



Nortel Ethernet Routing Switch 4500 Series

Release Notes — Software Release 5.1

Document status: Standard
Document version: 03.01
Document date: 14 December 2007

Copyright © 2007, Nortel Networks
All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

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. The software license agreement is included in this document.

Trademarks

*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks. All other products or services may be trademarks, registered trademarks, service marks, or registered service marks of their respective owners. The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

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

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

Nortel 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

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

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

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

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

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

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

Contents

Introduction	7
Topics in this document	8
File names for this release	9
Hardware features in Release 5.1	9
General hardware features	9
New software features in Release 5.1	11
Nortel Secure Network Access (NSNA)	12
DHCP Snooping	13
Dynamic ARP Inspection	14
802.1x Multiple Host Single Authentication	14
802.1x NEAP Support (MAC Authentication)	14
ADAC (including 802.1ab support)	15
Virtual LACP	16
BPDU Filter	16
Logout CLI Enhancement	18
Factory default command	18
Write memory and save config command	18
Autosave Configuration Enhancement	18
Username Password Enhancement	19
ASCII Script Config support	19
New Unit Quick to Config	20
Improved Syslog Capabilities	21
Stack Counters	21
Stack Monitor	22
Configurable SNMP trap port	22
Stack Loopback test	23
Port Operational status Enhancements	23
Show Port Enhancement	24
RMON Scaling	24
Supported software and hardware capabilities	24
Browser Support for JDM Online Help	25
Issues resolved in Release 5.1	25
Known limitations and considerations in Release 5.1	26

6 Contents

Netscape for JDM Online Help	30
Related information	30
Publications	31
How to get help	31
Getting help from the Nortel web site	31
Getting help over the phone from a Nortel Solutions Center	32
Getting help from a specialist using an Express Routing Code	32
Getting help through a Nortel distributor or reseller	32

Introduction

These are the Release Notes for the Nortel Ethernet Routing Switch 4500 Series, Software Release 5.1.

The Nortel Ethernet Routing Switch 4500 Series product family is a stackable system which provides the high-performance, convergence-ready, secure, and resilient Ethernet connectivity required by today's application and competition driven enterprise networks. The Ethernet Routing Switch 4500 Series product deliver 10/100, 10/100/1000, and 10 Gigabit switching with Power over Ethernet (PoE) models for simplified network deployments which drives lower Total Cost of Ownership.

Switch stacks can be made up of any models within the Ethernet Routing Switch 4500 Series family, making this an ideal solution for enterprises with fast Ethernet or Gigabit users - or a combination of both. As a single-stacked entity, all switches are managed through a single IP address and offer the same high resiliency and common feature set simplifying management and deployment across the network.

The Nortel Ethernet Routing Switch 4500 Series is a line of enterprise mid-range stackable switches that support:

- Power over Ethernet
- redundant power options
- edge networks connectivity
- resilient stack operation for up to eight switches in a stack

The 1U high switch models in the Nortel Ethernet Routing Switch 4500 Series support a wide range of connectivity speeds and PoE.

The Nortel Ethernet Routing Switch 4500 Series, supported by software release 5.1, includes the following switch models:

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

ATTENTION

An existing ERS 4500 Series stack must first be upgraded to Release 5.1 software before adding and enabling any of the new ERS 4500 Series models (4526T, 4526T-PWR, 4524GT, 4526GTX, and 4526GTX-PWR).

Configurations can vary from a stand-alone switch to a stack of up to eight 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.

The Nortel Ethernet Routing Switch 4500 Series, Release Notes provide the latest information about Software Release 5.1 and includes operational issues not included in the documentation suite. For a complete list of ERS 4500 Series documentation suite, see "[Related information](#)" (page 30). The information in these Release Notes supersedes applicable information in other documentations.

Topics in this document

The following topics are discussed in this document:

- "[File names for this release](#)" (page 9)
- "[Hardware features in Release 5.1](#)" (page 9)
- "[New software features in Release 5.1](#)" (page 11)
- "[Supported software and hardware capabilities](#)" (page 24)
- "[Browser Support for JDM Online Help](#)" (page 25)
- "[Issues resolved in Release 5.1](#)" (page 25)
- "[Known limitations and considerations in Release 5.1](#)" (page 26)
- "[Netscape for JDM Online Help](#)" (page 30)
- "[Related information](#)" (page 30)
- "[How to get help](#)" (page 31)

File names for this release

" [Software Release 5.1 Components](#)" (page 9) describes the Nortel Ethernet Routing Switch 4500 Series, Software Release 5.1 software files. File sizes are approximate.

Software Release 5.1 Components

Module or file type	Description	File Name	File Size (bytes)
Standard runtime image software version 5.1.0.000	Standard image for the Nortel Ethernet Routing Switch 4500 Series	4500_510000.img	5,306,484
Standard runtime image software version 5.1.0.001	Secure image for the Nortel Ethernet Routing Switch 4500 Series	4500_510001s.img	5,552,312
Boot/diagnostic software version 5.1.0.7	Switch diagnostic software	4500_5107_diag.bin	1,580,460
Java Device Manager software version (6.0.9.0)	Device Manager software image for Windows NT, Windows XP, Windows 2003, Windows 2000, and Vista	jdm_6090.exe	170,755,822
Java Device Manager software version for Solaris UNIX (6.0.9.0)	Device Manager software image for Solaris	jdm_6090_solaris_sparc.sh	181,208,765
Java Device Manager software version for Linux (6.0.9.0)	Device Manager software image for Linux	jdm_6090_linux.sh	176,359,101
Software Release 5.1 Management Information Base (MIB) definition files	MIB definition files	Ethernet_Routing_Switch_45xx_MIBs_5.1.0.zip	1,078,849

Hardware features in Release 5.1

This section summarizes the hardware features for Nortel Ethernet Routing Switch 4500 Series switches. There are five new hardware models that are supported starting with software release 5.1: 4526T, 4526T-PWR, 4524GT, 4526GTX, and 4526GTX-PWR.

General hardware features

All switches in the series provide the following general hardware features:

- 1 front-mounted USB host port

- 1 front-mounted DB9 console port
- 2 rear-mounted Hi-stack stacking connectors
- SFP support, including T1 and 100FX on the 4526FX, 4526T, 4526T-PWR, 4550T, 4550T-PWR, and 4524GT models
- IEEE 802.3 10BASE-T support
- IEEE 802.3u 100BASE-T support
- IEEE 802.3ab 1000BASE-T support
- Auto-negotiation
- MDI/MDI-X auto-sensing

Hardware description by model

Model	Model-specific features
4526FX	24 100BaseFX ports (MTRJ connector) plus 2 10/100/1000 SFP combo ports Redundant power slot for DC/DC converter installation
4526T	24 10/100BaseTX RJ-45 ports plus 2 10/100/1000/SFP combo ports Redundant power slot for DC/DC converter installation
4526T-PWR	24 10/100BaseTX RJ-45 ports with PoE plus 2 10/100/1000/SFP combo ports Integrated redundant power connector for RPS 15 cable Connection
4550T	48 10/100BaseTX RJ-45 ports plus 2 10/100/1000 SFP combo ports Redundant power slot for DC/DC converter installation
4550T-PWR	48 10/100BaseTX RJ-45 ports with PoE plus 2 10/100/1000 SFP combo ports Integrated redundant power connector for RPS 15 cable connection
4524GT	24 10/100/1000BaseTX RJ-45 ports and 4 shared SFP ports Redundant power slot for DC/DC converter installation
4526GTX	24 10/100/1000BaseTX RJ-45 ports and 4 shared SFP ports plus 2 10GE XFP slots Redundant power slot for DC/DC converter installation

Model	Model-specific features
4526GTX-PWR	24 10/100/1000BaseTX RJ-45 ports with PoE and 4 shared SFP ports plus 2 10GE XFP slots Integrated redundant power connector for RPS 15 cable Connection
4548GT	48 10/100/1000BaseTX RJ-45 ports and 4 shared SFP ports Redundant power slot for DC/DC converter installation
4548GT-PWR	48 10/100/1000BaseTX RJ-45 ports with PoE and 4 shared SFP ports Integrated redundant power connector for RPS 15 cable connection

The T1 SFP provides full-duplex Fast Ethernet to T1 connectivity. The part number for this model is AA1419075-E6. This device can be used with the Ethernet Routing Switches 4526FX, 4526T, 4526T-PWR, 4550T, 4550T-PWR, and 4524GT.

New software features in Release 5.1

Ethernet Routing Switch 4500 Series, Software Release 5.1 provides the following new features or feature improvements:

- Security Configuration
 - "Nortel Secure Network Access (NSNA)" (page 12)
 - "DHCP Snooping" (page 13)
 - "Dynamic ARP Inspection" (page 14)
 - "802.1x Multi Host Single Authentication" (page 14)
 - "802.1x NEAP Support (MAC Authentication)" (page 14)
- Configuration — VLANs, Spanning Tree, and MultiLink Trunking
 - "ADAC (including 802.1AB support)" (page 15)
 - "Virtual LACP" (page 16)
 - "BPDU Filter" (page 16)
- System Configuration
 - "Logout CLI Enhancement" (page 18)
 - "Factory default command" (page 18)
 - "Write memory and save config command" (page 18)
 - "Autosave configuration Enhancement" (page 18)

- "Username Password Enhancement" (page 19)
- "ASCII Script Config support" (page 19)
- "New Unit Quick to Config" (page 20)
- System Monitoring
 - "Improved syslog capabilities" (page 21)
 - "Stack Counters" (page 21)
 - "Stack Monitor" (page 22)
 - "Configurable SNMP trap port" (page 22)
 - "Stack Loopback test" (page 23)
 - "Port oper status Enhancements" (page 23)
 - "show port Enhancement" (page 24)
 - "RMON Scaling" (page 24)

Nortel Secure Network Access (NSNA)

Release 5.1 provides full Nortel Secure Network Access (NSNA) functionality through SSCP with NSNA Release 1.6.1.2 and is ready to support future NSNA enhancements.

ATTENTION

When configuring an ERS 4500 Series Switch on NSNA Release 1.6.1.2, select ERS 5500 as switch type.

NSNA is not supported with MSTP in this release.

The NSNA Fail_open enhancement provides the ability for customers to deploy NSNA on switches at remote sites and still access the network. If connections to the SNAS fail, then clients are placed in a fail_open VLAN.

VLAN transition with MAC DB enables the ERS 4500 Series products to support this new functionality which is in development for NSNA v2.0. This supports MAC processing whereby NSNA has a list of MAC addresses that can be trusted (or not) by the system. It provides the ability to transition a PVID on a port based on a devices MAC address.

After configuring NSNA, the Autosave feature must be disabled using the following command:

```
4548GT(config)#no autosave enable
```

Use the following command when making future configuration changes:

```
4548GT(config)#copy config nvram
```

Only 128 filters for each precedence level are available for each chip (1/1-24, 2/25-48, and so on) due to the limitation on number of VoIP VLANs supported. Each VoIP VLAN consumes two filters on the same precedence level.

Example: If there are five VoIP VLANs defined, then NSNA red filter is enabled on 12 ports per chip.

Completing the combinations, the Red default filter set can be applied to the following number of ports for the given specified VoIP VLANs:

- 1VoIP VLANs -> 24 ports (128 / (1 VoIP VLANs * 2 filters))
- 2VoIP VLANs -> 24 ports (128 / (2 VoIP VLANs * 2 filters))
- 3VoIP VLANs -> 21 ports (128 / (3 VoIP VLANs * 2 filters))
- 4VoIP VLANs -> 16 ports (128 / (4 VoIP VLANs * 2 filters))
- 5VoIP VLANs -> 12 ports (128 / (5 VoIP VLANs * 2 filters))

For more information about NSNA, see *Nortel Ethernet Routing Switch 4500 Series Security — Configuration* (NN47205-505).

DHCP Snooping

Dynamic Host Configuration Protocol (DHCP) Snooping is a security feature which enables network administrators to limit the propagation of DHCP messages around the network.

Uplink ports or ports which are connected to DHCP server must be set to trusted mode and all other ports must be set to untrusted. This ensures that DHCP offers or leases are only forwarded by trusted ports. Untrusted ports are only allowed to originate DHCP requests and associated control messages. Any other DHCP packets received by an untrusted port will be dropped. This ensures that devices connected to DHCP untrusted ports cannot generate bogus DHCP offers or control messages, thus reducing attackers' ability to respond to DHCP requests with bogus IP information.

In addition to filtering DHCP replies on untrusted ports, DHCP snooping verifies the source of the DHCP packets and stores information in a DHCP binding table. When a switch receives a DHCP REQUEST packet on an untrusted switch port and the switch port belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

DHCP filters need to be installed on a port when one of the following application is enabled:

- NSNA (ports in red state)
- DHCP Snooping (ports in VLAN with DHCP snooping enabled)

For more information about DHCP Snooping, see *Nortel Ethernet Routing Switch 4500 Series Security — Configuration* (NN47205-505).

Dynamic ARP Inspection

Dynamic ARP inspection is a security feature that restricts IP ARP traffic on switch ports by filtering traffic based on the information stored in the DHCP binding table. Turning on this feature helps prevent attacks where neighboring devices on the same VLAN attempts to spoof ARP replies, so that the device can intercept traffic.

When Dynamic ARP inspection is enabled, ARP traffic is filtered by the switch and matched against entries in the DHCP binding table. The switch forwards ARP response on an untrusted port only when the source IP address matches an entry in the DHCP binding table for that port. Otherwise, the ARP traffic is not forwarded.

The Dynamic ARP inspection feature is managed from the CLI and JDM. To use this feature, DHCP snooping must also be enabled globally for the appropriate ports.

For more information about Dynamic ARP Inspection, see *Nortel Ethernet Routing Switch 4500 Series Security — Configuration* (NN47205-505).

802.1x Multiple Host Single Authentication

Ethernet Routing Switch 4500 Series software release 5.1 introduces the ability to support Multiple Host (MAC) Single Authentication (MHSA). This enables the support of a finite number of EAP or non-EAP devices on a port after the first device successfully authenticates.

For an EAP-enabled port with MHSA enabled, only one device on that port has to complete EAP authentication. Once this is completed, subsequent MAC addresses registering on that port will be allowed to send traffic without authentication as long as there is one authorized host on that port.

For more information about 802.1x Multi Host Single Authentication, see *Nortel Ethernet Routing Switch 4500 Series Security — Configuration* (NN47205-505).

802.1x NEAP Support (MAC Authentication)

This feature supports the authentication of devices on EAP-enabled ports which do not have EAP supplicants such as printers. Authentication for NEAP devices is performed according to the devices MAC address which can be either configured locally on the switch or authenticated by a RADIUS server.

NEAP MAC support can be enabled or disabled globally or on each port basis. Both global and per-port options must be enabled for the feature to work on a port. These options are separate for user-configured NEAP MAC Address checks and for RADIUS Authentication of MACs when not in the configured list.

When a new MAC is seen on a port, if the NEAP feature is enabled on the port, the switch consults the User Configured List of NEAP MAC addresses first. If a match is found, the MAC is allowed on the port and is kept in an Allowed list. If the MAC is not in the User Configured List, the switch generates a RADIUS request for the MAC address (based on the anyport configuration parameters) and performs RADIUS Authentication. If this is successful, the MAC will be allowed on the port.

NEAP anyport allows greater flexibility in the assignment of the RADIUS authentication password, allowing the customer greater flexibility in controlling NEAP access while still maintaining security. The password attribute on the RADIUS server can be a combination of the MAC address, Switch IP, Unit, and Port number.

CLI Command Syntax:

```
eapol multihost non-eap-pwd-fmt [ ip-addr | mac-addr |  
port-number ]
```

For more information about 802.1x NEAP Support (MAC Authentication), see *Nortel Ethernet Routing Switch 4500 Series Security — Configuration* (NN47205-505).

ADAC (including 802.1ab support)

Auto-Detection and Auto-Configuration (ADAC) enables plug-n-play configuration for network devices such as IP phones to simplify network deployment as well as Adds/Moves/Changes. Once a device is detected by the Auto-Detection functionality, then Automatic-Configuration applies the appropriate VLAN and QoS settings to the port for that device. ADAC can support two main types of device detection through Auto-Detect. The first is through a device's MAC address and the second is through a device's 802.1ab System Capabilities TLV. By default, an ERS 4500 Series system contains a list of pre-configured MAC addresses for Nortel IP handsets to enable rapid detection of Nortel devices. Other devices or other vendor's products can be recognized by configuring additional MAC address ranges or leveraging 802.1ab if the other device provides the appropriate functionality.

ADAC on the ERS 4500 Series uses the 802.1ab (LLDP) System Capabilities TLV to detect a LLDP enabled IP phone rather than using LLDP MEDs. This System Capabilities TLV is a mandatory component of

any LLDP implementation. Any IP phone which supports LLDP should according to RFC2011 and 802.1ab standard set the fifth bit set to 1 in the Systems Capability TLV and transmit it as part of the LLDPDU. Upon receiving the LLDPDU, if the ERS 4500 Series port is configured for ADAC and 802.1ab discovery, the switch will inspect the LLDPDU for this bit setting in the Systems Capability TLV. If present, then the ERS 4500 Series will determine that the device sending the LLDPDU is an IP phone and triggers ADAC for that device on that port.

For more information about ADAC, see *Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and Multilink Trunking* (NN47205-501).

Virtual LACP

In many enterprise networks, it is required that a trunk link fail over to the other link in sub-second interval when there is a failure in the link between the local and the remote end points. This requirement can be met if the network can inform both ends of the link in the event of a communication loss. Virtual Link Aggregation Control Protocol (VLACP) is used to detect end-to-end failure by propagating link status between ports that are logically connected point-to-point either directly or indirectly across an intermediate network.

For more information about Virtual LACP, see *Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and Multilink Trunking* (NN47205-501).

BPDU Filter

The Bridge Protocol Data Unit (BPDU) Filtering feature allows the network administrator to control how Spanning Tree BPDUs are controlled within a network to help prevent against malicious attacks against the network.

The main purpose of a Spanning Tree is to eliminate loops in a network. A bridge that participates in the Spanning Tree Protocol exchanges information through configuration messages known as BPDUs. Based on the BPDU information all the bridges will then select a single bridge with the best bridge ID as the Root. This process is called the Root selection process. When a new bridge joins the network or an existing bridge leaves the network the Root selection process is repeated and the new Root is selected due to the network change.

BPDU Filtering provides network protection by enabling:

- Blocking of unwanted Root selection processes when an edge device is added to the network. This would prevent unknown devices or malicious users from altering the existing Spanning Tree topology.
- Block the BPDU Flooding of the switch from an unknown device.

BPDU Filtering can be enabled on a per port basis or across all ports at once. Each port has its own timer configurable between 10 seconds and 65535 seconds to determine how long a port will be disabled if a BPDU is received on that port. If the timer is set to 0 and a BPDU is received on that port, the port will be administratively disabled until it is explicitly enabled by an authorized network administrator.

The user is allowed to enable or disable BPDU Filtering on per port basis. Each port has its own timer. This timer is user configurable and the valid range of this timer is between 10 seconds and 65535 seconds. The port timer is disabled if it is configured as 0. This feature is supported only on non-MLT ports.

When a port receives a BPDU on which BPDU Filtering is enabled, the following actions take place:

- The port will immediately be placed in the operational disable state.
- A SNMP trap and a log message are generated. The log message will be:
BPDU received on port with BPDU Filtering enabled. Port X has been disabled.
- The port timer starts and the port will stay operationally disabled until the port timer expires. If the timer is disabled or the switch is reset before the timer countdown is expired, the port if temporarily disabled by the BPDU Filter application will stay in a disabled state.
- If a user is trying to disable BPDU Filtering while the timer is running, the timer countdown is stopped and the port if temporarily disabled by the BPDU Filter application stays in a disabled state. If the BPDU Filtering is disabled in a port, the user must manually enable the port to bring it back to the normal mode.

CLI Commands Syntax:

```
show spanning-tree bpdu-filtering [<Fast Ethernet>]
[port<portlist>]
spanning-tree bpdu-filtering [port<portlist>] {[enable]
[timeout {0 | <10-65535>}]}
no spanning-tree bpdu-filtering [port<portlist>]
[enable]
default spanning-tree bpdu-filtering [port <portlist>]
[enable] [timeout]
```

For more information about BPDU Filter, see *Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and Multilink Trunking* (NN47205-501).

Logout CLI Enhancement

The logout command is modified to function differently than the exit command by providing a disconnection from the switch similar to issuing the logout command on a Unix system. Entering the command `logout` from CLI, when connected through the Serial Console connection, will return your session back to the login or banner screen. If connected through Telnet or SSH, then issuing the logout command will terminate and close the current session. The help messages displayed by typing "?" are updated. Logout now says "Exit from the EXEC and end the current session" and Exit says "Exit from current context".

For more information about Logout CLI Enhancement, see *Nortel Ethernet Routing Switch 4500 Series System — Configuration* (NN47205-500).

Factory default command

The `restore factory-default` command is used to set the switch back to default configuration. The command offers a `-y` flag so that the command will execute immediately without requesting additional user confirmation.

CLI Commands Syntax:

```
restore factory-default [-y ]
```

For more information about Factory default command, see *Nortel Ethernet Routing Switch 4500 Series System — Configuration* (NN47205-500).

Write memory and save config command

Two additional CLI commands are now available to save switches running configurations to NVRAM. These new commands, `write mem` and `save config`, function identically to the `copy config nvram` command.

CLI Commands Examples:

```
4526FX# write memory
4526FX# save config
```

For more information about Write Memory and Save Config command, see *Nortel Ethernet Routing Switch 4500 Series System — Configuration* (NN47205-500).

Autosave Configuration Enhancement

The ability to set autosave is now extended to the WebUI (JDM and CLI initiated in v5.0 release). By default autosave is enabled which ensures that the switch regularly saves its configuration to NVRAM. In some rare cases, a switch may corrupt the configuration if autosave is enabled and the switch is turned-off at the exact same moment that autosave is performing an

update to the configuration file. By turning off autosave, customers can reduce the probability of this configuration corruption occurring. Remember, if autosave is disabled, the configuration must be explicitly saved.

For more information about Autosave Configuration Enhancement, see *Nortel Ethernet Routing Switch 4500 Series System — Configuration (NN47205-500)*.

Username Password Enhancement

This enhancement improves security by enabling the configuration of a username field to existing local switch authentication. Only one read-only (RO) and one read/write (RW) user is supported on the switch or stack and these parameters are applied to the stand-alone or stack environment based on the current operating mode.

Username Command:

```
<username> <password> [ ro | rw ]
```

ATTENTION

The ERS 4500 Series switches do not allow changes to the username through WEB interface, because of non availability of User management in the WEB interface. You can use the CLI for changing the username and this new username is also used to authenticate in the WEB interface.

For more information about Username Password Enhancement, see *Nortel Ethernet Routing Switch 4500 Series System — Configuration (NN47205-500)*.

ASCII Script Config support

This feature provides a unified mechanism for a switch or a stack of switches to load ASCII configuration files from a TFTP server or USB drive. The ASCII Configuration table provides a way of controlling which ASCII configuration files are loaded when the system boots. Each entry in the table contains the path to an ASCII configuration file, indicating one of the following:

- The file is downloaded from the network using the IP address and filename retrieved from BOOTP
- The file is downloaded from a TFTP server using a specified IP and filename
- The file is downloaded from USB using a specified filename and USB port of a given unit. The USB port of the base unit is used by default If no unit number is given.

Each entry in the ASCII Script Table contains a boot priority column. A non-Zero boot priority will indicate that the entry will be attempted to be loaded at boot time. ASCII configuration entries are attempted in increasing priority order until a successful file is loaded. Lower priority entries are loaded first, or if equal priority the first entry in the table is loaded first.

CLI Command Example:

Set row 10 in the ASCII configuration script table, specifying a file to be loaded on boot from USB with load-on-boot priority 20.

```
45xx(config)# script 10 load-on-boot 20 usb unit 1
test.cfg
```

Download and run a configuration script using the ASCII Configuration Script Table:

```
45xx(config)# script run 2 usb unit 3 test.cfg
```

For more information about ASCII Script Config support, see *Nortel Ethernet Routing Switch 4500 Series System — Configuration* (NN47205-500).

New Unit Quick to Config

This feature enables automatic configuration of new units added to existing stacks, which significantly reduces the time to deployment. When adding a new unit to an existing stack, the new switch loads pre-configured information from templates stored on the base-unit of the stack. These templates store details such as: VLAN IDs, port speed, duplex mode, PVID and spanning tree groups.

By default, this feature is disabled. Once enabled it keeps track of the MAC address of all units in a stack in order to detect which unit is a new unit.

CLI Command syntax (In Config mode):

```
4526T(config)# quickconfig enable
4526T(config)# no quickconfig enable
4526T(config)# default quickconfig
```

CLI Command Syntax (In Privileged Exec mode):

```
4526T# quickconfig start-recording
```

ATTENTION

Enter a period "." to end recording of commands.

For more information about New Unit Quick to Config, see *Nortel Ethernet Routing Switch 4500 Series System — Configuration* (NN47205-500).

Improved Syslog Capabilities

The Improved Syslog Capabilities feature has two goals:

- To provide a method for capturing software faults in the syslog application as critical customer messages.
- To provide a CLI interface to display and clear last software exception generated in the system.

The Improved Syslog Capabilities feature is supported on the Enterprise Routing Switch 4500 Series products.

The feature is developed to ensure that all software exceptions generated in the system are captured in the system log application as critical customer messages. The following information is saved in a log entry message:

- Information about the software fault
- Fault task name
- Exception type
- Program Counter
- Stack Pointer

This feature provides a CLI interface used to display or to clear the last software exception trace. In the case of a system software crash, the user can gather the necessary information about the exception to report to the Nortel Solutions Center.

If a software exception occurs in the system, a critical customer message is logged. The feature does not affect the usage mode of syslog application.

CLI Command Syntax:

```
show system last-exception [ unit { <1-8> | all } ]
clear system last-exception [ unit { <1-8> | all } ]
```

For more information about Improved syslog capabilities, see *Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Stack Counters

Version 5.1 software introduces the ability to display statistics for the stacking ports on each of the switches in a stack. Customers can diagnose network problems more easily now by viewing the stack port statistics.

CLI Command Syntax:

```
show stack port-statistics [ unit <1-8>]
```

For more information about Stack Counters, see *Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Stack Monitor

Many complex systems are monitored and controlled through Ethernet networks. When these systems are connected to stackable switches, it becomes more important to be able to actively monitor the health of members of switches forming a stack. The Stack Monitor feature actively monitors the number of units in a stack and will generate SNMP traps and log messages should the number of units change from the configured value.

Each time the number of units in a stack changes, the trap sending timer is reset and the current number of stack units is compared with the configured number of stack units. If it is not equal, the switch will send a trap and log a message to Syslog. The traps are sent from a standalone unit or the base unit of the stack. When the trap sending timer reaches the configured number of seconds at which traps are sent, the switch sends a trap and logs a message to Syslog and restarts the trap sending timer. The Syslog message will not be repeated unless the stack configuration changes. This prevents the log being filled with stack configuration messages.

Stack Monitor is disabled by default. When this feature is enabled on a stack, the current stack size is captured and used as the expected stack size. Alternatively the user can choose a different value and set it after enabling the feature. Stack Monitor can be configured through CLI and JDM.

CLI Commands Syntax:

```
stack-monitor [enable] [stack-size <2-8>] [trap-  
interval <10-3600>]  
no stack-monitor [enable]  
default stack-monitor [enable] [stack-size <2-8>]  
[trap-interval <10-3600>]  
show stack-monitor
```

For more information about Stack Monitor, see *Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Configurable SNMP trap port

A new command provides the ability to change the SNMP trap UDP port from port 162 to between 1 – 65535. To set the SNMP trap port back to UDP port 162, use the default SNMP port command.

CLI Command Syntax:

```
snmp-server host <host ip> [port <trap port>]
{[v1 <community-string> | v2c <community-string>
<1-214748364>] [retries <0-255>]} | v3 {auth|no-
auth|auth-priv} <username> {inform [ timeout <0-255>]}
default snmp port
```

For more information about Configurable SNMP trap port, see *Nortel Ethernet Routing Switch 4500 Series Security — Configuration* (NN47205-505).

Stack Loopback test

The Stack Loopback test is used to assist in the diagnose of a bad port or stacking cable on a switch, thus ensuring the most appropriate component is replaced, rather than replacing the whole stack.

The Stack Loopback test provides 2 types of tests: internal (test the stack ports) and external (test the stack cable). Both tests require that the switch is removed from stack and have no traffic on the switch. It is recommended to perform the internal test before the external test to pinpoint a potential problem.

For more information about Stack Loopback test, see *Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Port Operational status Enhancements

The show interfaces command now shows the port operational status in addition to the current up/down status. While a port may be up, there are a number of different scenarios when the port is not forwarding traffic. This enhancement enables other statuses to be displayed so that network operators can easily determine the status of a port through a single interface command.

The **verbose** keyword is used to display the status of the interfaces with EAP, STP and VLACP. If the terminal width is set to more than 80 characters (for example, 110) then the output will be in a table format.

For more information about Port Operational Status Enhancements, see *Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Show Port Enhancement

The Show Port enhancement provides the ability to show all the configuration information for a specific port through CLI in one simple command. The `config` keyword displays detailed information specific to the port configuration. The `verbose` keyword is specific to show port operational status enhancement.

CLI Command syntax:

```
show interfaces <portlist> config
```

For more information about Show port Enhancement, see *Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

RMON Scaling

The number of RMON alarm instances per stack is increased from 400 to 800 with release 5.1 for the ERS 4500 series products.

For more information about RMON Scaling, see *Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Supported software and hardware capabilities

The following table summarizes the known limits for the Nortel Ethernet Routing Switch 4500 Series, Software Release 5.1 and Device Manager 6.0.9.0.

Supported capabilities for the Nortel Ethernet Routing Switch 4500 Series

Feature	Maximum number supported
egress queues	4
VLANs	256
Spanning Tree Group instances (802.1s)	8
MAC addresses	8000
Stacking bandwidth (full stack of 8 units)	320 Gb/s: 40 Gb/s per switch
Stack, units per	8
MultiLink Trunking (MLT), Link Aggregation (LAG) groups	6
Links per MLT/LAG	4
802.1x (EAP) clients per port, running in MHMA	32
802.1x (EAP) clients per stack	384

Browser Support for JDM Online Help

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

- Firefox
- Internet Explorer
- Netscape

Issues resolved in Release 5.1

The following table describes the issues in previous software releases for the Ethernet Routing Switch 4500 Series that have been resolved in Software Release 5.1.

Issues resolved in ERS 4500 Series Software Release 5.1

Reference Number	Description
Q01496548	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.
Q01557789	You cannot download the SSH authorization key from a USB device on a non-base units in a stack. Result: In release 5.1, the SSH authorization key can be downloaded from an USB Mass Storage Device inserted in any of the units of a stack.
Q01542038	MAC addresses added to the MAC Security table using the CLI do not appear in the MAC Security table.
Q01614537	Link Layer Discovery Protocol (LLDP) local-mgmt-addr type-length-value element (TLV) becomes disabled on ports from temporary base unit in a stack.
Q01606162	When setting QoS on a port to trusted role, the switch allocates 21 classifiers per trusted port. It is not possible to apply trusted role to all switch ports, due to the resources available. To apply application prioritization across all switch ports on the ERS 4500, set the port type to unrestricted. This prioritizes traffic based on the 802.1p priority and allows filters to be configured based on specific application needs. For example, assign all packets marked with DSCP EF priority, such as with VoIP, to the highest priority queue.
Q01592862-05	Password: In some situations, the local switch password may become corrupted when the stack breaks with all of the base unit LEDs flashing on all switches.
Q01722282	Telnet: When running the nmap portscan utility, the telnet server of the switch stops receiving incoming telnet sessions. All current telnet sessions remain established.
Q01762354	STP: If a hub is connected to an ERS 4500 port and a local loop is created on that hub, then the ERS 4500 port goes into the blocking state as expected. However, when the loop is removed on the hub, the ERS 4500 port remains in STP blocking state until the port is reset.

Reference Number	Description
Q01763251	IP Connectivity: When WhatsUpGold software is used to continuously poll the switch using ping, telnet, and SNMP, the switch IP address no longer responds to IP management traffic after running this software for a number of hours.
Q01765743	Shutdown command: The shutdown command do not copy the currently running configuration file to the nvram before locking the system, even though the on-screen message indicates that this is copied.
Q01774611	MAC security: When autosave is disabled and the configuration is manually saved, the MAC security information is not saved to NVRAM.

Known limitations and considerations in Release 5.1

"Ethernet Routing Switch 4500 Series known limitations since Release 5.0" (page 26) describes limitations known to exist in Software Release 5.1.

Ethernet Routing Switch 4500 Series known limitations since Release 5.0

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. SOLUTION: Connect ports using the same set speed or use auto-negotiation on each switch.
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. SOLUTION: 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	Web UI: The Web interface supports only alpha-numeric characters. Use only alpha-numeric characters in the creation of elements. For example, if you create a VLAN in the CLI or the Device Manager using characters that are not alpha-numeric, you cannot delete the VLAN within the Web Interface.
Q01514147	CLI: 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.
Q01524259	Web UI: STP participation cannot be modified for LACP-enabled ports. This condition does not impair switch operation.
Q01536648	CLI: If the HTTP port default value of 80 is changed, you must use the CLI command <code>default http-port</code> to restore the HTTP port value to the default value.
Q01540397	STP: If Spanning Tree operation is not used on an LACP port, you must disable STP after you configure LACP.

Reference Number	Description
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.
Q01773986	AppleTalk: The creation of an AppleTalk protocol VLANs or user defined protocol VLAN with the type 32923 is not supported.
Q01747940	Port Mirroring: Issuing the <code>qos agent reset-default</code> command does not free resources used by Port-Mirroring. This is due to higher precedence used for all ports when Port-Mirroring is enabled with one of the following modes: Asrc, Adst, AsrcBdst, AsrcBdstOrBsrcAdst, AsrcOrAdst, XrxYtxOrYrxXtx, XrxYtx.
Q01738338	Different results can be obtained by using meter and shaper with same parameters. This is due to the adding of the VLAN encapsulation. Metering is applied to packets received by a port before adding VLAN encapsulation. Shaping is applied to packets sent on a port, after the port is added to the VLAN encapsulation.
Q01749777	Port Mirroring: When all QoS precedence levels are in use for one or multiple ports, port mirroring can not be enabled. The workaround is to reconfigure QoS to free up a precedence level for those ports.

Ethernet Routing Switch 4500 Series known limitations for Release 5.1

Reference Number	Description
Q01741021	NSNA: The ERS 4500 typically supports up to 2 NSNA VoIP VLANs to configure across all ports on a switch as each NSNA VoIP VLAN consumes 2 filters.
Q01391509-02	SNMP: The object <code>do1qTpFdbAddress (1.3.6.1.2.1.17.7.1.2.2.1.1)</code> is not available for snmp queries. Use <code>dot1dTpFdbAddress (1.3.6.1.2.1.17.4.3.1.1)</code> object to provide similar functionality.
Q01764161	ADAC: 802.1AB (LLDP) System Capabilities TLV is used to detect a LLDP enabled IP phone rather than using LLDP MEDs. Any IP Phone which supports LLDP should set the 5th bit to 1 in the Systems Capability TLV. Upon receiving the LLDP PDU if the ERS 4500 port is configured for ADAC and 802.1AB discovery, the switch inspects the LLDP PDU for this bit setting in the Systems Capability TLV. If present, then the ERS 4500 determines that the device sending the LLDP PDU is an IP Phone and triggers ADAC for the device on that port.
Q01766909	WebUI: The local switch username can only be modified from the CLI and not through Web or JDM. Once the username is changed through the CLI, you can use the new username to authenticate through the Web interface as well.
Q01751051	Guest VLAN: EAP enabled port is not moved to guest VLAN, if guest VLAN and original VLAN are associated with different STGs. EAP port will not forward traffic in guest VLAN or original VLAN; if the EAP authentication succeeds, packets will be transmitted properly in the original VLAN.

Reference Number	Description
Q01753536	NSNA: When setting up additional filters for NSNA VLANs there is only 1 free precedence available for creating user ACLs for the NSNA Yellow VLAN and 2 free precedence available for creating user ACLs for the NSNA Red VLAN .
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.
Q01723410	NSNA: After a NSNA enabled switch is rebooted, Nortel IP Phones with firmware 0623C3C may not be able to connect to the BCM. In order to reestablish the connection to the call server they must be power cycled.
Q01749862	WebUI: One should avoid creating configurations in CLI or JDM using non-alphanumeric characters in names. As these characters are sometimes reserved in HTML it may display the names incorrectly in the WebUI.
Q01748510	NSNA: All NSNA configured VLANs must belong to the same Spanning Tree Group (STGs). Setting NSNA VLANs to different STGs is not supported as it may cause problems during dynamic VLAN movement.
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.
Q01739372	<p>NSNA: After configuring NSNA it is recommended to disable the autosave to NVRAM function. Please be aware that configuration changes have to be explicitly saved to NVRAM.</p> <div style="border: 1px solid black; padding: 10px; text-align: center;"> <p>ATTENTION</p> <p>Certain applications may delay saving data for a short period of time to optimize storage access. It is recommended to delay issuing a save of the current configuration to NVRAM for 30 seconds after completing complex configuration commands.</p> </div>
Q01495527	JDM: Port-mirroring cannot be configured or viewed using JDM.
Q01766331	DMLT: If a unit within a stack which has DMLT link is defaulted and if there is an inconsistency in the VLAN configurations on the DMLT ports then the DMLT connection is disabled.

Reference Number	Description
Q01723421	NSNA: If an end device which is connected behind an IP Phone is moved to another IP Phone, the show nsna client command displays the end device's MAC address as present on multiple ports. Workaround: plug another device into the original IP Phone or wait until MAC address aging occurs.
Q01740590	NSNA: When a large number of NSNA login or logout events are occurring in parallel, occasionally a few may fail. Workaround: The NSNAs resets the switch port after a few minutes and the customer can then log back in. Alternatively if the user disconnects and reconnects the link to the switch, they can re-authenticate.
Q01769859	MIBS: The index value returned ipAdEntIfIndex(1.3.6.1.2.1.4.20.1.2) is not associated with a physical interface on the switch, but is an index into the IP management addresses configured for the stack and or switch. Some network management applications may incorrectly associate this index with a physical port index and if that port is down as reported by will report ifOperStatus the network management application will report the IP address as unreachable despite the fact that the device is reachable through ICMP (ping) and other IP connectivity from the network management station.
Q01672222	RMON: etherStatsJabbers object is not incremented. As the Ethernet Routing Switch 4500 supports jumbo frames (up to 9216), the Jabber counter will always be displayed as zero (0). Information about framing errors can be found using etherStatsCRCAAlignErrors counter.
Q01756596	NSNAS: With NSNAS 1.6.1.2 an error window appears on PC client tunnelguard login. Clicking ok, allows authentication to continue. No functional impact.
Q01753980	NSNA: If clients come up during the time when nsna is connecting to switch and gets port information - those clients may need to re-do dhcp (if they are dynamic clients). This can be done from windows command line: ipconfig /release and ipconfig /renew.
Q01659099	AAUR: If a stack is powered up simultaneously running v5.1 software and one unit in the stack is running v5.0, then the Automatic Agent upgrade of that unit to v5.1 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 to v5.1 software.
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".

Reference Number	Description
Q01767481	Factory default command: The <code>restore factory-default</code> command is used to set the switch back to default configuration. The command offers a "-y" flag so that the command will execute immediately without requesting additional user confirmation.
Q01768273	EAP: Radius accounting is working only for EAPOL clients. Radius accounting management session(s) (Web, Telnet or SSH connection to the switch) are not supported by the current implementation of radius accounting. ERS 4500 Series switch does not send a radius accounting "on" or a radius accounting "off" message.

Netscape for JDM Online Help

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.

Step	Action
1	Start the Netscape browser.
2	From the Tools menu, select Options . <i>An Options window opens.</i>
3	In the Security and Privacy panel of the Options window, click Site Controls . <i>An Options - Site Controls window opens.</i>
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—

Related information

This section lists the information sources that relate to the Nortel Ethernet Routing Switch 4500 Series, Software Release 5.1.

Publications

Refer to the following publications for information about the Nortel Ethernet Routing Switch 4500 Series, Software Release 5.1:

- *Nortel Ethernet Routing Switch 4500 Series Regulatory Information* (NN47205-100)
- *Nortel Ethernet Routing Switch 4500 Series Installation* (NN47205-300)
- *Nortel Ethernet Routing Switch 4500 Series Overview — System Configuration* (NN47205-500)
- *Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking* (NN47205-501)
- *Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502)
- *Nortel Ethernet Routing Switch 4500 Series Configuration — Quality of Service* (NN47205-504)
- *Nortel Ethernet Routing Switch 4500 Series Security — Configuration* (NN47205-505)
- *Installing SFP and XFP Transceivers and GBICs* (NN47205-301)
- *Nortel Ethernet Routing Switch 4500 Fault Management — Troubleshooting* (NN47205-700)

How to get help

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

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

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

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

Getting help over the phone from a Nortel Solutions Center

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

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

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Nortel Ethernet Routing Switch 4500 Series

Release Notes — Software Release 5.1

Copyright © 2007, Nortel Networks
All Rights Reserved.

Publication: NN47205-400 (322818-C)
Document status: Standard
Document version: 03.01
Document date: 14 December 2007

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

Sourced in Canada, India and the United States of America

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

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

All other trademarks are the property of their respective owners.

