NORTEL

Nortel Ethernet Routing Switch 4500 Series

Release Notes — Release 5.3

Release: 5.3
Document Revision: 05.01

www.nortel.com

NN47205-400

Nortel Ethernet Routing Switch 4500 Series
Release: 5.3
Publication: NN47205-400
Document release date: 25 May 2009

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OFANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Contents

Software license

This section contains the Nortel Networks software license.

THE SOFTWARE DESCRIBED IN THIS DOCUMENT IS FURNISHED UNDER A LICENSE AGREEMENT AND MAY BE USED ONLY IN ACCORDANCE WITH THE TERMS OF THAT LICENSE.

Nortel Networks Inc. software license agreement

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

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

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

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

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

4. General

1. 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).
2. 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.
3. 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.
4. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
5. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
6. 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.

New in this release

The following sections detail what’s new in Nortel Ethernet Routing Switch 4500 Series Release Notes — Software Release 5.3.

Features

See the following sections for information about feature changes.

- “802.1X or Non-EAP and Guest VLAN on same port” (page 13)
- “802.1X or Non-EAP with Fail_Open VLAN” (page 13)
- “802.1X or Non-EAP with VLAN name” (page 14)
- “802.1X or Non-EAP Last Assigned VLAN” (page 14)
- “802.1X or Non-EAP use with Wake On LAN” (page 14)
- “RADIUS Management Accounting” (page 14)
- “RADIUS Request use Management IP” (page 14)
- “SNMP Traps for DHCP Snooping / DAI / IPSG” (page 15)
- “Disable CLI Audit Log Command” (page 15)
- “Configure Asset ID” (page 15)
- “Show Environmental” (page 15)
- “Nortel Automatic QoS” (page 15)
- “MLT Enable / Disable whole trunk (MLT shutdown ports on disable)” (page 15)
- “ASCII Download Enhancements” (page 16)
- “MAC Flush” (page 16)
- “WebUI MIB Web Page” (page 16)
- “WebUI Trap Web Page” (page 16)

Other changes

See the following sections for information about changes that are not feature-related.

New hardware

The Nortel Ethernet Routing Switch 4524GT-PWR is a new additional hardware model added to the 4500 series Ethernet Routing Switches. For more information, see *Nortel Ethernet Routing Switch 4500 Series Installation,* (NN47205-300).

File names for upgrade

File names are updated; see "File names for this release" (page 19).

Hardware and software compatibility

Hardware and software compatibility information is moved to this document. See "Hardware and software compatibility" (page 31).

Introduction

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Nortel Ethernet Routing Switch 4500 Series, Software Release 5.3.

For information on how you can upgrade your version of Device Manager, see *Nortel Ethernet Routing Switch 4500 Series Fundamentals*, (NN47205-102).

The Nortel Ethernet Routing Switch 4500 Series, supported by software release 5.3, includes the following switch models:

- Nortel Ethernet Routing Switch 4524GT
- Nortel Ethernet Routing Switch 4524GT-PWR
- Nortel Ethernet Routing Switch 4526FX
- Nortel Ethernet Routing Switch 4526GTX
- Nortel Ethernet Routing Switch 4526GTX -PWR
- Nortel Ethernet Routing Switch 4526T
- Nortel Ethernet Routing Switch 4526T-PWR
- Nortel Ethernet Routing Switch 4548GT
- Nortel Ethernet Routing Switch 4548GT-PWR
- Nortel Ethernet Routing Switch 4550T
- Nortel Ethernet Routing Switch 4550T-PWR

Configurations can vary from a stand-alone switch to a stack of up to 8 switches. A stack can consist of any combination of switches. One of the benefits of operating Nortel Ethernet Routing Switch 4500 Series switches in a stack is management efficiency; a stack is managed with a single IP address and software is available as a single image across all models.

These Release Notes provide the latest information about Software Release 5.3, as well as operational issues not included in the documentation suite.

For a complete list of documentation in the 4500 Series suite, see *Nortel Ethernet Routing Switch 4500 Series Documentation Road Map* (NN47205-101) .

The information in these Release Notes supersedes applicable information in other documentation.

Navigation

The following topics are discussed in this document:

Important notices and new features

This section contains a brief synopsis of the new features in release 5.3 and any important notices.

Navigation

This section includes the following sections:

New features in Release 5.3

This section lists the new features supported on the Nortel Ethernet Routing Switch 4500 Series switches.

New features

The following sections provide a brief description of the new software features.

802.1X or Non-EAP and Guest VLAN on same port

This feature removes previous limitations by providing the ability to simultaneously configure 802.1X, Non-EAP and Guest VLAN on the same port for a more universal port configuration. In this release you do not have to configure a port to support Guest VLANs or Non-EAP or 802.1X; one port can support all 3 functions.

802.1X or Non-EAP with Fail_Open VLAN

This feature provides network connectivity for EAP-enabled or non-EAP-enabled ports to reach specific network resources when the switch is not able to reach the RADIUS server. When connectivity to the RADIUS server is lost, the system moves all authenticated devices into the configured Fail Open VLAN. When connectivity to the RADIUS server is restored, the system moves devices back to their previously-authenticated networks.

802.1X or Non-EAP with VLAN name

This feature enables the Ethernet Routing Switch 4500 to match RADIUS assigned VLANs based on either the VLAN number or a VLAN name. Previously, a match was based on the VLAN number of the Tunnel-Private-Group-Id attribute returned by the RADIUS server.

802.1X or Non-EAP Last Assigned VLAN

This feature was initially implemented in Ethernet Routing Switch 4500 Series Maintenance Release 5.1.3 and now is supported in this major release. The 802.1X or Non-EAP last assigned RADIUS VLAN function allows you to configure the switch so that the last received RADIUS-VLAN assignment is always honored on a port.

802.1X or Non-EAP use with Wake On LAN

The Ethernet Routing Switch 4500 Release 5.3 documentation now provides information about how to configure 802.1X or Non-EAP functionality to support Wake on LAN (WoL). The WoL networking standard allows you to power up a shut down computer from a sleeping state remotely.

RADIUS Management Accounting

RADIUS Management Accounting provides the ability to record the management login activities to the switch. The switch returns an authentication message to the RADIUS server for logging purposes. The accounting records are generated when you access the switch through the console, telnet, SSH, or Web based management, or when you disconnect the session by logoff or timeout.

RADIUS Request use Management IP

The feature allows you to configure the switch to follow strict use of the Management IP address when routing is enabled. By default, the switch uses any of the configured IP instances as the source IP address for RADIUS requests generated by the switch but, for some networks, the management IP address of the switch or stack must be used specifically. Enabling RADIUS Request use Management IP ensures that the switch uses the Management VLAN IP address as the source IP address for RADIUS requests when routing is enabled.

SNMP Traps for DHCP Snooping / DAI / IPSG

This feature allows you to enable or disable SNMP Traps for the following security applications:

- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- IP Source Guard (IPSG)

SNMP Trap generation enables the system to send real-time alerts to management stations to display errors that can warn about potential intrusions.

Disable CLI Audit Log Command

Stackable switches support an NNCLI Audit function which, by default, automatically records a history of all NNCLI commands entered using the console port (serial port), Telnet, and Secure Shell (SSH). A configuration option is available in this release to disable NNCLI audit logging.

Configure Asset ID

This feature provides the capability to assign a customer-specific asset identification string (Asset ID) for the stack or any unit in the stack. The Asset ID can consist of any alphanumeric string up to 32 characters long.

Show Environmental

The show environmental functions, available using NNCLI, Device Manager, and Web-based management, provide the option to display real time switch environmental parameters for the switch or a stack.

Show Environmental reports the following parameters for each switch:

- power supply status
- fan status
- switch system temperature

Nortel Automatic QoS

When you enable Nortel Automatic QoS, the switch recognizes Nortel application traffic and will prioritize the traffic through the switch. Nortel Automatic QoS is enabled or disabled globally and the feature offers a simplified and resource-efficient mechanism to prioritize Nortel application traffic within your network.

MLT Enable / Disable whole trunk (MLT shutdown ports on disable)

This feature enables a change in the operation of ports in a MLT/DMLT group.

If you enable the MLT shutdown ports on disable functionality, then the system changes the state of the ports which make up the MLT/DMLT group to correspond to the status of the MLT/DMLT group.

For example, if the MLT/DMLT is enabled, then the administrative status of all ports within that group is enabled. If the MLT/DMLT is disabled, then all links which are part of the MLT group are disabled, with the exception of the Destination Lookup Failure (DLF) link.

ASCII Download Enhancements

This feature records information log messages about the download status of ASCII configuration files.

MAC Flush

This feature provides a direct way to clear MAC addresses from the Forwarding Data Base.

MAC Flush provides the following options to clear MAC address entries:

- clearing a single MAC Address
- clearing all MAC addresses from a port or list of ports
- clearing all MAC addresses from a trunk (MLT/LAG)
- clearing all MAC addresses from a particular VLAN
- clearing all MAC addresses

WebUI MIB Web Page

You can use the Web User Interface MIB page to query SNMP objects on the switch.

WebUI Trap Web Page

You can use the Web User Interface Trap page to enable or disable traps received by the SNMP trap receiver.

Supported software and hardware capabilities

The following table lists supported software and hardware scaling capabilities in Ethernet Routing Switch 4500 Series Software Release 5.3. The information in this table supersedes information contained in any other document in the suite.

Table 1
Supported software and hardware scaling capabilities

Feature	Maximum number supported
Egress queues	8 hardware queues, 4 enabled in software

Feature	Maximum number supported
MAC addresses	8000
Stacking bandwidth (full stack of 8 units)	320 Gb/s: 40 Gb/s per switch
Maximum number of units in a stack	8
Layer 2	
VLANs	256
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	8
Maximum MAC Learning rate on an MLT trunk	500 new MAC addresses per second
Links or ports for MLT, DMLT or LAG	4
Spanning Tree Group instances (802.1s)	8
Nortel Spanning Tree Groups	8
DHCP Snooping table entries	512
Layer 3	
ARP entries	1256
Static ARP entries	256
Dynamic ARP entries	1000
IPv4 route entries	292
Static routes	32
Local routes	256
Management routes	4
UDP Forwarding entries	128
DHCP relay entries	256
Miscellaneous	
IGMP multicast groups	512
802.1x (EAP) clients per port, running in MHMA	32
802.1x (EAP) clients per switch/stack	384
LLDP Neighbors per port	16
LLDP Neighbors	800
RMON alarms	800
RMON events	800
RMON Ethernet statistics per unit in stack	84
RMON Ethernet history per unit in stack	124
Telnet instances	4 concurrent sessions
Web instances	2 concurrent sessions

Filter, meter and counter resources

The following table details filter, meter and counter resources used on the Ethernet Routing Switch 4500 when various applications are enabled.

Note: Filters will use the highest available precedence.

Table 2
Filter, meter and counter resources

Feature	Observation	QoS			NonQos	
		Filters	Meters	Counter	Filters	Meters
EAPOL		0	0	0	2	0
ADAC		0	0	0	1	0
DHCP Relay	L2 mode	0	0	0	2	1
DHCP Relay	L3 mode	0	0	0	2	1
DHCP Snooping		0	0	0	2	1
NSNA	**Red**					
	Precedence 5	3	1	1	0	0
	Precedence 4	1	1	1	0	0
	Precedence 3	2	1	1	0	0
	Precedence 2	1	1	1	0	0
	Precedence 1	1	1	1	0	0
NSNA	**Yellow**					
	Precedence 6	3	0	1	0	0
	Precedence 5	1	0	1	0	0
	Precedence 4	1	0	1	0	0
	Precedence 3	2	0	1	0	0
	Precedence 2	1	0	1	0	0
	Precedence 1	1	0	1	0	0
NSNA	**Green**					
	Precedence 1	1	0	1	0	0
MAC Security		0	0	0	0	0
IP Source Guard		0	0	1	11	0
Port Mirroring	Mode XrxYtx	1	0	0	0	0
Port Mirroring	XrxYtx or YrxXtx	2	0	0	0	0
Port Mirroring	AsrcBdst, Asrc, Adst	1	0	0	0	0
Port Mirroring	AsrcBdst or BscrAdst, Asrc or Adst	2	0	0	0	0

Feature	Observation	QoS			NonQos	
QoS	Trusted	0	0	0	0	0
QoS	**Unstrusted**					
	Precedence 2	1	0	1	0	0
	Precedence 1	1	0	1	0	0
QoS	Unrestricted	0	0	0	0	0
UDP Forwarding		0	0	0	1	1

Software licenses

Nortel Ethernet Routing Switch 4500 Series Software Release 5.3 does not currently support software licenses.

File names for this release

The following table describes the Nortel Ethernet Routing Switch 4500 Series, Software Release 5.3 software files. File sizes are approximate.

Table 3
Software Release 5.3 components

Module or file type	Description	File name	File size (bytes)
Standard runtime image software version 5.3.0.8	Standard image for the Nortel Ethernet Routing Switch 4500 Series	4500_530008.img	6,223,292
Secure runtime image software version 5.3.0.9	Secure image for the Nortel Ethernet Routing Switch 4500	4500_530009s.img	6,478,676
Boot/diagnostic software version 5.3.0.3	Switch diagnostic software	4500_5303_diag.bin	1,589,514
Device Manager software version for Windows	Device Manager software image for Windows NT, Windows Vista, Windows XP, Windows 2003, Windows 2000	jdm_6190.exe	215,374,828
Device Manager software version for UNIX	Device Manager software image for Solaris	jdm_6190_solaris_sparc.sh	239,377,242

Table 3
Software Release 5.3 components (cont'd.)

Module or file type	Description	File name	File size (bytes)
Device Manager software version for Linux	Device Manager software image for Linux	jdm_6190_linux.sh	218,569,562
Software Release 5.3 Management Information Base (MIB) definition files	MIB definition files	Ethernet_Routing_Switch_45xx_MIBs_5.3.0.zip	1,577,796

Supported traps and notifications

For information about SNMP traps generated by the Ethernet Routing Switch 4500 Series, see Nortel *Ethernet Routing Switch 4500 Series Troubleshooting* (NN47205-700).

Device Manager installation requirements

Device Manager is supported on Windows, Solaris, and Linux.

For more information about Device Manager installation requirements, see *Nortel Ethernet Routing Switch 4500 Series Fundamentals* (NN47205-101).

Windows

The minimum system requirements for installing Device Manager on Microsoft Windows Vista, Windows 2000 and Windows XP are:

- 512 MB of RAM
- 400 MB space on hard drive

Solaris

Solaris™/Sun™OS 2.8, 2.9, and 2.10/5.8, 5.9, and 5.10
Device Manager requires Solaris 8 as a minimum requirement. The minimum system requirements for installing Device Manager on Solaris are:

- 512 MB RAM
- 400 MB space on hard drive

Linux

The minimum system requirements for installing Device Manager on Linux are:

- 512 MB RAM
- 400 MB space on hard drive

Upgrading software

To upgrade to the new software release 5.3, Nortel recommends that you upgrade the diagnostic software to the 5.3.0.3 version, and then upgrade the agent version to release 5.3.

The following table describes possible image locations:

Table 4
Possible scenarios

Image	Location
Local Agent Image	Agent image in the flash memory of the unit.
Local Diagnostic Image	Diagnostic image in the flash memory of the unit
5.1.0.7 Diagnostic Image	Diagnostic image released in 5.1
5.2.0.3 Diagnostic Image	Diagnostic image released in 5.2
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.3

You can upgrade the Agent Image in your switches from an earlier release image.

Use the following procedure to upgrade the Agent Image from release 5.0, 5.1 or 5.2 to release 5.3:

Upgrading Agent Image from release 5.0, 5.1 or 5.2 to release 5.3.

Step	Action
1	Upgrade the diagnostic image from the earlier release to release 5.3.0.3 diagnostic image.
2	Upgrade the agent image from release 5.0, 5.1 or 5.2 to release 5.3 agent image.

--End--

> ***Note:*** If an existing stack contains mismatched Diagnostics, the Base Unit cannot accept the agent image. If an error occurs when you try to upgrade the software, run the `Show Tech` command to determine whether the software and Diagnostics versions match.

Updating switch software

You can update the version of software running on the switch through either NNCLI, Device Manager or Web-based management.

Before you attempt to change the switch software, ensure that the following prerequisites are in place:

- The switch has a valid IP address.
- A Trivial File Transfer Protocol (TFTP) server is on the network that is accessible by the switch and that has the desired software version loaded.
- If you change the switch software on a port; using a USB Mass Storage Device, ensure that the Mass Storage Device has the desired software version and is inserted into the front panel USB port.
- If you use NNCLI, ensure that NNCLI is in Privileged EXEC mode.
- If you use Device Manager, ensure that SNMP is enabled.
- If you use Web-based management, ensure that you use **read/write** access.

See the following sections for details about updating switch software:

- “General software upgrade instructions” (page 22)
- “Changing switch software in NNCLI” (page 23)
- “Changing switch software in Device Manager” (page 24)
- “Changing switch software in Web-based management” (page 26)

General software upgrade instructions

Use the following procedure to upgrade the Nortel Ethernet Routing Switch 4500 Series software:

Step	Action
1	Backup the binary configuration file to a TFTP server.
2	Upgrade the boot or diagnostic code, if a new version is available. The system reboots after this step.
3	Upgrade the software image.

--End--

Changing switch software in NNCLI

Perform the following procedure to change the software version that runs on the switch with NNCLI:

Step **Action**

1 Access NNCLI through the Telnet protocol or through a Console connection.

2 From the command prompt, use the download command with the following parameters to change the software version:

```
download [address <ipv6_address> | <a.b.c.d>] {image
<image name> |
image-if-newer <image name> | diag <image name> |
poe_module_image <image name>} [no-reset] [usb]
```

3 Press **Enter**.

--End--

The software download occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download. Depending on network conditions, this process may take up to 10 minutes.

When the download is complete, the switch automatically resets unless you used the `no-reset` parameter. The software image initiates a self-test and returns a message when the process is complete.

During the download, the switch is not operational.

Job aid—download command parameters

The following table describes the parameters for the `download` command.

Table 5
NNCLI download command parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td colspan="2">The <b>image, image-if-newer, diag</b>, and <b>poe_module_image</b> parameters are mutually exclusive; you can execute only one at a time.

The address <ip> and usb parameters are mutually exclusive; you can execute only one at a time.</td></tr>
</table>

Parameter	Description
address <ipv6_address> | <a.b.c.d>	The IPv4 or IPv6 address of the TFTP server you use. The address <ipv6_address> | <a.b.c.d> parameter is optional and if you omit it, the switch defaults to the TFTP server specified by the `tftp-server` command unless software download is to occur using a USB Mass Storage Device.
image <image name>	The name of the software image to be downloaded from the TFTP server.
image-if-newer <image name>	This parameter is the name of the software image to be downloaded from the TFTP server if it is newer than the currently running image.
diag <image name>	The name of the diagnostic image to be downloaded from the TFTP server.
poe_module_image <image name>	The name of the Power over Ethernet module image to be downloaded from the TFTP server. This option is available only for 4500 Series switches that support Power Over Ethernet.
no-reset	This parameter forces the switch to not reset after the software download is complete.
usb	In the switch, this parameter specifies that the software download is performed using a USB Mass Storage Device and the front panel USB port.

Changing switch software in Device Manager

To change the software version running on the switch that uses Device Manager, perform the following procedure.

Step	Action
1	Connect to the switch using **Device Manager** .
2	From Device Manager menu, select **Edit, File System**.
3	Select the **Config/Image/Diag file** tab if it is not already selected.
4	Specify the information necessary to perform the download.
5	Click **Apply**.

--End--

The software download occurs automatically after you click Apply. This process erases the contents of flash memory and replaces it with the new software image. Do not interrupt the download. Depending on network conditions, this process can take up to 10 minutes. When the download is complete, the switch automatically resets and the new software image initiates a self-test. During the download, the switch is not operational.

Job aid—File System screen fields

The following table describes the File System screen fields.

Table 6
File System screen fields

Field	Description
TftpServerInetAddress	The IP address of the TFTP server on which the new software images are stored for download.
TftpServerInetAddressType	The type of TFTP address. • Unknown • IPv4 • IPv6
BinaryConfigFileName	The binary configuration file currently associated with the switch. Use this field when you work with configuration files; do not use this field when you download a software image.
ImageFileName	The name of the image file currently associated with the switch. If needed, change this field to the name of the software image to be downloaded.
FwFileName (Diagnostics)	The name of the diagnostic file currently associated with the switch. If needed, change this field to the name of the diagnostic software image to be downloaded.
UsbTargetUnit	Indicates the unit number of the USB port to be used to upload or download a file.
Action	This group of options represents the actions taken during this file system operation. The options applicable to a software download are • dnldImg: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. • dnldFw: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. • dnldConfig: Download a configuration to the switch. • dnldImgFromUsb: Download a new software image to the switch using the front panel USB port. This

Field	Description
	option replaces the image regardless of whether it is newer or older than the current image. • dnldImgIfNewer: Download a new software image to the switch only if it is newer than the one currently in use. • dnldConfigFromUsb: Download a configuration to switch using the front panel USB port. • dnldImgNoReset: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • dnldFwNoReset: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • upldConfig: Upload a configuration to the switch from a designated location. • dnldFwFromUsb: Download a new diagnostic software image to the switch from the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image.
Status	Display the status of the last action that occurred since the switch last booted. The values that are displayed are • other: No action occurred since the last boot. • inProgress: The selected operation is in progress. • success: The selected operation succeeded. • fail: The selected operation failed.

Changing switch software in Web-based management

To change the software version running on the switch that uses Web-based management, perform the following procedure.

Step	Action
1	Log in to Web-based management.

2 Navigate to the Software Download Management page by selecting **Configuration, Software Download** .

3 Specify the information needed to complete the software download procedure.

4 Click **Submit**.

--End--

The software download occurs automatically after you click Submit. This process erases the contents of flash memory and replaces it with the new software image. Do not interrupt the download. Depending on network conditions, this process can take up to 10 minutes. When the download is complete, the switch automatically resets and the new software image initiates a self-test.

During the download, the switch is not operational.

Job aid—software download page fields

The following table describes the software download page fields:

Table 7
Software download page fields

Field	Description
Current Running Version	The version of software currently running on the switch.
Local Store Version	The version of software currently stored in flash memory.
Software Image File Name	The name of the software image to be downloaded to the switch. This field is optional if you perform a diagnostics image download only. The field is 1 to 30 characters in length.
Diagnostics Image File Name	The name of the diagnostics image to be downloaded to the switch. This field is optional if you perform a software image download only. The field is 1 to 30 characters in length.
Select Target	The target from which the software images are downloaded. Select either TFTP Server or USB as the download target.

Field	Description
TFTP Server IP Address	The IP address of the TFTP Server to be used in the software download.
Start TFTP Load of New Image	The type of software download to perform. Select the appropriate option from the list: • **No**: Perform no software download. • **Software Image**: Perform a download of the software image specified in the **Software Image File Name** field regardless of whether it is newer than the current software image. • **Diagnostics**: Perform a download of the diagnostics image specified in the **Diagnostics Image File Name** field. • **Software Image If Newer**: Perform a download of the software image specified in the **Software Image File Name** field only if it is newer than the current image. • **Download without Reset**: Perform a download of the specified software images and do not reset the switch at the end of the process.

Setting IP parameters with the ip.cfg file on a USB memory device

If the switch does not obtain an IP address through BootP, you can load the ip.cfg file from the USB memory device.

You can specify one or more of the optional parameters in the ip.cfg file. All of the parameters are optional.

The following table describes the ip.cfg file parameters:

Table 8
ip.cfg file optional parameters

Parameter	Description
IP <xx.xx.xx.xx>	Specifies the IP address for the switch. Example: 192.168.22.1
Mask <xx.xx.xx.xx>	Specifies the network mask. Example: 255.255.255.0
Gateway <xx.xx.xx.xx>	Specifies the default gateway. Example: 181.30.30.254
SNMPread <string>	Specifies the SNMP read community string. Example: public

Parameter	Description
SNMPwrite <string>	Specifies the SNMP write community string. Example: private
VLAN <number>	Specifies the management VLAN-ID. Example: VLAN 1
USBdiag <string>	Specifies the file name of the diagnostic image to load from the USB device. Example> ers4500/ers4500_5.1.0.4.bin
USBascii <string>	Specifies the file name of the ASCII configuration file to load from the USB device. Example: customer1.cfg
USBagent <string> NEXTIP, NEXTMask, and NEXTGateway	Specifies the file name of the agent image to load from the USB device and specifies IP addresses for the next boot. Example: ers4500/ers4500_5.2.0.0.img

The ip.cfg file loads information from the ASCII configuration file in order of precedence. For example, if you have an ip.cfg file with the following commands:

```
USBascii ip.txt
IP 181.30.30.113
Mask 255.255.255.0
Gateway 181.30.30.254
```

The stack IP becomes 181.30.30.113 no matter what IP address is in the ip.txt file.

If you have an ip.cfg file with the following commands:

```
IP 181.30.30.113
Mask 255.255.255.0
Gateway 181.30.30.254
USBascii ip.txt
```

The stack IP will be the IP address defined in the ip.txt file.

If the ip.cfg file specifies an image or agent code, the switch loads the software, even if the same version is already installed on the switch. This is the correct operation of the system as ip.cfg ensures that the appropriate software is always upgraded on the units.

Use the factory default command to reset the switch to the factory default after you insert the USB memory device in the USB port. The USB memory device must contain the properly formatted ip.cfg file in the root directory.

Use the following procedure to reset the switch to the factory default settings with the NNCLI:

Step	Action
1	Enter `boot default`.
2	Enter `y` to confirm the reset. *The Ethernet Routing Switch 4500 restarts with factory default settings and attempts to read the ip.cfg file from an installed USB drive within three minutes. The Nortel Ethernet Routing Switch 4500 banner page appears while the switch retrieves the ip.cfg file.*

--End--

ATTENTION

While the system retrieves the ip.cfg file from the USB memory device, the Nortel banner page displays. If you use the serial console while the system restarts, you will see the Nortel banner page during the restart. Do not attempt to access the switch for at least three minutes.

The system does not display a message to indicate the ip.cfg file download from the USB memory device is in progress.

Use the following procedure to check the status of the download three minutes after the Nortel banner page displays:

Step	Action
1	Press **CTRL** and **y** keys together. *Two possible responses indicate a pass or fail status.* • Pass: The system opens the first page of menu. • Fail: The system prompts you for an IP address.

--End--

You can confirm the successful download with the `show ip` command. If the USB ip.cfg file download succeeded, all parameters read from the ip.cfg file show as present in the switch and become part of the runtime configuration.

Save the configuration with the NNCLI command, `copy config nvram`. After the successful ip.cfg file download from the USB memory device, you can manage the switch through Telnet and SNMP.

If you load any diagnostic or agent images with ip.cfg, you must have the diagnostic or agent images on the same USB memory device. You must restart the system after you download the ip.cfg files. To ensure that diagnostic and agent image downloaded successfully, check in the system log or audit log. If the operation is successful, reboot the switch or stack to display the new diagnostic and agent images.

If you download an ASCII file, you must enter the settings after the download. You do not need to restart the switch or stack if you download an ASCII file.

Hardware and software compatibility

This section provides hardware and software compatibility information.

XFP and SFP transceiver compatibility

The following table lists the XFP and SFP transceiver compatibility.

Table 9
XFP and SFP transceiver compatibility

Supported SFPs and XFPs	Description	Minimum software version	Part number
Small form factor pluggable (SFP) transceivers			
1000BASE-SX SFP	850 nm LC connector	5.0.0	AA1419013-E5
1000BASE-SX SFP	850 nm MT-RJ connector	5.0.0	AA1419014-E5
1000BASE-LX SFP	1310 nm LC connector	5.0.0	AA1419015-E5
1000BASE-CWDM SFP	1470 nm LC connector, up to 40 km	5.0.0	AA1419025-E5
1000BASE-CWDM SFP	1490 nm LC connector, up to 40 km	5.0.0	AA1419026-E5
1000BASE-CWDM SFP	1510 nm LC connector, up to 40 km	5.0.0	AA1419027-E5
1000BASE-CWDM SFP	1530 nm LC connector, up to 40km	5.0.0	AA1419028-E5
1000BASE-CWDM SFP	1550 nm LC connector, up to 40 km	5.0.0	AA1419029-E5

Supported SFPs and XFPs	Description	Minimum software version	Part number
1000BASE-CWDM SFP	1570 nm LC connector, up to 40 km	5.0.0	AA1419030-E5
1000BASE-CWDM SFP	1590 nm LC connector, up to 40 km	5.0.0	AA1419031-E5
1000BASE-CWDM SFP	1610 nm LC connector, up to 40 km	5.0.0	AA1419032-E5
1000BASE-CWDM SFP	1470 nm LC connector, up to 70 km	5.0.0	AA1419033-E5
1000BASE-CWDM SFP	1490 nm LC connector, up to 70 km	5.0.0	AA1419034-E5
1000BASE-CWDM SFP	1510 nm LC connector, up to 70 km	5.0.0	AA1419035-E5
1000BASE-CWDM SFP	1530 nm LC connector, up to 70 km	5.0.0	AA1419036-E5
1000BASE-CWDM SFP	1550 nm LC connector, up to 70 km	5.0.0	AA1419037-E5
1000BASE-CWDM SFP	1590 nm LC connector, up to 70 km	5.0.0	AA1419039-E5
1000BASE-CWDM SFP	1610 nm LC connector, up to 70 km	5.0.0	AA1419040-E5
1000BSE-T SFP	Category 5 copper unshielded twisted pair (UTP), RJ-45 connector	5.0.0	AA1419043-E5
1000BASE-SX DDI SFP	850 nm DDI LC connector	5.2.0	AA1419048-E6
1000BASE-LX DDI SFP	1310 nm DDI LC connector	5.2.0	AA1419049-E6
1000BASE-BX bidirectional SFP	1310 nm, single fiber LC (Must be paired with AA1419070-E5)	5.2.0	AA1419069-E5
1000BASE-BX bidirectional SFP	1490 nm, single fiber LC (Must be paired with AA1419069-E5)	5.2.0	AA1419070-E5
100BASE-FX SFP	1310 nm LC connector	5.0.0	AA1419074-E6
T1 SFP	1.544 Mbit/s Fast Ethernet to T1 remote bridge, RJ-48C	5.1.0	AA1419075-E6
1000BASE-BX SFP	1310nm LC connector, up to 40km (Must be paired with AA1419077-E6)	5.3	AA1419076-E6

Supported SFPs and XFPs	Description	Minimum software version	Part number
1000BASE-BX SFP	1490nm LC connector, up to 40km (Must be paired with AA1419076-E6)	5.3	AA1419077-E6
10 Gigabit Ethernet SFP transceivers			
10GBASE-LR/LW XFP	1-port 1310 nm SMF, LC connector	5.2.0	AA1403001-E5
10GBASE-SR XFP	1-port 850 nm MMF, LC connector	5.1.0	AA1403005-E5
10GBASE-ZR/ZW XFP	1550 nm SMF LC connector	5.1.0	AA1403006-E5
10GBASE-LRM XFP	1310 nm, up to 220 m over MMF, DDI	5.2.0	AA1403007-E6

See *Nortel Ethernet Routing Switch 4500 Series Installation*, (NN47205-300) for more information.

Browsers for Online Help

Nortel supports the following browsers for Device Manager Online Help:

- Netscape
- Internet Explorer

Netscape specifics

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 online Help, perform the following procedure once, before requesting Help on a topic.

Configuring Netscape

Step	Action
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.

--End--

Supported standards, RFCs and MIBs

The following sections list the standards, RFCs and MIBs supported in Release 5.3.

Standards

The following IEEE Standards contain information pertinent to the Nortel Ethernet Routing Switch 4500 Series:

- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1s (Multiple Spanning Trees)
- IEEE 802.1w (Rapid Reconfiguration of Spanning Tree)
- IEEE 802.1X (EAPOL)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.1v (VLAN Classification by Protocol and Port)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3af (Power over Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet over Fiber-Optic)

RFCs and MIBs

For more information about networking concepts, protocols, and topologies, consult the following RFCs and MIBs:

- RFC 791 (IP)
- RFC 894 (IP over Ethernet)
- RFC 792 (ICMP)
- RFC 793 (TCP)

- RFC 1350 (TFTP)
- RFC 826 (ARP)
- RFC 768 (UDP)
- RFC 854 (Telnet)
- RFC 951 (BootP)
- RFC 1213 (MIB-II)
- RFC 1493 (Bridge MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2665 (Ethernet MIB)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 1757 (RMON)
- RFC 1271 (RMON)
- RFC 1157 (SNMP)
- RFC 1112 (IGMPv1)
- RFC 2236 (IGMPv2)
- RFC 1945 (HTTP v1.0)
- RFC 2865 (RADIUS)
- RFC 2674 (Q-BRIDGE-MIB)
- RFC 3410 (SNMPv3)
- RFC 3411 (SNMP Frameworks)
- RFC 3413 (SNMPv3 Applications)
- RFC 3414 (SNMPv3 USM)
- RFC 3415 (SNMPv3 VACM)
- RFC 3412 (SNMP Message Processing)
- RFC 3576 Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC 4673 RADIUS Dynamic Authorization Server MIB
- RFC 2131 BootP/DHCP Relay Agent

The following table lists IPv6 specific RFCs.

Table 10
Supported RFCs

Standard	Description	Compliance
RFC 2460	Internet Protocol v6 (IPv6) Specification	Supported
RFC 2461	Neighbor Discovery for IPv6	Supported
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 4443	Internet Control Message Protocol (ICMPv6)	Support earlier version of RFC (2463)
RFC 4301	Security Architecture for the Internet Protocol	Not supported
RFC 4291	IPv6 Addressing Architecture	Support earlier version of RFC (3513)
RFC 4007	Scoped Address Architecture	Supported
RFC 4193	Unique Local IPv6 Unicast Addresses	Not supported
RFC 4293	Management Information Base for IP	Mostly supported
RFC 4022	Management Information Base for TCP	Mostly supported
RFC 4113	Management Information Base for UDP	Mostly supported
RFC 1981	Path MTU Discovery for IPv6	Supported
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Supported
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack. No support for tunneling yet.
RFC 3162	RADIUS and IPv6	Supported
RFC 1886	DNS Extensions to support IPv6	Supported

Resolved issues

The following table lists the issues resolved for release 5.3.

Table 11
Resolved issues

Reference number	Description
Q01542038	**CLI, MAC SECURITY, STAND-ALONE UNIT**: MAC addresses added to the MAC Security table using the CLI now appear correctly in the MAC Security table.
Q01844743	**IPv6**: The install command and ip.cfg files now also support IPv6 as well as IPv6 configuration
Q01861555-02	**SNMP**: The SNMP objects s5ChasComDescr and s5ChasComSerNum are now available.
Q01867064	**NSNA**: An unknown device (static IP device not added to the NSNAS MAC database) will be correctly displayed with the **`show nsna client`** command after you reboot an IP phone which is connected between the device and the switch.
Q01869115	**IPv6**: If the stack is operating in Stack Forced mode and you want to set a switch IPv6 address, you no longer need to first delete the active IPv6 interface and then re-configure the switch IPv6 address.
Q01869210	**UDP Forwarding**: Now the switch issues a warning message if there are insufficient QoS filter resources available to enable UDP forwarding.
Q01876069-01	**NSNA**: A MAC authenticated session is no longer displayed on SNAS after the PC sends a DHCP release.
Q01879707	**EAP**: If the RADIUS key is reconfigured on the switch, then EAP or Non-EAP clients now automatically reauthenticate if reauthentication is enabled..
Q01882221	**IGMP**: The total number of Multicast groups are now displayed in Device Manager.
Q01910247	**DHCP Relay**: When forwarding DHCP packets, the DHCP Relay function no longer clears the DSCP markings on any incoming DHCP request packet.
Q01913212	**NSNA**: QoS filers used for NSNA can now be configured before or after NSNA is globally enabled on any switch port.

Reference number	Description
Q01920502-01	**Port Mirroring**: When port mirroring runs in XrxYtx mode with multiple MLT groups, port mirroring is activated without requiring a reboot of the switch.
Q01926349-01	**LLDP**: Nortel IP Phones can now correctly identify a switch using LLDP when connected to the ERS 4500.
Q01929409-01	**IPSG**: When moving a port to a different VLAN on which IPSG is enabled, the IPSG filter is now correctly removed from the previous port.
Q01930178	**IPv6, Web UI**: Configuration of the switch using the Web User Interface is now possible when using an IPv4 and/or an IPv6 address.
Q01948199	**IP.CFG**: The system no longer ignores the last character from the SNMP community string specified in the IP.CFG file.
Q01966011	**QoS, NNCLI**: A new NNCLI command, `show qos port`, displays information about the current QoS state of a port.
Q01966352	**SNTP**: SNTP can no longer be enabled on the switch unless either or both the primary and secondary SNTP server addresses are configured.
Q01969702	**AUR**: A warning or confirmation message is now displayed when configuration files are manually restored.
Q01981344	**AAUR/DAUR**: The feature now correctly functions in certain situations where the new unit has 5.0 or 5.1 agent or diagnostics.
Q01986547	**ACG**: RADIUS accounting is now fully supported in ASCII Configuration Generator (also known as show running config).
Q01992543	**NNCLI**: The command interpreter has been modified so that ’sh’ can be used as an abbreviation for the ’show’ command in all contexts. To provide a unique context for the shutdown command, you will need to enter ’shu’.
Q02002640-02	**Routing**: If the status of a static route is changed—for example disabled, then re-enabled—while the link to the next hop router is unreachable, then not all static routes become available when the connection to the next hop router returns to service.
Q02004709-03	**Web UI**: Under a certain type of Denial of Service attack against the HTTP server, the switch may crash.
Q02005179	**TACACS+**: An incorrect message, which was displayed when trying to authenticate after rebooting the stack, is no longer produced.
Q02009713-02	**Telnet**: In certain situations when you Telnet from the switch to an unreachable IP address, the switch CPU could reach 100% usage for a sustained time.

Known issues and limitations

Use the information in this section to learn more about known issues and limitations. Where appropriate, use workarounds provided for the known issues and limitations.

Navigation

Known issues and limitations

The following section lists known issues and limitations in Ethernet Routing Switch 4500 Series Software Release 5.3.

Table 12
Known issues and limitations

Reference number	Description
Q01496548	**Link-up during boot**: During reboot or power up operations, but before the agent code loads, the switch may provide an intermittent link to devices connected to front panel ports. Regardless, no traffic switching occurs until the agent code load completes.
Q01540397	**STP**: If Spanning Tree operation is not used on an LACP port, you must disable STP after you configure LACP.
Q01565427	**SONMP**: A change in the operation of Nortel’s SONMP-based auto topology means that directly connected BayStack 450 switches report a physical auto topology change every 70 seconds to the ERS 4500 switch. You can ignore this auto topology change message where there is a direct connection from the ERS 4500 to a BayStack 450 switch.

Reference number	Description
Q01585285	**JDM, Web UI, ASCII Configuration**: When loading an ASCII configuration file using DM or Web UI it is recommended that the switch has minimal configuration changes from default. Otherwise existing switch/stack configuration might cause warning or error messages that force the ASCII configuration to exit with a FAIL status. **Workaround**: Apply ASCII configuration from DM or WebUI to a switch or stack with basic configuration. Alternatively a currently configured switch/stack can be reconfigured using an ASCII configuration via CLI (console, telnet, SSH) since the system ignores warning and error messages and configuration continues until last ASCII file line executes.
Q01659099	**AAUR**: If a stack is powered up simultaneously running v5.1 or v5.2 software and one of the units in the stack is running v5.0, then the Automatic Agent upgrade of that unit to the latest software may not occur. In such situations the v5.0 unit can be forced to upgrade by delaying the powering on of that unit, or cycling the power on that unit to force AAUR to upgrade that unit.
Q01672222	**Jumbo Frames**: As the Ethernet Routing Switch 4500 supports jumbo frames (up to 9216), the Jabber counter will always be displayed as zero (0). **Workaround**: You can find information about framing errors in the etherStatsCRCAlignErrors counter.
Q01859015	**XFP**: The system may not display an older AA1403005 XFP as a supported XFP.
Q01878544	**NSNA**: For a MAC authenticated client, if the MAC address is deleted from the SNAS database, the SNAS does not send a reset event to the switch, so the client will remain in its currently assigned VLAN. **Workaround**: After deleting the MAC address from the SNAS database, disable then re-enable the port on which the device is located.
Q01879824	**EAP**: When an authenticated PC, initially placed behind an IP phone, is moved to another switch port and authenticated again, the “show eapol multihost status” command may incorrectly show the MAC address of the PC as being authenticated at both the old and new switch port location. **Workaround**: To avoid this situation, reauthentication should be enabled on the IP phone port, then the PC MAC address will be cleared from the old port when re-authentication occurs.
Q01893356-01	**NSNA**: After rebooting a switch or stack with NSNA MAC based clients connected, the switch may incorrectly report the devices in the RED VLAN even through they are actually in the Green VLAN. **Workaround**: Execute shutdown, then no shutdown commands on the corresponding ports.

Reference number	Description
Q01921829	**LLDP**: If 802.1 TLV for VLANs are already enabled for advertisement on a port, then the advertisement will not be updated to reflect any new VLAN additions. **Workaround**: Disable and re-enable TLV advertisement for the respective ports.
Q01931688	**USB**: As a precaution, when using the switch USB port, wait at least 5 to 10 seconds after insertion of a USB device before removing the device. The same 5 to 10 second pause should also be observed after removal of a USB device before inserting another USB device into the same switch unit.
Q01935593	**NSNA**: If you connect the SNAS directly to the switch with IP Routing with DHCP Relay enabled and you disable then re-enable NSNA on the switch, the switch will then be unable to reconnect to the SNAS. **Workaround**: Disable and re-enable the switch on the SNAS to regain switch to SNAS connectivity.
Q01970577	**EAP, Fail Open VLAN**: When a device is moved into or out of the Fail Open VLAN, there is no notification to the end client that the VLAN has been changed. **Workaround**: It is therefore recommended that if Fail Open VLAN is used, you should set the DHCP lease time to a short period so that clients would regularly refresh their IP address leases. Alternatively, if a client has been moved to the Fail Open VLAN, then issuing a DHCP release and renew on the client will obtain a new IP address appropriate for the Fail Open VLAN.
Q01977243	**QoS**: Non QoS applications, such as UDP Forwarding and IP Source Guard, should be configured prior to configuration of QoS policies to avoid the potential conflict in filter precedence order which can result when the binary configuration file is reloaded. In some rare cases, when QoS precedences are configured before non-QoS applications that use filters—for example: UDP Forwarding, NSNA, and IP Source Guard—the QoS information saved in the binary configuration file may not be correctly reloaded to the switch. The greater the number of filter-using non-QoS applications per port the greater the probability that the QoS information in the binary configuration file may be reloaded incorrectly. If the QoS information in the binary configuration file is reloaded incorrectly, some of the QoS precedences may not be configured correctly.
Q01977650	**IPv6, install command, software downgrade**: If a switch has an IPv6 address but no IPv4 management address configured and you downgrade to release 5.2, when you reboot the switch the install menu appears and prompts you for IPv4 management parameters. **NOTE**: All IPv6 settings are retained during the downgrade to Release 5.2 and the prompt for IPv4 management parameters appears only because there is no configured IPv4 information. **Workaround**: To leave the install menu and return to the normal NNCLI, press **CTRL+C**.

Reference number	Description
Q01979384	**IPv6**: Due to the short, or transient, nature of TCP connections for HTTP requests it is likely that IPv6 HTTP connections may not be displayed in show IPv6 TCP connection command. This behavior is considered normal. **Workaround**: If simultaneous Web page refresh commands are issued, then a `show IPv6 TCP connection` command will display active TCP connections for the Web session.
Q01981920	**EAP, Fail Open VLAN**: An EAP or Non-EAP client could be assigned to the Fail Open VLAN in normal operation if the VLAN name or ID returned from the RADIUS server matches the VLAN assigned for the Fail Open VLAN. **Workaround**: Ensure that the Fail Open VLAN name or ID used does not match one of the returned RADIUS VLANs.
Q01984470-01	**LLDP, 100FX SFP**: The LLDP advertises the dot3 Autonegotiation capabilities for slow speed SFPs as 1Gbps instead of the actual SFP link speed. This does not impact the forwarding of traffic over the SFP.
Q01984478	**EAP, Fail Open VLAN**: Non-EAP (NEAP) clients connected to the non-base unit of a stack will not be displayed as being authenticated when Fail Open VLAN is activated. This is a display issue as the NEAP clients on non-base units are, in fact, authenticated. Authentication will be correctly displayed when the clients revert to their normal VLAN when RADIUS server connectivity resumes.
Q01986757	**NSNA**: If you add a new classifier to the NSNA yellow QoS set (exceeding the resources), the yellow filters may not be applied.
Q01991335-01	**MLT/DMLT**: It may be possible to change the VLAN membership of administratively disabled MLT/DMLT ports. If you change the VLAN assignment on administratively disabled MLT/DMLT ports, the system prevents them from being added back into the MLT/DMLT group because the VLAN assignments of the links within the groups are inconsistent. If you want to change the VLAN membership for a MLT/DMLT group, you must: • disable all ports which are members of that group or disable the MLT/DMLT • make the necessary VLAN changes to all group members • re-enable the port or MLT/DMLT
Q01999027, Q01999072	**RSTP**: When operating as an RSTP root bridge and the base unit in a stack is reset, or the stack transitions to standalone mode, the SNMP trap message indicating a change in RSTP root may not always be generated. **Workaround**: A local log message for nnRstNewRoot is always generated.

Reference number	Description
Q02002291	**EAP, RADIUS Assigned VLAN**: The MAC address table temporarily displays duplicate entries for 802.1X clients using RADIUS assigned VLANs on non-base units in a stack and the MAC address table temporarily displays the MAC address in the original VLAN and the new RADIUS assigned VLAN. The system clears the duplicate entry from the original VLAN when MAC aging occurs on the port—the default MAC aging timer is set to 300 seconds. **Workaround**: As this is a temporary display issue, no functional impact should be observed. You can reduce the MAC aging timer setting to remove the duplicate display from the MAC table more rapidly.
Q02002916	**Asset ID**: The stack asset ID cannot be changed on a unit if that unit is no longer operating in stack mode. To change the stack asset ID you need to do one of the following: • Add the unit back into the stack. • Perform a factory default on the unit.
Q02002922	**RADIUS**: The Management VLAN must have an IP address assigned to enable management of the switch when using RADIUS authentication.
Q02005157	**Management VLAN**: When operating in Layer 3 mode, using the Management VLAN for normal routing may result in lost connectivity to the Management IP address. **Workaround**: If connectivity problems occur to the management IP address, clear the ARP cache.
Q02005676	**USB, ASCII Audit Log**: When you download an ASCII configuration from a USB storage device, the ASCII audit log incorrectly indicates that the configuration was loaded from the console. The system should have indicated that the configuration, including the specified file name, was successfully loaded from the USB device.
Q02006431	**MAC Security**: In the MAC security table, if you perform a repetitive add-remove of the same MAC address then connectivity for that client fail. **Workaround**: If connectivity for a connected device is lost, you can restore connectivity by generating a link down-up event by using one of the following methods: • unplugging and replugging the client port • using the `shutdown port` and `no shutdown port` NNCLI commands
Q02006993, Q02007429	**LLDP**: The LLDP location based TLV information for "Longitude" and "Datum" may not be correctly restored on a non-base unit in a stack. This can occur when a unit is upgraded to a new release or when AUR restores the configuration.

Reference number	Description
Q02007591	**QoS**: In order to simulate non-matching action using classifier-block, the most specific condition needs to be placed last in the classifier-block. Example: In order to deny all traffic received from network 10.0.0.0/8, excepting IP address 10.10.10.100/32, you can use the following method: **Step** **Action** **1** To define the most general condition, use the NNCLI command **`qos ip-element 1 src-ip 10.0.0.0/8`**. **2** To define most specific condition, use the NNCLI command **`qos ip-element 2 src-ip 10.10.10.100/32`**. **3** To define for both filters, use the NNCLI commands **`qos classifier 1 set-id 1 element-type ip element-id 1`** and **`qos classifier 2 set-id 2 element-type ip element-id 2`**. **4** To place the classifier related to the most general condition into the classifier block first, use the NNCLI command **`qos classifier-block 1 block-number 1 set-id 1 in-profile-action 1`**. **5** To place the classifier related to most general condition into classifier block last, use the NNCLI command **`qos classifier-block 2 block-number 1 set-id 2 in-profile-action 9`**. **6** To configure the QoS policy, use the NNCLI command **`qos policy 1 port 17 clfr-type block clfr-id 1 preced 6 track-statistics individual`**. **--End--**
Q02008078	**EAP**: If a binary configuration file contains EAP configurations, then EAP can be enabled when loading the binary configuration file even if no IP address is set on the switch. This could result in some connectivity issues because a switch without an IP address cannot perform appropriate 802.1X authentication to the RADIUS server. **Workaround**: Ensure that a management IP address is configured before loading a binary configuration file containing EAP configuration.
Q02011548	**NSNA**: After units are rebooted in an operational stack, some static MAC authentication clients may be incorrectly displayed as a 0.0.0.0 IP address instead of the correct IP address. This is a display issue only and does not affect functionality. **Workaround**: Use the SNAS to show the correct IP associations.

Reference number	Description
Q02013766	**EAP**: When a port is configured for RADIUS Last Assigned VLAN, if the last RADIUS authentication for that port does not contain QoS priority, then the port priority will be either the one manually configured or the one received for the previous authenticated client.
Q02013848	**Port mirroring mode**: The port mirroring mode asrc and adst cannot mirror packets generated by the CPU such as: LACPDUs, LLDPDUs, BPDUs, and SONMP. **Workaround**: CPU-generated packets can be mirrored with port-mirroring mode XTX.
Q02016200	**CPU utilization**: The CPU utilization reported for the ’last 10 minute interval’ may be higher than actual if the CPU was loaded at 100% for the first 5 minutes then returns to an idle state for the next 5 minutes. All other values are correctly calculated. The value will be properly displayed after 30 minutes if the CPU load returns to normal activity levels.
Q02016728-01	**IPv6, ASCII Load on Boot**: The ASCII Load on Boot feature cannot download the configuration file from the TFTP server if only an IPv6-based TFTP server is configured. **Workaround**: Configure the switch with an IPv4 management address.
Q02017737	**QoS**: Modification of a QoS action will not be applied as long as the action is referenced by an active QoS policy. **Workaround**: Disable, then re-enable the QoS policy to apply the modified QoS action.
Q02019507	**EAP, Guest VLAN, ADAC**: When Guest VLAN is enabled on a port where an IP Phone authenticates using ADAC, after authentication of the IP Phone a PC connected to the switch will no longer have access to the Guest VLAN. **Workaround**: Use of the DHCP signature method to authenticate the IP Phone will enable the switch to support Guest VLAN functionality after the IP Phone has been authenticated.
Q02019722	**Web based management, show environmental**: Temperature is not displayed in the Web UI for the base unit if the Secure agent image is used. **Workaround**: Use Device Manager or NNCLI to view the information.
Q02019728	**Web based management, show environmental**: Temperature is not displayed in the Web UI for units that have an RPS connected. **Workaround**: Use Device Manager or NNCLI to view the information.
Q02019768	**ACG**: The SNTP IPv6 address is not saved in the ASCII configuration file. **Workaround**: Use a binary configuration to correctly store the SNTP server IPv6 address.

Reference number	Description
Q2020144-01	**Security, Audit Log**: When audit logging is enabled and you change the password using NNCLI, the audit log records the password in clear text when running the standard agent image with password security disabled. If you run the Secure image, the password is obscured in the audit log. **Workaround**: Do one of the following: • Enable password security. • Disable the audit log before changing the switch password.
Q02021402	**EAP, Guest VLAN, Fail Open VLAN**: When a PC is connected behind an IP Phone and the port enters and then leaves the Fail Open VLAN it can take up to 90 seconds before the port transitions into the Guest VLAN.
Q02021599	**EAP, Guest VLAN**: If a Guest VLAN is configured for a port and the EAP supplicant being used sends an EAP logoff message to the switch, then the switch may subsequently restrict any traffic within the Guest VLAN for that port. **NOTE**: Standard Windows supplicants do not exhibit this problem. **Workaround**: You can restore the port to normal Guest VLAN operational mode by any of the following methods: • Unplug and replug the cable from the client port. • Use the NNCLI commands `shutdown port` and `no shutdown port`. • Disable and re-enable EAP on the port using the NNCLI commands `eap status authorized` and `eap status auto`. • Disable and re-enable EAP globally using the NNCLI commands `no eapol` and `eapol enable`.
Q02027769	**EAP**: When EAP performs authentication through TTLS, the first authentication between the supplicant and the switch may fail but subsequent authentications will succeed. **Workaround**: If authentication fails when using EAP-TTLS, do one of the following: • Wait 30 seconds for the client to re-authenticate successfully. • Use an alternative EAP authentication mechanism for the client.
Q02027845	**EAP, ADAC, LLDP, IP Phone**: When you use a third party IP Phone with ADAC, if LLDP is used as the discovery mechanism the phone will not authenticate through EAP. **Workaround**: Add the MAC address range for the third party IP Phone into ADAC for discovery. Then ADAC can perform discovery correctly and EAP can authenticate the IP Phone.

IPv6 limitations

The following table lists limitations specific to the implementation of IPv6 in this release.

Table 13
IPv6 limitations

Reference number	Description
1	IPv6 Management should only be configured from a base unit in stack.
2	Only one IPv6 address can be configured and it will be associated to the management VLAN.
3	No DHCP/BOOTP, Stateless Address Autoconfiguration or IPv6 loopback address is supported for the management address.
4	The only IPv4 to IPv6 transition mechanism supported is dual-stack (no tunnelling).

Nortel Ethernet Routing Switch 4500 Series

Release Notes — Release 5.3

Release: 5.3
Publication: NN47205-400
Document revision: 05.01
Document release date: 25 May 2009

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OFANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

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

www.nortel.com