Nortel Ethernet Routing Switch 5000 Series

Release Notes — Release 6.0

NN47200-400

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

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

New in this release

The following sections detail what’s new in Nortel Ethernet Routing Switch 5000 Series Release Notes — Release 6.0.

Features

See the following sections for information about feature changes.

- "Dual agent support" (page 12)
- "IGMPv3 snooping support" (page 12)
- "PIM-SM" (page 12)
- "IPv6 " (page 12)
- "Many-to-many port mirroring (Ethernet Routing Switch 5600 Series only)" (page 12)
- "MIB and Trap Web pages" (page 13)
- "NSNA enhancements" (page 13)
- "ASCII download log enhancements" (page 13)
- "RMON entry scaling" (page 14)
- "DoS attack prevention package (DAPP) support" (page 14)
- "Improved sytem log capabilities (exception errors)" (page 14)
- "SMLT enhancements" (page 14)

Other changes

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

New hardware

Nortel Ethernet Routing Switch 5000 Series introduces new switches that complement the Ethernet Routing Switch 5500 Series. The new switches provide increased bandwidth, use the same software image as the 5500 Series switches, and allow you to customize your stack.

File names for upgrade

See "File names for this release" (page 14) for the file names for this release.

Windows Vista

Release 6.0 supports Windows Vista.

Hardware and software compatibility

The following sections provide a synopsis of hardware and software compatibility considerations.

Complete integration of all release 5.1 features

Release 6.0 incorporates all the features of all previous releases and maintenance builds up to and including all release 5.1 customer builds. (NOTE: The intent is to support most maintenance builds on the v5.1 stream in v6.0, however, there may be instances when there is a v5.1.x that will not be supported because it was not available at the time of integration into the v6.0 stream.)

See *Nortel Ethernet Routing Switch — Release Notes, Software Release 5.1* (NN47200-400) for more information on release 5.1 features.

Document changes

This document is reformatted to comply with the Nortel Customer Documentation Standards. For more information, see *Nortel Ethernet Routing Switch 5000 Series Documentation Roadmap*, NN47200-101.

Introduction

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Nortel Ethernet Routing Switch 5000 Series, release 6.0.

For information on how you can upgrade your version of Device Manager, see *Nortel Ethernet Routing Switch 5000 Series Fundamentals*, NN47205-102.

The Nortel Ethernet Routing Switch 5000 Series, supported by software release 6.0, includes the following switch models:

- 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
- Nortel Ethernet Routing Switch 5698-TFD
- Nortel Ethernet Routing Switch 5698-TFD-PWR
- Nortel Ethernet Routing Switch 5650-TD
- Nortel Ethernet Routing Switch 5650-TD-PWR
- Nortel Ethernet Routing Switch 5632-FD

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 5000 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 6.0, as well as operational issues not included in the documentation suite.

For a complete list of documentation in the Nortel Ethernet Routing Switch 5000 Series suite, see *Nortel Ethernet Routing Switch 5000 Series Documentation Road Map* (NN47200-101).

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

Important notices and new features

This section contains a brief synopsis of the new features in release 6.0 and any important notices.

Navigation

This section includes the following sections:

New features in release 6.0

Ethernet Routing Switch 5000 Series, release 6.0 provides the following new hardware, features or feature enhancements:

New hardware in release 6.0

Release 6.0 introduces the following Ethernet Routing Switch 5600 Series switches:

- Nortel Ethernet Routing Switch 5698-TFD
- Nortel Ethernet Routing Switch 5698-TFD-PWR
- Nortel Ethernet Routing Switch 5650-TD
- Nortel Ethernet Routing Switch 5650-TD-PWR
- Nortel Ethernet Routing Switch 5632-FD

You can use the Ethernet Routing Switch 5600 Series switches as stand-alone switches, in a hybrid stack with your existing Ethernet Routing Switch 5500 Series switches, or in a pure stack of Ethernet Routing Switch 5600 Series switches.

The Ethernet Routing Switch 5600 Series switches provide more power through optional power supply modules. For power supply options and specifications, see *Nortel Ethernet Routing Switch 5000 Series Installation* (NN47200-300).

For complete descriptions of the new switches and installation instructions for the Ethernet Routing Switch 5600 Series, see *Nortel Ethernet Routing Switch 5000 Series Installation* (NN47200-300).

Software features in release 6.0

Dual agent support

This feature provides support for two agents and configurations for either Ethernet Routing Switch 5500 or 5600 Series pure stacks, or for mixed stacks containing both products, however, Dual Agent Functionality is not supported on the Ethernet Routing Switch 5510. The requirement is for the Agent image to selectively boot the device using either agent specified. In addition, the ability to specify when one agent image will become the primary (immediate, next reboot, or scheduled reboot) will be available.

IGMPv3 snooping support

Release 6.0 supports basic IGMPv3 snooping.

PIM-SM

Release 6.0 supports basic multicast routing. PIM-SM is a licensed feature which has been added to the existing Advanced License for the 5000 series. PIM-SM only operates in stand-alone mode in this release.

Ethernet Routing Switch 5600 Series hardware that operates in stand-alone mode, as well as Ethernet Routing Switch 5520 or 5530 switches in stand-alone mode support PIM-SM. The Ethernet Routing Switch 5510 does not support PIM-SM.

IPv6

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

Many-to-many port mirroring (Ethernet Routing Switch 5600 Series only)

Release 6.0 supports many-to-many port mirroring on Ethernet Routing Switch 5600 Series switches.

This functionality is only available on the Ethernet Routing Switch 5600 Series hardware. A maximum of 4 port mirroring instances can be configured based on some rules. A Hybrid stack supports only one port-mirroring instance (the default instance) as in Ethernet Routing Switch 5500 Series.

In a pure Ethernet Routing Switch 5600 Series hardware stack with stack oper-mode configured to hybrid only one port-mirroring instance is available. This rule is not applicable to standalone because stack oper-mode mode is valid only on stack. So on a Ethernet Routing Switch 5600 standalone with stack oper-mode configured as hybrid all 4 port mirroring instances will be allowed.

All existing traffic identification modes for mirroring are supported. You can configure many-to-many port mirroring with Web-based management. Device Manager does not support Port Mirroring.

MIB and Trap Web pages

A new Web page allows you to selectively configure traps and trap receivers. The page follows the standard web design conventions and has each trap and trap receiver listed. The Web page allows you to enter additional trap receivers and modify existing ones. The Web page lists all available traps and allows you to selectively enable or disable each one.

The new MIB Web Page application offers a way to access the SNMP MIB objects for each unit from Web-based management, with the help of the **Get**, **Get-Next** and **Walk** buttons.

NSNA enhancements

Release 6.0 supports Fail Open and VLAN Change Based on MAC Authentication.

ASCII download log enhancements

The ASCII Download Log feature logs messages that describe the result of the ASCII Configuration File download, especially the failed commands, as informational customer messages.

Combination image

The Combination (Combo) Agent Image contains the header of the image and two agent images, a 56xx agent image and a 55xx agent image.

Ethernet Routing Switch 5500 software releases before release 6.0 do not support the Combo image.

A stand-alone unit or a stack that uses the Ethernet Routing Switch 5000 Series Software Release 6.0 can download a combo image.

This software release (6.0) will be available in two different formats, a file in Combo format version 6.0 and a file in 55xx image format version 6.0. The 55xx image format in this release is necessary because all the current 55xx releases do not support the Combo image.

Combo Diagnostic Image

The Combo Diagnostic Image contains the header of the image and two Diagnostic images, a 56xx diagniostic image and a 55xx diagnostic image.

Ethernet Routing Switch 5500 software releases before release 6.0 do not support the Combo diagnostic image.

This diagnostic release for the new software release (6.0) will be available in two different formats, a file in Combo format and a file in 55XX format. The 55XX image format in this release is necessary because all the current 55XX releases do not support the Combo diagnostic image.

RMON entry scaling

Release 6.0 increases the number of RMON entry scaling entries for the RMON Alarm Table and RMON event tables to 800. The previous limit was 150. You can configure RMON entry scaling with NNCLI, ACG, and Device Manager.

DoS attack prevention package (DAPP) support

Release 6.0 introduces DAPP on Ethernet Routing Switch 5600 Series switches.

Ethernet Routing Switch 5600 ASICs have a number of pre-configured virus and DoS signatures built in. This release provides a method of quickly enabling the preconfigured virus and DoS signatures to provide additional levels of protection within the network while simultaneously preserving filters. You can configure DAPP with NNCLI, ACG, Device Manager, and on a separate Web page.

Improved sytem log capabilities (exception errors)

Release 6.0 provides additional system log capabilities and adds exception error numbers to the system log.

SMLT enhancements

Release 6.0 adds square and mesh topology support.

File names for this release

Table 1 "Software Release 6.0 Components" (page 15)describes the Nortel Ethernet Routing Switch 5000 Series, software release 6.0 software files. File sizes are approximate.

Table 1
Software Release 6.0 Components

Module or file type	Description	File Name	File Size (bytes)
ERS 5600 Series Standard Runtime Image Software	Standard non SSH combo image for the Ethernet Routing Switch 5000 Series	5xxx_600004.img	15 312 828
ERS 5600 Series Standard Runtime Image Software	Standard SSH combo image for the Ethernet Routing Switch 5000 Series	5xxx_600005s.img	15 838 236
ERS 5500 Series Standard Runtime Image Software	Standard non SSH 55xx image for the Ethernet Routing Switch 55xx Series	55x0_600004.img	7 456 924
ERS 5500 Series Secure Runtime Image Software	Standard SSH 55xx image for the Ethernet Routing Switch 55xx Series	55x0_600005s.img	7 718 252
ERS 5600 Series Diagnostic Image	Ethernet Routing Switch 5000 Combo diagnostic software	5xxx_60006_diags.bin	2 464 932
ERS 5500 Series Diagnostic Image	Ethernet Routing Switch 5500 diagnostic software	55x0_60006_diags.bin	830 980
ERS 5500/5600 Series MIBs	MIB definition files	Ethernet_Routing_Switch_5xxx_MIBs_6.0.0.zip	1 392 613
Device Manager software version for Windows	Device Manager software image for Windows NT, Windows Vista, Windows XP, Windows 2003, Windows 2000		
Java Device Manager software version for Solaris UNIX (6.0.11.0)	Device Manager software image for Solaris		
Java Device Manager software version for Linux (6.0.11.0)	Device Manager software image for Linux		
Readme file	Device Manager readme file		

Device Manager support for the ERS5500 and ERS5600 v6.0.0 will be in Java Device Manager v6.1.6 targeted for availability from www.nortel.comby 2008-12-19.

Supported software and hardware capabilities

The following table lists the known limits for the Ethernet Routing Switch 5000 Series, release 6.0 and Device Manager 6.0.1.0. These capabilities will be enhanced in subsequent software releases.

Table 2
Supported capabilities in Ethernet Routing Switch 5000 Series switches

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. See *Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking* (NN47200-502) for more information.
Nortel SNA VLANs	One Red VLAN per switch. Nortel recommends a maximum of five Yellow VLANs, five Green VLANs, and five VoIP VLANs per switch for release 6.0.
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.
Aggregation groups (link aggregation)	32
Ports per aggregation group	8
IGMP maximum number of unique groups	240 (for Layer 2) and 1000 (for Layer 3)
EAPoL 802.1x supplicants	All ports
MAC addresses in fdb	16 Kb
Number of routes (dynamic, static and local)	2000[1]
ARP records	1500
Static ARP	256
IP interfaces	256
Static routes	up to 512
Spanning Tree Groups	8
Aggregation groups (link aggregation)	32
Ports per aggregation group	8

Feature	Maximum number supported
MAC addresses in fdb	16 Kb
OSPF areas	4 (3 areas plus area 0)
OSPF adjacencies	64
VRRP interfaces	64
ECMP	4 paths[2]
DHCP Snooping Binding table entries	512
DHCP relay forward paths	512
IP Management routes	4
PIM-SM multicast entries	Up to 500 for 55xx series Up to 1000 for 56xx series

[1] Total number of routes (dynamic and static) supported.
[2] Not supported on 5510 switches.

Nortel Ethernet Routing Switch 5520 phone dongle

The part number for the Nortel Ethernet Routing Switch 5520 (5520-24T/48T-PWR) universal phone dongle is DY4311046.

Ensuring Device Manager Online Help displays correctly

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

- Netscape
- Internet Explorer

If you use Netscape as your Web browser, to ensure that the topics and table of contents display correctly when making a context call to on-product Help, perform the following procedure once before requesting Help on a topic:

1. Start the Netscape browser.
2. From the **Tools** menu, select **Options**. (An **Options** window opens.)
3. In the **Security and Privacy** panel of the **Options** window, click **Site Controls**. (An **Options - Site Controls** window opens.)
4. Ensure that the **Site List** tab is selected.
5. Select **Local Files** in the **Master Settings** area of the window.
6. Select **Internet Explorer** in the **Rendering Engine** area of the window.
7. Click **OK** to close the **Options - Site Controls** window.

Additional information for the feature software license file

When you create a license file to enable licensed features on an Ethernet Routing Switch 5000 Series switch with the Nortel Electronic Licensing Portal at www.nortellicensing.com, you must specify a file name. Follow the instructions on the License Certificate within the License Kit, or see *Nortel Ethernet Routing Switch 5000 Series Fundamentals* (NN47200-104) for more information. You must use the following rules when you generate and name the file:

- 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 software

To upgrade to the new software release 6.0, Nortel recommends that you upgrade the diagnostic software to the 6.0.0.4 version, and then upgrade the agent version to release 6.0.

Note: If you have version 5.x software on your Ethernet Routing Switch 5000 Series switches with an Advanced License file installed, use the following steps to upgrade your software.

Identify the corresponding Ethernet Routing Switch 5000 Series switch Advanced License deposit in the License Bank and click Details.

Locate the License file name in the transaction and click Download to download the Advanced License file and reinstall it on Ethernet Routing Switch 5000 Series switch or switch stack to enable configuration of the release 6.0 feature, PIM-SM (which has been added to the Advanced License).

The following table describes possible image locations:

Table 3
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
Pre-5.0 Diagnostic Image	Diagnostic image released before 5.0.
5.0 Diagnostic Image	Diagnostic image released in 5.0
6.0 Diagnostic Image	Diagnostic image released in 6.0

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

Table 4
Agent Image downgrade or upgrade chart

Local Agent Image version	Download Agent Image version			
	4.x	5.0	5.1	6.0
5.0	Yes	Yes	Yes—if Local Diagnostic Image is 5.0 Diag Image.	Yes—if Local Diagnostic Image is 5.0 Diag version or 6.0 Diag version.
5.1	Yes	Yes	Yes	Yes
6.0	Yes	Yes	Yes	Yes
4.x	Yes	Yes	No	No

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

Table 5
Diagnostic Image downgrade or upgrade chart

Local Agent Image version	**Download Diagnostic Image version**		
	Before release 5.0	5.1	6.0
5.0	Yes	Yes	Yes
5.1	No	Yes	Yes
6.0	No	Yes	Yes

Use the following procedure to upgrade the Agent Image from release 5.0 or 5.1 to release 6.0:

Upgrading Agent Image from release 5.0 or 5.1 to release 6.0

Step Action

1 Upgrade the diagnostic image from the earlier release to release 6.0 diagnostic image.

2 Upgrade the agent image from release 5.0 or 5.1 to release 6.0 agent image.

—End—

Use the following procedure to upgrade the Agent Image from release 4.x to release 6.0

Upgrading Agent Image from release 4.x to release 6.0

Step Action

1 Upgrade the agent image from release 4.x to release 5.0.

2 Upgrade the diagnostic image the earlier release to release 6.0 diagnostic image.

3 Upgrade the agent image from release 5.0 to release 6.0.

—End—

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

Supported standards, MIBs, and RFCs

This section lists the standards, MIBs, and RFCs supported by the Nortel Ethernet Routing Switch 5000 Series.

Standards

The following IEEE Standards contain information that applies to the Nortel Ethernet Routing Switch 5000 Series:

- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1X (EAPOL)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3x (Flow Control)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.1ab (Link Layer Discovery Protocol)

RFCs

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

- RFC 791 (IP)
- RFC 894 (IP over Ethernet)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 1350 (TFTP)
- RFC 826 (ARP)
- RFC 768 (UDP)
- RFC 854 (Telnet)
- RFC 951 (BootP)

- RFC 1213 (MIB-II)
- RFC 1493 (Bridge MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2665 (Ethernet MIB)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 1757 (RMON)
- RFC 1271 (RMON)
- RFC 1157 (SNMP)
- RFC 1112 (IGMPv1)
- RFC 1945 (HTTP v1.0)
- RFC 2131 (DHCP)
- RFC 2236 (IGMPv2)
- 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)

The following table lists 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

Standard	Description	Compliance
RFC 4291	IPv6 Addressing Architecture	Support earlier version of RFC (3513)
RFC 4007	Scoped Address Architecture	Supported
RFC 4193	Unique Local IPv6 Unicast Addresses	Not supported
RFC 4293	Management Information Base for IP	Mostly supported
RFC 4022	Management Information Base for TCP	Mostly supported
RFC 4113	Management Information Base for UDP	Mostly supported
RFC 1981	Path MTU Discovery for IPv6	Supported
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Supported
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack. No support for tunneling yet.
RFC 3162	RADIUS and IPv6	Supported
RFC 1886	DNS Extensions to support IPv6	Supported

Resolved issues

The following table lists the issues resolved for release 6.0:

Issues resolved in release 6.0

The following table describes the issues in previous software releases for the Ethernet Routing Switch 5000 Series that have been resolved in release 6.0.

Table 6
Issues resolved in Ethernet Routing Switch 5000 Series release 6.0

Change Request Number	Documented issue
Q01193666	Pinging the virtual IP address from the master VRRP routing switch is now supported.
Q01200004	Ping delay resolved.
Q01295448	With release 6.0, 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.

Change Request Number	Documented issue
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 then 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, **`cli password ?`**). The omitted commands are: • **`cli password stack serial <password>`** • **`cli password stack telnet <password>`** • **`cli password stack read-only <password>`** • **`cli password stack read-write <password>`** Resolved.
Q01402425-01	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. 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. ***Note:*** Also see CR Q01387506-01 directly below. Resolved.
Q01387506-01	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. ***Note:*** If running MAC security, ensure you have a 48-port unit as the BU (see CR Q01402425-01 directly above). Resolved.

Change Request Number	Documented issue
Q01338594	ACG configuration files do not save LLDP information successfully. Resolved.
Q01327042 Q01326930	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. Workaround: Upload the license using the CLI prior to globally enabling ECMP or OSPF on the JDM. Resolved.
Q01340389	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.
Q01357858	Proprietary TLV is not available for MLT, however 802.3 link aggregation is supported. Resolved.
Q01362571	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.
Q01362573	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.
Q01366773	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.
Q01372515	OSPF virtual link is not supported in release 6.0. Any display for this feature is strictly informational. Resolved.
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. Resolved.
Q01305076	For release 6.0, 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 **`copy config nvram`** command. Additionally, Nortel recommends that you avoid using the **`copy config nvram`** command in ASCII configuration files. Resolved.

Change Request Number	Documented issue
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. Resolved.
Q01246853	You may receive an error message when performing TDR tests using cable lengths greater than 60 m. Resolved.
Q01927798	You cannot change the management VLAN after the switch or stack IP address is assigned in Layer 2 mode. Resolved.

Known issues and limitations

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

Known issues

See the following table for a list of known anomalies for the Ethernet Routing Switch 5000 Series release 6.0.

Table 7
Ethernet Routing Switch 5000 Series known issues

Change Request Number	Description
Q01280422	The switch may display “0” for the root port (spanning tree), rather than “None”.
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.
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 `ip ipfix flush` command and its parameters do not display in the menu when you enter an `ip ipfix ?` command query (Global configuration mode).

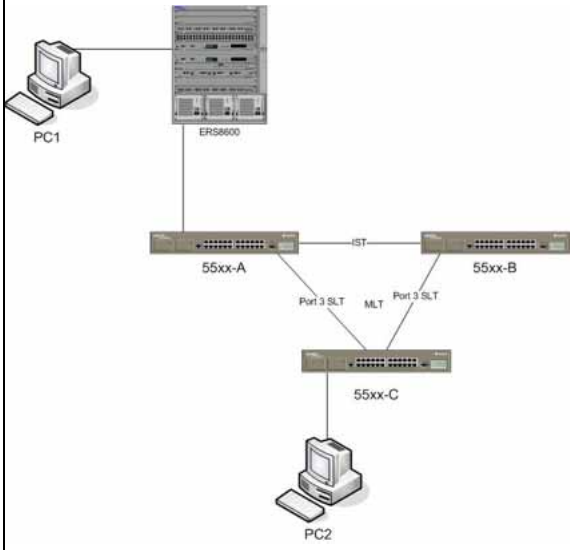
Change Request Number	Description
Q01346792	If you are unable to get the switch to transmit LLDP network policy type, length, and value (TLV), ensure that the following two conditions are true: • ADAC is enabled on the port • “Filter Unregistered Frames” option is set to “Disabled” on the ADAC-enabled port Refer to *Nortel Ethernet Routing Switch 5500 Series Overview – System Configuration* (NN47200-500) for more information.
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).
Q01370360	When using the CLI, you may see an inconsistency in output for the **`show spanning-tree <mstp|rstp> port <config|status> <port>`** 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 NNCLI, CI and Web-based management 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.

Change Request Number	Description
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: • 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>
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).
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. 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.

Change Request Number	Description
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 **show qos diag** 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 **no autosave enable**, while NSNA is enabled. If you need to save a configuration, use the explicit save to nvram command, **copy config nvram**.
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	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. To prevent a loop, always assign non SMLT/SLT ports to different VLANs. 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.
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.

Change Request Number	Description
Q01720549	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. To work around this problem, static routes must be used.
Q01721397	For the 10 G or XE port, the oversize counter does not increment. For the 1 G or regular port, the oversize counter only increments if the packet that it receives is between 1519 and 9216 bytes.
Q01722655 Q01723309	The **`vlacp port`** CLI command in Agent v5.1 no longer accepts multicast MAC addresses for the **`funcmac-addr`** parameter. • 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, `Configuration script execution Failed`, is generated if the **`vlacp port ALL funcmac-addr`** 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 **`funcmac-addr`** parameter needs to be manually modified to the 5.1 default value of 0.0.0 or a unicast address.
Q01723954	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.
Q01728569	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.

Change Request Number	Description
Q01728586	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. • Message `Stack port 1 DOWN` or `Stack port 2 DOWN` means Cascade-Down link is down. • Message `Stack port 1 UP` or `Stack port 2 UP` means Cascade-Down link is down. • Message `Stack port 3 DOWN` or `Stack port 4 DOWN` means Cascade-Up link is down. • Message `Stack port 3 UP` or `Stack port 4 UP` means Cascade-Up link is down.
Q01731450	The OSPF neighbor state intermittently remains in `Exch Strt` when routing is disabled and enabled for an ABR with virtual link configured. Workaround: To return the OSPF neighbor to the `full` state; disable then re-enable routing.
Q01736809	To enable IPSG, you must enable both DHCP Snooping and Arp Inspection on the switch and configure the port as **`untrusted`**.
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 IPSG, use the **`show qos diag`** 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
Q01737679	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. 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.

Change Request Number	Description
	 PC1 ERS8600 55xx-A IST 55xx-B Port 3 SLT MLT Port 3 SLT 55xx-C PC2 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. To force the 86xx to take the first route, you must configure VRRP with Backup/Master enabled on both SMLT switches. 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.
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.
Q01653932	When you enable IPSG on a list of ports, it is enabled one port at a time. In addition, IPSG will try to setup IP filters with binding entries currently defined for the port. In the case of a trunk, DHCP binding entries are defined only for the first member of the trunk. Workaround: Once you enable IPSG on all trunk ports, administratively disabled and enabled all trunk ports to force DHCP Snooping and IPSG to update all IP entries to all trunk ports.
Q01452496	Do not administratively disable port mirrored ports in MSTP mode.
Q01370981	Dynamic passive devices that redo DHCP may be displayed as a PC.
Q01446613	The total number of allowed EAP and non-EAP MACs must not exceed 32.
Q01252555	You can login after SNAS receives all port info from the switch.

Change Request Number	Description
Q01362768	Any modifications to the SNAS MAC DB will not take effect on the fly.
New in release 6.0	
Q01861619	Device Manager, like many SNMP-based applications, uses both SNMP v1 and v2c to discover and communicate with the device being accessed. To create a community string that will permit login on the device using Device Manager, you must create two entries for that string in the VACM tables, one for v1 security model and one for v2c
Q01900660	Static mrouter ports that belong to a MLT or a LAG may not become active after a restart of the peer switch. Workaround: Disable and enable IGMP snooping for the VLANs on the ports that should be active.
Q01777263	When you change an area from Stub to Non-Stub, former Stub area does not immediately learn AS External routes. It may take several minutes to be learned. To pass this issue, execute a **`no ip routing/ip routing`** Global Configuration command.
Q01895538	You need to disable IGMPv3 on an Ethernet Routing Switch 5000 Series release 6.0 snooping device when you connect it to PP8600 PIM-SSM devices.
Q01905556	After a successful MAC address Non-EAP Local or Radius authentication, other ports forward traffic to the Non-EAP enabled ports with an unexpected delay of 20 to 60 seconds.
Q01925597	After a restart, pluggable module information may intermittently display incorrectly through the Console Interface or NNCLI when you view it from another unit in the stack.
Q01925298	If you try to set a static router port as a Port Monitor from the NNCLI, the setting does not save and an error occurs. Workaround: Use the Port Mirroring menu in the Console Interface.
Q01915680	You cannot capture SLPP PDUs on the emitting device with MAC-based port mirroring modes.
Q01910326	When you use LACP with trunk members from each unit in a stack, the **`show lldp local-sys-data dot3`** command shows the link from last unit as Aggregated even after the LACP aggregation does not exist anymore.
Q01906362 Q01906362-01	If you connect radius authenticated Non-EAP clients through L2 devices to a 56xx or 55xx unit, and then move one client from an L2 device to another L2 device, user-based policies configured for that client do not move to the new port with the authenticated client. If you set UBP to high-security-local, the port will not authenticate the client after the move.
Q01902081	Before you download an ASCII configuration file from Device Manager, you must ensure that another download is not currently in progress with the ASCIIConfigManualDldStatus field. You can find the field here in Device Manager: **Edit, File System, ASCIIi Config File, ASCIIConfigManualDldStatus**

Change Request Number	Description
Q01895110	After you restart the stack, some NSNA MAC authenticated devices in the green VLAN or green filter may remain with red IP although the VLAN is green. Workaround: Run a **shutdown** command, followed by a **no shutdown** command.
Q01849554	The stack picture on Web-based management may not display the unit order correctly.

Q01422549	For 6.x software release, you can only configure STP 802.1d-port-compliance feature using NNCLI.
	Example: Enable 802.1d-port-compliance with NNCLI
	`5530-24TFD#spanning-tree 802.1d-port-compliance enable`
	Example: Disable 802.1d-port-compliance with NNCLI
	`5530-24TFD#no spanning-tree 802.1d-port-compliance enable`
	You cannot configure the 802.1d-port-compliance feature with the ASCII file.

Q01850763	Multiple ports may display the same NSNA client MAC address if you inject traffic with the same address in multiple ports while displaying NSNA clients.
Q01915112	Workaround: The unicast routes to reach PIM RP and Source must be through directly connected neighbors. These unicast routes should not span across the L2 DUT(s). Do not configure an SPT or RPT path for PIM through the L2 boxes.
Q01860831	If you connect a PC behind a phone when the switch is in FO state, the VLAN ID for the IP phone may be displayed as Red after the SNAS reconnects to the switch.
Q01877773-01 Q01879130-01	For a client that uses a DHCP assigned address: If the IP address is assigned while the client is in FO VLAN, that address will continue to be used by client until the lease time expires, even if during this time the client moves to another NSNA VLAN (which requires a new IP address be assigned to client through DHCP).
Q01891705	When the switch receives continuous routed data IP packets with TTL=1, OSPF hellos may be dropped and adjacencies may be lost as a result.
Q01861555	The traps from MIB S5-Chassis-Trap (s5ctr.mib) send the values of two objects to the receiver: `s5ChasComType`, which is a numeric OID of little use to the user; and `s5ChasComOperState`, which is a value between 1 and 12. Currently, the objects `s5ChasComDescr` and `s5ChasComSerNum` are not yet available in these traps.
Q01890586	After you restart the stack in NSNA solution, some PCs may appear with 0.0.0.0 IP on **show nsna client** command. However, the PCs have the right IP and can access network resources.
Q01753980-01	If new clients come up while NSNAS is connecting to a switch and is getting port information, those clients may need to redo DHCP (if they are dynamic clients). This can be done from Windows command line: **ipconfig /release ipconfig /renew**

Change Request Number	Description
Q01923243	Ethernet Routing Switch 5000 Series switches do not guarantee data integrity if you reset the power during the first 5 mins of operation or during a (periodic) flash sync operation.
Q01895935	ADAC-enabled telephony ports on a base unit may not be re-authenticated after you reset the stack.
Q01893906	This is a boundary condition for a specific scenario. If you take a small number of source (S) and group (G) entries and keep on changing the (S, G) values, the buffer fills and there is no room for a new value. Workaround: Take a number of (S, G) entries and then do not change the values of (S, G). You may change the value as long as you do not reach the maximum for Ethernet Routing Switch 5000 Series switches.
Q01924380	With short stack cables, the software download may fail repeatedly due to FCS errors. Replace the stack cable if this happens.
Q01920139	PIM:All (S,G) entries do not get installed on SDR or DDR. Although you may not see this issue in the very first boot, it may happen in your setup if you do a failover or something else that tries to change the installed (S,G). Workaround: a) Keep the number of (S,G) small (under 400) to reduce the possibility that this problem will occur. b) If you do encounter this issue, reboot the PIM units in your system to clear the buffer.
Q01910052	When you connect PCs with EAP authentication enabled behind IP phones that are discovered through ADAC, the authentication process may fail after stack restart. Workaround: Disable EAP, reboot the stack and then re-enable EAP.
Q01906093	If you upload the ASCII configuration file from the switch with the front panel UI button, it may result in a software exception. Use a different user interface to upload the ASCII configuration.
Q01904918	This is a specific scenario, in which the data is sent through the (distribution layer) L3 switch (DR) on a VLAN which spans through a L2 switch to another L3 (non-DR) PIM switch. In a freshly restarted system, you will not see this issue, but if you reboot the L2 switch, you will not receive the traffic from the L3 switch (non-DR) that spans in the VLAN across the L2 switch. Workaround: a) If you have this kind of topology, do not restart the L2 switch alone. b) If you do reboot the L2 switch and get into this state. then you must restart the L3 (PIM switches) to reconnect the traffic.
Q01920502	Port Mirroring mode XrxYtx does not work (traffic is not mirrored) after a restart if the X and Y ports are in different MLTs. Workaround: Disable and enable the port mirroring mode.
Q01920498	Port Mirroring mode XrxYtx does not monitor broadcast or multicast traffic (in X and out Y) if the monitor port and X+Y ports are in different VLANs.
Q01916316	When a unit leaves or joins the stack, it disrupts multicast traffic for about 30 seconds.

Change Request Number	Description
Q01911582	After you restart the stack, few dynamic ports may not move to Red and VoIP VLANs.
Q01904189	When you authenticate IP Phones with non-EAP or ADAC, and then restart the base unit or the last unit, not all ports may be authenticated after the restarted unit rejoins the stack. Workaround: Disable and then enable ADAC on the respective ports.
Q01900513	OSPF hello packets may not be captured on 5530 ports when you use ADST Mac address based mirroring mode.
Q01897761	When you use Device Manager with IGMP, it may display some incorrect information in the **ActiveQuerier** and **QuerierPort** fields under **VLAN, VLANs, Snoop** menu. This is a known issue.
Q01895450	When you authenticate IP Phones using non-EAP and ADAC becomes operationally disabled, it may take up to 300 seconds (5 mins) until EAP clears the multihost non-eap-mac table. If this is not desirable, EAP can be bounced on the respective ports.
Q01895070	After you restart a switch or stack with Fail Open enabled (NSNAS connected in the network), some devices may show as a green IP in the red VLAN. If you run the `shutdown/ no shutdown` command, the ports on stack will resolve the issue for both PCs and passive devices. Or, you can enter the `ipconfig /release; ipconfig /renew` command on the PC command line.
Q01893356	After you restart the stack, some NSNA MAC authenticated devices (in the green VLAN or green filter) may remain with a red IP although the VLAN is green. Run the `shutdown/ no shutdown` command to resolve the issue.
Q01865091	NSNA static MAC authenticated clients may not be re-authenticated on Base unit after it is restarted.
Q01440362	If you use DHCP relay on multiple hops, Nortel recommends that you configure the DHCP forward path on all hops to the DHCP server.
Q01909890	If you use a policy to filter a multicast flow with a system classifier with known-mcast or unknown-mcast options configured, it will only match non-IP traffic for the Ethernet Routing Switch 5600 Series.
Q01921407	In certain topologies, when you connect multiple PIM routers to the same L2 device, both the DR and non-DR routers may install the same OIF, resulting in duplicate packets for receivers across the L2 device. Workaround: Connect only a single PIM router to the L2 device.
Q01929584-01	When you use Web-based management with an IPv6 address, the response time may be noticeably slower than when you use Web-based management with an IPv4 address.
Q01839477	If you unplug an IP phone that is on a call or receives line tone, all of the other phones on the VoIP VLAN receive UDP packets (30-35 packets/sec) with the Source Address=BCM and Destination Address=IP-phone of the removed IP phone. The packet flood lasts 20-25 seconds.

Change Request Number	Description
Q01937764	The rate for multicast traffic on 10 G ports on the 5000 Series can fluctuate with 120 groups and 240 clients at smaller packet sizes. This is because 10 G ports have multicast rate limiting set to 10 percent by default. If you increase the allowed rate or disable rate limiting on the 10 G ports, you will fix the issue.
Q01939961	When you configure multiple port-mirroring instances with MAC-based address modes, the MAC address table in WEB/CI only displays the MAC address from the first port mirroring instance.
Q01931881	Do not restart the base unit of a stack that previously forwarded neighboring ports on an Ethernet Routing Switch 8600. If you restart only the base unit of the stack, the Spanning Tree neighbor ports may go to Spanning Tree Blocking state. Workaround: Restart the entire stack.
Q01945517	Starting with release 6.0, the Ethernet Routing Switch 5000 Series switches support four SSH sessions. Nortel recommends that you have no more than two concurrent SSH Console sessions. The remainder of the SSH sessions are intended for NSNA communication with the SNAS.
Q01946719	The load balance will not take effect on Ethernet Routing Switch 5500 Series units if the port of the L3 ingress traffic is on the same ASIC with an active trunk member.
Q01893913	In the PIM mroute table, the number of S, G entries displayed may exceed the number of supported entries when scaling beyond the supported limits.
Q01901336	The switch cannot forward multicast traffic through Non-Local Static Routes. The switch does forward multicast traffic through other route types such as a local next-hop.
Q01905825	TDR tests on a 100 MB-only capable unit do not show the expected results. There is an inconsistency in showing the TDR results between 56XX units and 55XX units. On both kind of units the TDR results in the situation from above will not show the Pair1 and NormalCableLength as expected. On a 56XX unit, TDR test shows the Pair1Length as 0 Meter. On a 55XX unit, TDR test shows the Pair1Status as `Forced mode`, with a much higher value for Pair1Length than normal.
Q01897761	When you use Device Manager with IGMP, you will see some incorrect information displayed about **ActiveQuerier** and **QuerierPort** fields when you click **VLANs, VLANs, Snoop** . This is a known issue.
Q01426394	With nine VRRP instances and overnight traffic, you may observe a single VRRP bounce.
Q01932595	When you enable IGMP proxy, the display may not show all IGMP groups on upstream routers. This is a display issue only.

Change Request Number	Description
Q01939345	The Device Manager does not display the status of all power supplies with the front panel LEDs. You can see the status of the Power supply under **Edit, Chassis, Power Supply**.
Q01945335	On an Ethernet Routing Switch 56xx unit, port mirroring mode XrxYtx does not mirror broadcast, multicast and unknown unicast if the X and Y mirrored ports are in different MLTs.
Q01948343	In some situations on a pure 56xx stack (mirrored ports are not on the same unit in the stack or traffic enters one unit and exits another one from the stack), port mirroring modes XrxYtx, XrxYtxOrYrxXtx, XrxOrYtx and MAC-based mirroring modes may multiply the unicast traffic that exits the stack. The problem is not present if multicast or broadcast traffic is mirrored. The problem is not present in port mirroring modes XrxYtx, XrxYtxOrYrxXtx, or XrxOrYtx if the monitor port is placed on base unit.
Q01950311	If you enable ARP-inspection on NSNA or ADAC Voice VLAN, the IP-phones only work properly on the base unit.
Q01950071	If you disable VLACP on an Ethernet Routing Switch 5698 unit before you start the unit, you cannot enable the unit with the **`vlacp enable`** command in Global Configuration mode. Workaround: Disable, then enable VLACP on the unit.
Q01954180	You cannot disable the **AlwaysBroadcast** parameter on a VLAN when you toggle off from Device Manager or set the value from the MIB Browser tool.
Q01953968	In a standalone ERS5632FD unit or stack that contains an ERS5632FD unit, if the system uses 10 G ports in an MLT configuration, do not enable DHCP snooping globally. If you enable DHCP globally, it could cause the unit to restart. If you use this configuration, upgrade the stack to the maintenance software release 6.0.1 from the Technical Support site at www.nortel.com as described in the Release Notes. With release 6.0.1, you can enable DHCP snooping.
Q01914709	When you download the ACG file with default settings from a SSH session, the ssh commands will fail (this is because SSH is already enabled on that unit).
Q01947854	When a PIM interface comes up, it identifies as a DR. Then DR election on that multi-access link happens after exchange of hello messages. If for some reason DR is flapped, by the time DR is down, the non-DR becomes the DR and therefore it installs (*,G) and (S,G) for a particular steam. When the original DR comes back again, the re-election of DR happens with exchange of hello messages. In this time frame (Before DR re-election is completed), if the IGMP reports and multicast traffic are sent on the multi-access link, then both non-DR and DR PIM routers may install the (*,G) & (S,G) entry as DR. This is an assert condition. The assert mechanism in this scenario may not work and may lead to duplicate packets as both DR and non-DR will have (S,G) for the same stream for a single multi-access link.

Change Request Number	Description
	To avoid this, make sure that only the DR has the (*,G) entry in the system. Workaround: If this condition occurs, disable and enable PIM on the non-DR and DR.

Q01944831	With release 6.0.0, there may be connectivity issues with Telnet and Web-based management connections to the IPv6 management interface when the traffic between the Ethernet Routing Switch 5000 Series switch and the host PC passes through a switch that drops frames larger than 1522 bytes. This happens because the default MTU for the IPv6 management interface is 1522 bytes, and must be set to a lower value of 1500 bytes.
	To change the MTU for the IPv6 interface from the Command Line Interface, type the following
	`enable`
	`configure terminal`
	`interface vlan 1`
	`ipv6 interface mtu 1500`

The following table lists known Ethernet Routing Switch 5000 Series considerations:

Table 8
Ethernet Routing Switch 5000 Series considerations

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	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: • 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	While downloading the image file, you may receive the following error message: "Error reading image file." 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).
8	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.
9	The IPFIX sampling data rate cannot be changed because of a related hardware limitation.

Item	Description

10	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.
	Three traps are sent.
	• 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.`
	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.
	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.

11	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.
12	Nortel recommends that you do not enable IP Source Guard on trunk ports.
13	Nortel recommends that you do not enable Critical-IP functionality with VRRP in an SMLT environment.

VLACP issue

It has been found that in some situations, using VLACP on the Ethernet Routing Switch 5500/5600 the switches will remove a link from service due to variations in the arrival time of VLACP messages (VLACP PDUs) from the far end. The issue may exist between the Ethernet Routing Switch 5500/5600 and Ethernet Routing Switch 8300/8600 when running short timers and default timeout interval of 3 time-outs. The Ethernet Routing Switch 5500/5600 switches maintain a rolling history of the last 3 received VLACP PDUs and calculate the time variance across and between these

VLACP messages. If the time variance of the last 3 VLACP PDUs falls outside predefined thresholds, the Ethernet Routing Switch 5500/5600 will remove the link from service.

As a workaround, customers should increase the VLACP timeout value from the default value of 3 to 5 or more. This will stop the Ethernet Routing Switch 5500/5600 switches from taking the link down due to the above mentioned variations in VLACP timing. It should be noted that even though the timeout value has been set to 5, due to the sampling function, if variance occurs outside the threshold for any 3 consecutive VLACP PDUs then the link will be removed from service until VLACP can re-establish a correctly timed communication. However, a value of 5 has been determined to be sufficient for this workaround.

Port or ifIndex offset issue

In the past, the SNMP ifIndex assumed that each unit had a maximum of 64 ports, so logical port 65 would be unit 2, port 1 in the stack. Now that Nortel offers 98 port units on the Ethernet Routing Switch 5600 Series, there are 128 logical port numbers for each unit. That means that port 129 is unit 2, port 1.

At the SNAS, for 6.0 stacks or switches, use **`switch_type ERS5500`**.

If you restart the switch or stack after the stack is up and stable, SNAS may display incorrect unit and port numbers with a 64 offset, instead of a 128 offset. This is only a display issue and the unit and port numbers are correct at the switch.

To correct the display at the SNAS, disable and enable the switch at the SNAS. The display now shows the correct unit and port numbers at the SNAS.

If your PCs have a connectivity issue, reset DHCP.

The next SNAS patch release will include the Ethernet Routing Switch 5600 Series option and will resolve this issue. (Q01949332)

Filter resource consumption

Various Ethernet Routing Switch 5000 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.

Table 9
Mask and filter requirements for applications

Application	Category	Masks required	Filters required
Ethernet Routing Switch 5500 Series			
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
QoS (trusted policy)	QoS	1	19
QoS (NTonNT)	QoS	1	4
IGMP	Non QoS	2	10
Port Mirroring (MAC-based)	Non QoS	2	2
EAP Authetication (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	17	17
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	3
OSPF	Non QoS	1	3
IP Source Guard	Non QoS	1	10
Ethernet Routing Switch 5600 Series			
Broadcast ARP and ARP Inspection	Non QoS	1	1

Application	Category	Masks required	Filters required
DHCP Relay or DHCP Snooping or NSNA DHCP	Non QoS	1	2
QoS (default untrusted policy)	QoS	2	2
QoS (DAPP with status tracking)	QoS	1	1
QoS (NTonNT)	QoS	1	4
Port Mirroring (MAC-based)	Non QoS	1	2
EAP Authetication (EAPoL packet filter)	Non QoS	1	2
IPFix	Non QoS	1	1
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	3
OSPF	Non QoS	1	3
IP Source Guard	Non QoS	1	11
PIM	Non QoS	1	1

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.

On the Ethernet Routing Switch 5600 Series switches, the resources are shared across group of ports. Each group of ports has 16 masks and 256 filters available for each mask. By default, the system statically consumes one mask and one filter for ARP filtering on all ports, leaving 15 available masks for each group and 256 available filters for each mask and group 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 5000 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.

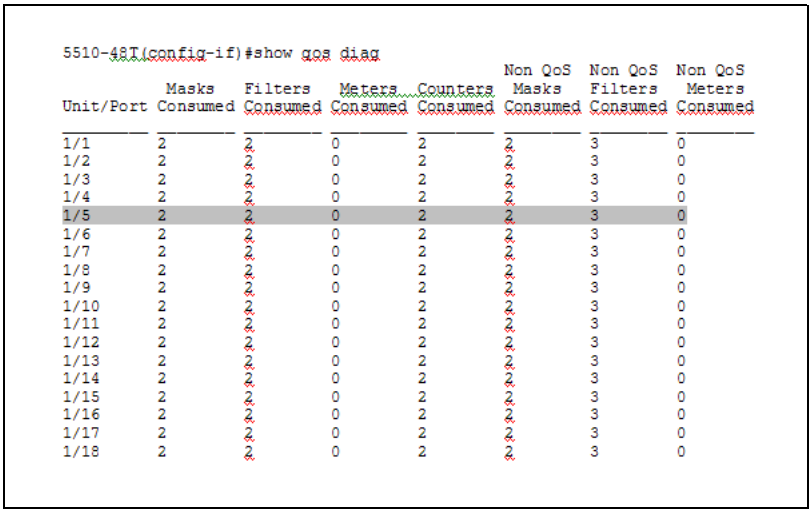
On the Ethernet Routing Switch 5500 Series switches, the available masks and filters available on a port can be determined by adding the total number of QoS and non QoS masks in use and the total number QoS and non QoS filters in use on a port and then subtracting that number from 16 masks and 128 filters, respectively.

On the Ethernet Routing Switch 5600 Series switches, the output of the **`show qos diag`** allows you to count the unused masks to determine the number of available masks for a particular port. The 5600 Series switches share resources across a group of ports. The filters used by QoS or non QoS applications on a port for a specific mask determine the available filters for that mask for all ports from that group.

On the Ethernet Routing Switch 5600 Series switches, you can determine the number of the filters available for a mask from a group of ports by adding the total number of QoS and Non QoS filters in use and subtracting that number from 256. If the number of filters in use for a mask is equal to 256, that mask cannot be used on other ports from the same group.

On the Ethernet Routing Switch 5500 Series switches, 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.

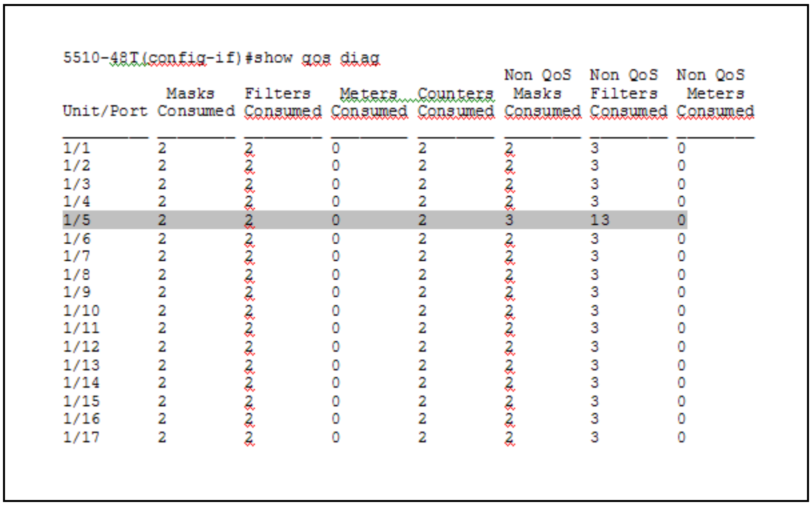
Figure 1
show qos diag before



```
5510-48T(config-if)#show qos diag
                                                Non QoS  Non QoS  Non QoS
           Masks    Filters   Meters   Counters  Masks    Filters   Meters
Unit/Port Consumed Consumed Consumed Consumed Consumed Consumed 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.

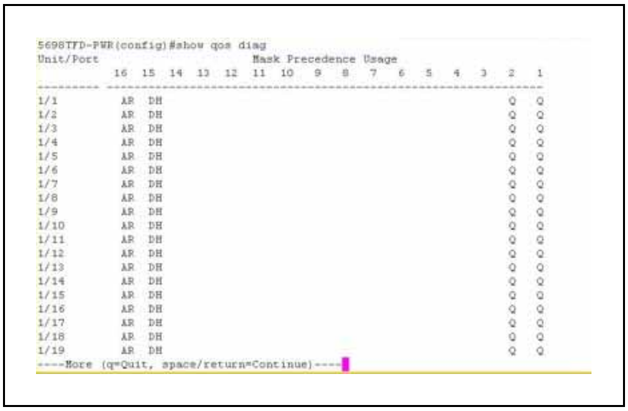
Figure 2
show qos diag after



```
5510-48T(config-if)#show qos diag
                                                Non QoS  Non QoS  Non QoS
           Masks    Filters   Meters   Counters  Masks    Filters   Meters
Unit/Port Consumed Consumed Consumed Consumed Consumed Consumed 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
```

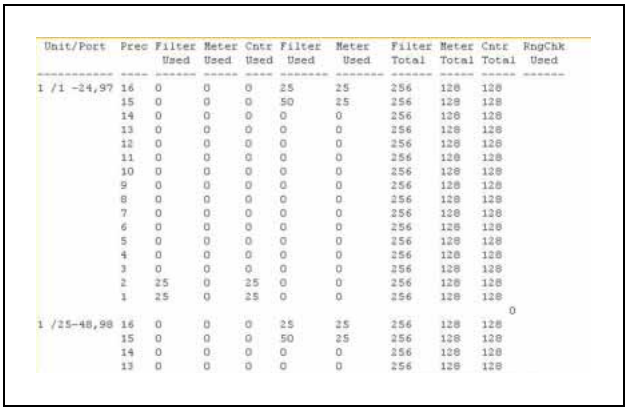
On the Ethernet Routing Switch 5600 Series switches, to enable IP Source Guard on a port requires 1 mask and 11 filters. To verify that IP Source Guard can be enabled on port 5, you can view the **`show qos diag`** output display and determine that port 5 is currently using a total of 4 masks (QoS plus non-QoS). IP Source Guard uses the next available mask and from the output display, you can see that there are 256 filters available for mask 14, which meets the IP Source Guard requirement of 1 mask and 11 filters. The following figures show the **`show qos diag`** display before enabling IP Source Guard on port 5.

Figure 3
show qos diag before



```
5698TFD-PWR(config)#show qos diag
Unit/Port                     Mask Precedence Usage
           16  15  14  13  12  11  10   9   8   7   6   5   4   3   2   1
---------- --------------------------------------------------------------
1/1        AR  DH                                                   Q   Q
1/2        AR  DH                                                   Q   Q
1/3        AR  DH                                                   Q   Q
1/4        AR  DH                                                   Q   Q
1/5        AR  DH                                                   Q   Q
1/6        AR  DH                                                   Q   Q
1/7        AR  DH                                                   Q   Q
1/8        AR  DH                                                   Q   Q
1/9        AR  DH                                                   Q   Q
1/10       AR  DH                                                   Q   Q
1/11       AR  DH                                                   Q   Q
1/12       AR  DH                                                   Q   Q
1/13       AR  DH                                                   Q   Q
1/14       AR  DH                                                   Q   Q
1/15       AR  DH                                                   Q   Q
1/16       AR  DH                                                   Q   Q
1/17       AR  DH                                                   Q   Q
1/18       AR  DH                                                   Q   Q
1/19       AR  DH                                                   Q   Q
----More (q=Quit, space/return=Continue)----
```

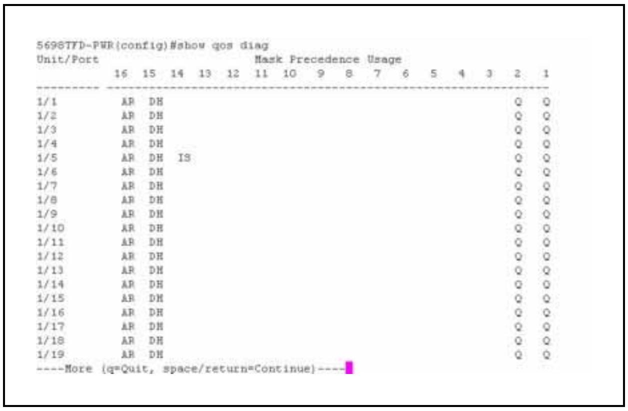
Figure 4
show qos diag before continued



```
Unit/Port   Prec Filter Meter Cntr Filter  Meter   Filter Meter Cntr  RngChk
                  Used   Used Used  Used    Used   Total  Total Total  Used
----------- ---- ------ ----- ---- ------- ------- ------ ----- ----- ------
1 /1 -24,97 16   0      0     0    25      25      256    128   128
            15   0      0     0    50      25      256    128   128
            14   0      0     0    0       0       256    128   128
            13   0      0     0    0       0       256    128   128
            12   0      0     0    0       0       256    128   128
            11   0      0     0    0       0       256    128   128
            10   0      0     0    0       0       256    128   128
            9    0      0     0    0       0       256    128   128
            8    0      0     0    0       0       256    128   128
            7    0      0     0    0       0       256    128   128
            6    0      0     0    0       0       256    128   128
            5    0      0     0    0       0       256    128   128
            4    0      0     0    0       0       256    128   128
            3    0      0     0    0       0       256    128   128
            2    25     0     25   0       0       256    128   128
            1    25     0     25   0       0       256    128   128
                                                                   0
1 /25-48,98 16   0      0     0    25      25      256    128   128
            15   0      0     0    50      25      256    128   128
            14   0      0     0    0       0       256    128   128
            13   0      0     0    0       0       256    128   128
```

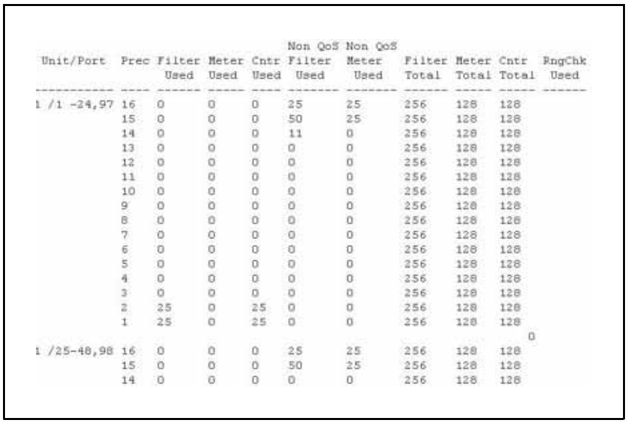
The following figures show the **`show qos diag`** display after enabling IP Source Guard on port 5.

Figure 5
show qos diag after



```
5698TFD-PWR(config)#show qos diag
Unit/Port                       Mask Precedence Usage
            16  15  14  13  12  11  10   9   8   7   6   5   4   3   2   1
--------- ----------------------------------------------------------------
1/1         AR  DH                                                   Q   Q
1/2         AR  DH                                                   Q   Q
1/3         AR  DH                                                   Q   Q
1/4         AR  DH                                                   Q   Q
1/5         AR  DH  IS                                               Q   Q
1/6         AR  DH                                                   Q   Q
1/7         AR  DH                                                   Q   Q
1/8         AR  DH                                                   Q   Q
1/9         AR  DH                                                   Q   Q
1/10        AR  DH                                                   Q   Q
1/11        AR  DH                                                   Q   Q
1/12        AR  DH                                                   Q   Q
1/13        AR  DH                                                   Q   Q
1/14        AR  DH                                                   Q   Q
1/15        AR  DH                                                   Q   Q
1/16        AR  DH                                                   Q   Q
1/17        AR  DH                                                   Q   Q
1/18        AR  DH                                                   Q   Q
1/19        AR  DH                                                   Q   Q
----More (q=Quit, space/return=Continue)----
```

Figure 6
show qos diag after continued



```
                                   Non QoS Non QoS
Unit/Port   Prec Filter Meter Cntr Filter  Meter   Filter Meter Cntr  RngChk
                  Used  Used  Used  Used    Used   Total  Total Total  Used
----------- ---- ------ ----- ---- ------- ------- ------ ----- ----- ------
1 /1 -24,97 16   0      0     0    25      25      256    128   128
            15   0      0     0    50      25      256    128   128
            14   0      0     0    11      0       256    128   128
            13   0      0     0    0       0       256    128   128
            12   0      0     0    0       0       256    128   128
            11   0      0     0    0       0       256    128   128
            10   0      0     0    0       0       256    128   128
            9    0      0     0    0       0       256    128   128
            8    0      0     0    0       0       256    128   128
            7    0      0     0    0       0       256    128   128
            6    0      0     0    0       0       256    128   128
            5    0      0     0    0       0       256    128   128
            4    0      0     0    0       0       256    128   128
            3    0      0     0    0       0       256    128   128
            2    25     0     25   0       0       256    128   128
            1    25     0     25   0       0       256    128   128
                                                                   0
1 /25-48,98 16   0      0     0    25      25      256    128   128
            15   0      0     0    50      25      256    128   128
            14   0      0     0    0       0       256    128   128
```

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.

This application only runs on the Ethernet Routing Switch 5500 Series switches.

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

Table 10
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
QoS BPDU blocker interface	1	1

Nortel Ethernet Routing Switch 5000 Series

Release Notes — Release 6.0

Publication: NN47200-400
Document status: Standard
Document version: 04.01
Document date: 12 December 2008

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.