



Ethernet Routing Switch 5500 Series

Release Notes — Software Release 5.1

Document status: Standard
Document version: 03.02
Document date: 22 October 2007

Copyright © 2007, Nortel Networks
All Rights Reserved.

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

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

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

Restricted rights legend

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

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

Statement of conditions

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

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

Nortel 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

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

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

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

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

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

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

Contents

Introduction	7
File names for this release	7
New software features in Release 5.1	8
2K Route Scaling	9
BX SFP support	9
Demo license support	10
DHCP for stack or switch address	10
DHCP snooping - ARP inspection MIB - ACG support	10
EAP and 802.1x enhancements	11
IEEE 802.1ab and ADAC linkage	11
IP Source Guard	11
L2 MAC address in IPFIX	12
L3 commands	12
MAC flush	13
Multinetting on VLAN	14
NSNA enhancements	14
OSPF enhancements	14
SMLT enhancements	15
SSCP support	15
Stack and 10 Gb port congestion counter	15
Stack loopback test	16
Stack port counters	17
Stack monitor	17
Time zone support	17
UBP and EPM support	17
JDM and SNMP error code enhancements	18
Supported software and hardware capabilities	18
Layer 3 scaling limitations	19
Additional information for the feature software license file	19
Upgrading diagnostic software	20
Issues resolved in Release 5.1	20
Known issues and temporary limitations in Release 5.1	23
Known limitations	30

Filter resource consumption	32
Masks and filters inventory check	33
QoS Interface Security Application	35
Related documentation	36
How to get help	36
Getting help from the Nortel web site	36
Getting help over the phone from a Nortel Solutions Center	37
Getting help from a specialist using an Express Routing Code	37
Getting help through a Nortel distributor or reseller	37

Introduction

The following release notes provide the most recent information on the Nortel* Ethernet Routing Switch 5500 Series, Software Release 5.1. These release notes supplement the information that the documentation suite provides.

The Nortel Ethernet Routing Switch 5500 Series includes the following switches:

- Nortel Ethernet Routing Switch 5510-24T
- Nortel Ethernet Routing Switch 5510-48T
- Nortel Ethernet Routing Switch 5520-24T-PWR
- Nortel Ethernet Routing Switch 5520-48T-PWR
- Nortel Ethernet Routing Switch 5530-24TFD

For a complete list of documentation in the 5500 Series suite, see "[Related documentation](#)" (page 36).

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

File names for this release

"[Software Release 5.1 components](#)" (page 7) describes the Ethernet Routing Switch 5500 Series, Software Release 5.1 software files. File sizes are approximate.

Software Release 5.1 components

Module or file type	Description	File Name	File Size (bytes)
Standard runtime image software version 5.1	Standard non SSH image for the Ethernet Routing Switch 5500 Series	55x0_50014.img	5 968 388

Module or file type	Description	File Name	File Size (bytes)
Secure runtime image software version 5.1	Standard SSH image for the Ethernet Routing Switch 5500 Series	5510_50015s.img	6 203 368
Boot/diagnostic software version 5.0.0.04	Switch diagnostic software	55x0_50004_diags.bin	812 036
Java Device Manager software version for Windows (6.0.7.0)	Device Manager software image for Windows NT, Windows XP, Windows 2003, Windows 2000	jdm_6070.exe	168 000 623
Java Device Manager software version for Solaris UNIX (6.0.7.0)	Device Manager software image for Solaris	jdm_6070_solaris_sparc.sh	178 413 011
Java Device Manager software version for Linux (6.0.1.0)	Device Manager software image for Linux	jdm_6070_linux.sh	173 563 347
Readme file	Device Manager readme file	readme_v6.0.7.0.txt	
Software Release 5.1 Management Information Base (MIB) definition files	MIB definition files	Ethernet_Routing_Switch_55xx_MIBs_5.1.0.zip	951 917

New software features in Release 5.1

Ethernet Routing Switch 5500 Series, Software Release 5.1 provides the following new features or feature improvements:

- ["2K Route Scaling" \(page 9\)](#)
- ["BX SFP support" \(page 9\)](#)
- ["Demo license support" \(page 10\)](#)
- ["DHCP for stack or switch address" \(page 10\)](#)
- ["DHCP snooping - ARP inspection MIB - ACG support" \(page 10\)](#)
- ["EAP and 802.1x enhancements" \(page 11\)](#)
- ["IEEE 802.1ab and ADAC linkage" \(page 11\)](#)
- ["IP Source Guard" \(page 11\)](#)
- ["L2 MAC address in IPFIX" \(page 12\)](#)
- ["L3 commands" \(page 12\)](#)
- ["MAC flush" \(page 13\)](#)

- "Multinetting on VLAN" (page 14)
- "NSNA enhancements" (page 14)
- "OSPF enhancements" (page 14)
- "SMLT enhancements" (page 15)
- "SSCP support" (page 15)
- "Stack and 10 Gb port congestion counter" (page 15)
- "Stack loopback test" (page 16)
- "Stack port counters" (page 17)
- "Stack monitor" (page 17)
- "Time zone support" (page 17)
- "UBP and EPM support" (page 17)
- "JDM and SNMP error code enhancements" (page 18)

2K Route Scaling

Route support is increased on the 5520 and 5530 to 2K routes (from 512). Nortel supports up to 2000 routes (local plus static plus dynamically learned), on the 5520 and 5530.

On the 5520 and 5530, you can configure 256 local IP interfaces and 512 static routes through the Nortel Networks Command Line Interface (NNCLI), ASCII Configuration Generator (ACG), or Java Device Manager (Device Manager). The remainder of the 2000 routes are learned by OSPF and RIP dynamic routing.

BX SFP support

Many customers have high density gigabit requirements, but lack the fiber density to deploy. BX SFPs helps alleviate this issue by allowing a single strand of fiber to facilitate communication.

Nortel introduces support for 1000BaseBX10 modules with release 5.1. The modules are single fiber, bidirectional SFP transceivers. Two types of modules are available:

- 1310nm (BX10-U) transceiver
- 1490nm (BX10-D) transceiver

The 1000BaseBX10-D device is always connected to a 1000BaseBX10-U device with a single strand of standard single-mode fiber. The operating transmission range is up to 10 km. The fiber uses a GBIC LC connector on each end.

If the 1000BaseBX10-U is not connected to the 1000BaseBX10-D device, the signals are not received properly and the Link LED does not illuminate.

You can configure BX SFP Support through the NNCLI, ACG, or Device Manager.

Demo license support

In Release 5.1, Nortel offers a 30-day trial version of the feature license that is monitored by the software.

The customer installs the license, and the software tracks the 30-day trial period. After the 30 days expire, the software sends a message or trap to the administrator indicating the expiry. The license then becomes inactive and disables all advanced features activated by the demo license, with the exception of SMLT. The next reboot disables the SMLT feature.

You can configure Demo License Support through the NNCLI or ACG.

DHCP for stack or switch address

Release 5.1 introduces DHCP capability, allowing each individual TCP/IP host in a network to obtain an IP address, netmask, and gateway IP address.

The DHCP client will be available on equipment that is connected to a DHCP server or a DHCP relay. The server must be available in the management VLAN and must have an IP address pool available for leasing.

The port to which you connect the DHCP server must reside in the management VLAN. In a stacked configuration, the DHCP server can be connected to any unit, but the port must reside in the management VLAN.

DHCP is provided as an option in the 5.1 software—existing switch defaults are preserved. The 5.1 software has DHCP disabled—the user must select this option to activate it.

Configurable using NNCLI, ACG, and Device Manager.

DHCP snooping - ARP inspection MIB - ACG support

MIB and ACG support for DHCP snooping and ARP inspection is introduced in Release 5.1 software.

Provision of the MIB support enables users to configure and maintain these two features from remote configuration tools, such as Device Manager. ACG support means the user has an auto-generated ASCII configuration script that reflects the current DHCP snooping and ARP inspection configuration state.

In Release 5.1, the NNCLI has been updated to use the DHCP snooping and ARP inspection MIB support. There are no modifications to either the DHCP Snooping or the ARP inspection NNCLI syntax.

EAP and 802.1x enhancements

Enhancements to the functionality/support of non EAP clients on EAP-enabled ports include:

- Support in NNCLI to configure Nortel IP phones as a non-EAP “type” on EAP-enabled ports
- Allow a RADIUS-assigned VLAN in Multiple Host (MAC) with Multiple Authentication (MHMA) mode
- Unicast mode support for EAP request (EapReqId) discovery packets

The MHMA “mode” is a per port option for EAP-enabled ports. A finite number of users (that is, devices), each with a different MAC address, is allowed on a port. Each of the users must successfully complete EAP authentication for the port to allow traffic with the corresponding MAC addresses. Traffic from the authorized hosts only is allowed on that port.

The software default is to have Radius VLAN Assignment disabled for ports in MHMA mode. Commands now exist for the user to apply a RADIUS-assigned VLAN in MHMA mode.

IEEE 802.1ab and ADAC linkage

Nortel introduced the 802.1ab and Auto Detection Auto Configuration (ADAC) features to Release 5.0 to address converged applications.

In Release 5.1, the functionality of 802.1ab and ADAC is combined: ADAC uses 802.1ab/LLDP as the detection mechanism to determine the identity of the attached device (that is, a Nortel IP phone that supports 802.1ab Media Endpoint Devices type, length, and value descriptions [MED TLV]). The Auto Configuration functionality of ADAC applies the configuration to the port.

Configurable using NNCLI, ACG, and Device Manager.

IP Source Guard

Release 5.1 introduces two new features that use a binding table to enforce specified levels of security and eliminate certain spoofing scenarios:

- DHCP snooping
- ARP inspection

IP Source Guard is a Layer 2 port-based security feature that works closely with information in the DHCP Snooping Binding Table. It prevents IP spoofing by allowing only IP addresses obtained through DHCP snooping.

When a connecting client receives a valid IP from the DHCP server, a filter is installed on the port to allow only traffic from the assigned IP address. When the user enables IP Source Guard on an untrusted port that has DHCP snooping enabled, an IP filter entry is created/deleted for that port automatically based on the IP information stored in the corresponding DHCP-Snooping Binding Table entry. A port IP filter is changed if the corresponding Snooping Binding Table entry is created/deleted.

This feature is enabled or disabled for each port. Nortel recommends that you do not enable IP Source Guard on trunk ports.

A maximum of 10 IP addresses are allowed on an IP Source Guard-enabled port. Once that limit is reached, no more filters are set up on the port, and traffic from IP addresses other than those 10 is dropped.

Configurable using NNCLI, ACG, and Device Manager.

L2 MAC address in IPFIX

IP Flow Information eXport (IPFIX) IP flows are defined by an IP Source Address (SA), an IP Destination Address (DA), the IP Protocol Type, the Type of Service (ToS), and the ingress port. For TCP or UDP protocols, an IP flow is defined by two additional parameters: source port and destination port.

Release 5.1 increases the functionality of IPFIX by providing L2 MAC address information as part of the flow information. The MAC is provided for both the Source and Destination devices.

Information is displayed in the current display formats (NNCLI and Web interfaces) – there are additional fields to accommodate the MAC address information. Both local viewing of information and export to a third party collector is supported.

L3 commands

Nortel is implementing new commands and enhancing other commands for L3 configuration (that is, the dynamic routing protocols and their command set). The following are the NNCLI commands and enhancements.

Commands for the following are added:

- Clear OSPF statistics counters (in a stack, can only be executed on the base unit)

```
clear ip ospf counters [<vid>]
```

- Clear UDP forwarding statistics counters (in a stack, can only be executed on the base unit)

```
clear ip forward-protocol udp counters [<vid>]
```

- Traceroute (in a stack, can only be executed on the base unit)

```
traceroute <hostname|ipaddr> -m <1-255>
traceroute <hostname|ipaddr> -p <0-65535>
traceroute <hostname|ipaddr> -q <1-255>
traceroute <hostname|ipaddr> -w <1-255>
traceroute <hostname|ipaddr> -v
traceroute <hostname|ipaddr> <1-1464>
```

Commands for the following are enhanced:

- Display software IP routing table

```
show ip route summary
```

- Display software ARP table

```
show ip arp static
```

- Ping

```
ping <hostname|ipaddr> -t <1-120>
ping <hostname|ipaddr> count <1-9999>
ping <hostname|ipaddr> datasize <64-4096>
ping <hostname|ipaddr> interval <1-60>
ping <hostname|ipaddr> timeout <1-120>
ping <hostname|ipaddr> debug
ping <hostname|ipaddr> continuous
```

These commands are not added to the ACG.

MAC flush

Previous versions of software for the 5500 Series switches provided no direct method for flushing addresses from the MAC Address Table. Release 5.1 introduces a MAC flush command to correct that limitation.

MAC Flush allows users to flush the following from the MAC Address Table:

- a single MAC Address
- all addresses in the MAC Address Table
- a port or a list of ports
- a trunk
- a VLAN

MAC Flush deletes only dynamically learned addresses. The addresses marked with AGELOCK, SECRET, or STATIC, and inserted in the MAC Address Table by applications such as MAC Security, or Port Mirroring, are not flushed out.

Configurable using NNCLI, Web, and Device Manager.

Multinetting on VLAN

Previous to Release 5.1, only one IP interface (primary) could be configured for each VLAN (that is, all hosts connected to a specific VLAN would all be in the same IP subnet). Multinetting allows multiple IP interfaces (that is, multiple IP subnets) to be assigned to a single VLAN. Additional interfaces that the user configures for a VLAN are referred to as secondary interfaces. Nortel supports one primary and up to eight secondary interfaces for each VLAN.

Configurable using NNCLI, ACG, and Device Manager

NSNA enhancements

The Nortel Secure Network Access (NSNA) feature provides controlled network access for devices on a switch NSNA port. (Added in software releases 5.0.3 and 5.0.4., and documented in Release 5.1.)

OSPF enhancements

Release 5.1 brings enhancements to OSPF:

- Host route – Allows a router to advertise to its neighbors all hosts that are directly attached to that router's interfaces. Up to 32 host routes can be configured.
- Virtual links – The OSPF network can be partitioned into multiple areas. However, a backbone area must exist and be contiguous, and every non-backbone area must be connected to the backbone area using either a physical or a logical link. In a network where a physical connection between the non-backbone area and backbone area is impossible, use of a virtual link provides the logical connection through another non-backbone area, called the transit area. Virtual links can be created manually or automatically. The 5500 Series switch supports up to 16 virtual links.
- When 5500 Series switches are stacked, and a unit leaves the stack and becomes standalone, the router ID is automatically changed to its default value if IP blocking is turned off and OSPF is globally enabled. This prevents duplication of a router ID in the OSPF routing domain. The new router ID value is temporary, that is, it is not saved to NVRAM. Therefore, upon reset, the old router ID is restored.

Configurable using NNCLI, ACG, and Device Manager.

SMLT enhancements

Split MultiLink Trunking (SMLT) works in standalone and stacked environments in Release 5.1. Nortel supports the following SMLT configurations in Release 5.1:

- Triangle SMLT – both standalone and stack
- Square SMLT – standalone only

Stack SMLT allows a full stack of eight switches to have interswitch trunking (IST) connections to another stack of switches, which provides greater redundancy and bandwidth aggregation.

Square configuration allows additional, more complex and resilient network designs. Nortel supports two square configurations:

- standalone 5500 Series IST peers connected to 8600 IST peers
- standalone 5500 Series IST peers connected to a second set of standalone 5500 Series IST peers

In a square configuration, Nortel supports standalone configuration only (standalone peer ISTs). Connection from the “core” of a square configuration requires static routes pointing to the virtual router (VR) IP address.

SSCP support

Switch-SNAS Communication Protocol (SSCP) is the communication protocol used between the Nortel Secure Network Access Switch 4050 and NSNA network access switches (such as the Ethernet Routing Switch 5500). The protocol allows the Nortel SNAS 4050 to make configuration changes on a switch. The Ethernet Routing Switch 5500 supports SSCP communication.

Beginning with Release 1.5 of the Nortel SNAS 4050 software, the Nortel SNAS 4050 no longer requires the network access device to support SSCP.

SSCP is described in the *Nortel SNAS 4050 User Guide*. For Ethernet Routing Switch 5500 Series Release 5.1, see *Ethernet Routing Switch 5500 Series Configuration — Security (NN47200-501)* for commands related to NSNA where SSCP communication is configured or established.

Stack and 10 Gb port congestion counter

Release 5.1 delivers additional counters that help to diagnose traffic congestion on the 10 Gb ports due to oversubscription.

10 Gb port congestion counter: A counter exists for each 10 Gb port on the Ethernet Routing Switch 5530. Each counter details the number of packets dropped due to “buffer full” conditions.

Command:

```
show port-statistics port <portlist>
```

Stack congestion counters: Coupled with the counter for each 10 Gb port, there is a counter for each stack up and stack down port. This counter displays (on a per unit basis) the number of packets dropped on stack up or stack down ports due to “buffer full” conditions.

Commands:

```
show stack port-statistics {down-stack|up-stack} [<unit  
1-8>]
```

```
clear stack port-statistics {down-stack|up-stack}  
[<unit 1-8>]
```

Configurable and viewable using the NNCLI and Device Manager.

Stack loopback test

The stack loopback test allows the customer to quickly test the switch stack ports and the stack cables.

If you experience stack problems, the stack loopback test helps you determine if the root cause is a bad stack cable or a damaged stack port.

There are two types of loopback tests: internal loopback test and external loopback test. The purpose of the internal loopback test is to verify that the stack ports are functional. The purpose of the external loopback test is to verify that the stack cable is functional.

For accurate results, the internal loopback test must be run before the external loopback test.

Run these tests on a standalone switch. No traffic should run through the switch while it is under test.

Commands:

```
stack loopback-test internal
```

```
stack loopback-test external
```

Configurable using NNCLI.

Stack port counters

Counters exist for the uplink and access ports of the 5500 Series switch. Release 5.1 extends similar functionality to the stack ports.

Rather than displaying a separate counter for each internal 10 Gb link on the stack, the stack port counter aggregates or adds the internal stack up and stack down counters for each stack port and displays the result to the user.

Command example: `show stack port-statistics down-stack unit 1`

The purpose of displaying the stack port counters is to verify that the stack ports are functional.

Configurable and viewable using the NNCLI.

Stack monitor

When enabled, the stack monitor uses a set of control values to set the expected stack size and to control the frequency of trap sending. The stack monitor detects and informs the user about problems with the stack units. Generally, this means that the stack monitor sends traps when a unit did not stack after a reset, a stack did not form as intended, and so on.

Time zone support

All 5500 Series switches support Simple Network Time Protocol (SNTP). The 5530 also supports real-time clock (RTC). However, there is currently no mechanism to automatically adjust a 5500 Series switch for specific time zones. This means that all time-stamping on log messages is the time of the SNTP server, rather than being adjusted for regional time zones.

The SNTP Time Zone & Daylight Saving time feature allows user to set local time characteristics.

The feature is supported in a stack environment (propagation of date and time values within a stack).

Configurable using NNCLI, ACG, and Device Manager.

UBP and EPM support

In Release 5.0, users configured User-Based Policies (UBP) for a switch using Web configuration pages. Release 5.1 offers users the option of centrally updating UBP information using the Enterprise Policy Manager (EPM).

Configurable using NNCLI, ACG, Device Manager, and the Web.

JDM and SNMP error code enhancements

Release 5.1 adds more informative error code messages to the JDM and SNMP.

Supported software and hardware capabilities

The following table lists the known limits for the Ethernet Routing Switch 5500 Series, Software Release 5.1 and Device Manager 6.0.7.0. These capabilities will be enhanced in subsequent software releases.

Refer to *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.2 (217468-A)* for detailed information on hardware and software capabilities for the Ethernet Routing Switch 5500 Series.

Supported capabilities in the 5500 Series switches (Release 5.1)

Feature	Maximum number supported
VLANs	256
Protocol-based VLANs	Depending on the protocol specified, the number of protocol VLANs supported at one time varies between 3–7. Refer to <i>Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking (NN47200-502)</i> for more information.
Nortel SNA VLANs	1 Red VLAN per switch. Nortel recommends a maximum of 5 Yellow VLANs, 5 Green VLANs, and 5 VoIP VLANs per switch for release 5.0.
Nortel SNA ports	All ports. Note: The 5530 has two 10 Gigabit (Gb) ports. You can configure these as uplink ports only. You cannot configure these as dynamic ports.
ARP records	1500
IP interfaces	256
Static routes	up to 512
Spanning Tree Groups	8
Aggregation groups (link aggregation)	32
Ports per aggregation group	8
IGMP maximum number of unique groups	240
EAPoL 802.1x supplicants	All ports
MAC addresses in fdb	16 Kb
Number of routes (dynamic, static and local)	2000 ¹ or 512 ²
OSPF areas	4
OSPF adjacencies	64

Feature	Maximum number supported
VRRP interfaces	64
ECMP	4 paths ¹
¹ Supported on 5520 and 5530 switches only. ² Supported on 5510 switches.	

Layer 3 scaling limitations

The following are Layer 3 scaling limitations for the Ethernet Routing Switch 5500 Series, Software Release 5.1:

- No information yet

Additional information for the feature software license file

When you create the Software License file at the site identified in the license kit, you must specify a file name (see *Nortel Ethernet Routing Switch 5500 Series Overview – System Configuration* (NN47200-500) for instructions to obtain the Advanced Routing License Features Activation Kit (part number 322515-A)). The file naming restrictions are the following:

- A maximum of 63 alphanumeric characters
- Lowercase only
- No spaces or special characters allowed
- Underscore (_) is allowed
- The dot (.) and three-character file extension are required

For example, abcdefghijk_1234567890.lic.

The format of the file that you upload to the license generation tool (and that contains the list of MAC addresses) must be as follows:

- ASCII file format
- One MAC address per line
- No other characters, spaces, or special characters allowed
- MAC must be in hexadecimal, capitalized format, with each pair of characters separated by colons (XX:XX:XX:XX:XX:XX)
- The file must contain the correct MAC addresses. Any incorrect MAC addresses will result in the licensed features not working on designated units.
- The number of MAC addresses must not exceed the number of MAC addresses allowed for the License Authorization Code entered for a particular file:
 - AL1016001 = 2 MAC addresses (1 stack/standalone unit)

- AL1016002 = 20 MAC addresses (10 stacks/standalone units)
- AL1016003 = 100 MAC addresses (50 stacks/standalone units)
- AL1016004 = 200 MAC addresses (100 stacks/standalone units)

Upgrading diagnostic software

When you add a new unit with FW: 4.2 and Agent: 4.2.x installed to an existing stack running FW: 5.0.0.4 and Agent: 5.1.0.0, you must download FW: 5.0.0.4 to the stack for future agent upgrades after the new unit joins the stack through AUR.

Use the following procedure to upgrade the diagnostic software.

Upgrading diagnostic software

Step	Action
1	Add new unit (FW: 4.2, Agent: 4.2) to the stack (FW: 5.0.0.x, Agent: 5.1.0.0)
2	Reset the new unit so it joins the stack. (Through AUR).
3	Download diagnostics version 5.0.0.x to the stack.
4	Download agent 5.1.0.0 to the stack.

—End—

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

Issues resolved in Release 5.1

The following table describes the issues in previous software releases for the Ethernet Routing Switch 5500 Series that have been resolved in Software Release 5.1.

Issues resolved in 5500 Series Software Release 5.1

Reference number	Documented issue
Q01193666	Pinging the virtual IP address from the master VRRP routing switch is now supported.
Q01200004	Ping delay resolved.

Reference number	Documented issue
Q01295448	With Release 5.0, when configuring IPFIX, the Exporter IP is not configurable. Therefore the exporter address is one of the routable interfaces. Resolved.
Q01305224	Each port on the 5520 is restricted to 11 interface IDs. Depending on your configuration, you may be unable to select the complete list of interface applications on an Ethernet Routing Switch 5520 because of the permitted number of interface IDs. Resolved.
Q01324425	A PC can disappear from the Nortel SNA client list after you perform a Time Domain Reflectometry (TDR) test on a Nortel SNA dynamic port. Workaround: Nortel recommends that you avoid running a TDR test on a Nortel SNA port. Resolved.
Q01334161	When a port is NSNA enabled, the CLI allows you to disable CIST learning even though that port belongs to CIST and MSTI. Whenever a port is added to a new VLAN in RSTP or MSTP mode, it automatically becomes STP enabled for that group. This is different from the Nortel STPG mode, where the port is not automatically enabled on the STP group. Resolved.
Q01376770	Note that you should not disable global IP routing on the 5500 Series switch when the switch has an IST enabled. The CLI returns a reminder message if you attempt to disable IP routing with an IST enabled. The JDM also returns an error message, although the message is more generic than that returned from the CLI. Resolved.
Q01378866	When VLAN configuration control (VCC) is set to automatic, avoid changing tagging on ADAC ports. Resolved.
Q01386170	An ACG file will display error messages for RIP settings when you attempt to download the file if the file contains more than 64 IP VLANs. If using the CI, the download stops at the first error message. Resolved.
Q01402433-01	The CLI commands used to set the CLI password on a stack are not displayed when using ? to request CLI help for the command (that is, <code>cli password ?</code>). The omitted commands are: <ul style="list-style-type: none"> • <code>cli password stack serial <password></code> • <code>cli password stack telnet <password></code> • <code>cli password stack read-only <password></code> • <code>cli password stack read-write <password></code> Resolved.

Reference number	Documented issue
Q01402425-01	<p>MAC address security in a stack is limited to the highest port number of the base unit if that unit is a 5510-24T or 5530-24TFD model. Port numbers higher than 24 are not allowed when a 5510-24T is the base unit and ports higher than 26 are not allowed when a 5530-24TFD is the base unit.</p> <p>For example, if the stack consists of a 5530-24TFD as the base unit and unit 2 is a 5510-48T, ports 2/25 through 2/48 cannot be used for MAC-based security in learning mode.</p> <p>Note: Also see CR Q01387506-01 directly below.</p> <p>Resolved.</p>
Q01387506-01	<p>In hybrid (mixed) stack configurations, Nortel recommends that the higher model number unit be made the base unit. In instances where a 5530-24TFD is to be part of the stack, Nortel recommends that this unit be made the base unit to utilize the full range of features present on this unit.</p> <p>Note: If running MAC security, ensure you have a 48-port unit as the BU (see CR Q01402425-01 directly above).</p> <p>Resolved.</p>
Q01338594	ACG configuration files do not save LLDP information successfully. Resolved.
Q01327042 Q01326930	<p>No useful error message appears when you try to enable ECMP or OSPF on the JDM without the software license. You cannot, however, enable ECMP or OSPF without the license.</p> <p>Workaround: Upload the license using the CLI prior to globally enabling ECMP or OSPF on the JDM. Resolved.</p>
Q01340389	<p>The switch allows you to change rate limiting on active DMLT ports while one or more units having DMLT members are down. However, Nortel recommends you avoid configuration changes of any kind while some units (with DMLT members) are down, as you may experience unexpected results. Resolved.</p>
Q01357858	Proprietary TLV is not available for MLT, however 802.3 link aggregation is supported. Resolved.
Q01362571	<p>There is no message or information provided after you download the software license file using the Web interface. You will not receive notification that the license has loaded successfully or not. Note that you must reset the switch for the license to be activated. Resolved.</p>
Q01362573	<p>When you open the license download page using the Web-based interface, there is no help file information in the configuration section for loading the license file. Resolved.</p>
Q01366773	<p>Avoid enabling Nortel SNA on a brouter port—the port is not added to the Red VLAN in this case. Release 5.0 does not support Nortel SNA on a brouter port. Resolved.</p>
Q01372515	<p>OSPF virtual link is not supported in Software Release 5.0. Any display for this feature is strictly informational. Resolved.</p>

Reference number	Documented issue
Q01381116	For Release 5.0, ensure you set LACP timeout to "Long" if you have more than eight LACPs and eight links per LACP. Resolved.
Q01382613	A root is not elected on an MLT if the VID for an MLT port belongs to a VLAN for an inactive MSTI. Ensure the PVID belongs to a VLAN for an active MSTI. This is related to a hardware limitation. Resolved.
Q01384306	Note that the JDM displays information for RIP Poison enable/disable inconsistently. Workaround: Use the CLI. Resolved.
Q01386369	If using OSPF MD5 authentication, note that in the case of authentication failure, only the enterprise-specific traps are logged to the syslog.
Q01305076	For Software Release 5.0, you cannot load the software license file from a USB device. Resolved.
Q01404072	After entering any other command, wait at least twenty (20) seconds before using the <code>copy config nvram</code> command. Additionally, Nortel recommends that you avoid using the <code>copy config nvram</code> command in ASCII configuration files. Resolved.
Q01730928	Nortel recommends that you do not execute the Stack loopback test until the switch has completes the bootup process. If you execute this test during the bootup process, it may produce unpredictable results.

Known issues and temporary limitations in Release 5.1

See "[Ethernet Routing Switch 5500 Series known limitations](#)" (page 23) for a list of known anomalies for the 5500 Series Software Release 5.1.

See also *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0 (217468-A)* and *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.3.1 (217468-C)* for more information on known hardware and software limitations for the Ethernet Routing Switch 5500 Series.

Ethernet Routing Switch 5500 Series known limitations

Reference number	Description
Q01246853	You may receive an error message when performing TDR tests using cable lengths greater than 60 m. Sample error message: <pre>5530-24TFD>ena 5530-24TFD#tdr test 7 %WARNING: TDR test will impact the traffic flow. Diagnosing port 7... 5530-24TFD# Test error: 16384</pre>

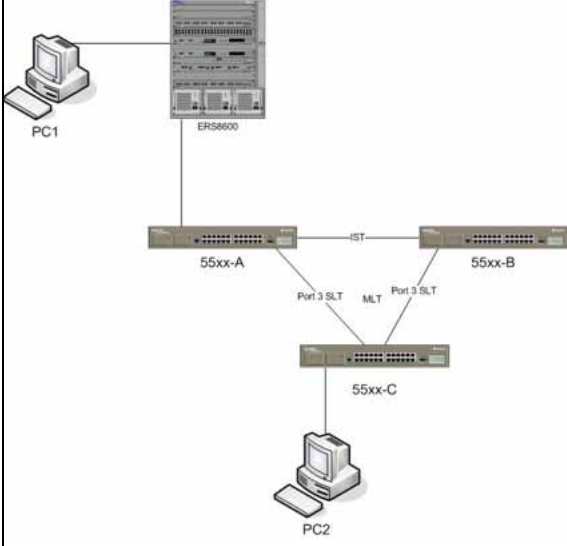
Reference number	Description
Q01280422	The switch may display "0" for the root port (spanning tree), rather than "None".
Q01300926 Q01328936 Q01331097 Q01345613	Note that the greater the number of VRRP instances you have, the greater the risk of VRRP bounces (Release 5.0 supports 64 VRRP instances). To help alleviate VRRP bounces, when you configure FAI on VR instances, set the FAI to 600 ms or higher. In general, for a large number of VRRP instances, Nortel recommends that you use a higher advertisement interval.
Q01309758	If LACP is enabled on a port that you configure as a Nortel SNA uplink port, the switch does not allow you to disable LACP on that port.
Q01319650	When you have VRRP and traps enabled, OSPF convergence may slow down.
Q01333595	If you add a network device to the switch, and that device does not require PoE, disable PoE on that port.
Q01334543	The switch does not return a meaningful message when you attempt to add five or more IP prefix lists into a policy.
Q01339715	The IPFIX flush menu item is present and functioning in the CLI, although the <code>ip ipfix flush</code> command and its parameters do not display in the menu when you enter an <code>ip ipfix ?</code> command query (Global configuration mode).
Q01346792	If you are unable to get the switch to transmit LLDP network policy type, length, and value (TLV), ensure that the following two conditions are true: <ul style="list-style-type: none"> • ADAC is enabled on the port • "Filter Unregistered Frames" option is set to "Disabled" on the ADAC-enabled port <p>Refer to <i>Nortel Ethernet Routing Switch 5500 Series Overview – System Configuration</i> (NN47200-500) for more information.</p>
Q01353603	When attempting to download the license file using the JDM after a previous attempt, the switch may return a "commitFailed" error. You may also receive this error if you enter an invalid license file name.
Q01366965	The CLI behavior related to PoE TLVs (MED "Extended Power-Via-MDI" and DOT3 "Extended Power-Via-MDI") is inconsistent when enabling them for transmission on non-PoE switches (no error message is generated in either instance).
Q01368144	Note that the default value for VLACP fast timers differs between the Ethernet Routing Switch 8600 Release 4.1 and Ethernet Routing Switch 5500 Series Release 5.0. The default value is 200 ms on the 8600, and 500 ms on the 5500 Series switch. Note also that the supported VLACP ranges on the 5500 Series and 8600 switches are 10–20000 ms and 400–20000 ms, respectively.

Reference number	Description
Q01370360	When using the CLI, you may see an inconsistency in output for the <code>show spanning-tree <mstp rstp> port <config status> <port></code> commands in MSTP or RSTP mode. This only occurs when there is no link on the port for which you are viewing statistics.
Q01371237	The 5500 Series switch supports 32 MLT groups. These can be configured using the CLI, JDM, and the Web interface. Note that the CI allows you to configure only six of the 32 MLT groups.
Q01379149	You must ensure you set the same speed on link partners. That is, if the speed for a port is set to 10 Mbps, any device connected to that port (for example, an IP phone), must also be running at 10 Mbps.
Q01380260	You may experience an inconsistency between the base unit (BU) and non-base unit (NBU) ports when using the EAPoL authentication process with UBPs. Specifically, on the NBU, if a policy cannot be installed, the switch will send a success and then immediately send a failure.
Q01384613	There is a scaling limitation for TLV in the 802.1ab feature. If you have an 8-unit stack that is fully connected and has 256 VLANs configured, you might experience that the DOT1 VLAN name TLV is not sent properly.
Q01385870	You can configure port mirroring using the CLI and CI only.
Q01391522	When using the CI to create STP groups, you may receive "The Group has no VLAN members" error message, which then interferes with subsequent configuration. Toggle the STP group field to continue configuration.
Q01394363	There is a discrepancy between the CI and the JDM when viewing port statistics displayed for received packets.
Q01395852	If OSPF is enabled, you may receive an OSPF syslog message on the NBU while the system is coming up. This occurs because OSPF checks for the license, but the license information is not available until the stack is formed.
Q01319058	In a Nortel SNA setup, you may experience temporary loss of Nortel SNA functionality when UDP forwarding has approached maximum capacity. Workaround: Configure a filter on the port that connects to the SNAS (or depending on your configuration, on the port connected to the switch that, in turn, connects to the SNAS) to isolate Nortel SNA SSCP traffic received by the CPU. The CLI commands to configure a filter are the following: <ul style="list-style-type: none"> • qos ip-element <element id> src-ip <ipaddr/mask> • qos classifier <value> set-id <value> element-type ip element-id <value> • qos action <value> update-1p <value> • qos policy <value> port <portlist> clfr-type class clfr-id <value> in-profile-action <action id> prec <value>

Reference number	Description
Q01374774	When you simultaneously reset two or more non-adjacent stack members causing other members to be isolated from the stack, the stack may fail the DB exchange when the reset units attempt to re-join the stack. Workaround: Reset the base unit, or change the ports status for a stack (down/up).
New for 5.1	
Q01622383	MLT/Mac-sec: Traffic does not recover after reboot on a MLT with mac-sec enable until you reboot the standalone.
Q01618770	To upgrade the SSH from Rel. 4.x.x to Rel. 5.1, you must first upgrade to 5.0. Use the following procedure to upgrade from Rel. 4.x.x to Rel. 5.1. <ol style="list-style-type: none"> 1. Upgrade the agent image from Rel. 4.xx to Rel. 5.0 2. Upgrade the diag. image to Rel. 5.0.0.4 (this diag. image was released with agent Rel. 5.1) 3. Upgrade the agent image from Rel. 5.0 to Rel. 5.1.
Q01415261	If a MAC is not present in the MAC-db at the SNAS, it is learned on a switch port and entered as a dynamic PC into the NSNA client list. Adding the same MAC to the MAC-db after that will not authenticate the MAC. The port will need to be reset or NSNA disabled and enabled at the port to remove it from the client list for subsequent authentication of that MAC.
Q01650221	NSNA dynamic ports must have Spanning Tree Learning mode Fast Learning or Disabled when NSNA is globally enabled. STP Normal Learning mode will not be restored if NSNA is disabled.
Q01637116	Adding or deleting host routes for hosts directly attached to the router in non-backbone area is not advertised by the router without disabling and enabling OSPF on the switch.
Q01471387	Ping to the VRRP IP addresses on the switch from local console or telnet is not supported.
Q01680155	Nortel recommends that you do not make any changes that might affect NSNA behavior when you have clients connected.
Q01681616	If you remove a connected route, none of the static routes depending on it will be added back as Non Local Static Routes if there is another route which can be used as Next Hop for these routes.
Q01680918	The <code>show qos diag</code> command may not show correct data if the device is in the middle of a filter installation.
Q01655103	Tagged ports shared between a VLAN in STPG 1 / CIST and a VLAN removed from all spanning tree groups will block traffic for both VLANs if the STP state is not 'Forwarding' in STPG 1 / CIST.
Q01650225	Due to the nature of NSNA, Nortel recommends that you disable autosave with <code>no autosave enable</code> , while NSNA is enabled. If you need to save a configuration, use the explicit save to nvram command, <code>copy config nvram</code> .

Reference number	Description
Q01421487	STPG: When a Topology Change is in place, some MAC addresses may not be aged out from the MAC address table after the Forwarding Delay interval.
Q01688004 Q01689623	<p>Nortel recommends that you do not connect both SMLT aggregation switches to the same network or end device (PC or workstation) through non SMLT/SLT ports. When non SMLT/SLT ports are connected together on the same VLAN with the IST ports, it creates a loop in the network.</p> <p>To prevent a loop, always assign non SMLT/SLT ports to different VLANs.</p> <p>For instance, if switches A and B are both SMLT aggregation switches and ports 5 on both switches are non SMLT/SLT ports, and you connect ports 5 of both switches to the same PC configured as a TFTP server, you must assign port 5 of switch A to VLAN 100 and port 5 of switch B to VLAN 200. IST ports may or may not be a member of VLANs 100 and 200.</p>
Q01426066	In a busy network which has more than 400 L3 routes and 2000 MAC addresses, if one of the SMLT aggregation switches goes down and then comes back up, each aggregation switch must ageout its own MAC and ARP tables, and then relearn the new MACs and ARPs. During this process, contention for system resources will cause new MAC addresses and new ARPs to be processed slowly, possibly resulting in flooding and packet loss for about 20-30 seconds.
Q01693817	Nortel recommends that you do not run TDR tests while the device is in a transient state, such as when units are being rebooted or are joining the stack.
Q01711153	IPFIX may report incorrect byte or packet count due to software limitations.
Q01720549	<p>In an SMLT environment, all IST traffic (switched or routed) is blocked from egress on SMLT / SLT ports that are currently in SMLT mode. This is achieved through programming the PORT_TRUNK_EGRESS table corresponding to the IST trunk appropriately. However, when the IST ports and SMLT / SLT ports reside on the same 5695 device, the EGRESS_MASK table needs to be programmed too. Currently, when an IST / SMLT port goes up or down, the corresponding entry in the EGRESS_MASK table is cleared, resulting in a loop. In the Regatta 5.0 code base, this situation is corrected by re-executing the block IST call that reprograms the two tables correctly. This call is made whenever an IST port goes up/down or an SMLT port comes up and the trunk is already in SMLT mode.</p> <p>To work around this problem, static routes must be used.</p>
Q01721397	<p>For the 10 G or XE port, the oversize counter does not increment.</p> <p>For the 1 G or regular port, the oversize counter only increments if the packet that it receives is between 1519 and 9216 bytes.</p>

Reference number	Description
Q01722655 Q01723309	<p>The <code>vllacp port</code> CLI command in Agent v5.1 no longer accepts multicast MAC addresses for the <code>funcmac-addr</code> parameter.</p> <ul style="list-style-type: none"> When an ASCII configuration file uploaded from a switch running Agent: v5.0.0 is downloaded to a switch running Agent: v5.1.0, an error, <code>Configuration script execution Failed</code>, is generated if the <code>vllacp port ALL funcmac-addr</code> command in the file is applied to a multicast address. After you upgrade the agent from Agent: v5.0.0 to Agent: v5.1.0, any multicast MAC address previously configured for the interface <code>funcmac-addr</code> parameter needs to be manually modified to the 5.1 default value of 0.0.0 or a unicast address.
Q01723954	<p>When you configure a DMLT as an IST or SMLT in a stack, Nortel recommends that you have at least one DMLT link on the base unit. If you have a DMLT link on the base and if the base goes out and temp-base takes over, the traffic recovery process is much faster. Traffic loss is reduced.</p>
Q01728560	<p>ADAC Port Type values:</p> <ul style="list-style-type: none"> CS—Call Server Port U—Uplink Port T—Telephone Port
Q01728569	<p>Continuous observation of IPFIX data uses a lot of memory on the switch and burdens the switch CPU to the point where it can't do other tasks. Therefore, the switch checks the network traffic at each second beat, rather than looking at every packet to maintain IPFIX records. When you use IPFIX, the traffic volumes are an estimate rather than the actual measured flow volume.</p>
Q01728586	<p>There are 4 internal ports for two Cascade links. Internal ports 1 and 2 are associated with Cascade-Down link and internal ports 3 and 4 are associated with Cascade-Up link.</p> <ul style="list-style-type: none"> <code>Message Stack port 1 DOWN</code> or <code>Stack port 2 DOWN</code> means Cascade-Down link is down. <code>Message Stack port 1 UP</code> or <code>Stack port 2 UP</code> means Cascade-Down link is down. <code>Message Stack port 3 DOWN</code> or <code>Stack port 4 DOWN</code> means Cascade-Up link is down. <code>Message Stack port 3 UP</code> or <code>Stack port 4 UP</code> means Cascade-Up link is down.
Q01731450	<p>The OSPF neighbor state intermittently remains in <code>Exch Strt</code> when routing is disabled and enabled for an ABR with virtual link configured. Workaround: To return the OSPF neighbor to the <code>full</code> state; disable then re-enable routing.</p>

Reference number	Description
Q01736809	To enable IPSPG, you must enable both DHCP Snooping and Arp Inspection on the switch and configure the port as <code>untrusted</code> .
Q01737603	The correct way to log out of the Web-based management interface is to go to the main menu and choose Administration > Logout . If you close the browser window, you will be unable to log back into the Web-based management interface for the configured idle period.
Q01736807	To confirm that there are sufficient filter or mask resources available for you to enable IPSPG, use the <code>show qos diag</code> command to display the filter and mask resource use by a port that is a member of a QoS interface group. The number of QoS plus nonQoS masks cannot exceed a total of 15 for each port as there are only 15 available masks on the DUT. Also, the number of QoS plus nonQoS rules cannot exceed a total of 128 for each port. For more information, see "Filter resource consumption" (page 32) .
Q01737679	<p>In an SMLT environment, the traffic received on an IST port is categorized into two groups: IST switched and routed packets. To prevent a loop condition, the switch must block IST switched packets (broadcast, multicast, and unknown unicast traffic) from egressing to any SMLT or SLT ports.</p> <p>However, SMLT switch must be able to forward IST routed packets to any specific SMLT or SLT port as requested by the routing engine. A hardware limitation, ERS55xx blocks both IST switched and routed packets from exiting SMLT or SLT ports. As a result, some of the L3 traffic will be lost. When you configure ERS55xx with both SMLT and L3 dynamic routing protocols (OSPF, RIP), you must avoid the topology in which the L3 traffic received on an SMLT switch is routed to the other SMLT peer because it is a better route.</p> 

Reference number	Description
	<p>In the preceding figure, 86xx has two routes to reach PC2. The first route is to 55xx-a and then 55xx-c. The second route is to 55xx-b and then 55xx-c. If 8600 uses second route, the traffic from PC1 will never reach PC2.</p> <p>To force the 86xx to take the first route, you must configure VRRP with Backup/Master enabled on both SMLT switches.</p> <p>Then static route with the best cost to the VRRP must be added to 86xx to make sure 86xx always chooses 55xx-a as the next hop to reach PC2.</p>
Q01738603	If you use the non-EAP phone feature in Layer 3 mode with DHCP Relay, it may disrupt Layer 3 connectivity. Nortel recommends that you deploy this feature only in Layer 2 mode.
Q01738540	A hardware limitation means that once you program the filter, it blocks all IPs that are not allowed. The switch does not show which IP was dropped.
Q01738600	When you enable NSNA, DHCP clients connected to non-NSNA ports will not receive DHCP packets sent from NSNA uplink server ports. Nortel recommends that you connect the DHCP server through a non-NSNA uplink port.

Known limitations

The following is a list of the known limitations for the Ethernet Routing Switch 5500 Series, Software Release 5.1.

Known limitations

Item	Description
1	Some terminal programs can cause the Console Interface to crash if you enter a RADIUS secret containing the character "k". The issue has been reproduced using Tera Term Pro (version 2.3), as well as Minicom (version 2.1) on a Linux system.
2	Nortel recommends that you avoid using MAC security on a trunk (MLT).
3	Failed attempts to log in (using TACACS+ authentication and accounting) are not stored in the accounting file.
4	When switches are in MSTP mode and connected using a trunk (MLT), and at least one MSTI is configured, the switch can return an incorrect STPG root if you change the mode to STPG and reset the switches.
5	When you use the JDM/Web to configure and add VLAN ports to an STG other than the default STG, STG membership of the port may change. In that case, the new STG participation of that port will be disabled. Workaround: Enable participation of the ports in the new STG after you enable the STG.

Item	Description
6	<p>On the 5530-24TFD, the following (NT-OCP) SFPs cannot be inserted side by side (that is, in neighboring slots) because of the SFP size. The SFPs are listed as manufacturer part number/Nortel part number:</p> <ul style="list-style-type: none"> • TRP-G1H5BC470N4 / AA1419025 • TRP-G1H5BC490N4 / AA1419026 • TRP-G1H5BC510N4 / AA1419027 • TRP-G1H5BC530N4 / AA1419028 • TRP-G1H5BC550N4 / AA1419029 • TRP-G1H5BC570N4 / AA1419030 • TRP-G1H5BC590N4 / AA1419031 • TRP-G1H5BC610N4 / AA1419032 • TRP-G1H7BC470N4 / AA1419033 • TRP-G1H7BC490N4 / AA1419034 • TRP-G1H7BC510N4 / AA1419035 • TRP-G1H7BC530N4 / AA1419036 • TRP-G1H7BC550N4 / AA1419037 • TRP-G1H7BC570N4 / AA1419038 • TRP-G1H7BC590N4 / AA1419039 • TRP-G1H7BC610N4 / AA1419040
7	<p>While downloading the image file, you may receive the following error message: "Error reading image file."</p> <p>Workaround: Typically, this issue can be resolved by simply restarting the image download. If this does not resolve the issue, Nortel recommends that you try an alternate method to download the image to the switch (that is, the Web Interface).</p>
8	<p>When a remote server log is configured and the remote logging is enabled, the CLI audit task sends messages to the syslog server regardless of the logging level.</p>
9	<p>The IPFIX sampling data rate cannot be changed because of a related hardware limitation.</p>

Item	Description
10	<p>Release 5.1 introduces a Demo License, which enables OSPF, ECMP, VRRP, SMLT, and IPFIX, or any combination thereof for a period of 30-days. At the end of the 30-day trial period, the features will be disabled, with the exception of SMLT. Due to the manner in which SMLT is implemented through cabling, and the fact that Spanning Tree Protocol needs to be disabled, a loop would be formed on the network if SMLT was disabled as a feature. Therefore, the following actions will take place to minimize the potential network impact.</p> <p>Three traps are sent.</p> <ul style="list-style-type: none"> • The first trap is sent five days prior to expiration of the license. Trap: bsnTrialLicenseExpiration: Trial license 1 will expire in 5 day(s). • The second trap is sent one day prior to the expiration of the license. Trap: bsnTrialLicenseExpiration: Trial license 1 will expire in 1 day(s). • The last trap is sent upon termination of the license. Trap: bsnTrialLicenseExpiration: Trial license 1 has expired. <p>At this point, all license features are disabled except SMLT. SMLT will remain enabled until there is a stack/unit reset. Once the stack/unit is reset, the feature will be disabled, and a loop will be formed if there has been no intervention to remove/disable the ports participating in the IST.</p> <p>Therefore, Nortel recommends that upon receiving the first trap that the administrator begin to manually disable that feature and ensure that any cabling loop is removed.</p>
11	<p>When you configure IPFIX to work with NetQoS, Nortel recommends that you disable the SNMP polling by NetQoS device. To do this, remove the community string associated with the ERS 5500 Series switch on NetQoS device.</p>
12	<p>Nortel recommends that you do not enable IP Source Guard on trunk ports.</p>
13	<p>Nortel recommends that you do not enable Critical-IP functionality with VRRP in an SMLT environment.</p>

Filter resource consumption

Various Ethernet Routing Switch 5500 Series applications consume filter resources. These filter resources are a combination of masks and filters, sometimes also referred to as rules. A filter specifies the bit pattern to match, while a mask specifies the bit position to be matched and the evaluation precedence of the filters. Some applications (for instance, BaySecure, Port Mirroring, IGMP) require a set number of masks and filters enable them.

The following table summarizes the applications that require mask and filter resources.

Mask and filter requirements for applications

Application	Category	Masks required	Filters required
Broadcast ARP and ARP Inspection	Non QoS	1	1
DHCP Relay or DHCP Snooping or NSNA DHCP	Non QoS	1	2
QoS (default untrusted policy)	QoS	2	2
IGMP	Non QoS	2	10
Port Mirroring	Non QoS	1	2
EAP Authentication (EAPoL packet filter)	Non QoS	1	1
BaySecure (ERS5520/30 only)	Non QoS	1	32
EAP MHMA Allowed Clients (5520/30)	Non QoS	1	32
IPFix	Non QoS	1	1
QoS Interface Applications	QoS	16	16
NSNA MAC Intruder	Non QoS	1	32
NSNA (R/Y/G filters)	QoS	5	8
ADAC	Non QoS	1	1
RIP	Non QoS	1	1
UDP Bcast	Non QoS	1	1
VRRP	Non QoS	1	1
OSPF	Non QoS	1	1
IP Source Guard	Non QoS	1	10

On the Ethernet Routing Switch 5500 Series switches, each port has 16 masks and 128 filters available. By default, 1 mask and 1 filter are statically consumed by the system for ARP filtering, leaving 15 available masks and 127 available filters for QoS and other non QoS applications to configure dynamically.

Masks and filters inventory check

You can use the `show qos diag` command to assess the current filter resource usage for each port on the Ethernet Routing Switch 5500 Series switches. The `show qos diag` command displays the number of QoS masks and filters and non-QoS masks and filters consumed on each port. You can determine whether an application that requires filter resources can be enabled on a port by verifying that the number of available masks and filters meet the mask and filter requirements of that particular application.

The available masks and filters available on a port can be determined by adding the total number of QoS and non QoS masks in use and the total number QoS and non QoS filters in use on a port and then subtracting that number from 16 masks and 128 filters, respectively.

Note that the `show qos diag` command displays only QoS-enabled ports, regardless of whether the port is consuming filter resources or not.

As an example, to enable IP Source Guard on a port requires 1 mask and 10 filters. To verify that IP Source Guard can be enabled on port 5, you can view the `show qos diag` output display and determine that port 5 is currently using a total of 4 masks (QoS plus non-QoS) and 5 filters (QoS plus non-QoS). This means that 12 masks and 123 filters are available for use, which meets the IP Source Guard requirement of 1 mask and 10 filters. The following figure shows the `show qos diag` display before enabling IP Source Guard on port 5.

Before enabling IP Source Guard

```
5510-48T(config-if)#show qos diag
```

Unit/Port	Masks Consumed	Filters Consumed	Meters Consumed	Counters Consumed	Non QoS Masks Consumed	Non QoS Filters Consumed	Non QoS Meters Consumed
1/1	2	2	0	2	2	3	0
1/2	2	2	0	2	2	3	0
1/3	2	2	0	2	2	3	0
1/4	2	2	0	2	2	3	0
1/5	2	2	0	2	2	3	0
1/6	2	2	0	2	2	3	0
1/7	2	2	0	2	2	3	0
1/8	2	2	0	2	2	3	0
1/9	2	2	0	2	2	3	0
1/10	2	2	0	2	2	3	0
1/11	2	2	0	2	2	3	0
1/12	2	2	0	2	2	3	0
1/13	2	2	0	2	2	3	0
1/14	2	2	0	2	2	3	0
1/15	2	2	0	2	2	3	0
1/16	2	2	0	2	2	3	0
1/17	2	2	0	2	2	3	0
1/18	2	2	0	2	2	3	0

The following figure shows the `show qos diag` display after enabling IP Source Guard on port 5.

After enabling IP Source Guard

```
5510-48T(config-if)#show qos diag
```

Unit/Port	Masks Consumed	Filters Consumed	Meters Consumed	Counters Consumed	Non QoS Masks Consumed	Non QoS Filters Consumed	Non QoS Meters Consumed
1/1	2	2	0	2	2	3	0
1/2	2	2	0	2	2	3	0
1/3	2	2	0	2	2	3	0
1/4	2	2	0	2	2	3	0
1/5	2	2	0	2	3	13	0
1/6	2	2	0	2	2	3	0
1/7	2	2	0	2	2	3	0
1/8	2	2	0	2	2	3	0
1/9	2	2	0	2	2	3	0
1/10	2	2	0	2	2	3	0
1/11	2	2	0	2	2	3	0
1/12	2	2	0	2	2	3	0
1/13	2	2	0	2	2	3	0
1/14	2	2	0	2	2	3	0
1/15	2	2	0	2	2	3	0
1/16	2	2	0	2	2	3	0
1/17	2	2	0	2	2	3	0

QoS Interface Security Application

The QoS Interface Security application targets a number of common network attacks. Support includes ARP spoofing prevention, DHCP snooping, DHCP spoofing prevention, detection for the common worms SQLSlam and Nachia; and the Denial of Service (DoS) attacks Xmas, TCP SynFinScan, TCP FtpPort, and TCP DnsPort. Due to the lack of filter resources (i.e. masks) to enable the QoS Interface Security application as a whole, you can select individual security applications.

The following table summarizes the mask and filter resource requirements for individual QoS Interface Security applications.

Mask and filter resource requirements

QoS Interface Security Application	Masks required	Filters required
ARP Spoofing Prevention	5	5
DHCP Snooping	1	1
DHCP Spoofing Prevention	2	2
DoS SQL Slam	1	1
DoS Nachia	1	1
DoS Xmas	1	1
DoS TCP SynFinScan	1	1
DoS TCP FtpPort	2	2
Dos TCP DnsPort	2	2

Related documentation

The following table lists the documentation that is part of the Ethernet Routing Switch 5500 Series, Software Release 5.1 suite. A CD is provided with the device that contains the most up to date documentation at the time the unit was shipped.

Related documentation

Part Number	Title
NN47200-300	<i>Nortel Ethernet Routing Switch 5500 Series Installation</i>
NN47200-500	<i>Nortel Ethernet Routing Switch 5500 Series Overview – System Configuration</i>
NN47200-501	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — Security</i>
NN47200-502	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking</i>
NN47200-503	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — IP Routing Protocols</i>
NN47200-504	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service</i>
NN47200-505	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — System Monitoring</i>
NN47200-302	<i>Nortel Ethernet Routing Switch 5500 Series Release 5.1 Installation - SFP</i>
217070-A	<i>Installing the Nortel Ethernet Redundant Power Supply 15</i>
215081-A	<i>DC-DC Converter Module for the Baystack 5000 Series Switch</i>

How to get help

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

Getting help from the Nortel web site

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

www.nortel.com/support

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

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

Getting help over the phone from a Nortel Solutions Center

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

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

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

www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Ethernet Routing Switch 5500 Series

Release Notes — Software Release 5.1

Copyright © 2007, Nortel Networks
All Rights Reserved.

Publication: NN47200-400
Document status: Standard
Document version: 03.02
Document date: 22 October 2007

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

Sourced in Canada and the United States of America.

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

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

