Nortel Ethernet Routing Switch 4500 Series

Release Notes — Release 5.4

Release: 5.4
Document Revision: 06.01

www.nortel.com

NN47205-400

Nortel Ethernet Routing Switch 4500 Series
Release: 5.4
Publication: NN47205-400
Document release date: 19 May 2010

Contents

Software license

This section contains the Nortel Networks software license.

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

Nortel Networks Inc. software license agreement

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

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

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer

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

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

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

4. General

1. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).
2. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
3. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
4. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
5. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
6. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

New in this release

The following sections detail what's new in Nortel Ethernet Routing Switch 4500 Series Release Notes — Software Release 5.4.

Navigation

Features

See the following sections for information about feature changes.

Other changes

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

Enterprise Device Manager

Enterprise Device Manager (EDM) replaces both the integrated Web-based Management and separate Device Manager applications previously used to manage and configure the Ethernet Routing Switch 4500 Series switches.

EDM is a fully integrated graphical user interface delivered as a Web-based application that runs in a Web browser. To enhance ease of use, the EDM application has the look and feel of Device Manager (previously known as JDM).

EDM navigation has been enhanced. To access command tabs from the EDM navigation tree, the documented procedures specify using a double-click to open the tab in the work area. With the enhancement, you can access all objects in the navigation tree with a single click.

ATTENTION
With the introduction of Enterprise Device Manager (EDM) the use of Device Manager (sometimes referred to as JDM) is no longer supported because the use of JDM to control the switch could lead to potential corruption of the switch configuration.

ATTENTION
If you upgrade the software on your switch, and if you are managing the switch with EDM, then you should refresh the browser cache on your end device to ensure that EDM loads the latest tabs for all respective features.

Introduction

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Nortel Ethernet Routing Switch 4500 Series, Software Release 5.4.

For information on how you can obtain and use the embedded version of Enterprise Device Manager (EDM), see *Nortel Ethernet Routing Switch 4500 Series Fundamentals*, (NN47205-102).

The Nortel Ethernet Routing Switch 4500 Series, supported by software release 5.4, includes the following switch models:

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

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

These Release Notes provide the latest information about Software Release 5.4, as well as operational issues not included in the documentation suite.

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

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

Navigation

The following topics are discussed in this document:

Important notices and new features

This section contains a brief synopsis of the new features in Release 5.4 and any important notices.

Navigation

This section includes the following topics:

New features in Release 5.4

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

New features

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

802.1AB (LLDP) MED Network Policy CLI

You can configure 802.1AB MED network policies to dynamically configure voice VLAN, DSCP, priority, and VLAN tagging on the switch for voice traffic received from an IP phone. When you enable LLDP and configure the MED network policies on the switch, the switch sends the network

policies to the IP Phone. The IP phone processes the data in the LLDP PDU and transmits the voice traffic with the appropriate VLAN ID, VLAN tagging, DSCP and priority information.

You can configure MED network policies on a switch port that has ADAC enabled. The network policies have priority over the ADAC configuration on the port.

802.1D Compliancy Support

To prevent broadcast storms in a complex network, when a port drops and comes back up frequently you can use 802.1d Compliancy Support. When you configure 802.1d compliance mode, the system sets the Spanning Tree Protocol (STP) state of the port to disabled when the port link is down.

ADAC and Auto QoS Interoperability

This enhancement adds interoperability between QoS and ADAC. When you enable Auto QoS, ADAC is notified and changes the DSCP remarking of ingress voice traffic according to DSCP = 0x2F. When you disable Auto QoS, ADAC is notified and changes the DSCP remarking of ingress voice traffic back to DSCP = 0x2E.

ADAC Enhancements

Auto-Detect Auto-Configuration (ADAC) Enhancements deliver increased flexibility to your system by providing the following:

- expanded support that allows for up to 8 ADAC uplinks and 8 call-server links—individual ports or any combination of MLT, DMLT or LAG—per switch or stack
- the ability to change the non-ADAC VLANs on a port without disabling ADAC (in previous software versions you were requried to disable ADAC in order to change the non-ADAC VLANs on a port)

Additional SFP Support

The following table lists the additional SFPs supported by ERS 4500 Release 5.4.

Nortel PEC	Description
AA1419050-E6	1-port 1000BaseXD DDI SFP (connector: LC) - 1310nm.
AA1419051-E6	1-port 1000BaseXD DDI SFP (connector: LC) - 1550nm.
AA1419052-E6	1-port 1000BaseZX DDI SFP (connector: LC) - 1550nm.
AA1419053-E6	1-port 1000BaseCWDM SFP (connector: LC) - 1470nm , 40km.
AA1419054-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1490nm , 40km.
AA1419055-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1510nm , 40km.

Nortel PEC	Description
AA1419056-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1530nm , 40km.
AA1419057-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1550nm , 40km.
AA1419058-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1570nm , 40km.
AA1419059-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1590nm , 40km.
AA1419060-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1610nm , 40km.
AA1419061-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1470nm , 70km.
AA1419062-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1490nm , 70km.
AA1419063-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1510nm , 70km.
AA1419064-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1530nm , 70km.
AA1419065-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1550nm , 70km.
AA1419066-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1570nm , 70km.
AA1419067-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1590nm , 70km.
AA1419068-E6	1-port 1000BaseCWDM DDI SFP (connector: LC) - 1610nm , 70km.
AA1419071-E6	1-port 1000Base DDI SFP (connector: LC) - 1550nm , 120km.

Automatic QoS and 802.1AB MED Interoperability

Automatic QoS and 802.1AB MED Interoperability enhances Automatic QoS implementation on the switch so you can use both features simultaneously. With the enhancement, if you configure 802.1AB MED, the switch publishes the private Automatic QoS DSCP value to the end device rather than the default value defined by the network policy. NOTE: Automatic QoS was formerly called NT-on-NT.

DHCP Client

With Dynamic Host Configuration Protocol (DHCP) client, you can use either DHCP or BootP to assign an IPv4 address to the management VLAN. Using DHCP client, the switch can retrieve IP address, netmask, default gateway, and Domain Name Server (DNS) information for a maximum of three DNS servers. Because the switch should not perform as a DHCP relay while DHCP client is operating, DHCP client operates only when the switch is started up.

DHCP Option 82 Support

DHCP option 82 support is an extension of Dynamic Host Configuration Protocol (RFC3046 and RFC3993) that enables the switch to insert additional information into DHCP requests coming from client workstations.

When you enable option 82, in either Layer 2 or Layer 3 mode, the switch inserts additional port-based subscriber information into the DHCP packets traversing the switch enroute to the DHCP server. The DHCP server can then store this additional subscriber information within the IP allocation record to assist with tracking of end device locations.

When a VLAN is operating in Layer 2 mode, DHCP Snooping must be enabled for DHCP Option 82 to function. When a VLAN is operating in Layer 3 (IP Routing) mode, the DHCP Option 82 function requires that DHCP Relay is appropriately configured. To use DHCP Option 82 with DHCP relay, you must enable DHCP relay globally on the switch and client VLANs.

For more information about DHCP option 82 with DHCP relay, see *Nortel Ethernet Routing Switch 4500 Series Configuration — IP Routing and Multicast* (NN47205-506).

DHCP Snooping Improvements

Release 5.4 adds DHCP Snooping Improvements that include:

- a larger DHCP Snooping table—1024 entries for each unit or stack better supports IP Phone and PC deployments
- the ability to manually add entries to, or delete entries from, the DHCP snooping table so that you can protect statically configured IP devices with applications, such as Dynamic ARP Inspection (DAI) and IP Source Guard (IPSG), that rely on DHCP Snooping table entries

Dual Syslog Server Support

You can use the Dual Syslog Server Support feature to configure a second Syslog server to run in tandem with the first. If you configure a second Syslog server, the switch sends syslog messages simultaneously to both Syslog servers to ensure that syslog messages are logged, even if one of the servers becomes unavailable.

Dynamic Route Table Allocation

The ERS 4500 with Release 5.4 now suppots dynamic routing protocols such as RIPv1/v2, OSPFv2, and Route Policies. ***Note***: You require an Advanced software license to use OSPFv2.

Because the ERS 4500 hardware is limited to a maximum of 512 active IPv4 routes in the routing table, you can use the Dynamic Route Table Allocation feature to fine-tune routing allocation. With this feature, routes can be allocated between entries for local routes (IPv4 VLAN interfaces) and entries for static routes (including non-local static routes). The remaining route entries are available for dynamic routing protocols such as RIP and OSPF.

EAP and non-EAP MultiVLAN capability

With the EAP and non-EAP MultiVLAN capability, you can assign multiple EAP and non-EAP hosts to different VLANs on the same port.

Energy Saver

Energy Saver (ES) can reduce network infrastructure power consumption without impact to network connectivity. ES reduces direct power consumption by up to 40% because it uses intelligent switching capacity reduction in off-peak mode. ES can also use Power over Ethernet (PoE) port power priority levels to shut down PoE ports and provide more power savings. You can configure ES using NNCLI and EDM.

Erasable NNCLI Audit Log

You can erase the contents of the NNCLI audit log on a switch, should circumstances arise that require the log contents to be cleared. For example, you could clear the NNCLI audit log contents on switches that are being decommissioned.

To prevent the NNCLI audit log contents from being accidently erased, you can apply the no-erase function. This function can be applied only one time on a switch and is not reversible.

IPFIX

IP Flow Information eXport (IPFIX) allows you to monitor the traffic flows on Ethernet Routing Switch platforms. The basic operation of IPFIX allows you to sample packets on a particular observation point over a period of time and record statistics on all flows.

IPFIX is part of the base functionality of the Ethernet Routing Switch 4500 Series switches.

MLT and LAG Scaling

MultiLink Trunking (MLT) and Link Aggregation Groups (LAG) scaling supports up to 32 trunk groups with up to 8 links per trunk for MLT, Distributed MultiLink Trunking (DMLT) and 802.3ad LAG.

Non-Local Static Routes

Non-Local Static Route (NLSR) is similar to static routes except that the NLSR next hop of the static route is not directly connected to the network entity. NLSR provides connectivity to remote networks by using static routes with a remote gateway. Where there are two or more ways to reach a network, NLSR can reduce the number of static routes by adding only one static route with a remote gateway. NLSR manages static routes where the next hop is not local and is reachable through another route. When a non-local route is added to the best route, the non-local next hop is retrieved from the routing table and the information is used to add the new static route.

Open Shortest Path First

Open Shortest Path First (OSPF) is a dynamic routing protocol that discovers network topology and calculates the shortest path to each destination based on cumulative cost.

OSPF can reduce central processing unit (CPU) and memory resource requirements in a large network by partitioning the network into contiguous areas. OSPF guards against attack by supporting authentication.

QoS Agent Operational Mode

You can enable or disable overall QoS Agent operation using NNCLI. This allows you to easily and temporarily disable all QoS settings for debugging system configuration issues. All user-defined QoS configuration, as well as QoS Agent defaults, are impacted.

QoS DSCP Mutation

In the current QoS implementation of Trusted interface class, the IPv4 traffic received on trusted interfaces is remarked at the layer 2 level. That is, the 802.1p user priority value is updated based on the DSCP value in the packet at ingress and the configured DSCP-to-CoS mapping data. The remarked CoS value is used for queuing at egress and, possibly, for downstream packet processing in a tagged VLAN environment.

In some situations you may want to remark the incoming DSCP value of a packet. Previously you could only use filers or ACLs to remark the DSCP value of a packet.

Now, with the new DSCP Mutation feature, you can use the DSCP-to-CoS Mapping table to remark the DSCP value of a packet. Using the mapping table to remark a packet reduces configuration complexity and significantly reduces filter and ACL use.

QoS Egress Queue Shaping

Release 5.4 provides a new capability to perform egress shaping on a per port per egress queue basis. Minimum and maximum shaping rates can be specified for from 1 to 8 egress queues, depending on the currently-configured QoS Queue Set, on a per-port basis.

QoS IP/L2 Filter Options

The following filtering options are included in this release to introduce a new QoS IP/L2 filtering functionality. This functionality provides greater flexibility in QoS options to customers.

- New Layer 3 (IP) filtering options—IPv4 Flags, TCP Control Flags, and IPv4 Option
- Additional Layer 2 filtering options—Frame Tag and Frame Type
- Existing packet type filtering options—Unknown IP Multicast, Known IP Multicast, Unknown Non-IP Multicast, Known Non-IP Multicast, Non-IP Traffic

QoS Queue Set Support

You can now select from 8 different egress queue sets, supporting from 1 to 8 egress queues, to be used for packet queuing and scheduling at egress. You can also specify the amount of buffer sharing that occurs across ports. Egress queue set selction and buffer sharing allows you greater flexibility to tune the egress queue configuration and buffer utilization of the switch to the types of traffic and congestion which occur on your network. The default queue configuration with this release is set to 2 priority queues with a medium level of buffer sharing.

RADIUS Accounting Enhancements (RFC2866)

The switch can use RADIUS Accounting Enhancements (RFC2866), in particular, the Framed-IP-Address attribute, to send detailed RADIUS accounting updates to the RADIUS server. You can use this feature to improve integration with the Nortel Identity Engines security platform.

RADIUS Server Reachability

You can use RADIUS Server Reachability to configure the switch to use ICMP packets or dummy RADIUS requests to determine the reachability of the RADIUS server.

Routing Information Protocol

Routing Information Protocol (RIP) is a distance vector routing protocol used to discover routes in a network based on information from directly-connected routers. RIP implementation is useful in large networks where static route administration is impractical. RIP adds routes to networks in the routing table, but has no image of the overall network because it relies on neighbor information.

Routing Policies

Release 5.4 supports the following routing policies:

- In/Accept policies can be applied to incoming route updates before they are added to the routing table. For RIP, In/Accept policies can be

applied to all incoming packets with one policy for each RIP interface. For OSPF, In/Accept policies can be applied to external routes based on the advertising router ID, and there is only one policy for the entire switch. In/Accept policies are applied before addition to the routing table from the OSPF Link State Database (LSDB).

- Out/Announce policies are applied to outgoing route updates before the route packets are sent. For RIP, Out/Announce policies can be applied to all outgoing packets and have one policy for each RIP interface. There is no Out/Announce policy supported for OSPF.
- Redistribute policies provide notification when a route is added to, or deleted from, the route table. RIP does not support Redistribute policies. For OSPF, redistributed routes are sent as external routes and there is one policy for the entire switch.

Running Configuration NNCLI Display Commands

The operation of the **show running-config** NNCLI command has been modified. By default, **show running-config** displays only parameters that differ from the default configuration. With Release 5.4, you can use the **verbose** qualifier to display the entire ASCII configuration for the switch or stack, or you can use the **module** qualifier in the command to display the ASCII configuration for a specific feature.

The operation of the **copy running-config tftp** NNCLI command has been modified. By default, **copy running-config tftp** copies the complete contents of the running configuration file to a specified file on the TFTP server. With Release 5.4, you can use the **module** qualifier in the command to display the ASCII configuration for a specific feature, or you can use the **verbose** qualifier to copy the entire ASCII configuration for the switch or stack.

The operation of the **copy running-config usb** NNCLI command has been modified. By default, **copy running-config usb** copies the complete contents of the running configuration file to a USB mass storage device. With Release 5.4, you can use the **module** qualifier in the command to display the ASCII configuration for a specific feature, or you can use the **verbose** qualifier to copy the entire ASCII configuration for the switch or stack.

Show Software Status

Now you can display the currently loaded and operational switch or stack software status for both agent and diagnostic loads as well as the status of any loaded software licenses.

The **show boot** CLI command allows you to view the status of the agent and/or diagnostic images.

The **show sys-info** and **show tech** commands have been enhanced to display the loaded and operational diagnostic and agent software as well as the currently loaded and operational software licenses.

Software Licensing

Software Licensing provides a mechanism to license a set of product features based on the license you purchase.

In the licensing portal you get a license activation key along with the license kit you purchase for a given product. On the licensing portal (genlic), you can generate a license using the license activation key and the MAC address of the switch. To license a stack, use the MAC address of the base unit. The licensing portal generates an encrypted and compressed binary file that you can download to the switch.

The current licensing infrastructure supports a maximum of 10 license files on the end device. The system validates each license file on the end device, independent of all other license files.

Licenses are available as single or multiple (10) licenses. You can apply each license to a switch or stack. Licenses can be combined into one license file on the licensing portal. To ease administration, you can use this one license file across multiple stacks in larger sites. Rather than purchase individual licenses, it is more effective to purchase a package of 10 licenses.

Software licensing is currently available in 2 levels for ERS 4500: Basic and Advanced. When you purchase an ERS 4500 switch, the Base License is present as part of the agent code software and does not need to be loaded onto the switch separately. If you purchase and apply an Advanced License, then you gain access to all of the features included in Basic and Advanced licensing. In Release 5.4 the new feature, OSPF, requires an Advanced License.

Release 5.4 includes a licensing enhancement for switch stacks called Licensing Automatic Unit Replacement (LAUR). LAUR builds a virtual license, based on the loaded license file and the registered MAC address of the stack. The stack continues to use the virtual license file even if the base unit fails and is replaced. This means that you do not need to regenerate a new license file when you replace a failed base unit in a stack.

For more information about software licensing, see *Nortel Ethernet Routing Switch 4500 Series, Fundamentals* (NN47205-102).

Sticky MAC Address

Sticky MAC address enhances MAC address security for users that require a high level of control and simpler configuration and operation. Sticky MAC address secures the MAC address to a specified port so that if the address moves to another port, the system raises an intrusion event. When you use Sticky MAC address, the switch performs initial auto-learning of MAC addresses and can store the automatically learned addresses across switch reboots.

Time Delay Reflectometer

The Time Domain Reflectometer (TDR) provides a diagnostic capability to test connected cables for defects (such as short pin, pin open, and so on). You can perform cable diagnostics on any port in the switch or stack, and you can initiate multiple port tests simultaneously. You can initiate TDR tests and obtain test results from the NNCLI or the EDM.

Traffic Profile Filter Set Support

A filter set is an ordered list that contains classifiers/blocks and the associated action and meter criteria to be applied to traffic that matches the classifier data. Release 5.4 introduces Traffic Profile Filter Set support which allows you to construct and apply a series of policies—classifiers/actions/meters—to an interface in a flexible and streamlined way. Traffic Profile Filter Sets support advanced traffic identifcation and flexible metering options on a per-policy and per-classifier basis. Modifications to the set are allowed while it is in use. Traffic Profile Filter Set Support provides improvements over the existing Access Control List (ACL) support.

Supported software and hardware capabilities

The following table lists supported software and hardware scaling capabilities in Ethernet Routing Switch 4500 Series Software Release 5.4. 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	Configurable 1–8
MAC addresses	8000
Stacking bandwidth (full stack of 8 units)	320 Gb/s: 40 Gb/s per switch
QoS precedence	8 per ASIC
QoS rules per ASIC	128 rules per precedence
Maximum number of units in a stack	8
Layer 2	

Feature	Maximum number supported
VLANs	256
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	32
Maximum MAC Learning rate on an MLT trunk	500 new MAC addresses per second
Links or ports for MLT, DMLT or LAG	8
Spanning Tree Group instances (802.1s)	8
Nortel Spanning Tree Groups	8
DHCP Snooping table entries	1024
Layer 3	
ARP entries (local, static & dynamic)	1792
Local ARP Entries (local IP interfaces)	256
Static ARP entries	256
Dynamic ARP entries	1280
IPv4 route entries (local, static & dynamic)	512
Static routes	32 (configurable 0-32)
Local routes	64 (configurable up to 2-256)
Dynamic routes (RIP & OSPF)	416 (configurable up to 510)
Dynamic routing interfaces (RIP & OSPF)	64
OSPF areas	4 (3 areas plus area 0)
OSPF Adjacencies	16
OSPF Link State Advertisements	10,000
OSPF Virtual Links	4
Management routes	4
UDP Forwarding entries	128
DHCP relay entries	256
DHCP relay forward paths	512
Miscellaneous	
IGMP multicast groups	512
802.1x (EAP) clients per port, running in MHMA	32
802.1x (NEAP) clients per switch/stack	384
802.1x (EAP & NEAP) clients per switch/stack	768
LLDP Neighbors per port	16
LLDP Neighbors	800
RMON alarms	800

Feature	Maximum number supported
RMON events	800
RMON Ethernet statistics	110
RMON Ethernet history	249

Filter, meter and counter resources

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

Note: Filters will use the highest available precedence.

Table 2
Filter, meter and counter resources per port

Feature	Observation	QoS			NonQos	
		Filters	Meters	Counter	Filters	Meters
EAPOL		0	0	0	2	0
ADAC		0	0	0	1	0
DHCP Relay	L2 mode	0	0	0	0	0
DHCP Relay	L3 mode	0	0	0	0	0
DHCP Snooping		0	0	0	2	1
NSNA	**Red**					
	Precedence 5	3	1	1	0	0
	Precedence 4	1	1	1	0	0
	Precedence 3	2	1	1	0	0
	Precedence 2	1	1	1	0	0
	Precedence 1	1	1	1	0	0
NSNA	**Yellow**					
	Precedence 6	3	0	1	0	0
	Precedence 5	1	0	1	0	0
	Precedence 4	1	0	1	0	0
	Precedence 3	2	0	1	0	0
	Precedence 2	1	0	1	0	0
	Precedence 1	1	0	1	0	0
NSNA	**Green**					
	Precedence 1	1	0	1	0	0
MAC Security		0	0	0	0	0

Feature	Observation	QoS			NonQos	
IP Source Guard		0	0	1	11	0
Port Mirroring	Mode XrxYtx	1	0	0	0	0
Port Mirroring	XrxYtx or YrxXtx	0	0	0	2	0
Port Mirroring	AsrcBdst, Asrc, Adst	1	0	0	0	0
Port Mirroring	AsrcBdst or BscrAdst, Asrc or Adst	2	0	0	0	0
QoS	Trusted	0	0	0	0	0
QoS	**Unstrusted**					
	Precedence 2	1	0	1	0	0
	Precedence 1	1	0	1	0	0
QoS	Unrestricted	0	0	0	0	0
UDP Forwarding		0	0	0	1	1
OSPF		0	0	0	3	0
RIP		0	0	0	1	0
IPFIX		0	0	0	1	1

File names for this release

The following table describes the Nortel Ethernet Routing Switch 4500 Series, Software Release 5.4 software files. File sizes are approximate.

Table 3
Software Release 5.4 components

Module or file type	Description	File name	File size (bytes)
Standard runtime image software version 5.4.0.008	Standard image for the Nortel Ethernet Routing Switch 4500 Series	4500_5.4.0.008.img	7,341,832
Secure runtime image software version 5.4.0.009s	Secure image for the Nortel Ethernet Routing Switch 4500	4500_5.4.0.009s.img	7,610,140
Boot/diagnostic software version 5.3.0.3	Switch diagnostic software	4500_5.3.0.3.bin	1,589,514
Enterprise Device Manager Help Files	Help files required for Ethernet Routing Switch 4500	ERS_4500_Help_EDM.zip	1,582,517

Table 3
Software Release 5.4 components (cont'd.)

Module or file type	Description	File name	File size (bytes)
Enterprise Device Manager plug-in	Ethernet Routing Swtich 4500 Enterprise Device Manager plug-in for Configuration and Orchestration Manager	ers4500v5.4.0.0.war	2,810,439
Software Release 5.4 Management Information Base (MIB) definition files	MIB definition files	Ethernet_Routing_Switch_45xx_MIBs_5.4.0.zip	1,647,436

Supported traps and notifications

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

Supported Web browsers for Enterprise Device Manager

The following is a list of Internet Web browsers supported by EDM:

- Mozilla Firefox 3.5
- Microsoft Internet Explorer 7.0

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

Upgrading software

To upgrade to the new software release 5.4, Nortel recommends that you upgrade the diagnostic software to the 5.3.0.3 version, and then upgrade the agent version to release 5.4.

The following table describes possible image locations:

Table 4
Possible scenarios

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

Image	Location
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.3
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.4

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

ATTENTION
A switch that has an agent runtime image prior to release 5.2.0 should not be added to a stack running 5.4.0 or later software. To add a switch with an agent code prior to 5.2.0, you should at a minimum upgrade the agent code to at least 5.2.0 versions before adding the switch to the stack. When loading software release 5.4 it is mandatory that the switches are loaded with 5.3.0 or later diagnostic software due to the increased size of the 5.4 runtime agent code. The recommended diagnostic version is 5.3.0.3 or later.

Switches with agent runtime software older than 5.2.0 cannot perform an automatic diagnostic upgrade (DAUR) to the version which is operational in the stack. For switches with older diagnostics that cannot handle the larger 5.4.0 or later agent runtime image, the stack management software with 5.4 software does not automatically upgrade a switch with agent code earlier than 5.2.0. If a switch with software release prior to 5.2 is added into a stack, the unit is not allowed to join the stack and the base unit on that switch will flash rapidly to indicate an issue. The switch system log will provide information that the switch could not be upgraded and had mismatching software.

Use the following procedure to upgrade the Agent Image from release 5.0, 5.1, 5.2, or 5.3 to release 5.4:

Upgrading Agent Image from release 5.0, 5.1, 5.2, or 5.3 to release 5.4.

Step	Action
1	Upgrade the diagnostic image from the earlier release to release 5.3.0.3 diagnostic image.
2	Upgrade the agent image from release 5.0, 5.1, 5.2, or 5.3 to release 5.4 agent image.

--End--

ATTENTION
If units connected in a stack contain different diagnostics versions than the Base Unit, then those particular units will not join the stack. Use the **`Show Tech`** command to determine whether the software and diagnostics versions match on all units in stack.

Affects of upgrade on trap notifications

ATTENTION
All trap notifications are enabled after you upgrade to Release 5.4 software, regardless of whether you disabled them prior to the upgrade

You can use the following procedures to restore trap functionality.

To restore trap notification functionality, use the following NNCLI procedure:

Step	Action
1	Use the following NNCLI command to remove traps created in R5.3: `no snmp-server host X.Y.Z.T 'community name'` .
2	Reconfigure trap notification, using either NNCLI or EDM.

--End--

To reconfigure traps, use the following EDM procedure:

Step	Action
1	From the Navigation tree, click **Edit**.
2	From the Edit tree, click **Snmp Server**.
3	In the work area, select the **Community** tab.
4	Create a community string— you must specify the Notify View name.
5	In the work area, select the **Host** tab to create an SNMP host— use the community you created in the previous step.
6	On the **Host** tab, use the **Notification** button to activate or deactivate individual traps.
7	In the work area, select the **Notification Control** tab to activate or deactivate individual traps per device.

--End--

To reconfigure traps, use the following NNCLI procedure—v1 host example with password security enabled:

Step	Action
1	To create a community—from the global configuration prompt, enter the following command: **snmp-server community notify-view nncli**.
2	To create an SNMP host using the community you created in the previous step—from the global configuration prompt, enter the following command: **snmp-server host 10.100.68.3 port 162 v1 filter TestFilter**.

--End--

To reconfigure traps, use the following NNCLI procedure—v1 host example with password security disabled:

Step	Action
1	To create an SNMP community—from the global configuration prompt, enter the following command: **snmp-server community CommunityName notify-view nncli**.
2	To create an SNMP host using the community you created in the previous step—from the global configuration prompt enter the following command: **snmp-server host 10.100.68.3 port 162 v1 CommunityName filter TestFilter**.

--End--

To set the Notification Type per receiver, use the following NNCLI procedure:

Step	Action
1	From the global configuration prompt, enter the following command: **snmp-server notify-filter TestFilter +org**.
2	From the global configuration prompt, enter the following command: **snmp-server notify-filter TestFilter -linkDown**.
3	From the global configuration prompt, enter the following command: **snmp-server notify-filter TestFilter -linkUp**.

--End--

To display the notification types associated with the notify filter, use the following NNCLI procedure:

Step	Action
1	From the global configuration prompt, enter the following command: **show snmp-server notification-control**.

--End--

To enable or disable the Notification Type per device, use the following NNCLI procedure:

Step	Action
1	From the global configuration prompt, enter the following command: **no snmp-server notification-control linkDown**.
2	From the global configuration prompt, enter the following command: **no snmp-server notification-control linkUp**.

--End--

Updating switch software

You can update the version of software running on the switch through either NNCLI or Enterprise Device Manager.

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

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

See the following sections for details about updating switch software:

- “General software upgrade instructions” (page 33)
- “Changing switch software in NNCLI” (page 33)
- “Changing switch software in EDM” (page 34)

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>	<ipv4_address>] {image <image name>	image-if-newer <image name>	diag <image name>	poe_module_image <image name>} [no-reset] [usb] [unit <unit number>]`**
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 8 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.

ATTENTION
During the download process, the management functionality of the switch is locked. Normal switching operations will continue to function..

Job aid—download command parameters

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

Table 5
NNCLI download command 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> | <ipv4_address>	The IPv4 or IPv6 address of the TFTP server you use. The address <ipv6_address> | <ipv4_address> 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 [unit <unit number>]	In the switch, this parameter specifies that the software download is performed using a USB Mass Storage Device and the front panel USB port. Use the unit number parameter to specify which switch contains the USB.

Changing switch software in EDM

Use the following procedure to change the software version running on the switch that uses EDM.

Step	Action
1	From the navigation tree, click **Edit**.
2	In the Edit tree, click **File System**.
3	In the work area, on the **Config/Image/Diag file** tab, configure the parameters required to perform the download.
4	On the toolbar, 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 8 minutes.

When the download is complete, the switch automatically resets and the new software image initiates a self-test.

ATTENTION
During the download process, the management functionality of the switch is locked. Normal switching operations will continue to function.

Job aid—File System screen fields

The following table describes the File System screen fields.

Table 6
File System screen fields

Field	Description
TftpServerInetAddress	Indicates the IP address of the TFTP server on which the new software images are stored for download.
TftpServerInetAddressType	Indicates the type of TFTP address. • IPv4 • IPv6
BinaryConfigFileName	Indicates 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.

Field	Description
BinaryConfigUnitNumber	When in standalone mode, and loading a binary configuration file that was created from a stack, this object specifies the unit number of the portion of the configuration file to be extracted and used for the standalone unit configuration. If this value is 0, it is ignored.
ImageFileName	Indicates the name of the image file currently associated with the switch. If needed, change this field to the name of the software image to be downloaded.
FwFileName (Diagnostics)	The name of the diagnostic file currently associated with the switch. If needed, change this field to the name of the diagnostic software image to be downloaded.
UsbTargetUnit	Indicates the unit number of the USB port to be used to upload or download a file.
Action	This group of options represents the actions taken during this file system operation. The options applicable to a software download are • dnldImg: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. • dnldFw: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. • dnldConfig: Download a configuration to the switch. • dnldImgFromUsb: Download a new software image to the switch using the front panel USB port. This 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

Field	Description
	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. • upldImgToUsb: Upload image to USB port • upldConfigToUsb: Upload binary config to USB port

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.

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: 181.30.30.254
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
USBdiag <string>	Specifies the file name of the diagnostic image to load from the USB device. Example> ers4500/ers4500_5.1.0.4.bin

Parameter	Description
USBascii <string>	Specifies the file name of the ASCII configuration file to load from the USB device. Example: customer1.cfg
USBagent <string> NEXTIP, NEXTMask, and NEXTGateway	Specifies the file name of the agent image to load from the USB device and specifies IP addresses for the next boot. Example: ers4500/ers4500_5.2.0.0.img

The ip.cfg file loads information from the ASCII configuration file in order of precedence.

For example, if you have an ip.cfg file with the following commands:

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

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

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

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

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

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

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

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

Step	Action
1	Enter **boot default**.
2	Enter **y** to confirm the reset. *The Ethernet Routing Switch 4500 restarts with factory default settings and attempts to read the ip.cfg file from an installed USB drive within three minutes. The Nortel Ethernet Routing Switch 4500 banner page appears while the switch retrieves the ip.cfg file.* The delay until the device or devices are reset to factory default is approximately 3 minutes, but is dependant on the size of the stack and the configuration used.

--End--

ATTENTION
While the system retrieves the ip.cfg file from the USB memory device, the Nortel banner page appears. 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
1000BASE-CWDM SFP	1470 nm LC connector, up to 40 km	5.0.0	AA1419025-E5
1000BASE-CWDM SFP	1490 nm LC connector, up to 40 km	5.0.0	AA1419026-E5
1000BASE-CWDM SFP	1510 nm LC connector, up to 40 km	5.0.0	AA1419027-E5
1000BASE-CWDM SFP	1530 nm LC connector, up to 40km	5.0.0	AA1419028-E5
1000BASE-CWDM SFP	1550 nm LC connector, up to 40 km	5.0.0	AA1419029-E5
1000BASE-CWDM SFP	1570 nm LC connector, up to 40 km	5.0.0	AA1419030-E5
1000BASE-CWDM SFP	1590 nm LC connector, up to 40 km	5.0.0	AA1419031-E5
1000BASE-CWDM SFP	1610 nm LC connector, up to 40 km	5.0.0	AA1419032-E5
1000BASE-CWDM SFP	1470 nm LC connector, up to 70 km	5.0.0	AA1419033-E5

Supported SFPs and XFPs	Description	Minimum software version	Part number
1000BASE-CWDM SFP	1490 nm LC connector, up to 70 km	5.0.0	AA1419034-E5
1000BASE-CWDM SFP	1510 nm LC connector, up to 70 km	5.0.0	AA1419035-E5
1000BASE-CWDM SFP	1530 nm LC connector, up to 70 km	5.0.0	AA1419036-E5
1000BASE-CWDM SFP	1550 nm LC connector, up to 70 km	5.0.0	AA1419037-E5
1000BASE-CWDM SFP	1570 nm LC connector, up to 70 km	5.0.0	AA1419038-E5
1000BASE-CWDM SFP	1590 nm LC connector, up to 70 km	5.0.0	AA1419039-E5
1000BASE-CWDM SFP	1610 nm LC connector, up to 70 km	5.0.0	AA1419040-E5
1000BSE-T SFP	Category 5 copper unshielded twisted pair (UTP), RJ-45 connector	5.0.0	AA1419043-E5
1000BASE-SX DDI SFP	850 nm DDI LC connector	5.2.0	AA1419048-E6
1000BASE-LX DDI SFP	1310 nm DDI LC connector	5.2.0	AA1419049-E6
1000BaseXD DDI SFP	1310nm LC connector	5.4	AA1419050-E6
1000BaseXD DDI SFP	1550nm LC connector	5.4	AA1419051-E6
1000BaseZX DDI SFP	1550nm LC connector	5.4	AA1419052-E6
1000BaseCWDM SFP	1470nm LC connector, up to 40km	5.4	AA1419053-E6
1000BaseCWDM DDI SFP	1490nm LC connector, up to 40km	5.4	AA1419054-E6
1000BaseCWDM DDI SFP	1510nm LC connector, up to 40km	5.4	AA1419055-E6
1000BaseCWDM DDI SFP	1530nm LC connector, up to 40km	5.4	AA1419056-E6
1000BaseCWDM DDI SFP	1550nm LC connector, up to 40km	5.4	AA1419057-E6
1000BaseCWDM DDI SFP	1570nm LC connector, up to 40km	5.4	AA1419058-E6
1000BaseCWDM DDI SFP	1590nm LC connector, up to 40km	5.4	AA1419059-E6

Supported SFPs and XFPs	Description	Minimum software version	Part number
1000BaseCWDM DDI SFP	1610nm LC connector, up to 40km	5.4	AA1419060-E6
1000BaseCWDM DDI SFP	1470nm LC connector, up to 70km	5.4	AA1419061-E6
1000BaseCWDM DDI SFP	1490nm LC connector, up to 70km	5.4	AA1419062-E6
1000BaseCWDM DDI SFP	1510nm LC connector, up to 70km	5.4	AA1419063-E6
1000BaseCWDM DDI SFP	1530nm LC connector, up to 70km	5.4	AA1419064-E6
1000BaseCWDM DDI SFP	1550nm LC connector, up to 70km	5.4	AA1419065-E6
1000BaseCWDM DDI SFP	1570nm LC connector, up to 70km	5.4	AA1419066-E6
1000BaseCWDM DDI SFP	1590nm LC connector, up to 70km	5.4	AA1419067-E6
1000BaseCWDM DDI SFP	1610nm LC connector, up to 70km	5.4	AA1419068-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
1000Base DDI SFP	1550nm LC connector, 120km.	5.4	AA1419071-E6
100BASE-FX SFP	1310 nm LC connector	5.0.0	AA1419074-E6
T1 SFP	1.544 Mbit/s Fast Ethernet to T1 remote bridge, RJ-48C	5.1.0	AA1419075-E6
1000BASE-BX SFP	1310nm LC connector, up to 40km (Must be paired with AA1419077-E6)	5.3	AA1419076-E6
1000BASE-BX SFP	1490nm LC connector, up to 40km (Must be paired with AA1419076-E6)	5.3	AA1419077-E6
10 Gigabit Ethernet SFP transceivers			
10GBASE-LR/LW XFP	1-port 1310 nm SMF, LC connector	5.2.0	AA1403001-E5

Supported SFPs and XFPs	Description	Minimum software version	Part number
10GBASE-SR XFP	1-port 850 nm MMF, LC connector	5.1.0	AA1403005-E5
10GBASE-ZR/ZW XFP	1550 nm SMF LC connector	5.1.0	AA1403006-E5
10GBASE-LRM XFP	1310 nm, up to 220 m over MMF, DDI	5.2.0	AA1403007-E6

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

Supported standards, RFCs and MIBs

The following sections list the standards, RFCs and MIBs supported in Release 5.4.

Standards

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

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

RFCs and MIBs

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

- RFC 791 (IP)
- RFC 894 (IP over Ethernet)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 768 (UDP)
- RFC 854 (Telnet)
- RFC 951 (BootP)
- RFC 1058 (RIP v1)
- RFC 1213 (MIB-II)
- RFC 1350 (TFTP)
- 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
- RFC 1583 (OSPF v2)
- RFC 1850 (OSPF v2 MIB)
- RFC 2328 (OSPF v2)
- RFC 2453 (RIP v2)
- RFC 2474 (Diffserv)
- RFC 2475 (Diffserv)
- RFC 2866 (RADIUS Accounting)
- RFC 3046 (DHCP Relay Agent Information Option)
- RFC 3993 (DHCP Subscriber-ID suboption)
- RFC 3917 (IP Flow Information Export [IPFix])
- RFC 3954 (Netflow Services Export v9)

IPv6 specific RFCs

The following table lists IPv6 specific RFCs.

Table 9
Supported IPv6 specific RFCs

Standard	Description	Compliance
RFC 2460	Internet Protocol v6 (IPv6) Specification	Supported
RFC 2461	Neighbor Discovery for IPv6	Supported
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 4443	Internet Control Message Protocol (ICMPv6)	Support earlier version of RFC (2463)
RFC 4301	Security Architecture for the Internet Protocol	Not supported
RFC 4291	IPv6 Addressing Architecture	Support earlier version of RFC (3513)
RFC 4007	Scoped Address Architecture	Supported
RFC 4193	Unique Local IPv6 Unicast Addresses	Not supported

Standard	Description	Compliance
RFC 4293	Management Information Base for IP	Mostly supported
RFC 4022	Management Information Base for TCP	Mostly supported
RFC 4113	Management Information Base for UDP	Mostly supported
RFC 1981	Path MTU Discovery for IPv6	Supported
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Supported
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack. No support for tunneling yet.
RFC 3162	RADIUS and IPv6	Supported
RFC 1886	DNS Extensions to support IPv6	Supported

Resolved issues

The following table lists the issues resolved for release 5.3 and 5.4.

Table 10
Resolved issues

Reference number	Description
Q01532673	**CLI**: show running-config and copy running-config commands now provide the ability to display CLI commands for a specific feature using the ‘module’ qualifier.
Q01538672	**CLI**: show running-config and copy running-config commands now output only the configuration differences from the default configuration. To display the full configuration, you can now use the ‘verbose’ qualifier.
Q01540397	**802.3ad, LACP, STP**: You are no longer required to change the Spanning Tree status of a port after you configure 802.3ad/LACP/LAG. When you configure LACP on a port or add a member into a Link Aggregation Group (LAG), the port now correctly inherits the Spanning Tree status of the port.
Q01805723	**VLAN, MSTP**: The switch now supports the ability to assign VLAN ranges to MSTP MSTI instances.
Q01879824	**EAP, IP Phone**: When an authenticated PC which is connected through an IP Phone to the switch is moved to another switch port and re-authenticated, the "show eapol multihost status" command now correctly shows the MAC address of the PC as being authenticated at the new switch port location.
Q01912129-01	**ADAC**: Auto Detection Auto Configuration (ADAC) now supports the ability to assign up to 8 ports or MLT/DMLT/LAG for uplink or call server ports.
Q01930542	**Port Mirroring**: The port mirroring monitor port is now able to send and receive traffic while traffic is being mirrored to the port. This means that you can deploy devices on the monitor port which need to communicate with the network.
Q01931688	**USB**: It is no longer required to wait 5 to 10 seconds after insertion of a USB device before removing the device or 5 to 10 seconds after removal of a USB device before inserting another USB device into the same switch unit.
Q01938092-02	**QoS**: You can now specify a name for IP or Layer 2 QoS elements when you use the CLI.

Reference number	Description
Q01969771	**ACG**: ASCII download enhancements now provide additional error information when the TFTP server is not configured.
Q01970994	**EAP, RFC 3576**: You can now enable or disable RFC3576 replay protection.
Q01974064	**ASCII Load on Boot**: The system now logs an error message when the load-on-boot configuration file cannot be accessed.
Q01975164	**MIB, SNMP**: Previously the ifOperStatus reported the status of the IP Management interface based on the port status. Now the switch reports status based on the virtual status of the IP Management VLAN, meaning that if any port in the management VLAN is up, then the status of the management VLAN is reported as up.
Q01977177	**IPv6, Quickstart, CLI**: The CLI quickstart function now supports the configuration of an IPv6 management address.
Q01979964	**RADIUS, CLI**: An inconsistency which meant that you could not set the RADIUS secret to blank has now been corrected.
Q01981930	**EAP, NEAP, RAV**: if the RADIUS Assigned VLAN (RAV) returned by the server does not exist (that is it not already is configured on the switch), then the switch will now generates an SNMP trap and log message to indicate that the client was not moved into the RAV.
Q01984479-01	**LLDP, 100FX SFP**: the LLDP dot3 Autonegotiation capabilities advertisement now works correctly for slow speed SFPs rather than displaying them as 1Gbps.
Q01984478	**NEAP, Fail Open VLAN**: Non-EAP (NEAP) clients connected to the non-base unit of a stack are now correctly displayed when Fail Open VLAN is activated.
Q01985219	**EAP, NEAP**: when a large number of EAP and NEAP clients are authenticated on a port (for example 32 EAP and 32 NEAP clients), the commands to display EAP status now display the authenticated clients within normally expected response times.
Q01985368	**UDP Forwarding**: UDP packets are now correctly forwarded to all configured interfaces. It should be noted that under very high packet rates that some UDP broadcast packets could be dropped due to the CPU being busy.
Q01985803-01	**IPv6, CLI**: the error messages returned when incorrect IPv6 management commands are entered have been improved to better explain the various errors.
Q01991720	**EAP, CLI**: for improved diagnostics, the show eapol commands now displays a total number of EAP clients connected to the switch.
Q01992543	**CLI**: The command interpreter has been modified so that 'sh' can be used as an abbreviation for the 'show' command in all contexts. To provide a unique context for the shutdown command, you will need to enter 'shu'.
Q01994775	**RADIUS, MIB**: the switch now provides RADIUS accounting MIB support.
Q02000291-01	**SNTP, CLI**: inconsistency between the displays of the "show clock" and "show clock detail" commands has now been rectified.

Reference number	Description
Q02001358	**USB, CLI**: the show usb-files command has been enhanced to display sub-directories.
Q02002291	**EAP, RAV**: the MAC address table no longer displays temporary duplicate entries for 802.1X clients when using RADIUS assigned VLANs (RAV) on non-base units in a stack.
Q02002422	**EAP, RAV, Last Assigned VLAN**: when operating in MHMA mode with more than 3 active clients connected which use RADIUS assigned VLANs (RAV) and RADIUS last assigned VLAN is enabled, the port is no longer incorrectly placed in Forced Unauthorized state.
Q02002911	**RADIUS, IP Management**: a correct error message is now returned when no IP Management address is configured and you attempt to configure RADIUS on the switch.
Q02002916	**Asset ID**: the stack asset ID can now be reset on a unit which is no longer a member of a stack.
Q02002922	**RADIUS, IP Management**: if no IP Management address is configured and the switch is configure for RADIUS use IP Management, the switch will now attempt to communicate with the RADIUS server using one of the other IP interfaces configured.
Q02003409	**EAP, VoIP VLAN**: if you attempt to enable EAP VoIP VLAN, the feature now checks that each EAP VoIP VLAN is configured for a different VLAN ID.
Q02003926-01	**ADAC, LLDP**: when you configure ADAC and LLDP-MED the switch now correctly send LLDP network policy TLV on a port having an IP Phone.
Q02004829-01	**EAP, RADIUS Accounting**: the calling station ID and user ID information is now included in RADIUS accounting messages.
Q02005676	**USB, ASCII Audit Log**: when you download an ASCII configuration from a USB storage device, the ASCII audit log now correctly indicates that the configuration was loaded from USB and not the console.
Q02005748-01	**IPSG, IGMP**: IGMP multicast packets are now correctly processed on a port which has IP Source Guard (IPSG) enabled.
Q02006341	**TACACS+**: after multiple failures of both the primary and secondary TACACS+ server, the user is correctly authenticated on the primary server if it is reachable.
Q02006431	**MAC Security**: if you perform a repetitive add-remove of the same MAC address from the MAC security table, the client will now continue to authenticate and pass traffic as expected.
Q02006993, Q02007429	**LLDP**: the LLDP location based TLV information for "Longitude" and "Datum" is correctly restored on a non-base unit in a stack.
Q02007063	**SNTP, Daylight Savings**: the recurring command for daylight savings now features new qualifiers which allow setting the start and end of Daylight Savings time to the ‘first’ or ‘last’ occurrence of a day in the month. This makes setting Daylight Savings for recurring years more intuitive and simple.

Reference number	Description
Q02007488	**IGMP**: multicast groups are now always flushed when a port is shutdown.
Q02007591	**QoS**: you can now modify the evaluation order in a classifier block.
Q02008078	**EAP, binary configuration**: if a binary configuration file containing EAP configurations is loaded onto a switch with has no IP address set, then the EAP functionality will be automatically disabled on the switch to prevent loss of network connectivity.
Q02011787-01	**EAP**: an error message which was displayed in some situations when globally enabling EAP is no longer incorrectly displayed.
Q02016728-01	**IPv6, ASCII Load on Boot**: the ASCII Load on Boot feature can now download the configuration file from the TFTP server if only an IPv6-based TFTP server is configured.
Q02019507	**EAP, Guest VLAN, ADAC**: once any EAP or NEAP if authenticated on a port, the port is now correctly removed from the Guest VLAN (GVLAN) unless MHMA MultiVLAN is enabled.
Q02019507	**EAP, NEAP Guest VLAN, ADAC**: once any EAP or NEAP if authenticated on a port, the port is now correctly removed from the Guest VLAN (GVLAN) unless MHMA MultiVLAN is enabled.
Q02019768	**SNTP**: settings for SNTP are now correctly saved in ASCII configuration file.
Q02020144-01	**Audit Log**: a user with read-only privileges is no longer able to see passwords when they issue a show audit log command.
Q02021402	**EAP, Guest VLAN, Fail Open VLAN**: when a PC is connected behind an IP Phone and the port enters and then leaves the Fail Open VLAN, the port now transitions into the Guest VLAN within expected time.
Q02024587	**MAC Security**: if you decrease the maximum number of allowed addresses on a port, the addresses already learnt by MAC security are no longer flushed on the port if the number of addresses learnt is less than the maximum configured.
Q02027845	**EAP, ADAC, LLDP, IP Phone**: third party IP Phones can now be discovered via ADAC with LLDP and authenticated with EAP without having to manually add the MAC address range of the Phone into ADAC.
Q02031671	**RMON, CLI**: CLI commands are now available to allow you to display detailed RMON Ethernet & history statistics. • **`show rmon ethernet [port <port-list>]`** • **`show rmon ethernet packets [port <port-list>]`** • **`show rmon history port [port <port-list>]`** • **`show rmon history delta [port <port-list>]`**
Q02035271	**TACACS+**: TACACS+ parameters can now be configured and queried via SNMP MIB.
Q02035382	**NEAP, Guest VLAN, IP Phone**: traffic is now correctly forwarded in the Guest VLAN (GVLAN) for a NEAP device after an IP Phone is authenticated on the port.

Reference number	Description
Q02035415	**NEAP, Guest VLAN**: DHCP Request packets received from a NEAP device in the Guest VLAN (GVLAN) are now correctly forwarded.
Q02036749	**100FX SFP**: the 100Base-FX SFP type is now correctly displayed as FX instead of LX.
Q02039939	**EAP, Guest VLAN, EAP Failure**: when the switch returns an EAP failure, if the Guest VLAN (GVLAN) is configured, the device is now correctly placed in the GVLAN so that network connectivity is provided.
Q02042427-05	**DHCP Relay**: the switch now correctly forwards DHCP packets larger than 590 bytes. Note that you can configure the maximum packet size for DHCP relay.
Q02043105	**NEAP IP-Phone**: the switch correctly forwards the DHCP Discover packet to the DHCP server and the Nortel IP Phone is authenticated through DHCP signature. The switch now no longer incorrectly blocks the DHCP offer from the DHCP server to the IP Phone.
Q02047324	**CLI help**: inconsistencies in a numer of "show <feature> port" commands have been removed.
Q02050790	**EAP, Guest VLAN**: when Guest VLAN is not enabled on a port, DHCP request packets from unauthenticated clients are now correctly dropped.
Q02056032	**Binary Configuration, Unit Renumbering**: a binary configuration file which is saved to a TFTP server will now correctly provision units which have been renumbered.
Q02056838	**DHCP Relay**: DHCP Relay will now correctly forward DHCP packets larger than 590 bytes in size without a CRC. Some devices for example Avaya IP Phones can generate large DHCP requests of 1038 bytes.
Q02057570	**Protocol VLAN, IP Address**: the previous restriction which prohibited you from configuring an IP address on a protocol VLAN is now removed.
Q02058282	**ARP, CLI**: the switch now supports an enhancement to show ARP entries for a specified MAC address.
Q02058285	**ARP, CL**I: the switch now supports an enhancement to show ARP entries for a specified VLAN ID.
Q02058288	**Telnet, CLI**: the switch now supports an enhancement to allow you to specify the TCP port number when using the telnet command to connect to another device.
Q02059938	**DHCP Snooping, Dynamic ARP Inspection (DAI)**: ARP messages are no longer lost when a client IP address is released and re-obtained by DHCP in quick succession when the switch port is configured for DHCP Snooping and Dynamic ARP inspection.
Q02061265-01	**ADAC, MLT, DMLT, LAG**: if you configure an ADAC call server or uplink port as a MLT/DMLT or LAG then the “show adac” command now identifies the MLT/DMLT or LAG rather than just the first port of the link group.
Q02062951-01	**VLAN, CLI**: the switch now supports an enhancement to the “show vlan” command to display a summary of the VLAN configuration for the switch.

Reference number	Description
Q02065150	**QoS**: interface queue shaper now allows setting a value of 0 for shape-rate and shape-min-rate, in which case the appropriate shaping rate will not be set, this may be useful where you want to specify only the maximum shaping rate.
Q02065703	**ADAC**: changes to the call server and uplink port configurations can now be applied dynamically without having to disable then re-enable ADAC.
Q02071335	**Syslog, SNMP Traps, DMLT**: if you create a Distributed MLT (DMLT) which spans multiple units, then when you fail one of the units which has a port member of the DMLT, then multiple syslog or SNMP trap messages are no longer generated. A single entry for the given member of the DMLT is generated as expected.
Q02077416	**DHCP Snooping, Dynamic ARP Inspection (DAI)**: when DHCP Snooping and Dynamic ARP Inspection (DAI) are both configured on a port, IP Phones will now obtain their IP addresses without unexpected delays.
Q02084318	**DHCP Snooping**: When DHCP Snooping is enabled, devices which set the DHCP broadcast flag (for example some models of Cisco WLAN Access Points) are now correctly learnt by the DHCP Snooping function.
Q02089655	**LOG**: the default log option is changed from latch to overwrite. With the previous default setting of latch, if the log filled up then the most recent log events would be lost. Now with the setting changed to overwrite, if the log becomes full, the switch will begin to overwrite the oldest entries in the log, this ensures that the log contains the most recent log messaged.
Q02093522	**EAP, NEAP**: when one of the units in a stack of 8 is power cycled and the maximum number of 768 EAP/NEAP clients are active, then the EAP/NEAP users on the unit which was power cycled will be correctly re-authenticated.
Q02094770	**Password Aging, ACG**: the password aging time setting is now correctly saved to the ASCII configuration file.
Q02097604	**EAP, Fail Open VLAN**: when the switch looses reachability to the RADIUS server and Fail Open VLAN is configured, all EAP/NEAP and unauthenticated clients are moved into the Fail Open VLAN. Now all devices are correctly moved into the Fail Open VLAN and are able to access the network.
Q02100457	**EAP, unauthenticated user**: unauthenticated users can no longer gain access to the network by sending packets tagged with the VoIP VLAN through an IP Phone.
Q02109202	**ADAC, Avaya IP Phones**: ADAC LLDP detection now works correctly with all Avaya IP Handsets. Previously ADAC could only detect Avaya IP Handsets after they had successfully contacted the call server.
Q02113703-01	**RADIUS, ICMP**: the switch now supports the ability to configure reachability of the RADIUS server. The default method is to use ICMP, in some scenarios when ICMP is blocked by internal firewalls, the RADIUS reachability can be configured to use a dummy RADIUS request.

Known issues and limitations

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

Navigation

- Table 11 "Known issues and limitations" (page 55)
- “IPv6 limitations” (page 66)

Known issues and limitations

The following section lists known issues and limitations in Ethernet Routing Switch 4500 Series Software Release 5.3 and Release 5.4.

Table 11
Known issues and limitations

Reference number	Description
Q01496548	**Link-up during boot**: During reboot or power up operations, but before the agent code loads, the switch may provide an intermittent link to devices connected to front panel ports. Regardless, no traffic switching occurs until the agent code load completes.
Q01565427	**SONMP**: A change in the operation of the SONMP-based auto topology means that directly connected BayStack 450 switches report a physical auto topology change every 70 seconds to the ERS 4500 switch. You can ignore this auto topology change message where there is a direct connection from the ERS 4500 to a BayStack 450 switch.

Reference number	Description
Q01585285	**EDM, ASCII Configuration**: When loading an ASCII configuration file using EDM 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 EDM to a switch or stack that has a 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 the last ASCII file line executes.
Q01672222	**Jumbo Frames**: As the Ethernet Routing Switch 4500 supports jumbo frames (up to 9216), the Jabber counter will always be displayed as zero (0). **Workaround**: You can find information about framing errors in the etherStatsCRCAlignErrors counter.
Q01878544	**NSNA**: For a MAC authenticated client, if the MAC address is deleted from the SNAS database, the SNAS does not send a reset event to the switch, so the client will remain in its currently assigned VLAN. **Workaround**: Execute NNCLI commands **`shutdown`**, then **`no shutdown`** on the corresponding ports.
Q01893356-01	**NSNA**: After rebooting a switch or stack with NSNA MAC based clients connected, the switch may incorrectly report that the devices are in the RED VLAN even through they are actually in the Green VLAN. **Workaround**: Execute the CLI commands **`shutdown`**, then **`no shutdown`** on the corresponding ports.
Q01920357	**Port Mirroring, Bootp**: Due to a hardware limitation, the BOOTP packets cannot be mirrored if the mirror port is on the first ASIC (port 1-24).
Q01921829	**LLDP**: If 802.1 TLV for VLANs is already enabled for advertisement on a port, then the advertisement will not be updated to reflect any new VLAN additions. **Workaround**: Disable and re-enable TLV advertisement for the respective ports.
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 becomes unable to reconnect to the SNAS. **Workaround**: Disable and re-enable the switch on the SNAS to regain switch to SNAS connectivity.

Reference number	Description
Q01970577	**EAP, Fail Open VLAN**: When a device is moved into or out of the Fail Open VLAN, there is no notification to the end client that the VLAN has been changed. **Workaround**: It is recommended that if Fail Open VLAN is used, you should set the DHCP lease time to a short period so that clients regularly refresh their IP address leases. Alternatively, if a client has been moved to the Fail Open VLAN, then issuing a DHCP release and renew on the client obtains a new IP address appropriate for the Fail Open VLAN.
Q01977243	**QoS information**: Non QoS applications, such as UDP Forwarding and IP Source Guard, should be configured prior to configuration of QoS policies to avoid the potential conflict in filter precedence order which can result when the binary configuration file is reloaded. In some rare cases, when QoS precedences are configured before non-QoS applications that use filters—for example: UDP Forwarding, NSNA, and IP Source Guard—the QoS information saved in the binary configuration file may not be correctly reloaded to the switch. The greater the number of filter-using non-QoS applications per port, the greater the probability that the QoS information in the binary configuration file may be reloaded incorrectly. If the QoS information in the binary configuration file is reloaded incorrectly, some of the QoS precedences may not be configured correctly.
Q01979311-01, Q02103362, Q02136787	**Password, Security**: You cannot change the username and password for individual units in a stack when Telnet/SSH is used. **Workaround**: Username and password for individual units can be changed using the serial console connection on each unit or by using the EDM **switch option** to set passwords for all individual units in a stack.
Q01979384	**IPv6**: Due to the short, or transient, nature of TCP connections for HTTP requests it is likely that IPv6 HTTP connections may not be displayed when you use the CLI command **`show IPv6 TCP connection`**. This behavior is considered normal. **Workaround**: If simultaneous Web page refresh commands are issued, then a **`show ipv6 tcp connection`** command displays the active TCP connections for the Web session.
Q01981920	**EAP, Fail Open VLAN**: An EAP or Non-EAP client could be assigned to the Fail Open VLAN in normal operation if the VLAN name or ID returned from the RADIUS server matches the VLAN assigned for the Fail Open VLAN. **Workaround**: Ensure that the Fail Open VLAN name or ID that you use does not match one of the returned RADIUS VLANs.
Q01986757	**NSNA**: If you add a new classifier to the NSNA yellow QoS set (exceeding the resources), the yellow filters may not be applied.

Reference number	Description
Q01991335-01	**MLT/DMLT**: It may be possible to change the VLAN membership of administratively disabled MLT/DMLT ports. If you change the VLAN assignment on administratively disabled MLT/DMLT ports, the system prevents them from being added back into the MLT/DMLT group because the VLAN assignments of the links within the groups are inconsistent. If you want to change the VLAN membership for a MLT/DMLT group, you must: • Disable all ports which are members of that group or disable the MLT/DMLT. • Make the necessary VLAN changes to all group members. • Re-enable the port or MLT/DMLT.
Q01999027, Q01999072	**RSTP**: When operating as an RSTP root bridge and the base unit in a stack is reset, or the stack transitions to standalone mode, the system may not always generate the SNMP trap message indicating a change in RSTP root. **Workaround**: A local log message for nnRstNewRoot is always generated.
Q02005157	**Management VLAN**: When operating in Layer 3 mode, using the Management VLAN for normal routing may result in lost connectivity to the Management IP address. **Workaround**: If connectivity problems occur to the management IP address, clear the ARP cache.
Q02011548	**NSNA**: After units are rebooted in an operational stack, some static MAC authentication clients may be incorrectly displayed as a 0.0.0.0 IP address instead of the correct IP address. This is a display issue only and does not affect functionality. **Workaround**: Use the SNAS to show the correct IP associations.
Q02013766	**EAP, RADIUS Last Assigned VLAN**: When a port is configured for RADIUS Last Assigned VLAN, if the last RADIUS authentication for that port does not contain QoS priority, then the port priority will be either the one manually configured for that port or the one received for the previous authenticated client.
Q02013848	**Port Mirroring**: The port mirroring modes asrc and adst cannot mirror packets generated by the CPU such as: LACPDUs, LLDPDUs, BPDUs, and SONMP. **Workaround**: CPU-generated packets can be mirrored with port-mirroring mode XTX.
Q02016200	**CPU utilization**: The CPU utilization reported for the 'last 10 minute interval' may be higher than actual if the CPU was loaded at 100% for the first 5 minutes then returns to an idle state for the next 5 minutes. All other values are correctly calculated. The value will be properly displayed after 30 minutes if the CPU load returns to normal activity levels.

Reference number	Description
Q02027769	**EAP**: When EAP performs authentication through TTLS, the first authentication between the supplicant and the switch may fail but subsequent authentications will succeed. **Workaround**: If authentication fails when using EAP-TTLS, do one of the following: • Wait 30 seconds for the client to re-authenticate successfully. • Use an alternative EAP authentication mechanism for the client.
Q02059865	**EDM, startup**: With some browsers, especially if you have multiple tabs and/or many windows open concurrently, you may experience high CPU utilization on your browser platform for greater than 60 seconds while EDM is starting up and displaying the switch physical view. **Workaround**: When you start EDM, if you experience high CPU utilization on your browser platform for more than 60 seconds, reduce the number of open windows or tabs in your browser. **Note**: Faster load times of 15-30 seconds are typically seen when you use Firefox 3.5 as your browser, depending on your system setup.
Q02059869	**EDM, Energy Saver**: EDM does not display the PoE Savings and PoE Priority in the energy saver ports tab. **Workaround**: Use the CLI command **`show energy-saver interface`** to display information about energy saver and PoE savings port status.
Q02065289-01	**EDM, TACACS+**: You cannot use EDM to enable TACACS+ because, when you enable TACACS+, the system disables Web access to the switch. If you used EDM to enable TACACS+ you would lose EDM access for any subsequent operations. **Workaround**: Use only the CLI to disable or enable TACACS+.
Q02065308-01	**EDM, IGMP**: When the same IGMP group is present in multiple VLANs, EDM does not correctly display all IGMP groups. **Workaround**: Use the CLI command **`show igmp`** to display all IGMP groups.
Q02069415	**Energy Saver**: The switch does not display energy saving information for the ERS 4526FX model because the main ports on the 4526FX are 100FX and cannot be reduced in switching capacity.
Q02072781	**Energy Saver, SNTP**: If you enable energy saver and you define a local schedule, there is no guard-rail to prevent you from disabling SNTP. Be aware that if SNTP is disabled, and if you reboot the switch or stack, then energy saver cannot function after the reboot until you enable SNTP. **Workaround**: Re-enable SNTP.
Q02081441-01	**VLACP**: When you disable VLACP globally or on a per interface basis, the system forwards the following incorrect message to the syslog server: *Port X reenabled by VLACP*.
Q02086637	**Port Mirroring**: If you use port 1 as a mirror port in XrxYtx or XrxYtxOrYrxXtx port mirroring modes, then broadcast or multicast traffic mirrored to the port is doubled on the monitor port. **Workaround**: Use another port on the switch as the mirrored port.

Reference number	Description
Q02088900	**QoS, information**: The system performs bandwidth allocation for queues according to Strict Priority and WRR algorithm. When you configure shapers on queues with minimum rate, the system first queues traffic to ensure the minimum rate is achieved for all queues. The system then allocates the remaining egress bandwidth according to Strict Priority, WRR and shape maximum rate configured for each queue. In case the sum of shape minimum rates configured (queue shapers) exceeds the line rate, the minimum shape rate is assured for queue 1 and then the remaining bandwidth is distributed amongst the rest of the queues. The system uses the WRR algorithm to best assure that the minimum rates for the rest of the queues are achieved. **Note**: If you have ERS4500 and ERS5600, in the same scenario the ERS 5600 operates differently, depending on the active queue set, and may use strict priority, WRR and RR algorithms.
Q02089765	**EAP Packet-Mode:** The default EAP packet mode on the switch is set to multicast. When the EAP packet mode is set to multicast, the switch continues to send EAP requests at defined intervals (default is 30 seconds) until the maximum number of EAP clients configured for the port is reached. This behaviour is required for some EAP devices that need to receive a Request Identity in order to start EAP. **Workaround:** If your EAP client devices do not require Request Identity in order to start EAP, you can set the EAP packet mode to Unicast.
Q02092598	**NSNA, DHCP Snooping, Dynamic ARP Inspection (DAI)**: If NSNA trusted port is set in combination with DHCP Snooping and Dynamic ARP Inspection (DAI), then, occasionally, after a switch reboot, some PCs connected to the switch may be unable to correctly re-acquire an IP address and will appear in the **`show nsna client`** command with an IP address of 0.0.0.0. **Workaround**: Disconnect and reconnect the PC, or if using Windows, issue an ipconfig /release and then ipconfig /renew command and the PC will correctly reacquire an IP address.
Q02096780	**EAP, 384 ports, Intruder MAC**: If you enable or activate EAP on 384 ports simultaneously, while all clients are sending large volumes of traffic, then some intruder (unauthorized) MAC addresses may not appear in the MAC address table. This applies only to intruder addresses which are blocked and not allowed to forward traffic and it is not a security or connectivity problem.
Q02098348	**Telnet, ASCII Config**: If you configure a very short telnet timeout value and then you connect to the switch using telnet to execute the CLI command **`copy config`**, to save the ASCII configuration to USB or TFTP, the configuration file may be incomplete for large or complex stack configurations. **Workaround**: It is recommended to set the minimum telnet timeout value to 5 minutes.
Q02099762-01	**show running-config**: When you execute the **`show running-config`** or **`show running-config module`** commands the system may take a longer time than expected to display the output. In systems with very large and complex configurations of 8 units in a stack it can take up to 4 minutes to complete the display of the command. This is considered normal behavior.

Reference number	Description
Q02102857	**SNMP**: With the introduction of the unified SNMP Notification Control mechanism the following commands are now obsolete and they are hidden: • **snmp-server authentication-trap enable** • **snmp-server authentication-trap disable** • **no snmp-server authentication-trap** • **default snmp-server authentication-trap** **Workaround**: Use the new commands as follows: To enable the generation of authentication failure traps (enabled by default) use: **snmp-server notification-control authenticationFailure** To disable the generation of authentication failure traps use: **no snmp-server notification-control authenticationFailure** To disable the state of SNMP traps use: **show snmp-server notification-control**
Q02103062	**ACG, SNMPv3, Secure Image**: When you run the secure software image, an ASCII configuration file generated by the switch has the SNMPv3 user commands 'snmp-server user' commented out. This is expected behavor as the associated passwords cannot be output in clear text in the ASCII generated file due to security requirements. As a result when the configuration is loaded onto a switch with default configuration, the SNMPv3 users are not recreated. **Workaround**: Manually re-create the SNMPv3 users after loading the ASCII configuration.
Q02105435	**Energy Saver, PoE Savings Mode, IP Phone, STP**: For some firmware revisions on certain IP Phones, when an IP Phone is plugged in but not powered, the switch port may receive packets reflected from the IP Phone . **Workaround**: If you enable PoE Savings Mode in combination with energy saver, and you have IP Phones which exhibit this fault, to prevent the formation of excessive broadcast packets or network loops you should ensure that Spanning Tree Protocol or Rapid Spanning Tree Protocol is configured for these ports.
Q02107731	**OSPF, Scaling**: When you run OSPF with a high number of adjacencies (for example 64 OSPF neighbors) it is recommended that the total number of Link State Advertisement (LSA) entries in the OSPF Link State Database (LSDB) should not exceed 10,000.
Q02111347-01	**EDM, Firefox**: When you view very large tables in EDM, if you click on the **hiding non-editable** button in the Multiport Port Configuration section, Firefox may return an unresponsive script warning.

Reference number	Description
Q02115939, Q02115939-01	**BX SFPs**: When you connect two BX SFPs (Part Code AA1419069-E6 and AA1419070-E6) between Gigabit ERS4500 switches, in some cases the link may not be established. This has been found to occur only if the vendor of the BX SFP is Luminet (as identified by the vendor serial number starting with LUMNT) and the SFP is revision A. **Workaround**: To correctly establish the link, replace one of the BX SFPs with a later revision SFP.
Q02111920-01	**SNMP Traps**: When you use the CLI commands **`show snmp-server host`** and **`show snmp-server notify-filter`** there is no direct correlation between which filter is applied to which host. **Workaround**: To display the SNMP host-filter association in the appropriate order, issue the CLI command **`show running-config`**.
Q02111922-01	**SNMP Traps, Temporary Base Unit**: If you create new SNMP Trap notification filters while the stack is operating in Temporary Base Unit (TBU) mode (that is the Base Unit has failed) then the new filters are not saved and are lost upon stack reboot. **Workaround**: If the stack is operating in TBU mode, reset the stack and then create the required SNMP Trap notification filters.
Q02117918	**EDM, Multiport configuration**: When you use EDM to apply an operation to all ports, the system may generate a misleading error message if the change could not be applied to multiple ports. EDM provides only an error message indicating the first port for which it was unable to apply the configuration change.
Q02117928	**EDM, Internet Explorer**: When you use some versions of Internet Explorer to display a very wide table, the drop down boxes do not scroll correctly. **Workaround**: For a table with many columns in EDM, click on the cell then use the scrollbar to scroll the cell to the end.
Q02118229	**MIB, EAP, MHMA MultiVLAN**: If you disable the MHMA MultiVLAN option, the SNMP MIB object (bseeMultiHostStatusVid) that reports the VLAN associated with a client reports a value of either 4095 or 4096. The returned VLAN ID values of 4095 or 4096 indicates that the VLAN was not assigned to the client. This is normal, expected behavior in this scenario. Use the CLI command **`show eapol multihost status`** to confirm the VLAN ID assocaition.
Q02119017	**EDM**: To copy and paste text between text boxes in EDM you can use the keyboard shortcuts **Ctrl+C** to copy text and **Ctrl+V** to paste text.

Reference number	Description
Q02121817, Q02121820, Q02121827, Q02121828	**Energy Saver**: When energy saver is activated or deactivated, the link on a port transitions briefly. This brief transition can cause some devices to re-acquire connectivity, but, in most situations, end users do not notice the port transition. On the switch, the system clears the MAC address for the port and then re-learns it. If EAP or NEAP is enabled, EAP authentication restarts. **Workaround**: Avaya recommends that you disable energy saver on copper uplink ports because activating or deactivating energy saver on copper ports triggers a link down followed rapidly by a link up event. **Alternative**: Use fiber ports for uplinks because energy saver does not change fiber port status when energy saver is activated or deactivated..
Q02121888, Q02121890	**Energy Saver, Copper ports, RIP, OSPF**: When you activate or deactivate energy saver, the link on a port briefly transitions. This transition may cause OSPF neighbour connectivity to bounce or cause relearning of RIP routes. **Workaround**: Avaya recommends that you disable energy saver on copper uplink ports which have OSPF adjacencies or RIP routes active. Copper ports, OSPF adjacencies—If you use copper ports for which energy saver is enabled and OSPF adjacencies are exchanged over these links, you can set the “ip ospf advertise-when-down enable” parameter so that adjacencies are not bounced when the link transitions. Copper ports, RIP routes—If you use copper ports for which energy saver is enabled and RIP routes are exchanged over these links, you can set the “ip rip advertise-when-down enable” parameter so that RIP routes are not bounced when the link transitions. **Alternative**: If you use fiber ports for OSPF adjacencies or RIP route connections, energy saver will not cause a link transition.
Q02123667	**NEAP, Scaling**: The maximum recommended number of NEAP clients per switch/stack is 384. If more than 384 NEAP clients are authenticated, then, under certain failure conditions, some NEAP clients may not be properly authenticated. **Workaround**: Use the CLI commands **`shutdown`** then **`no shutdown`** to disable and enable a port to force NEAP clients to re-authenticate on selected ports.
Q02125107	**EAP, MHMA MultiVLAN, Guest VLAN**: Switch ports are not moved into the Guest VLAN (GVLAN) if you enable the GVLAN option after EAP clients have authenticated on the port. **Workaround**: It is recommended that you enable Guest VLAN (global or per port option) before EAP clients are authenticated. **Alternative**: you can globally disable EAP, configure GVLAN, then re-enable EAP globally.
Q02125156	**ADAC, QoS display**: When you enable ADAC, the CLI command **`show qos diag`** no longer displays ADAC as using a QoS precedence.

Reference number	Description
Q02126107	**ADAC, EAP, Guest VLAN**: If you configure both Guest VLAN (GVLAN) and ADAC untagged frames advanced mode on a port, then when a device is discovered by ADAC the port is moved from the GVLAN into the ADAC Voice VLAN. This results in lost connectivity for the GVLAN. If you disable ADAC globally, the client is removed from the ADAC Voice VLAN and placed in the initial port based VLAN with the PVID set to 1 (the default VLAN). **Workaround**: Avaya recommends you do not use ADAC untagged frames advanced mode in combination with EAP MHMA and Guest VLAN.
Q02126129-01	**EAP, Guest VLAN**: If you disable Guest VLAN (GVLAN) globally or per interface while authenticated clients are present, the system does not remove the port from the GVLAN. **Workaround**: It is recommended that you shut down the switch port before you disable GVLAN, either globally or per interface. Shutting down the port clears the authenticated clients so that the ports are correctly removed from the GVLAN.
Q02127043	**ADAC, EAP, Guest VLAN**: If you configure both Guest VLAN (GVLAN) and ADAC on a port and the system receives an EAP logoff message, the port is not moved correctly back into the GVLAN. **Note**: Some IP Phones may send a proxy EAP logoff message for the connected device if it is unplugged from the IP Phone. **Workaround**: If you configure GVLAN and ADAC and ports receive EAP logoff messages, then you should set the IP Phone to use DHCP Signature authentication (NEAP IP phone).
Q02127278	**ADAC, LLDP, EAP**: If an IP Phone has already been detected by ADAC and LLDP and then you subsequently configure NEAP IP Phone capability, the port does not authenticate the IP Phone via its DHCP signature (that is, NEAP IP Phone capability). **Workaround**: You can force the port to redetect and authenticate the IP Phone by one of the following: • Disable then enable ADAC globally. • Unplug and plug in the IP Phone into the port. • Transition the port connected to the IP Phone by issuing the CLI commands **`shutdown`** then **`no shutdown.`**
Q02128601	**EAP, NEAP IP Phone**: The system does not display the VLAN ID and priority of the NEAP IP Phone (DHCP signature authenticated client) when you use the CLI command **`show eapol multihost status`**. If traffic is untagged: the system forwards the IP Phone traffic correctly according to port PVID. If traffic uses the specified VLAN, if the frames are tagged: the system forwards the IP Phone traffic correctly according to port PVID. If traffic is untagged and MHMA MultiVLAN is enabled: the system forwards the IP Phone traffic to the first EAP VoIP VLAN. If traffic is tagged and MHMA MultiVLAN is enabled: the system forwards the IP Phone traffic to the specified VLAN.

Reference number	Description
Q02128609	**ADAC, EAP, MHMA MultiVLAN**: When you enable the MHMA MultiVLAN option and then execute the CLI command **`show eapol multihost non-eap-mac status`**, the system displays the VLAN ID and priority as N/A. However, client traffic is correctly forwarded according to assigned VLAN, untagged traffic is forwarded according to the port PVID or tagged traffic is forwarded in the tagged VLAN.
Q02130384	**SNMP Traps, Upgrade**: All SNMP trap notifications are enabled after you upgrade to R5.4.0 software, regardless of whether you disabled them prior to the upgrade. **Workaround**: Use the new SNMP notification control mechanism to select which SNMP traps ane enabled or disabled. For more information, see "Affects of upgrade on trap notifications" (page 30).
Q02132847	**EAP, QoS Traffic Profiles**: If you configure both QoS Traffic Profiles and EAP, in some circumstances after a switch reboot the QoS Traffic Profile may be set to a higher precedence than before the switch reboot. EAP packets could then be blocked by rules defined in the traffic profile. **Workaround**: To prevent EAP packet blocking in this situation, you can define a QoS policy instead of using a Traffic Profile. The same filtering capabilities are supported, but user defined policies use the same QoS precedence correctly before and after a reset.
Q02134140	**Port Mirroring**: If you set port mirroring to AsrcBdstOrBsrcAdst mode, the switch mirrors Layer 2 broadcast traffic with a MAC source address that equals Asrc to the monitor port.
Q02140511	**RADIUS, RADIUS reachability**: If you use the "radius reachability use-radius", the switch sends reachability requests with the username 'avaya' and a blank password. Because the Avaya ignition server does not allow accounts to be created with a blank password, the ignition server will log intrusion events when the dummy requests are regularly sent from the switch. **Workaround**: Use ICMP reachability for ignition server reachability.
Q02141284	**EDM**: If the browser device has multiple active IP addresses, EDM will only support multiple sessions from the same source IP address on the device. If different IP source addresses are used, the second or subsequent browsers will display the error message *503 Server Busy*. **Workaround**: If you require multiple EDM sessions from the same client device which has multiple IP interfaces, ensure the Web browser on the device uses the same source IP address.

Reference number	Description
Q02142035	**show runnning config, Rate Limiting**: If you configure Rate Limiting on the switch (that is you change rate limiting from the default settings), the ASCII configuration file generated by the CLI commands **`show running-config`** or **`copy running-config`** does not contain an "exit" line after the Rate Limiting feature. If you reload that ASCII configuration onto a switch, the missing “exit” command causes failure of subsequent commands in the ASCII configuration file. **Workaround**: You can add the missing "exit" line manually into the ASCII Config file. **Alternative**: If you use the verbose qualifier, the system generates the ASCII configuration file with the exit command present.
Q02142993	**TDR, ERS 4526FX**: On the ERS 4526FX model, you can issue the CLI commands **`tdr test`** and **`show tdr`** for the 100FX ports. The 100 FX ports on the ERS 4526FX model do not support TDR functionality, so the TDR tests are not actually performed and the information returned by the **`show tdr`** command is incorrect.
Q02143519	**NEAP, RADIUS Accounting**: When you enable RADIUS accounting, the system does not generate accounting messages for non-EAP (NEAP) clients that connect to the switch. Accounting messages are correctly generated for EAP clients and for users who log into the switch when RADIUS authentication is enabled.
Q02144052	**ADAC, MLT, ACG**: If you configure ADAC uplink or call server ports on a switch to be a member of an MLT/DMLT or LAG, then the ASCII configuration file generated by the switch contains an error in the "adac uplink-port" or "adac call-server-port" definitions. If you then reload this ASCII configuration file, processing of the ASCII file stops at these erroneous lines. **Workaround**: You can continue to save and restore the binary configuration file without any issues. **Alternative**: If you create an ASCII configuration file containing the error, you can edit the incorrect configuration lines for ADAC and the file will then load correctly onto the switch.

IPv6 limitations

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

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.

Reference number	Description
3	No DHCP/BOOTP, Stateless Address Autoconfiguration or IPv6 loopback address is supported for the management address.
4	The only IPv4 to IPv6 transition mechanism supported is dual-stack (no tunnelling).

Nortel Ethernet Routing Switch 4500 Series

Release Notes — Release 5.4

Release: 5.4
Publication: NN47205-400
Document revision: 06.01
Document release date: 19 May 2010

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

www.nortel.com