Nortel Ethernet Routing Switch 4500 Series

Release Notes — Software Release 5.2

NN47205-400

Document status: Standard
Document version: 04.01
Document date: 12 November 2008

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 OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Contents

New in this release

The following sections detail what’s new in Nortel Ethernet Routing Switch 4500 Series Release Notes — Software Release 5.2.

Features

See the following sections for information about feature changes.

- "IP local and static routes" (page 9)
- "BOOTP and DHCP RELAY" (page 10)
- "IP Source Guard" (page 10)
- "TACACS+" (page 10)
- "802.1X RFC 3576" (page 10)
- "802.1AB MED support" (page 10)
- "802.1AB Location TLV" (page 10)
- "IPv6 management" (page 10)
- "JDM PoE enhancements" (page 10)
- "Backup CONFIG file" (page 11)
- "Stack health check" (page 12)
- "Disable USB and Console" (page 12)
- "Stack Forced Mode " (page 12)
- "Diagnostics AUR (DAUR)" (page 13)
- "RSTP SNMP traps" (page 13)
- "Increase PoE power" (page 10)
- "IP.CFG enhancements" (page 11)
- "AUR improvements" (page 12)
- "Extended password history" (page 12)
- "Extended IP Manager" (page 14)
- "VLACP enhancement " (page 14)

- "CPU utilization" (page 14)
- "Show commands" (page 14)

Other changes

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

File names for upgrade

File names are updated; see "File names for this release" (page 16).

Windows Vista

Windows Vista was added to the section "Windows" (page 17).

Hardware and software compatibility

Hardware and software compatibility information is moved to this document. See "Hardware and software compatibility" (page 28).

Document changes

This document is reformatted to comply with the Nortel Customer Documentation Standards. For more information, see *Nortel Ethernet Routing Switch 4500 Series Documentation Roadmap*, NN47205-101.

Introduction

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Nortel Ethernet Routing Switch 4500 Series, Software Release 5.2.

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 5.2, includes the following switch models:

- Nortel Ethernet Routing Switch 4524GT
- 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 4550T
- Nortel Ethernet Routing Switch 4550T-PWR
- Nortel Ethernet Routing Switch 4548GT
- Nortel Ethernet Routing Switch 4548GT-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 5.2, 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" (page 9)
- "Resolved issues" (page 35)
- "Known issues and limitations" (page 39)

Important notices and new features

This section contains a brief synopsis of the new features in release 5.2 and any important notices.

Navigation

This section includes the following sections:

- "New features in Release 5.2" (page 9)
- "File names for this release" (page 16)
- "Hardware and software compatibility" (page 28)
- "Supported standards, RFCs and MIBs" (page 31)

New features in Release 5.2

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.

- "Software features in Release 5.2" (page 9)

Software features in Release 5.2

This section lists some of the software features supported on the Nortel Ethernet Routing Switch 4500 Series switches. For specific information, see *Nortel Ethernet Routing Switch 4500 Series Roadmap*, NN47205-101.

General software features The following sections summarize the main software features supported in this release.

IP local and static routes This release supports both local and static IP routing between VLANs and across the stack. This release supports a maximum of 256 local and 32 static routes along with a default route. You can enable or disable IP forwarding for all VLANs. IP Routing also supports the additional functionality of IP Blocking, UDP Forwarding and Proxy ARP.

BOOTP and DHCP RELAY This feature is used when you enable IP Routing on a VLAN, so that Bootp or DHCP requests can be relayed from the routed VLAN to the appropriate servers.

IP Source Guard This is a layer2 security feature which leverages the IP address binding learned through DHCP snooping. IP Source Guard ensures that only devices which have a valid IP address binding for a certain port are able to send traffic from that source IP address. Any other traffic with a different source unicast IP address will be blocked to prevent masquerading as a different IP address.

TACACS+ This feature provides access control for the management of the switch through one or more centralized TACACS+ servers as an alternative to RADIUS. Additionally, TACACS+ provides separate authentication, authorization and accounting services.

802.1X RFC 3576 This feature allows RFC 3576 compliant RADIUS servers or third party NAC devices to dynamically change the VLANs on the switches, without requiring the client to initiate the 802.1x/RADIUS exchange. Additionally, it allows the server to actively terminate the user session. RFC 3576 captures additional RADIUS commands to support unsolicited messages, disconnect and Change of Authorization, from the RADIUS server/NSNA.

802.1AB MED support This feature enables additional VoIP plug-n-play capabilities by supporting the advertisement of the switch capabilities via 802.1AB Media Descriptor (MED).

802.1AB Location TLV This feature enables phase I of E911 location based services through the provisioning of location based information for each port of the switch. This location information is then shared with the end device through 802.1AB Location Based TLV.

IPv6 management This feature provides management support for the switch or stack through IPv6. Functionality includes IPv6 host access to the switch, as well as access to a number of management functions over IPv6.

JDM PoE enhancements This feature provides JDM enhancements to enable you to configure port PoE priority and power limit. You can display actual power usage per port.

Increase PoE power Through the Energy Efficient design utilized on the ERS4500, certain models of the ERS4500 support additional PoE power budget delivery when operating on AC power in this software upgrade, effectively offering extra PoE for existing models. The ERS4526T-PWR and 4550T-PWR both deliver an additional 50 W of PoE for a maximum of 370 W when operating on AC only. The ERS4526GTX-PWR delivers an additional 40 W of PoE for a maximum of 360 W when operating on AC only. The PoE capacity of the 4548GT-PWR when operating on AC only remains unchanged at 320 W.

Backup CONFIG file This feature prevents the corruption of the configuration file in the case of a power failure occurring during the process of writing the configuration to NVRAM, through the creation of an automatic backup configuration file. When the switch boots, if it detects a corrupted primary configuration, the switch automatically loads the backup configuration file and generates an appropriate log entry.

IP.CFG enhancements Enhanced IP.CFG capability enables you to provision a switch with a file on a USB drive in this software release. These enhancements allow for case insensitive operation and improved logging as well as the ability to load diagnostic and agent code images from the USB drive during this provisioning activity.

Software release 5.2 provides the following enhancements to ip.cfg:

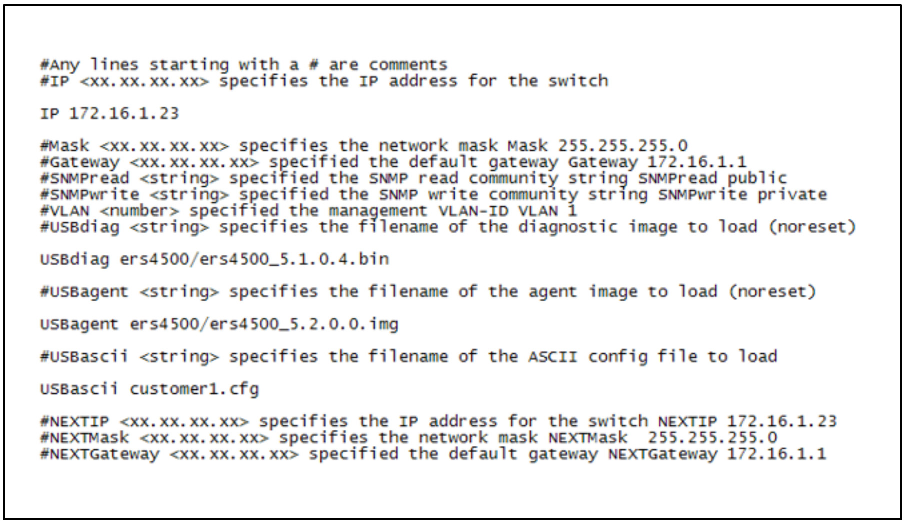
- If a properly formatted file exists on a USB port device, the switch uses that ip.cfg as the first option, rather than the last.
- The file name, ip.cfg, is case-insensitive.
- If there is an error parsing the ip.cfg file, a log entry provides an indication of the error encountered.
- Enables you to upload the specified image and diag from the USB drive without a switch or stack reset.
- Enables you to specify an ASCII configuration file to load from the USB drive.
- Enables you to set the next boot IP address for the switch.

The following limitations apply to ip.cfg:

- ip.cfg runs only on a base unit or stand-alone unit.
- The file cannot be more then 4096 bytes.
- The file cannot contain more then 200 lines.

The following graphic shows an example of an ip.cfg file.

Figure 1
ip.cfg file example



```
#Any lines starting with a # are comments
#IP <xx.xx.xx.xx> specifies the IP address for the switch

IP 172.16.1.23

#Mask <xx.xx.xx.xx> specifies the network mask Mask 255.255.255.0
#Gateway <xx.xx.xx.xx> specified the default gateway Gateway 172.16.1.1
#SNMPread <string> specified the SNMP read community string SNMPread public
#SNMPwrite <string> specified the SNMP write community string SNMPwrite private
#VLAN <number> specified the management VLAN-ID VLAN 1
#USBdiag <string> specifies the filename of the diagnostic image to load (noreset)

USBdiag ers4500/ers4500_5.1.0.4.bin

#USBagent <string> specifies the filename of the agent image to load (noreset)

USBagent ers4500/ers4500_5.2.0.0.img

#USBascii <string> specifies the filename of the ASCII config file to load

USBascii customer1.cfg

#NEXTIP <xx.xx.xx.xx> specifies the IP address for the switch NEXTIP 172.16.1.23
#NEXTMask <xx.xx.xx.xx> specifies the network mask NEXTMask  255.255.255.0
#NEXTGateway <xx.xx.xx.xx> specified the default gateway NEXTGateway 172.16.1.1
```

See "Setting IP parameters with the ip.cfg file on a USB memory device" (page 25) for more information about the ip.cfg file.

Stack health check This feature allows you to run a high level non-intrusive test to confirm stack operation and stack continuity so you can see the overall health of the stack.

Disable USB and Console This feature provides an enhancement to disable local management ports on the switch for improved security. You can explicitly disable or enable the Console and USB ports on the switch.

Extended password history This feature allows you to configure the number of password histories up from the current stored history of three passwords to ten histories.

Stack Forced Mode When you enable this feature in a stack of two switches, on the failure of a unit, the remaining switch retains the stack IP address ensuring continued management access to the remaining unit.

AUR improvements This feature introduces two enhancements to AUR functionality to improve operation in certain failure scenarios. The first enhancement provides the ability to disable configuration synchronization to the base unit after AUR performs the first synchronization. This ensures that if a unit configuration becomes corrupted, then that configuration is not automatically synchronized to the base unit.

Customers can explicitly force synchronization when automatic synchronization is disabled via an appropriate NNCLI command. The second AUR enhancement allows you to force the reload of a configuration to a switch in the stack using AUR if for some reason you suspect the configuration on the unit may be corrupted.

This feature is not compatible with a unit running release 5.0 software.

Diagnostics AUR (DAUR) This feature performs an upgrade of the diagnostics image on inserted units in the same way that AAUR performs this function for the agent code. When you enable or disable AAUR, you enable or disable DAUR.

This feature is not compatible with a unit running release 5.0 software.

RSTP SNMP traps The Rapid Spanning Tree Protocol (RSTP) SNMP traps feature provides the ability to receive SNMP notifications about the RSTP protocol. Syslog also logs the RSTP events.

The RSTP SNMP traps generate the following events:

- nnRstNewRoot: Generated when a new root bridge is selected in the topology.
- nnRstTopologyChange: Generated when a topology change is detected.
- nnRstProtocolMigration: Generated whenever a protocol migration appears on the port. There are two types of protocol migration: when the port sends STP BPDUs or when the port sends RSTP BPDUs.

See the *Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and Multi-Link Trunking* (NN47205-501) guide for configuration information for RSTP SNMP traps.

Examples The following examples show how each RSTP SNMP event appears in Device Manager (DM) and syslog trap logs:

nnRstNewRoot notification in DM trap log
nnRstNewRoot
dot1dBaseBridgeAddress.0=00:1d:42:37:d0:00 ,
nnRstDot1wOldDesignatedRoot.0=90:00:00:1d:42:37:d0:00 ,
dot1dStpDesignatedRoot.0=80:00:00:1d:42:36:0c:01

nnRstNewRoot notification in syslog

```
Trap:  RSTP New Root:  80:00:00:01:42:36:0C:01
```

nnRstTopologyChange notification in DM trap log
nnRstTopologyChange dot1dBaseBridgeAddress.0=00:1d:42:37:d0:00

nnRstTopologyChange notification in syslog

```
Trap:  RSTP Topology Change
```

sendSTP nnRstProtocolMigration notification in DM trap log

nnRstProtocolMigration
dot1dBaseBridgeAddress.0=00:1d:42:37:d0:00 ,
nnRstDot1dStpVersion.0=stpCompatible ,
nnRstPortNotificationMigrationType.13=sendstp

sendSTP nnRstProtocolMigration notification in syslog

```
Trap:  RSTP Protocol Migration Type:  Send STP for
Unit/Port:  1/13
```

sendRSTP nnRstProtocolMigration notification in DM trap log

nnRstProtocolMigration
dot1dBaseBridgeAddress.0=00:1d:42:37:d0:00 ,
nnRstDot1dStpVersion.0=rstp ,
nnRstPortNotificationMigrationType.13=sendrstp

sendRSTP nnRstProtocolMigration notification in syslog

```
Trap:  RSTP Protocol Migration Type:  Send RSTP for
Unit/Port:  1/13
```

Extended IP Manager The IP Manager allows you to limit access to the different switch functions (Telnet, Web-based management, SNMP and SSH) for both IPv4 and IPv6.

VLACP enhancement This release includes a number of enhancements which are detailed in the Resolved Issues section.

CPU utilization This feature provides CPU utilization for the last 10 seconds, 1 min, 1 hour, 24 hours and from system start. The information shows how the CPU was loaded for the specific time average and provides the CPU utilization as a percentage.

The memory utilization provides you with information on what percentage of the dynamic memory is currently used by the system. Also, the memory utilization shows a low watermark percentage which represents the lowest percentage of the dynamic memory available since system start.

Show commands This release adds the following show commands:

- show cpu-utilization
- show memory-utilization
- show mac-address-table
- show ip route

- show ip arp
- show ip dhcp-relay
- show lacp aggr
- show lacp port

Multi-Link Trunking Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups have been increased from 6 groups to 8 groups

Supported software and hardware capabilities

The following table lists supported software and hardware scaling capabilities in Ethernet Routing Switch 4500 Series Software Release 5.2. 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	4
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

Feature	Maximum number supported
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 stack	384
LLDP Neighbors per port	16
LLDP Neighbors	800
RMON alarms	800
RMON events	800
RMON Ethernet statistics	110
RMON Ethernet history	249

Software licenses

Nortel Ethernet Routing Switch 4500 Series Software Release 5.2 does not support software licenses at this time.

File names for this release

"Software Release 5.2 components" (page 16) describes the Nortel Ethernet Routing Switch 4500 Series, Software Release 5.2 software files. File sizes are approximate.

Software Release 5.2 components

Module or file type	Description	File name	File size (bytes)
Standard runtime image software version 5.2.0.008	Standard image for the Nortel Ethernet Routing Switch 4500 Series	4500_520008.img	5,788,748
Secure runtime image software version 5.2.0.009	Secure image for the Nortel Ethernet Routing Switch 4500	4500_520009s.img	6,043,828
Boot/diagnostic software version 5.2.0.3	Switch diagnostic software	4500_5203_diag.bin	1,589,532

Module or file type	Description	File name	File size (bytes)
Device Manager software version for Windows	Device Manager software image for Windows NT, Windows Vista, Windows XP, Windows 2003, Windows 2000	jdm_6150.exe	194,379,901
Device Manager software version for UNIX	Device Manager software image for Solaris	jdm_6150_solaris_sparc.sh	220,785,627
Device Manager software version for Linux	Device Manager software image for Linux	jdm_6150_linux.sh	199,977,947
Software Release 5.2 Management Information Base (MIB) definition files	MIB definition files	Ethernet_Routing_Switch_45xx_MIBs_5.2.0.zip	1,371,741

Supported traps and notifications

For a complete list of log messages generated by Ethernet Routing Switch 4500 Series Software Release 5.2, see Nortel *Ethernet Routing Switch 4500 Series Logs Reference* (NN47205-701).

For a complete list of SNMP traps generated by Ethernet Routing Switch 4500 Series Software Release 5.2, see Nortel *Ethernet Routing Switch 4500 Series Troubleshooting* (NN47205-700).

Device Manager installation requirements

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

See *Nortel Ethernet Routing Switch 4500 Series Fundamentals*, NN47205-101 for more information on Device Manager installation requirements.

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 5.2, Nortel recommends that you upgrade the diagnostic software to the 5.2.0.3 version, and then upgrade the agent version to release 5.2.

The following table describes possible image locations:

Table 2
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

You can upgrade the Agent Image in your switches from an earlier release image. The following table provides the Agent Image downgrade or upgrade chart:

Table 3
Agent Image downgrade or upgrade chart

Local Agent Image version	Download Agent Image version		
	5.0	5.1	5.2
5.0	Yes	Yes—if Local Diagnostic Image is 5.1.0.7 Diag Image.	Yes—if Local Diagnostic Image is 5.1.0.7 Diag version or 5.2.0.3 Diag version.
5.1	Yes	Yes	Yes
5.2	Yes	Yes	Yes

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

Upgrading Agent Image from release 5.0 or 5.1 to release 5.2

Step	Action
1	Upgrade the diagnostic image from the earlier release to release 5.2.0.3 diagnostic image.
2	Upgrade the agent image from release 5.0 or 5.1 to release 5.2 agent image.

—End—

> ***Note:*** If the you have an existing Stack with mismatched Diagnostics, the Base will not allow you to load the agent. If an error occurs when you try to upgrade the software, check that the software and Diagnostics versions all match by running the `Show Tech` command.

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 Nortel Ethernet Routing Switch 4500 Series 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 20)
- "Changing switch software in NNCLI" (page 20)
- "Changing switch software in Device Manager" (page 21)

- "Changing switch software in Web-based management" (page 24)

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

Table 4
download parameters

Parameter	**Description**
The **`image, image-if-newer, diag`**, and **`poe_module_image`** 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.	
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 Nortel Ethernet Routing Switch 4500 Series 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**.

The File System screen appears.

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 The following table describes the File System screen fields.

Table 5
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.

Field	Description
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 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.

Field	Description
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** . The Software Download Management page appears.
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 The following table describes the software download page fields:

Table 6
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.
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 7
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: 192.168.22.1
SNMPread <string>	Specifies the SNMP read community string. Example: public
SNMPwrite <string>	Specifies the SNMP write community string. Example: private
VLAN <number>	Specifies the management VLAN-ID. Example: VLAN 1

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 8
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
1000BaseCWDM SFP	1470 nm LC connector, up to 40 km	5.0.0	AA1419025-E5
1000BaseCWDM SFP	1490 nm LC connector, up to 40 km	5.0.0	AA1419026-E5
1000BaseCWDM SFP	1510 nm LC connector, up to 40 km	5.0.0	AA1419027-E5
1000BaseCWDM SFP	1530 nm LC connector, up to 40km	5.0.0	AA1419028-E5
1000BaseCWDM SFP	1550 nm LC connector, up to 40 km	5.0.0	AA1419029-E5

Supported SFPs and XFPs	Description	Minimum software version	Part number
1000BaseCWDM SFP	1570 nm LC connector, up to 40 km	5.0.0	AA1419030-E5
1000BaseCWDM SFP	1590 nm LC connector, up to 40 km	5.0.0	AA1419031-E5
1000BaseCWDM SFP	1610 nm LC connector, up to 40 km	5.0.0	AA1419032-E5
1000BaseCWDM SFP	1470 nm LC connector, up to 70 km	5.0.0	AA1419033-E5
1000BaseCWDM SFP	1490 nm LC connector, up to 70 km	5.0.0	AA1419034-E5
1000BaseCWDM SFP	1510 nm LC connector, up to 70 km	5.0.0	AA1419035-E5
1000BaseCWDM SFP	1530 nm LC connector, up to 70 km	5.0.0	AA1419036-E5
1000BaseCWDM SFP	1550 nm LC connector, up to 70 km	5.0.0	AA1419037-E5
1000BaseCWDM SFP	1590 nm LC connector, up to 70 km	5.0.0	AA1419039-E5
1000BaseCWDM SFP	1610 nm LC connector, up to 70 km	5.0.0	AA1419040-E5
1000Base-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
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

Supported SFPs and XFPs	Description	Minimum software version	Part number
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 on-line 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 5.2.

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 802.1X (EAPOL)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3x (Flow Control)
- IEEE 802.3ad (Link Aggregation)

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 9
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)

Standard	Description	Compliance
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 5.2.

Table 10
Resolved issues

Reference number	Description
Q01511719	**ACG**: MSTP/RSTP settings are now saved in the ASCII configuration when the ‘show running-config’ command is issued
Q01530630	**Telnet**: the number of active telnet sessions connected to the switch is now displayed.
Q01645390, Q01644606	**VLACP**: The VLACP PDU transmission interval is changed in event of a loss of LACP partner, this improved detection in certain failure scenarios.
Q01645430	**VLACP**: processing of the VLACP PDU messages has been changed to prevent false VLACP state recovery.
Q01728739-02	**DHCP** snooping: the CLI output now displays the current DHCP “Time-To-Expiry" in the output for learnt DHCP addresses.
Q01800043	**VLACP**: when only one switch is configured for VLACP, the link is maintained to allow configuration of the other end of the link to proceed.
Q01823184	**FDB**: the Show mac-address-table command now displays the MAC addresses for all VLANs by default.
Q01840036	**Password**: when changing the password on a stack, the password is now applied to all units in the stack. So that if a unit is removed from the stack the new password has been applied to that unit when operating in standalone mode.
Q01846113-01	**JDM**: now provides the ability to clear DHCP relay counters.
Q01859324	**LLDP**: the ‘show lldp neighbor’ command now displays the total number of neighbors. displays total neighbors
Q01870687	**AAUR**: A log message is produced whenever AAUR functions to upgrade agent code on a newly inserted unit.
Q01870703	**Bootp**: the switch will now load a configuration file from a TFTP server specified in a bootp response, this will allow Zero Touch Edge configuration.
Q01882805	**RMON**: provide an ‘show rmon alarm’ enhancement to sort RMON alarms in reverse order or via index.

Reference number	Description
Q01695470	**IPMGR**: provide the ability for IP Manager to control access for SSH sessions.
Q01495527	**DM**: port mirroring settings can now be viewed and modified in JDM with ERS4500.
Q01863632	**DM**: DHCP snooping table now displays a “Time-to-Expire” field for each learnt DHCP address.
Q01532525	**IPMC**: CLI now provides an output of the number of current multicast group.
Q01764161	**LLDP**: 802.1AB / Link Layer Discovery Protocol now supports MED functionality on ERS4500.
Q01766331	**DMLT**: If DMLT detects a VLAN inconsistency on a link, rather than disabling the trunk, DMLT now forces the VLAN configuration on the inconsistent link and then enables the trunk.
Q01769859	**SNMP**: When operating in Layer2 mode the index value returned ipAdEntIfIndex (1.3.6.1.2.1.4.20.1.2) will now be associated with the interface identified with the same value of ifIndex.
Q01749773	NSNA FO VLAN/filter-ID shouldn’t be set if the VLAN does not exist
Q01557789	**SSH**: You can now download the SSH authorization key from a USB device from non-base units in a stack.
Q01542038	**CLI, MAC Security**: MAC addresses added to the MAC Security table using the CLI now correctly appear in the MAC Security table.
Q01770094	**LAG**: 802.3ad LAGs now operate the same on the ERS4500 as on the ERS5500 and ES470. Now when a single link remains in a LAG, the switch continues to treat the LAG as an aggregation group. This means that if a LAG with 2 or more members is reduced to 1 link, then no longer will a STP or RSTP state change occur, which would have resulted in network reconvergence.
Q01773986	**AppleTalk**: Appletalk user defined protocol-vlans are now supported on the ERS4500.
Q01781349	**SNMP server**: The snmp-server host configuration is now correctly saved to the configuration file if autosave to NVRAM is disabled and the ’copy config nvram’ command is used.
Q01781360	**MAC Security**: When operating an ERS4500 stack with MAC security enabled, if the power is simultaneously removed from all but one non-base unit in the stack, then traffic on the remaining unit may be impacted. Depending on where the MAC addresses were previously learnt within the stack, they were intermittently treated as intruders by the MAC security application.
Q01781385	**Autosave / power down**: When operating in a stack of 3 or more ERS4500 switches with autosave disabled, if the base unit and other non-base units, with DMLT configured, were powered down simultaneously immediately after issuing the ‘copy config nvram’ command, then the DMLT configuration may become corrupted.

Reference number	Description
Q01788992, Q01788992-01, Q01812612	**IGMP/DMLT**: When an IGMP query was received across a DMLT connection and the IGMP query was not received on the first link in the DMLT, then the IGMP query was reflected back across the DMLT links.
Q01793281	**FDB**: When issuing the show mac-address-table command, the number of MAC addresses reported in the summary header would sometimes not equal the number of addresses displayed in the table. The list of MAC addresses displayed in the table was always correct.
Q01795339	**Autosave**: If autosave to NVRAM was disabled and the switch was then loaded with a binary configuration file, then sometimes the switch configuration may be reset to factory defaults. This did not occur if autosave was enabled (the default setting).
Q01815923	**MAC Security**: When operating an ERS4500 stack with MAC security enabled, if the power is simultaneously removed from all but one non-base unit in the stack, then MAC security may not correctly relearn addresses if devices are moved to different ports during this outage.
Q01822912	**SFP**: Some SFPs (AA1419043-E5 or AA1419043-E6) used in the ERS4500 would not display the full vendor specific information
Q01829977	**RPS15 Hot Swap**: In some circumstances, the ERS4500 may incorrectly report a s5CtrHotSwap trap indicating a change in availability of the RPS15. The switches DC_Good signal sampling algorithm has been improved to stop the generation of these false error messages
Q01830468	**PoE**: In some situations when a ERS4500 PWR switch is subjected to very high Electrostatic discharge (ESD) Cable Discharge events PoE will become disabled on all ports, but will again provide power if the switch is reset or the PoE subsystem is reset. The software now detects this event correctly and PoE functionality is restored.
Q01833016	**NEAP**: When a device such as an IP Phone is connected to the switch with 802.1X authentication enabled, in some situations when NEAP (Non-EAP Authentication) is used to authenticate the IP Phone, the ERS4500 incorrectly discards packets from that device due to the device being treated as an intruder.
Q01764161	**ADAC**: 802.1AB (LLDP) System Capabilities TLV is used to detect a LLDP enabled IP phone in combination with LLDP MED if enabled.
Q01680347	**RMON**: When renumbering the stack units, the RMON Alarm port indexes are not properly renumbered following the switch unit renumbering. If you are using RMON Alarms and subsequently renumber the stack units, you need to re-configure the RMON Alarms table.
Q01614537	**LLDP**: LLDP local-mgmt-addr TLV is not longer disabled when a temporary base unit takes over operation of a stack.
Q01839829	**Telnet**: When the login timeout is set to a short time period, every time this timeout expired for the console port a message ’login timeout serial connection was generated in the system log, which could fill up the log file with these messages.

Reference number	Description
Q01860630	**JDM**: For a MLT link, JDM incorrectly counted tagged packets that exceed 1518 byte as “FramesTooLong”
Q01837389-02	**SSH**: When attempting to connect to a Nortel switch from a Cisco router using SSH an invalid protocol version exchange can cause the SSH session to not establish.
Q01895395, Q01895523	**DHCP** Snooping: DHCP request packets which contain the padding option (0x00) in the vendor information field re incorrectly dropped. Some Lexmark network printers use this padding option and consequently could not receive a DHCP reply when DHCP snooping was enabled.
Q01899506	**Telnet**: If a telnet session to the switch has an active command running (for example tftp of a file) and that telnet session is terminated, a new telnet session will not be able to be established until the current command has completed.
Q01724940	**MLT/DMLT**: redistribution of traffic over links of a MLT or DMLT trunk is now more rapid when a failed link is restored to service.

Known issues and limitations

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

Navigation

- "Known issues" (page 39)
- "Known limitations" (page 39)

Known issues

The following section lists known issues in Ethernet Routing Switch 4500 Series Software Release 5.2.

Reference number	Description
Q01750467	**Rate Limiting Clarification**: When configuring rate limiting, the user configures a percentage of port bandwidth based upon the current operational speed. Rate limiting is implemented in the hardware based on packet per second. Based upon an average packet size of 500 bytes the packet per second rate is computed. For example, if a user had specified to limit the forwarding rate of broadcast packets to 1000 packets/second, any additional broadcast packets are discarded when the broadcast packet rate exceeds the threshold value. During each second first 1000 broadcast packets are allowed, then any additional broadcast packets which arrives on this port until the next second are discarded.
Q01683286	**RMON**: Owner configuration is lost after reboot. When configuring a RMON alarm with an owner, the owner configuration is not kept after reboot. The owner is displayed as "Entry from NVRAM".

Known limitations

The following table lists known limitations and workarounds for the Ethernet Routing Switch 4500 Series switches.

Table 11
Known limitations

Reference number	Description
Q01351184	**Port speed mismatch**: If you link two ports explicitly set for different speeds (for example one configured as 10BaseT and the other as 100BaseTX) the port link LED may indicate a link, but the switch does not establish a link. **Workaround**: Connect ports using the same set speed or use auto-negotiation on each switch.
Q01353078	**Diagnostics:** Autobaud is not supported. If you change the terminal speed and then reboot the unit, non relevant characters appear in the display. **Workaround**: Use only 9600 (baud rate) for terminal speed.
Q01374109	**PoE**: If you connect one type of Power over Ethernet switch to another, for example a 4548GT-PWR and a 4550T-PWR, one switch may deliver power to the other. This is due to the PoE Legacy Type Detection.**Workaround**: Legacy detection can be disabled on the switch if you are not using any PoE devices which require legacy detection. An alternate solution is to administratively disable Power over Ethernet on ports interconnecting any two Power over Ethernet switches.
Q01479196 Q01480192 Q01481181 Q01481218 Q01749862	**Web-based management**: Web-based management supports only alpha-numeric characters. Use only apha-numeric characters in the creation of elements. For example, if you create a VLAN in the NNCLI or the Device Manager using characters that are not alpha-numeric, you cannot delete the VLAN within the Web Interface.
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 remote devices connected to front panel ports. Regardless, no traffic switching occurs until the agent code load completes.
Q01514147	**NNCLI**: On the console, the SNMP server name is intentionally truncated to provide enhanced user experience. On the Web interface, the full SNMP server name appears.
Q01540397	**STP**: If Spanning Tree operation is not used on an LACP port, you must disable STP after you configure LACP.
Q01542038	**CLI, MAC SECURITY, STAND-ALONE UNIT**: MAC addresses added to the MAC Security table using the CLI do not appear in the MAC Security table. **Workaround**: Use the Web-based Manager or the Device Manager to add MAC addresses to the MAC Security table. **Note**: This condition does not occur in stacked switches.
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 local 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
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). You can view information about framing errors using the CRCAlignErrors counter. **Workaround**: You can find information about framing errors in the etherStatsCRCAlignErrors counter.
Q01739372	**NSNA**: After you configure NSNA, Nortel recommends that you disable the autosave to NVRAM function. Configuration changes must be explicitly saved to NVRAM.
Q01740590	**NSNA**: When a large number of NSNA login or logout events occur in parallel, a few may fail. **Workaround**: The NSNAs resets the switch port after a few minutes and you can log back in. You can also disconnect and reconnect the link to the switch to log in.
Q01747940	**Port Mirroring**: When Port-Mirroring is enabled with one of the following modes Asrc, Adst, AsrcBdst, AsrcBdstOrBsrcAdst, AsrcOrAdst, XrxYtxOrYrxXtx, XrxYtx, higher available precedence will be used for all ports. Issuing "qos agent reset-default" will not free resources used by Port-Mirroring.
Q01753980	**NSNA**: If clients come up when NSNAS connects to the switch and receives port information, those clients may need to redo DHCP (if they are dynamic clients). This can be done from the Windows command line: **`ipconfig/release ipconfig/renew`** . See *Nortel Ethernet Routing Switch 4500 Series Troubleshooting (NN47205-700)* for more information.
Q01659099	**AAUR**: If a stack is powered up simultaneously running v5.1 or v5.2 software and one of the unit 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.
New for release 5.2	
Q01585285	**JDM/WebUI/ ASCII Configuration**: When loading an ASCII configuration file via JDM or WebUI 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 JDM 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.

Reference number	Description
Q01844743	**IPv6**: the install command and ip.cfg files only support IPv4 configuration **Workaround**: Use the IPv6-specific commands in NNCLI, Device Manager or Web-based management to configure IPv6.
Q01859015	**XFP**: Older AA1403005 may not display correctly as a supported XFP.
Q01861555-02	**SNMP**: The objects s5ChasComDescr and s5ChasComSerNum are not yet available.
Q01867064	An unknown device (static IP device not added to the NSNAS MAC database) may not be displayed with the `show nsna client` command after you reboot the phone.
Q01869210	**UDP Forwarding**: If there are insufficient QoS filter resources available, the switch will not issue a warning message to indicate that UDP forwarding has not been setup on the ports. **Workaround**: use the show commands to display IPSG configuration status.
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 it it's 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.
Q01879707	**EAP**: If the RADIUS key configured on the switch and server do not match then 802.1X clients will not be authenticated. If the key on the switch is then modified to match that of the server, then client re-authentication must be forced so that the new key is utilized.
Q01879824, Q01881069	**NSNA**: When you move an authenticated PC placed behind an IP phone to another switch port and authenticate it again, the PC MAC address displays on both the old and new port NSNA tables. **Workaround**: To avoid this situation, enable re-authentication on the IP phone port. Re-authentication after the move will clear the PC MAC address from the NSNA tables.
Q01910247	**DHCP Relay**: When forwarding DHCP packets, the DHCP Relay function will clear any DSCP markings on the incoming DHCP request packet to 0x00.
Q01913824	**SSH, ACG**: If SSH is enabled on the switch and you load an ASCII configuration file containing SSH related commands, those commands will fail. **Workaround**: You must disable SSH on the switch before you load an ASCII configuration file containing SSH related commands.
Q01920502-01	**Port Mirroring**: when port mirroring runs in XrxYtx mode with multiple MLT groups, the port mirroring function is not enabled after the switch is rebooted. **Workaround**: Manually re-enable port mirroring on the switch after it is rebooted.
Q01865607-01	Nortel recommends that you do not enable IPSG on MLT, DMLT and LAG ports.

Reference number	Description
Q01869115	**IPv6**: If the stack is operating in Stack Forced mode and you want to set a switch IPv6 address, you must first delete the active IPv6 interface and then re-configure the switch IPv6 address. **Workaround**: Nortel recommends that you change the settings with the Console Interface to the switch or IPv4 to make such changes.
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 repective ports.
Q01929409-01	**IPSG**: When moving a port to a different VLAN on which IPSG is enabled, the IPSG filter remains active and may lead to blocking of IP traffic on that port. **Workaround**: the user should always disable IPSG on a port before moving the port to a different VLAN.
Q01935189	**QoS**: it is recommended that you configure all applications which assign filters (IP Source Guard, UDPForwarding) before you configure any QoS policies and QoS Access Lists.
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.
Q01930178	**IPv6, WebUI**: Configuration of the switch via the Web User Interface is not possible in this release when using an IPv6 address. **Workaround**: Use NNCLI or DM to configure IPv6 or use IPv4 for webUI access to the switch.
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.
Q01913212	**NSNA**: You must make any modifications to NSNA QoS filters before you enable NSNA globally or on any switch port.
Q01934002	**T1 SFP**: the switch will display the interface speed of the T1/E1 SFP as a 100 Mb/s connection even though the interfaces is operating at the appropriate WAN speed. The system uses this value for STP path cost and MLT utilization.
Q01948199	**IP.CFG**: The system ignores the last character from SNMP community string specified in the IP.CFG file **Workaround**: You need to add an extra character, such as underscore (_), to the end of the community string.

Reference number	Description
Q01877773, Q01879130	**NSNA**: If an end device is allocated a DHCP lease in the NSNA Fail_Open VLAN, the client will keep that address until the lease expired, even if the device is moved to another NSNA VLAN. **Workaround**: If a client is transitioned to a different NSNA VLAN then issuing ipconfig /release and ipconfig /renew will obtain a new DHCP lease.
Q01943166	**T1 SFP**: Nortel recommends that you enable egress traffic shaping on the port to 1.544 Mbps when using the T1 SFP to guarantee appropriate Quality of Service and traffic prioritization.
Q01950083	**Local Switch Username**: when you upgrade to Release 5.2.0, the user-configurable User Name will be reset to the default values (RO, RW). However, the upgrade retains the user-configurable passwords.

IPv6 limitations

The following table lists limitations specific to the implementation of IPv6 in release 5.2.

Table 12
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).
5	Access to WebUI using an IPv6 address is not supported in this release.

Nortel Ethernet Routing Switch 4500 Series

Release Notes — Software Release 5.2

Publication: NN47205-400
Document status: Standard
Document version: 04.01
Document date: 12 November 2008

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

LEGAL NOTICE

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 OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

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

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

Sun, Solaris, and Java - are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other coutries

SPARC is a trademark of SPARC International, Inc.

UNIX is a trademark of X/Open Company, Ltd.

All other trademarks are the property of their respective owners.