100BASE-FX port can operate only in full-duplex mode. The optical transceivers provide transmission ranges of up to 6562 ft (2 km) using 62.5 µm multimode fiber cable, or 4264 ft (1.3 km) using 50 µm multimode fiber cable. The 8324FX module provides Far End Fault Indication (FEFI) capability that identifies when the far end of the transmit fiber becomes disconnected.

New software features in this release

Ethernet Routing Switch 8300 Software Release 2.2 provides the following new features or feature improvements:

IP routing (Layer 3)

Routing Information Protocol (RIP) v1/v2

Routing Information Protocol (RIP) is a standard, dynamic routing protocol based on the Bellman-Ford (or distance vector) algorithm. It is used as an Interior Gateway Protocol (IGP). Ethernet Routing Switch 8300 Software Release 2.2 supports the use of RIP to exchange information with other routers to compute routes through an IPv4-based network. RIP is defined in RFC 1058 for RIP version 1 and RFC 2453 for RIP version 2.

Each router maintains a routing table, which lists the optimal route to every destination in the system. Each participating RIP router advertises its routing information by sending a routing information update at regular intervals. Neighboring routers use this information to recalculate their routing tables and retransmit the routing information. It is possible to maintain optimal routes for the entire system by using only information obtained from neighboring entities.

For information about configuring RIP, see *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B) or *Configuring IP Routing and Multicast Operations using Device Manager* (317338-B).

Route policies

The Ethernet Routing Switch 8300 can apply a number of filters to IP traffic to manage accept and announce policies for routing table information. Route policies can apply to direct, static, and RIP routes. The filtering process relies on IP prefix lists in the common routing table manager infrastructure.

For more information, see *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B) or *Configuring IP Routing and Multicast Operations using Device Manager* (317338-B).

UDP forwarding

The UDP forwarding feature is used to create protocols for forwarding UDP broadcasts from one IP interface to other router IP interfaces, or to a configured server IP address. This allows UDP broadcasts to be forwarded to an interface or server that includes additional services, as necessary.

For more information, see *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B) or *Configuring IP Routing and Multicast Operations using Device Manager* (317338-B).

Circuitless IP (CLIP)

Circuitless IP (CLIP) is a virtual (or loopback) interface that is not associated with any physical port. You can use the CLIP interface to provide uninterrupted connectivity to your switch as long as there is an actual path to reach the device. The CLIP interface functions like any other IP interface. The network associated with the CLIP interface is treated as a local network attached to the device. This route always exists and the circuit is always up because there is no physical attachment.

For more information, see *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B) or *Configuring IP Routing and Multicast Operations using Device Manager* (317338-B).

Other IP routing enhancements

- ICMP router discovery

  For more information, see *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B) or *Configuring IP Routing and Multicast Operations using Device Manager* (317338-B).

- IP forwarding

  For more information, see *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B) or *Configuring IP Routing and Multicast Operations using Device Manager* (317338-B).

- IP proxy ARP

  For more information, see *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B) or *Configuring IP Routing and Multicast Operations using Device Manager* (317338-B).

- IP static route to subnets not directly connected

  For more information, see *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B) or *Configuring IP Routing and Multicast Operations using Device Manager* (317338-B).

Security

SSH v1/v2 and Secure Copy

Secure Shell (SSH) is a client/server protocol that allows you to conduct secure communications over a network. SSH replaces remote logon utilities such as Telnet with an encrypted alternative. SSH supports a variety of the public/private key encryption schemes available. Using the public key of the host server, the client and server negotiate to generate a session key known only to the client and the server. This one-time key is then used to encrypt all traffic between the client and the server.

Secure CoPy (SCP) is a secure file transfer protocol. SCP replaces remote access utilities such as FTP with an encrypted alternative.

SSH protocol, version 2 (SSH v2) is a complete rewrite of the SSH v1 protocol. SSH v1 contains multiple functions in a single protocol. SSH v2 divides the functions among three layers:

- SSH Transport Layer (SSH-TRANS)

  The SSH transport layer manages the server authentication and provides the initial connection between the client and the server. Once established, the transport layer provides a secure, full-duplex connection between the client and server.

- SSH Authentication Protocol (SSH-AUTH)

  The SSH authentication protocol authenticates the client-side user to the server. SSH-AUTH defines three authentication methods: public key, host-based, password.

  SSH-AUTH provides a single authenticated tunnel for the SSH connection protocol.

- SSH Connection Protocol (SSH-CONN)

  SSH-CONN provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections.

For more information, see *Configuring and Managing Security using the NNCLI and CLI* (316804-C) or *Configuring and Managing Security using Device Manager* (317346-C).

802.1x enhancements (RADIUS MAC centralization)

This feature allows the centralization of MAC addresses for non-EAP clients (typically IP phones). An enable/disable flag is provided at the system level to globally enable or disable the RADIUS MAC centralization feature. Enabling RADIUS MAC centralization at port level takes effect only if the global flag is enabled.

With `allow-non-eap-clients` enabled, traffic from the unauthorized host is allowed on the port. To allow access for the non-EAP clients, the MAC address of that client must be added to the non-EAP MAC list. The MAC address (username) of the client that is to be allowed access to the network, and the corresponding password, must be configured on the RADIUS server. Traffic from clients that do not have a MAC address in the non-EAP MAC undergo RADIUS-based MAC authentication.

For a non-EAP client to be authenticated with RADIUS-based MAC authentication, an Access-Request packet is sent to the RADIUS server with the username and password attributes. If an entry is present for the non-EAP user, then the RADIUS server authenticates the user by sending an Access-Accept packet to the switch.

Traffic from a non-EAP client that does not have a MAC address present in the non-EAP MAC, and that cannot be authenticated by the RADIUS server, is discarded and a log message is generated.

For more information, see *Configuring and Managing Security using the NNCLI and CLI* (316804-C) or *Configuring and Managing Security using Device Manager* (317346-C).

RADIUS accounting

RADIUS accounting logs all of the activity of each remote user in a session to the centralized RADIUS accounting server.

When a client (typically a Network Access Server [NAS]) is configured to use RADIUS accounting, it sends an accounting-start packet to the RADIUS accounting server at the beginning of a session. The accounting-start packet contains a description of the service being delivered, and the user to whom it is being delivered. The RADIUS accounting server returns an acknowledgement that the packet has been received.

At the end of the session, the client sends an accounting-stop packet describing the type of service that was delivered. Optional statistics, such as elapsed time and input/output packets, can also be bundled in the accounting-stop packet. The RADIUS accounting server again returns an acknowledgement that the packet has been received.

For more information, see *Configuring and Managing Security using the NNCLI and CLI* (316804-C) or *Configuring and Managing Security using Device Manager* (317346-C).

TACACS+

The Ethernet Routing Switch 8300 supports the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ is a security application implemented as a client/server-based protocol that provides centralized validation of users attempting to gain access to a router or NAS.

TACACS+ differs from RADIUS in two important ways:

- TACACS+ is a TCP-based protocol
- TACACS+ uses full packet encryption, rather than just encrypting the password (RADIUS authentication request)

Note: TACACS+ encrypts the entire body of the packet, but uses a standard TACACS+ header.

TACACS+ provides management of users who access a device through any of the management channels: Telnet, rlogin, SSH v1, and SSH v2.

During the login process, the TACACS+ client initiates TACACS+ authentication and authorization sessions with the server.

For more information, see *Configuring and Managing Security using the NNCLI and CLI* (316804-C) or *Configuring and Managing Security using Device Manager* (317346-C).

CLI advanced tracking and logging

The CLI advanced tracking and logging feature encrypts and logs CLI and NNCLI commands in a PCMCIA file, which is accessible only to the RWA user. The CLI/NNCLI command logging feature provides a secured logging mechanism within the switch.

For more information, see *Managing Platform Operations* (317350-C).

Serviceability/Manageability

Far End Fault Indicator (FEFI)

FEFI is a feature available only on the 8324FX module, which is a 100BaseFX interface that does not support auto-negotiation. FEFI allows a local station to notify its link partner that a remote fault has occurred. The remote station then diagnoses which end of the link has the fault. For more information, see *Configuring Network Management using the NNCLI, CLI, and Device Manager* (316803-C).

Network Time Protocol (NTP)

The NTP feature is a protocol that allows synchronization of the local clock with an external clock. The Ethernet Routing Switch 8300 implements NTP as a client in unicast mode only.

For more information, see *Managing Platform Operations* (317350-C).

New commands and messages

Ethernet Routing Switch 8300 Software Release 2.2 adds a number of new CLI and NNCLI commands and system messages to enhance serviceability and management.

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

- *CLI Command Line Reference for the Ethernet Routing Switch 8300* (317360-C)
- *NNCLI Command Line Reference for the Ethernet Routing Switch 8300* (316810-C)
- *System Messaging Platform Reference Guide* (316806-C)

MD5 enhancement to calculate MD5 digest

The MD5 command calculates the MD5 digest for files on the switch's flash or PCMCIA. The output displays on the screen or can be stored in a file specified by the user. The command has an option to compare the calculated MD5 digest against a checksum file on flash or PCMCIA and display the compared output to the screen. By verifying the MD5 checksum, administrators can check if the file has been transferred properly to the switch. This command is available from both the boot monitor and runtime CLI.

The MD5 file (p83a2200.md5) provided with the Release 2.2 software contains the MD5 checksums of all Release 2.2 software files. Transfer your image files to the switch and use the MD5 command to ensure that the checksum of the images on the switch is the same as the checksum file.

For more information about using the MD5 checksum command, see *Upgrading to Ethernet Routing Switch 8300 Software Release 2.2* (318769-C).

Supported software and hardware capabilities

Table 3 lists the known limits for the Ethernet Routing Switch 8300 Software Release 2.2 and JDM 5.9.2.0 of the Ethernet Routing Switch 8300 Series software. These capabilities will be enhanced in subsequent software releases.

Table 3 Supported capabilities in the 8300 Series (Release 2.2)

Feature	Maximum number supported
VLANs	Up to 2047 VLANs; 200 have been tested and are officially supported in Release 2.2 **Note:** The range of valid ID numbers is greater than the maximum number of supported VLANs. The range for VLAN IDs is 1-4000.
Protocol-based VLANs	12 records, 50 VLANs maximum
ARP records	2500
IP interfaces	Up to 512 IP interfaces; 200 have been tested and are officially supported in Release 2.2
Local next hops	500
Static routes	1000
Spanning Tree groups	Up to 64; groups 1 through 25 have been tested and are officially supported in Release 2.2
Aggregation groups • 802.3ad static aggregation groups	31 • For 8348TX and 8324FX ports, you can use only Link Aggregation Groups 1-7 • For 8324GTX ports and CP I/O ports, you can use Link Aggregation Groups 1-31
Ports per aggregation group **Note**: All the ports MUST be of the same type (no mix of technology is supported)	4
IGMP maximum number of unique groups	2000
RIP scaling	• 8 routed VLANs • 750 RIP routes • 500 ARP entries • 1500 MAC entries • 8 STGs

Table 3 Supported capabilities in the 8300 Series (Release 2.2) (continued)

Feature	Maximum number supported
EAPoL 802.1x supplicants	Up to 3072 supplicants; 128 have been tested and are officially supported in Release 2.2
RADIUS MAC centralization clients	Up to 3072 clients; 64 have been tested and are officially supported in Release 2.2

Note: Jumbo Frames are not supported in Release 2.2. Thus, you should not use the **`mtu`** command in the NNCLI Global configuration mode. (Q00876423)

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 require 4096 media access control (MAC) addresses to use the Ethernet Routing Switch 8300 modules. The upgrade kit (DS1411015) that allows you to increase the MAC addresses on your Ethernet Routing Switch 8300 to a total of 4096 MAC addresses is available for this purpose. For more information about this kit, see *Adding MAC Addresses to the Passport 8000 Series Chassis* (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 module in the 8010 or 8006 chassis. Be aware, however, that when the 8348TX-PWR module is operating in the 8010 or 8006 chassis, it operates as an Ethernet Routing Switch 8348TX module.

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

Table 4 lists the transceivers supported by the Ethernet Routing Switch 8300.

Table 4 Supported SFP transceivers

Model	Product number
SFP transceivers:	
1000BASE-SX (LC Type)	AA1419013
1000BASE-SX (MT-RJ Type)	AA1419014
1000BASE-LX (LC Type)	AA1419015
1000 BaseT SFP (RJ-45)	AA1419043

Table 4 Supported SFP transceivers (continued)

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

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:

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.

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 *Network Design Guidelines* (316809-C).

Problems resolved in this release

Table 5 describes issues that have been fixed since the 8300 Series Release 2.1 in the following categories:

Table 5 Problems resolved, by type of issue

CR reference	Description
Hardware and platform	
Q00885284	If a login fails after three attempts when using the console port on a standby CPU, the console port locks for 60 seconds. At the end of 60 seconds, the lock is released, and the login prompt displays again. You no longer need to use Telnet or reset the standby CPU in order to unlock the console port.
Q00745966	If VCT test results show a normal status, you should ignore the values displayed in the PairErrLength field. They are not applicable.
CLI	
Q01029341, Q01006243-03	If PCMCIA logging is enabled and the remaining space in the /pcmcia directory is less than the required minimum, the SMP Logging error messages no longer repeat on the CLI. To enable logging when you swap a PCMCIA card, execute the following command: **`config log logToPCMCIA true`**

Table 5 Problems resolved, by type of issue (continued)

CR reference	Description
Q00884051	In the CLI and NNCLI, the Ethernet Routing Switch 8300 now supports commands to trace route policies. In the CLI, the command is **`trace route-policy`**. In the NNCLI, the command is **`trace route-map`**. However, the Ethernet Routing Switch 8300 does not support all parameters displayed on the switch. More generally, all route policies parameters related to OSPF and BGP are not supported in this release. The Ethernet Routing Switch 8300 Software Release 2.2 supports only direct, static, and RIP routes.
NNCLI	
Q00836588	When using RADIUS, all accounting data is now sent when you use the NNCLI. You can see all start, stop, on, off, and interim messages.
Q00842478	The current running status of the management port (speed, duplex, etc.) can now be displayed from the NNCLI using **`show bootconfig net`**.
Q00884051	In the CLI and NNCLI, the Ethernet Routing Switch 8300 now supports commands to trace route policies. In the CLI, the command is **`trace route-policy`**. In the NNCLI, the command is **`trace route-map`**. However, the Ethernet Routing Switch 8300 does not support all parameters displayed on the switch. More generally, all route policies parameters related to OSPF and BGP are not supported in this release. The Ethernet Routing Switch 8300 Software Release 2.2 supports only direct, static, and RIP routes.
Q00883983	The NNCLI help for **`no radius-server`** no longer displays `snmp` as an option.
Device Manager	
Q00867889	When viewing results under the VLAN tab for Bridge > Forwarding, you no longer see *unknown:6* displayed for MACs. The display now shows that it is a MAC discard.
Q00867972	In the Device Manager, when you convert a dynamically learnt MAC entry to manual edit, the Auto Learn tab now updates automatically. After selecting VLAN > MAC Learning > Auto Learn, choosing Auto Learn Action (default if none), highlighting the MAC entry, and clicking Apply to convert the entry to manual, you no longer need to exit the menu in order to refresh the list of MAC entries showing on the Auto Learn tab.
Q00870918	When you perform an internal loopback test on Ethernet Routing Switch 8393 data ports (for example, 5/7 and 5/8), the Device Manager, like the CLI, now shows an operating speed of 0.
Q00870966	When you select multiple ports in the Device Manager using Edit > Port, all valid tab options are available. The same tab options are available whether you are editing single or multiple ports.
Q00887001	In the Device Manager, when MLT ports are highlighted under the EAPoL tab, the Port Initialize and Port Reauthenticate fields now correctly display whether the parameter has been set to True or False.

Table 5 Problems resolved, by type of issue (continued)

CR reference	Description
Security	
Q01040742	You cannot reset the `max-non-eap-clients` parameter to a value lower than the current number of non-eap clients on the port. As a result, the `max-non-eap-clients` parameter always sets the upper limit for the number of allowable non-EAP clients. You can no longer get up to 8 non-EAP MACs through an EAP port when the value of the `max-non-eap-clients` parameter is decreased from a previously set value.
Layer 2 VLANs	
Q01045465	The Device Manager no longer allows you to violate the rule that a port cannot belong to more than one user-defined protocol-based VLAN with the same PID.
Q00889957	When you create user-defined, protocol-based VLANs with non-default optional parameters, such as name, color, and encapsulation, the protocol ID you define is now saved in the configuration file.
QoS	
Q00802732	Disabling the p-bit override changes a learned FDB entry's QoS level.
Filters	
Q00826795	You no longer need to keep ACL names to 15 characters or less. Longer ACL names will not cause a mis-alignment of fields when displaying the ACL. In addition, an ACL with a traffic type other than routed, bridged, or all will not cause a field mis-alignment.
IGMP	
Q00810854	The Ethernet Routing Switch 8300 no longer accepts joins when a client sends an IGMP report with a source address from a different subnet than the VLAN's subnet.
Miscellaneous	
Q00896254	The command to save disabled port mirrors used to execute in two stages: the port mirror was first saved as enabled, then disabled. A disabled port mirror is now saved directly as disabled.
Q00890827	If you enable fast-start on a port that is added or removed from an MLT, fast-start no longer becomes disabled on that port. As a result, you do not need to re-enable fast-start on that port.
Q00863759	Granting SNMP login via access policies has been removed. SNMP access to the switch is now governed by SNMPv3 user profiles. For information about configuring SNMP users, groups, and communities, see *Configuring and Managing Security using the NNCLI and CLI* (316804-C) or *Configuring and Managing Security using Device Manager* (317346-C).

Table 5 Problems resolved, by type of issue (continued)

CR reference	Description
Q00850119	The CP limit ability to shut down a port is not reduced when more than four ports are in the same VLAN.
Q00846062	Port error stats used to display in a column labelled `FCS Errors`. This was misleading, because the count includes FCS, CRC, and align errors. The label has now been changed to `FCS/Alignment Errors`.

Known limitations and considerations in this release

Table 6 describes issues known to exist in the 8300 Series Software Release 2.2 in the following categories:

Table 6 Known limitations, by type of issue

CR reference	Description
HARDWARE	
Q00988540	A copper SFP installed in an 8393 SFP port will only support 1000 Mbps speed and full duplex. Therefore, it cannot be connected to any device that only supports speeds of 100 Mbps or 10 Mbps. As well, the Ethernet Routing Switch 8300 does not support CANA on copper SFP ports because the speed and duplex on copper SFP ports are fixed at 1000 Mbps and full duplex.
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.
	The 8302AC power supply requires V2.1 software in order for the system to recognize it properly. If the system has a version of software prior to V2.1 and is booted with the 8302AC power supply in place, PoE will not be available.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
SOFTWARE	
Platform	
Q01157580	In Enterprise Switch Manager (ESM), the File/Inventory Manager (FIM) displays the Card Front Type for the 8324FX module as unknown.
Q01152303	The following error messages may display on the console: `snmpIoWrite sendto failed : bufSize = 108, pRemote = 0x86b1fc19, pLocal = 0x0 S_errno_EHOSTDOWN` `snmpIoWrite sendto failed : bufSize = 108, pRemote = 0x86b1fc19, pLocal = 0x0 S_errno_EHOSTDOWN` `snmpIoWrite sendto failed : bufSize = 108, pRemote = 0x86b1fc19, pLocal = 0x0 S_errno_EHOSTDOWN` These messages are benign and are the result of normal behavior when the management station is offline or not responding to ARP requests.
Q01151636	On reset, the switch does not set port status down for ports 6/1, 6/2, and 6/8. The following error message displays: `sysi2cwriterepread`
Q01147366	Be aware that the Ethernet Routing Switch 8300 does not provide a warning message when you delete the default SNMP-v3 user. Consider carefully before you delete the default user, so that you do not inadvertently lose SNMP access to the box.
Q01113202	Ping datasize option has no effect. No matter what datasize you specify, ping will always use 56 bytes.
Q01086424	When failing over CPUs, you may see the following message: • `cpldIsBoardOk: invalid slot number 0` The message occurs because of timing differences in processes transitioning between slave and master. The message is benign, and functionality is not affected. No action is required. The new master will initialize and continue to function normally.
Q01062155	Port utilization reported by monitor statistics is not accurate. The extent of discrepancy between the actual and observed rates depends on the traffic's frame size: larger frame sizes are more accurate.
Q01040803, Q0883620	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.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
Q01035465	File transfer from switch to host workstation can be slow with the **copy** command or TFTP client. You will not experience this problem with FTP. In this case, Nortel recommends that you use FTP, or execute a TFTP client on remote host workstation and use the GET operation.

Q01033494	When an image file is copied to the switch using the **copy** command, two messages display on the console if the command completes successfully.
	The first message confirms completion of the image data transfer through TFTP:
	`File [source file-path] - xxxx bytes successfully transferred`
	The second message confirms that the image has been saved to flash:
	`File [source file-path] - successfully written`
	If the second message does not display, then the file has not been successfully written to flash.

Q01029311	You cannot perform more than one configuration file save at a time. If a second configuration file save is initiated from a separate Telnet session while a file save is in progress, the second operation fails. The following messages display:
	`Another show or save in progress. Please try the command later.`
	`malloc: 0x3d0002`
	`S_objLib_OBJ_UNAVAILABLE`
	`Save boot to file <filename> failed.`

Q01026909	If you boot the Ethernet Routing Switch 8300 with no configuration file and then try to source a configuration file that contains RMON alarms, you can experience a number of instances of the following error message: `SNMP WARNING RMON not init before RmonAlarmCreate` The RMON configuration messages appear if RMON is not enabled. Alternatively, if RMON is enabled, then the RMON task initialization is delayed. Use **show rmon info** to check if RMON is enabled, and reconfigure the RMON alarms and events.
Q00972634	You may experience a delay of up to 10 seconds before the login prompt displays in a Telnet session.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
Q00904970, Q00861897	The `nocheck-sw-version` flag, dedicated for use by Nortel customer support engineers, 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 changed. 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 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.
Q00876457	The FTP password also applies to TFTP.
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.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
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	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.
Q00841620	Operations over FTP may be slow. It may take several minutes for flash writes for larger files. Do not attempt to abort FTP operations since it may cause flash corruption.
Q00830458	Use **`dos-format`** to format the PCMIA card only. Use **`format-flash`** to format the flash. If you use these commands on the wrong target, it may damage your flash.
Q00802594, Q00803154, Q00803806, Q00837041, Q00837034	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.
Q00799673	When sourcing a configuration file, even with **`verify config`** enabled, no error message will be generated if a configuration file fails to load due to errors.
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	
Q01153279, Q01153288	There are grammar and spelling errors in the descriptions for various RIP commands and options. Refer to *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B) for the correct descriptions.
Q01145580	On reboot or failover, CLI display defaults to 24 screen lines, even if a different value has been saved to the configuration file.
Q01145231	The command **`save config verbose`** causes a 0.0.0.0 mgmt-virt-address to be saved.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
Q01026921	If the **show logging file** command is typed after the logging file has been deleted, the following message displays: `can't seek to EOF & BOF <logfile path name> errno:3670026 S_dosFsLib_INVALID_PARAMETER` This indicates that the file cannot be found. The same error occurs whenever a log message should have been written, but the log file was no longer present on the system. A new log file is created after the error occurs.
Q01012518	If you attempt to copy a file to the /pcmcia directory after a previously installed PCMCIA card has been removed, the following message displays, to indicate that the operation failed: `Can't open directory "/pcmcia".` A number of error codes, starting with a hex number and the `(tShell):`, follow. Ignore these messages.
Q00957081	When a file is being copied to the flash, CPU utilization may show as 100% during the copy.
Q00876505, Q0855057	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.
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.
Q00860779	Passwords are currently encrypted in a file. This file mistakenly contains an invalid username `NNCLI`. For security reasons, Nortel does not provide the name of this file. If you want to reset the passwords, follow the instructions in *Configuring and Managing Security using the NNCLI and CLI* (316804-C).
NNCLI	
Q01157948	The value set for `local-next-hop` for static routes does not get saved across reboots. Even if the value has been set to false, it defaults to true on reboot.
Q01156840	The `show eapol multihost non-eap-mac status <ports>` command will not display consistent information about radius-mac-centralization clients unless you first execute a command that issues an authentication request.
Q01153279, Q01153288	There are grammar and spelling errors in the descriptions for various RIP commands and options. Refer to *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B) for the correct descriptions.
Q01151630	A maximum of 7 users can log in to the NNCLI at the same time using **rlogin**. An eighth **rlogin** attempt will just hang.
Q01036158	You cannot use the commands **ls** and **directory** while in the NNCLI. Instead, you must use the **dir** command.
Q01010343	In the NNCLI, the command **eapol re-authenticate** displays some garbage characters along with the EAP authentication messages.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
Q00901990	In the NNCLI, the *src-port-pair* field is not set when you use the range and mask operators. Instead, you can configure this field using the CLI and Device Manager. Note that you can configure the *dst-port* field in the NNCLI with the range and mask operators.
Q00869924, Q00876361	You cannot disable an access-policy in the NNCLI. However, you can still delete it. You can disable access policies from the Device Manager.
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	
Q01124947	If you add a TACACS source IP address in the Device Manager, it may not register in the CLI. By contrast, adding configuration information in the CLI will always change information in the Device Manager. To synchronize the Device Manager and CLI, set the Device Manager's rcTacacsServerSourceIPInterfaceEnabled field to true.

Q01122180	The Device Manager displays an inaccurate error message if you attempt to add more than 64 protocols to the UDP protocol table for UDP forwarding. The message that displays is:
	`rcIpUdpProtocolRowStatus.1000 0: undoFailed`
	In the CLI, the equivalent error message, which is correct, is:
	`IP WARNING reached max size 64 in the UdpProtocol Table`

Q01039044	The Device Manager reports an incorrect amount of PoE power for an installed 8302 Power Supply. The actual amount of power is half what the Device Manager indicates.

Q01024579	The Ethernet Routing Switch 8300 displays the following error message when you attempt to configure Guest VLAN in a spanning tree group in the Device Manager:
	`rcEapPortGuestVlanEnable.298: The specified operation is not allowed`
	The error message is incorrect and misleading. It should read as follows:
	`Port does not belong to the STG of the Guest Vlan`

Table 6 Known limitations, by type of issue (continued)

CR reference	Description

Q00862945	Be aware that the Device Manager may time out after converting MAC entries and refreshing the Allowed MAC table. You can prevent this problem by increasing the runtime memory allocation size. To do so:
	In a Windows environment:
	1. Open a command prompt.
	2. Go to the directory where Device Manager is installed.
	For example, if the install directory is C:/Program Files/JDM, in the command prompt window, type:
	`cd \Program Files\JDM`
	3. Enter the following command to launch Device Manager:
	`.\jre\bin\java - Xmx256m- DEMPATH=. -jar .\jdm.jar`
	In a UNIX environment:
	1. Go to the directory where Device Manager is installed.
	2. Enter the following command to launch Device Manager:
	`./jre/bin/java -Xmx256m -DEMPATH=. -jar ./jdm.jar`
	Note: The preferred memory size is 256 MB. The default value is 64 MB. Assign a suitable size based on your system environment. In a Windows environment, you require 256 MB of memory.

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	
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.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
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.
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.
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.
Q00867884	Be aware that in Interface Config mode, **`ip igmp last-member-query-int <value>`** will have no effect on the Ethernet Routing Switch 8300. This parameter is not supported.
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.
Q00827920	The agetime that displays under **`show vlan info advance`** actually applies to dynamic VLAN membership. In the Ethernet Routing Switch 8300, dynamic VLAN membership is not supported, so this agetime always appears as 0. Note that this differs from the FDB aging timer. To verify aging time, enter **`info`** under **`config vlan`** *<vid>* **`fdb-entry`**.

Table 6 Known limitations, by type of issue (continued)

<table>
<tr><th>CR reference</th><th>Description</th></tr>
<tr><td>Q00806545</td><td>For byProtocol VLANs, a certain number of “protocol-type” values are restricted (invalid), because the preconfigured VLAN types (IP/IPX/AppleTalk) already use these values.
Table 7 lists the currently restricted hex values for preconfigured VLAN protocol types.

Table 7 Restricted protocol-type values (current)
<table><tr><th>Protocol type</th><th>Hex value</th></tr><tr><td>XNS</td><td>0600</td></tr><tr><td>IP</td><td>0800</td></tr><tr><td>BANYAN VINES</td><td>0BAD</td></tr><tr><td>DEC LAT</td><td>6004</td></tr><tr><td>RARP</td><td>8035</td></tr><tr><td>SNA Ethernet2</td><td>80D5</td></tr><tr><td>AppleTalk</td><td>809B, 80F3</td></tr><tr><td>IPv6</td><td>86DD</td></tr><tr><td>IPX Ethernet2, IPX SNAP</td><td>8137, 8138</td></tr></table>
Table 8 lists additional protocol types, from the IANA Protocol Types listing (http://www.iana.org/assignments/ethernet-numbers), whose hex values are restricted:

Table 8 Restricted protocol-type values (additional)
<table><tr><th>Protocol type</th><th>Hex value</th></tr><tr><td>BANYAN VINES Loopback</td><td>0BAE</td></tr><tr><td>BANYAN VINES Echo</td><td>0BAF</td></tr><tr><td>DEC unassigned</td><td>8039-803C</td></tr><tr><td>DEC Ethernet Encryption</td><td>803D</td></tr><tr><td>DEC unassigned</td><td>803E</td></tr><tr><td>DEC LAN Traffic Monitor</td><td>803F</td></tr><tr><td>DEC unassigned</td><td>8040-8042</td></tr></table></td></tr>
<tr><td>Q00802887</td><td>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.</td></tr>
</table>

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
Q00784962	When you first activate unknown MAC discard, it causes the Auto-learn mode on that port to stop functioning.
Layer 3	
Q01156066	The switch does not respond to a solicitation message from source 0.0.0.0.

Q01148215	You cannot set route-discovery parameters for a non-routable VLAN (i.e., a VLAN without an IP address). If you attempt to do so, the switch may display the following error message:
	`Consistency check error Invalid port number`
	The error message should read:
	`Error: vlan <vid> is not set for routing`

Q01142905	When the commands to flush the IP table or all tables are executed, a RIP request is immediately sent out to solicit the updated RIP routes, rather than waiting for the update timer on the RIP peer switch to expire.
Q01109089	The RIP update timer can be set to a maximum value of 2147483647. The maximum value of the timeout timer is 259200. Note, however, that the RIP update time interval must be less than the timeout interval.
Q01092567	Router advertisement is not sent within the max_initial_advert_interval in the following cases: • The interface goes down or up. • IP forwarding is enabled or disabled. The Ethernet Routing Switch 8300 continues to send regular advertisements at random intervals within the MinAdvertisementInterval and MaxAdvertisementInterval range.
Q01028334	When configuring DHCP Relay for the first time on the Ethernet Routing Switch 8300, a **`save config`** is required when using the NNCLI. DHCP Relay will not work until you enter **`save config`**.
Multicast	
Q00889737, Q00889777, Q00889744	IGMP static receivers are not supported in the Ethernet Routing Switch 8300.
Q00843934	Traffic filters for IGMP join and leave packets are not effective if the port belongs to one or more IGMP interfaces.
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.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
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, **`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.
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	
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 cards 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.
Q00813681	When using **`config qos egress-counter-set`**, the NNCLI does not allow you to configure a VLAN, even though `VLAN` appears to be a valid command option. As a workaround, configure without specifying a VLAN to ensure that the egress counters are created properly.
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 `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.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
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.

Q00777592	After you set the dst-mac's ace-op parameter to a value other than `any` and `eq` in the Device Manager and then create an ACG, ports cannot be assigned to the ACG.
	The following are examples of the kinds of error messages that display:
	`8310-41:6/config/filter/access-list/1# config ether 4/7 filter create 1`
	`Error Handler:Gen lib error code: 5`
	`Error Handler:the unit is: 24 and the device: 24`
	`Error: Port = 4/7, Acl Port create operation FAIL`
	`8310-41:6/config/filter/access-list/1# config ether 4/5 filter create 1`
	`Error Handler:Gen lib error code: 5`
	`Error Handler:the unit is: 24 and the device: 24`
	`Error: Port = 4/5, Acl Port create operation FAIL`
	If you change the dst-mac's ace-op to `eq`, ports can be added without error messages.

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.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description
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	
Q01132066	Prompts for login and password occur prior to the authentication process. Authentication is always attempted in the following order: TACACS+, RADIUS, the local database. If both RADIUS and TACACS+ are enabled, TACACS+ authentication always occurs before RADIUS authentication. If TACACS+ fails because there are no valid servers, then the username and password are used for RADIUS authentication. If RADIUS also fails, then the username and password are used for the local database. If TACACS+ returns an access denied packet, then the user is offered a new authentication attempt (login/password prompts are re-issued — the authentication process is not passed to RADIUS).
Q01101658	When the RADIUS server has had EAP or Accounting disabled for a period of time, you may need to disable and re-enable the SBR network adapter card in order to ping the server.
Q01101113	You cannot log in to the switch with a WinSCP client. WinSCP is not supported on the Ethernet Routing Switch 8300.
Q01082576	CLI includes profiling in the RADIUS configuration commands. The Ethernet Routing Switch 8300 does not currently support RADIUS profiling. The CLI command **`config radius info cli profile enable`** is not supported.
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.
Q01042958, Q01042890	Session time values displayed for terminated and unauthenticated sessions in Multi-host Session Stats are incorrect. Values displayed for *`Session-Id`* and *`User-name`* are also incorrect for some sessions.
Q01038051	When EAP is enabled on a port, the port also needs to be configured as multihost if N+1 authorized users will be accessing the port. Otherwise, when the N+1 user accesses the port, EAP port status is changed to force-unauthorized and all currently authorized users are dropped.
Q01032071	The Ethernet Routing Switch 8300 does not meet the following requirements for 802.1x authentication related to the RADIUS authentication: • The switch does not return NAS-Port-Type or Called-Station-Id (port MAC address) in authentication requests. • The switch does not return NAS-Port-Type, Called-Station-Id, or Calling-Station-Id (user MAC address) in accounting requests. Full support for these options will be provided in a subsequent release.

Table 6 Known limitations, by type of issue (continued)

CR reference	Description

Q01026930	In rare cases, when the command **config ethernet <slot/port> eapol** is entered, the console on the Ethernet Routing Switch 8300 displays the following error message:
	`IoWrite sendto failed : bufSize = 123, pRemote = 0x2f50e7fe, pLocal = 0x0`
	`snmpIoWrite sendto failed : bufSize = 123, pRemote = 0x2f50e7fe, pLocal = 0x0`
	These messages are benign, and functionality is not affected.

Q01021626	Enabling port mirroring on an EAP-enabled port causes authentication failures.
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.
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.
Q00820269	SNMPv3 notification is not supported in v2.0.0.1 of the Ethernet Routing Switch 8300.
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	
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.

Documentation additions and corrections

Configuring router discovery using the NNCLI

The following information supplements material on configuring the router discovery feature.

Configuring IP Routing and Multicast Operations using the NNCLI and CLI (316800-B), Chapter 5, "Configuring IP Routing using the NNCLI", p. 129 and *NNCLI Command Line Reference for the Ethernet Routing Switch 8300* (316810-C), p. 270

Enabling router discovery

By default, router discovery is disabled on the switch. To enable router discovery globally, enter the following command in **Global Config** mode:

```
ip irdp enable
```

To disable router discovery, enter the following command in **Global Config** mode:

```
no ip irdp enable
```

To restore the default router discovery status, enter the following command in **Global Config** mode:

```
default ip irdp enable
```

Configuring router discovery on an interface

To configure router discovery on a specified VLAN interface, enter the following command in **Interface Config** mode:

```
ip irdp [vlan <vid>]
```

where:

<v*id*> is the VLAN ID.

This command includes the following options:

ip irdp [vlan <*vid*>] followed by:	
`address <ipaddr>`	The IP destination address to be used for broadcast or multicast router advertisements sent from the interface. The accepted values are: • 224.0.0.1 – the all-systems multicast address • 255.255.255.255 – the limited broadcast address The default is 255.255.255.255.
`enable`	If enabled, advertises the address on the interface. The default is enabled (true = advertise address). To disable router discovery advertisements on the interface, enter the following command: **`no ip irdp [vlan <vid>] enable`**
`holdtime <seconds>`	The TTL value (in seconds) of router advertisements sent from the interface. The range is 4 to 9000 seconds. The default is 1800 seconds.
`maxadvertinterval <seconds>`	The maximum time (in seconds) allowed between sending unsolicited broadcast or multicast router advertisements from the interface. The range is 4 to 1800 seconds. The default is 600 seconds.

ip irdp [vlan <*vid*>] followed by:	
`minadvertinterval <seconds>`	The minimum time (in seconds) allowed between sending unsolicited broadcast or multicast router advertisements from the interface. The range is 3 to 1800 seconds. The default is 450 seconds.
`preference <preference>`	Specifies the preference assigned to the address as a default router address, relative to other router addresses on the same subnet. A higher number indicates greater preference. • *preference* is an integer value with a range of -2147483648 to 2147483647. The default is 0.

To restore router discovery parameter values to their default settings on a specified VLAN interface, enter the following command in **Interface Config** mode:

```
default ip irdp [vlan <vid>] [address] [holdtime]
[maxadvertinterval] [minadvertinterval] [preference]
```

where:

<v*id*> is the VLAN ID.

To disable router discovery on a specified VLAN interface, so that the address is not advertised, enter the following command in **Interface Config** mode:

```
no ip irdp [vlan <vid>] enable
```

where:

<v*id*> is the VLAN ID.

Viewing router discovery settings

To view router discovery settings for a specified VLAN interface, enter the following command in **User EXEC** mode:

```
show ip irdp interface [vlan <vid>]
```

Figure 1 shows sample output for this command.

Figure 1 show ip irdp interface command output

```
Pubs_NNCLI_8300:5#show ip irdp interface vlan 2

================================================================================
                                        Vlan Ip Icmp Route Discovery
================================================================================
VLAN_ID  ADV_ADDRESS      ADV_FLAG LIFETIME   MAX_INT    MIN_INT    PREF_LEVEL
--------------------------------------------------------------------------------
2        255.255.255.255  true     1800         600        450        0
```

Configuring router discovery using the CLI

The following information supplements material on configuring the router discovery feature.

Configuring IP Routing and Multicast Operations using the NNCLI and CLI (316800-B), Chapter 6, "Configuring IP Routing using the CLI", p. 163 and *CLI Command Line Reference for the Ethernet Routing Switch 8300* (317360-C), p. 122

Configuring router discovery on an interface

Use the **`config vlan <vid> ip route-discovery`** command to configure router discovery on the specified VLAN.

The **`config vlan <vid> ip route-discovery`** command includes the following options:

`config vlan <vid> ip route-discovery` followed by:	
`info`	Displays router discovery settings for the interface.
`advertisement-address <ipaddr>`	The IP destination address to be used for broadcast or multicast router advertisements sent from the interface. The accepted values are: • 224.0.0.1 – the all-systems multicast address • 255.255.255.255 – the limited broadcast address The default is 255.255.255.255.
`advertise-flag <true|false>`	If set to true, advertises the address on the interface. The default is true.
`advertisement-lifetime <seconds>`	The TTL value (in seconds) of router advertisements sent from the interface. The range is 4 to 9000 seconds. The default is 1800 seconds.
`max-advertisement-interval <seconds>`	The maximum time (in seconds) allowed between sending unsolicited broadcast or multicast router advertisements from the interface. The range is 4 to 1800 seconds. The default is 600 seconds.

config vlan <*vid*> ip route-discovery followed by:	
`min-advertisement-interval <seconds>`	The minimum time (in seconds) allowed between sending unsolicited broadcast or multicast router advertisements from the interface. The range is 3 to 1800 seconds. The default is 450 seconds.
`preference-level <preference>`	Specifies the preference assigned to the address as a default router address, relative to other router addresses on the same subnet. A higher number indicates greater preference. The range is -2147483648 to 2147483647. The default is 0.

Showing IP router discovery information

To show whether or not route discovery is enabled on the device, use the following command:

```
show ip route-discovery
```

To display information about router discovery settings for a specified VLAN, use the following command:

```
config vlan <vid> ip route-discovery info
```

Figure 2 shows sample output for this command.

Figure 2 config vlan ip route-discovery info command output

```
Passport-8310:5# config vlan 2 ip route-discovery info

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

              advertisement-address : 255.255.255.255
                     advertise-flag : true
                 advertisement-lifetime : 1800
          max-advertisement-interval : 600
          min-advertisement-interval : 450
                    preference-level : 0
```

Default value of static routes local-next-hop parameter in the NNCLI

The default value of the local-next-hop parameter in the NNCLI is enabled. *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B), Chapter 5, “Configuring IP routing using the NNCLI”, p. 136, incorrectly states that the default is disabled.

Valid VLAN ID range

The valid range for VLAN ID numbers is 1–4000. The range is incorrectly stated in a number of places in *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (317347-C), in *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI* (316805-C), and in *Configuring VLANs, Spanning Tree, and Static Link Aggregation using Device Manager* (317348-C).

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" on page 55.

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)
- *Installing Ethernet Routing Switch 8300 Series Modules* (316796-C)
- *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)
- *Installing Ethernet Routing Switch 8300 Series Modules* (316796-C)
- *Installing GBIC and Gigabit SFP Transceivers* (318034-A)
- *Ethernet Routing Switch 8300 Power Considerations* (317223-C)
- *Upgrading to Ethernet Routing Switch 8300 Software Release 2.2* (318769-C)
- *Using Device Manager Diagnostic Tools* (317359-C)

Reference and Configuration Guides

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

- *CLI Command Line Reference for the Ethernet Routing Switch 8300* (317360-C)
- *Configuring and Managing Security using Device Manager* (317346-C)
- *Configuring and Managing Security using the NNCLI and CLI* (316804-C)
- *Configuring IP Routing and Multicast Operations using Device Manager* (317338-B)
- *Configuring IP Routing and Multicast Operations using the NNCLI and CLI* (316800-B)
- *Configuring Network Management using the NNCLI, CLI, and Device Manager* (316803-C)
- *Configuring QoS and Filters using the CLI* (317339-B)
- *Configuring QoS and Filters using Device Manager* (317340-B)
- *Configuring QoS and Filters using the NNCLI* (316801-B)
- *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (317347-C)
- *Configuring VLANs, Spanning Tree, and Static Link Aggregation using Device Manager* (317348-C)
- *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI* (316805-C)

- *Managing Platform Operations* (317350-C)
- *Network Design Guidelines* (316809-C)
- *NNCLI Command Line Reference for the Ethernet Routing Switch 8300* (316810-C)
- *System Messaging Platform Reference Guide* (316806-C)
- *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:

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**.

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.