Nortel Ethernet Routing Switch 5500 Series

Ethernet Routing Switch 5500 Series: Release Notes for Software Release 5.0.3

ATTENTION

Clicking on a PDF hyperlink takes you to the appropriate page. If necessary, scroll up or down the page to see the beginning of the referenced section.

NN47200-402 (323079-B)

Document status: Standard
Document version: 01.01
Document date: 30 October 2006

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

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

Trademarks

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

Restricted rights legend

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

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

Statement of conditions

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

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

Nortel Networks 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 MERCHANTABLITITY 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 foregoing 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

Context and topics

The 5500 Series Software Release 5.0.3 has been developed to provide support for Nortel Secure Network Access Solution (SNAS) Release 1.5 and supplants the previously released Software Release 5.0.2.

These release notes provide complete coverage of all information required to configure and manage Nortel Secure Network Access Solution (SNAS) Release 1.5 on the Nortel Ethernet Routing Switch 5500 Series. No other documents are provided or required. All other topics pertaining to the configuration and management of the Nortel Ethernet Routing Switch 5500 Series can be found in the Software Release 5.0 documentation. Refer to "Related Publications" (page 15) for a complete list of documents.

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

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

The following topics are discussed in this document:

- "Configuring Nortel Secure Network Access using the CLI" (page 35)
- "Configuring Nortel Secure Network Access using Device Manager" (page 49)

This guide provides information and instructions on the configuration and management of security on the 5500 Series Nortel Ethernet Routing Switch. Please consult any documentation included with the switch and the product release notes (see "Related Publications" (page 15)) for any errata before beginning the configuration process.

New software features in Software Release 5.0.3

The configuration and management of the Nortel SNAS 1.0 was originally documented in **Ethernet Routing Switch 5500 Series: Configuring and Managing Security (NN47200-501)**. This document devotes the following three chapters to this topic:

- **Implementing the Nortel Secure Network Access Solution**
- **Configuring Nortel Secure Network Access using the CLI**
- **Configuring Nortel Secure Network Access using the Device Manager**

These chapters are repeated in these release notes with updated information relating to the Nortel SNAS 1.5 release. Support for the 1.5 release is the only significant difference between Software Release 5.0 and 5.0.3. To move to these updated chapters, select one of the following:

- "Implementing the Nortel Secure Network Access solution" (page 19)
- "Configuring Nortel Secure Network Access using the CLI" (page 35)
- "Configuring Nortel Secure Network Access using Device Manager" (page 49)

Issues that have been resolved in this release can be found in "Issues resolved in Release 5.0.3" (page 11). Known issues and limitations of this release can be found in "Known limitations and considerations in Release 5.0.3" (page 12).

New software features in Nortel SNAS 1.5

The Nortel SNAS 1.5 release includes the following new features:

- **Performance and scalability enhancements**
  - — Up to four Nortel SNAS 4050 control points can be configured in a cluster to provide support for up to 8,000 concurrent users.
- **Hub support**

— Nortel SNAS now supports multiple devices on one port.

- **Non-SSCP platform support**

  — Nortel SNAS no longer requires the network access device to support the Switch-SNAS Communication Protocol (SSCP). The Nortel SNAS 4050 can be configured to operate with all Nortel Ethernet Switch and Ethernet Routing Switch products as well as third-party switches.

- **WLAN Controller support**

  — The Nortel SNAS 4050 can now interoperate with WLAN Controllers.

- **TunnelGuard Run-Once and Non-Continuous Agent**

  — Tunnel Guard now includes a Run-Once Java agent. After an endpoint has successfully transitioned to the GREEN zone, the Java agent is shut down. The endpoint is trusted for the duration of the session or until the endpoint is disconnected from the network.

- **Support for Mac OS X, Linux, and non-interactive devices**

  — Nortel SNAS now supports the authentication of devices running Mac OS X, Linux, and passive devices such as printers and video cameras.

- **MAC address policy service**

  — The Nortel SNAS 4050 now supports a MAC database to provide MAC-based authentication.

- **Flexible deployment**

  — An enforcement type that requires only filters has been added. With the new *filters_only* enforcement type, all ports remain in the Red VLAN and the Red, Yellow, and Green filters are applied to the ports there. With the *VLAN and filters* enforcement type, ports are assigned to the Red, Yellow, or Green VLAN and the Red, Yellow, or Green filters are applied to the ports when they are in the corresponding VLAN.

For information on the Nortel SNAS Release 1.5, see *Release Notes for Nortel Secure Network Access Solution Release 1.5 (NN47230-400).*

File names for 5500 Series Release 5.0.3

The following table describes the Ethernet Routing Switch 5500 Series Release 5.0.3 software files. File sizes are approximate.

Software Release 5.0.3 components

Module or file type	Description	File name	File size (bytes)
Runtime image software version	Switch agent software	5530_503005s.img	5 594 860
Boot/diagnostic software version	Switch diagnostic software	5530_500002_diag.bin	811 860
Java Device Manager software version for Windows	Device Manager software image for Windows NT, Windows XP, Windows 2003, Windows 2000	jdm_6020.exe	141 559 337
Java Device Manager software version for UNIX	Device Manager software image for Solaris	jdm_6020_solaris_sparc.sh	167 069 058
Java Device Manager software version for HP Unix	Device Manager software image for HP-UX	jdm_6020_hpux_pa-risc.sh	182 404 482
Java Device Manager software version for Linux	Device Manager software image for Linux	jdm_6020_linux.sh	167 658 882
Software Release 5.0.3 Management Information Base (MIB) definition files	MIB definition files	Ethernet_Routing_Switch_5510_MIBs_v5.0.2.003.zip	824 732
Software Release 5.0.3 Management Information Base (MIB) definition files	MIB definition files	Ethernet_Routing_Switch_5520_MIBs_v5.0.2.003.zip	824 964
Software Release 5.0.3 Management Information Base (MIB) definition files	MIB definition files	Ethernet_Routing_Switch_5530_MIBs_v5.0.2.003.zip	824 732

Displaying Device Manager online help

Nortel currently supports only Internet Explorer and Netscape as platforms for the display of Device Manager online help. To ensure that help topics and table of contents are displayed correctly in Netscape, the following procedure must be performed once before using the Device Manager help system:

1. Start Netscape.

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.

Issues resolved in Release 5.0.3

The following table lists the Nortel SNAS-related issues that have been resolved in Software Release 5.0.3. Issues marked as ***N/A*** in the **Workaround** column have been fixed in code.

Issues resolved in Release 5.0.3

Issue	Workaround	Change Request (CR) Reference
If a PC is moved to a different port and a renew operation is performed, the PC IP address reverts to 0.0.0.0 and the VLAN reverts to 1.	Execute the commands **`ipconfig /release`** and **`ipconfig /renew`** in the PC's command prompt.	Q01228894
After 5 attempts to download an incorrect DSA Authorization Key file from the CLI, unexpected switch behaviors occur. For example, a Telnet or SSH session cannot be opened or another host cannot be pinged.	N/A	Q01231314
Restrict disable MLT uplink is not valid. Multiple Uplinks are allowed in this release.	N/A	Q01256947
The switch sometimes returns error messages such as:*mRouteEntryDelete failed*, *panic: netJobAdd: ring buffer overflow!*, and *fe_procMod*. These are informational only and do not affect functionality.	N/A	Q01395633, Q01395963

The EAPoL operational traffic control value is not automatically refreshed when the EAPoL administrative traffic control is modified.	Perform a manual refresh by pressing CNTL+W on the keyboard.	Q01420608
When Nortel IP phone sets are connected to LLDP-enabled ports on a switch running Software Release 5.0, a memory leak can adversely affect switch performance.	N/A	Q01467048
Multicast packets can be lost on switches running Software Release 5.0 when an MLT link is lost and then recovers.	N/A	Q01463244
A memory leak is present in switches running Software Release 5.0 when EAP-enabled ports are disabled.	N/A	Q01466336
A memory leak is present in switches running Software Release 5.0 when a port with LLDP Configuration Notification enabled is disabled.	N/A	Q01469602

Known limitations and considerations in Release 5.0.3

The following table describes all known limitations and all discovered issues related to Software Release 5.0.3. You can refer to the Ethernet Routing Switch 5500 Series Release 5.0 Release Notes for issues specific to the ERS 5500.

Issue	**Change Request (CR) Reference**
A BPDU blocker configured with STG2 does not work after reboot.	Q01459111
Due to CLI restrictions an uplink port can only be entered in a limited number of VLANs.	Q01185566
If you disable and re-enable NSNA, you cannot authenticate PCs with green or yellow IP addresses in the red VLAN.	Q01186169
If you enable NSNA on a stack of 6 switches where all ports are dynamic, the console locks for 2 minutes.	Q01217035
The CLI command **`nsna port dyn/up`** fails if VLAN membership differs from the existing port.	Q01249003

Issue	Change Request (CR) Reference
In a stack of 8 switches, when you perform a reset and power off the unit or reset the stack, red clients cannot log in for 5 minutes.	Q01252555
Even when the phone signature is deleted, phones can obtain an IP address and connect to a call server.	Q01265045
You cannot disable LACP on NSNA uplink ports.	Q01309758
If UDP forwarding is applied and used close to maximum capacity, NSNA fails.	Q01319058
If you perform a TDR on the dynamic port, the PC disappears from the NSNA clients list.	Q01324425
The NSNAS does not differentiate between DHCP and Static IP-based passive devices. This can affect the output for the device on the network access device (edge switch), since the network access device gets information about the device (the IP address, for example) from the NSNAS.	Q01353509
If you have a dynamic device connected behind an IP phone with NSNA configured and enabled, and you change that device to a static IP and update the MAC database with this information, whether you disable/enable or unplug/plug the device, the MAC authorization does not work.	Q01362768
If you enable NSNA on a Brouter port, the port is not added to the red VLAN.	Q01366773
If you remove devices from the network and plug in new devices in those locations before the aging out period expires, the new devices are assigned an IP address, although the IP address may show up in the client list (show nsna client) as 0.0.0.0.	Q01369969
Dynamic passive devices that redo DHCP may be displayed as a PC.	Q01370981
When unplugging a device, Nortel recommends waiting 10 seconds before reconnecting the device.	Q01377725
Note that more Link Aggregation Groups (LAG) than are actually configured can be displayed on the switch console (show mlt) if one side of a group is a stack, and you power down all switches in the stack except the Base Unit (BU).	Q01409456
If you have MLTs configured, and you also configure MAC security, after you reboot the switch/stack, all traffic may be filtered -- even the traffic for MAC addresses that appear in the MAC Address Security Table (that is, learned MAC addresses). Nortel recommends that you avoid using Mac Security with MLT.	Q01413693
If a port on a 5510 is a member of a Layer 2 VLAN that has "unknown-mcast-no-flood" enabled, and there is multicast traffic to a MAC address that is configured as "unknown-mcast-allow-flood" on that VLAN, the traffic actually floods to all Layer 2 VLANs configured on that switch. This is a limitation of the Ethernet Routing Switch 5510 only.	Q01414703
Nortel recommends that the DHCP lease time for phones be set to at least 24 hours.	Q01415725

Issue	Change Request (CR) Reference
Wait at least 20 seconds after NSNA is fully configured before resetting the units. If you configure and enable NSNA on a stack, and then reboot the stack, units may leave the stack.	Q01416550
If you use an external power supply to connect an IP phone to the switch and then disconnect the phone, Nortel recommends that you reset the phone.	Q01418054
The MAC address MIB is not updated with intruder MACs on the 25-28 NBU ports of a 5510-24T and on the 27-48 NBU ports of a 5530 when either are used as BU.	Q01418935
When DHCP Snooping and ARP Inspection are implemented, console response on non-base units becomes very slow and, if the stack is rebooted, some units may not boot.	Q01421889
5500 Series ERSs are guaranteed to support up to 512 RIP routes. The actual upper limit on the number of RIP routes appears to be over 1200. If the upper limit on the number of RIP routes is exceeded, SNMP, Telnet, Web, and TFTP connections can go down. PING continues to work.	Q01423396
Clients are unable to authenticate if there is a delay of more than 1 minute in initialization because the operating system defaults to the local IP address.	Q01424744
If using DHCP relay on multiple hops, Nortel recommends that you configure the DHCP forward path on all hops to the DHCP server.	Q01440362
Nortel recommends that you do not remove a USB drive while the system is reading or writing to it.	Q01444863
When downloading a new image the following error message may appear, *Error reading image file.* Retry the download.	Q01445124
When using the Linux operating system you may have to manually link up then down to get the Linux PC to authenticate during a service network restart.	Q01446226
The total number of allowed EAP and non-EAP MACs must not exceed 32.	Q01446613
Do not administratively disable port mirrored ports in MSTP mode.	Q01452496
If you access the Device Manager Help for NSNA VLANs, the following message appears: Attention VLANs that you plan to configure as Nortel SNA VLANs must be empty (that is, they have no port members assigned). Ethernet Routing Switch 5500 Series, Software Release 5.0 does not support static devices, therefore you cannot assign ports manually to NSNA VLANs (all ports must be dynamic). Printers and static devices must be in non-NSNA VLANs. Nortel SNA VLANs cannot be associated with non-Nortel SNA ports. Disregard this message. In Release 5.0.3 VLANs that you plan to configure as Nortel SNA VLANs must be empty (that is, they have no port members assigned). Nortel SNA VLANs cannot be associated with non-Nortel SNA ports; therefore you cannot assign non-NSNA ports manually to enabled NSNA VLANs. Dumb and static devices that cannot authenticate	Q01458686

Issue	Change Request (CR) Reference
through Tunnel Guard can be connected to NSNA dynamic ports. In order to have network access their MAC addresses should be added in SNAS MAC database.	
Do not set an authentication password for OSPF on the Ethernet Routing Switch 5530 10 gigabit ports.	Q01464731
If additional VLANs are required on an existing uplink port, Nortel recommends that you disable NSNA on the uplink ports, using **`config-if# no nsna port x`** ,and reconfigure all of the VLANs on the uplink port.	Q01467244
The **`show ip ospf host-route`** command is not supported in this release.	Q01467398
After the system experiences a power cycle, the switch may lose its configuration. Nortel recommends that you issue the shutdown command before a power cycle.	Q01467410
When configuring a yellow filter for NSNA, if a subnet is specified, traffic will be restricted to that subnet; if no subnet is specified, the port will be open for all traffic.	Q01468284
If you configure many NSNA filters in large stacks while NSNA is enabled, the configuration may take longer than expected and may fail. Nortel recommends that you disable NSNA before configuring a large number of filters. After you have configured the filters, perform a global re-enable for NSNA.	Q01469177

Related Publications

For more information about the management, configuration, and usage of the Nortel Ethernet Routing Switch 5500 Series, refer to the publications listed in "Nortel Ethernet Routing Switch 5500 Series Documentation" (page 15).

Nortel Ethernet Routing Switch 5500 Series Documentation

Title	Description	Part Number
Nortel Ethernet Routing Switch 5500 Series Installation	Instructions for the installation of a switch in the Nortel Ethernet Routing Switch 5500 Series. It also provides an overview of hardware key to the installation, configuration, and maintenance of the switch.	NN47200-300

Title	Description	Part Number
Nortel Ethernet Routing Switch 5500 Series Overview - System Configuration	Instructions for the general configuration of switches in the 5500 Series that are not covered by the other documentation.	NN47200-500
Nortel Ethernet Routing Switch 5500 Series Security - Configuration	Instructions for the configuration and management of security for switches in the 5500 Series.	NN47200-501
Nortel Ethernet Routing Switch 5500 Series Configuration - VLANs, Spanning Tree, and MultiLink Trunking	Instructions for the configuration of spanning and trunking protocols on 5500 Series switches	NN47200-502
Nortel Ethernet Routing Switch 5500 Series Configuration - IP Routing Protocols	Instructions on the configuration of IP routing protocols on 5500 Series switches.	NN47200-503
Nortel Ethernet Routing Switch 5500 Series Configuration - Quality of Service	Instructions on the configuration and implementation of QoS on 5500 Series switches.	NN47200-504
Nortel Ethernet Routing Switch 5500 Series Configuration - System Monitoring	Instructions on the configuration, implementation, and usage of system monitoring on 5500 Series switches.	NN47200-505
Nortel Ethernet Routing Switch 5500 Series Release Notes - Software Release 5.0	Provides an overview of new features, fixes, and limitations of the 5500 Series switches. Also included are any supplementary documentation and document errata.	NN47200-400
Installing the Nortel Ethernet Redundant Power Supply Unit 15	Instructions for the installation and usage of the Nortel Ethernet RPSU 15.	217070-A
DC-DC Converter Module for the Baystack 5000 Series Switch	Instructions for the installation and usage of the DC-DC power converter.	215081-A
Installing SFP and XFP Transceivers and GBICs	Instructions for the installation and usage of small form-factor pluggable transceivers and gigabit interface converters.	318034-C

How to get help

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

Getting help from the Nortel web site

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

http://www.nortel.com/support

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

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

Getting help over the phone from a Nortel Solutions Center

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

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

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

http://www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

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

http://www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Implementing the Nortel Secure Network Access solution

This chapter includes the following topics:

Overview

The Nortel Ethernet Routing Switch 5500 Series can be configured as a network access device for the Nortel Secure Network Access (Nortel SNA) solution. The ERS 5500 Series is referred to as an NSNA network access device in the context of the Nortel SNA solution.

Host computers can connect using dynamic or static IP addressing. Windows, MacOSX, and Linux operating systems are supported. Access to the corporate network requires successful:

- authentication (username/password or MAC address)
- host integrity check and remediation (as needed and when configured)

Access to the network proceeds as follows:

1. Three enforcement zones - Red, Yellow, and Green - provide layered access to the corporate network. Connection requests are directed to a specific zone based on filter sets that are predefined on NSNA network access devices. The Red, Yellow, and Green enforcement zones can be configured using the filter sets in conjunction with unique VLANs for each zone, or by using the filter sets within a single (Red) VLAN. You can customize the filter sets, if necessary.
2. Initial connection requests are directed to the Red zone. The default Nortel SNA Red filter set allows access only to the Nortel SNAS 4050 and the Windows domain controller (or other network log on controller, for example, Novell netware log on). The connection remains in the Red zone pending successful authentication. Either the MAC address

of the host or a username/password of the end user can be used for authentication.

3. After successful authentication, a security agent, the TunnelGuard applet, provides host integrity checking. TunnelGuard can be configured to run once, continuously, or never. Integrity checking is performed on hosts that support Windows operating systems when TunnelGuard is set to run once or continuously.
4. If the TunnelGuard applet determines that the host does not meet the required integrity criteria, the host is placed in the Yellow zone. The Yellow zone provides access to the remediation network only.
5. If the host passes authentication, and integrity checking when configured, the connection is transferred to the Green zone. This provides the user with full access to the network, depending on the user profile.

Nortel IP phones are supported under the Nortel SNA solution though they are not required to pass authentication and integrity checking. Nortel IP phones are provided access to a preconfigured VoIP subnet, and are allowed a prespecified type of communication. The VoIP filters are such that they do not allow the VoIP traffic to go anywhere except to a specific subnet. This subnet is specified by the VoIP VLAN.

For more information about the Nortel SNA solution and deployment scenarios, refer to *Nortel Secure Network Access Solution Guide (320817-A)*. For information about configuring the Nortel SNAS 4050, refer to *Nortel Secure Network Access Switch 4050 User Guide (320818-A)*.

For information about configuring the Nortel Ethernet Routing Switch 5500 Series for the Nortel SNA solution using the CLI, see Configuring Nortel Secure Network Access using the CLI. For information about configuring the Nortel Ethernet Routing Switch 5500 Series for the Nortel SNA solution using Java Device Manager, see Configuring Nortel Secure Network Access using Device Manager.

Port modes

Nortel supports the following four modes of operation on a port:

- Default mode

  In this mode, the switch port does not have any user-based security (for example, 802.1x/EAP or Nortel SNA). You can, however, configure MAC-based security on these ports.

- 802.1x (client mode - that is, the 802.1 supplicant is present)

In this mode, the user is authenticated by EAP using an external authentication server, such as a RADIUS server. In this scenario, there is a client (for example, the EAP supplicant) present in the PC.

- Nortel SNA dynamic IP mode - Dynamic IP mode provides authentication by username/password or MAC address and host integrity checking by the TunnelGuard applet. Prior knowledge of the client PC is not required on the switch, and the client does not require any preinstalled software to operate in the Nortel SNA solution.

  Note: The Spanning Tree Protocol (STP) state of the dynamic Nortel SNA ports is set automatically when the edge switch boots in Rapid Spanning Tree Protocol or Multiple Spanning Tree Protocol (RSTP/MSTP) mode.

- Nortel SNA passive IP mode - Passive IP mode allows Nortel SNA to authenticate printers, fax machines, and other device where interactive communications with the SNAS 4050 are not normally available. This mode requires that the MAC address of the host client is registered in the Nortel SNAS 4050 MAC database. Authentication is based on the MAC address but is independent of the type of host. Security can be enhanced beyond the MAC address by specifying optional fields, including user name, switch unit, and switch port. Host integrity checking is not available with passive IP mode.

  Note: It is technically possible to configure ports in different modes within the same switch. However, a single port cannot be configured into multiple modes (for example, Nortel SNA and 802.1x are currently mutually incompatible).

Filters in the Nortel SNA solution

A corresponding Nortel SNA filter set is provisioned for Nortel SNA Red, Yellow, and Green enforcement zones. Nortel recommends that you use the default filter sets. You can, however, create customized filter sets and assign these to the Nortel SNA VLAN(s). You can also modify the default filters after you have enabled them and assigned them to the Nortel SNA VLAN(s).

For information about modifying the filter sets, see *Nortel Ethernet Routing Switch 5500 Series Configuration - Quality of Service (NN47200-504)* . For an example of the current default Nortel SNA filter set rules, see Default Nortel SNA filters.

Note: When the Nortel SNA filters are applied to a port, any existing QoS filters on that port are disabled, and the Nortel SNA filters are applied (pre-existing policies are re-enabled when Nortel SNA is disabled). See "Rolling back Nortel SNA mode to default mode" (page 33) and "Deploying the Nortel SNA solution in an active network" (page 31) for more information.

You can configure the Nortel SNA filters manually if, for example, you have specific parameters or proprietary applications.

In certain configurations, workstation boot processes depend on specific network communications. System startup can be negatively impacted if certain network communications are blocked by the initial Red filters. Ensure you are aware of which communications are required for system boot and user authentication prior to the Nortel SNA log on.

If you must configure filters manually to best address your circumstances, Nortel recommends that you use the default filters as your template. Manually configured custom filters must be included in the Nortel SNA filter set.

> ***Note:*** Nortel does not support Nortel SNA filter sets and non-Nortel SNA filter sets coexisting on Nortel SNA ports.

Red, Yellow, and Green VLANs must be configured on the Nortel SNA uplink ports of the NSNA network access device when the NSNA filters sets for each enforcement zone are assigned to specific VLANs. When only the filters sets are used, then a Red VLAN must be configured on the Nortel SNA uplink ports. To configure the uplink ports, use **`nsna port <portlist> uplink vlans <vidlist>`** (see Enabling Nortel SNA on ports). Only Nortel SNA ports (uplink or dynamic) can be in the Red, Yellow, Green, and VoIP VLANs. Nortel SNA ports become members of the Nortel SNA VLAN(s) when Nortel SNA is enabled. Manually attaching dynamic Nortel SNA ports to a non-Nortel SNA VLAN is not allowed.

Uplink ports can be members of non-Nortel SNA vlans.

The Nortel SNA software puts all user ports (dynamic NSNAports) in the Red, Yellow, or Green state dynamically. When the switch initially comes up, all Nortel SNA ports are moved to the Red state with Red filters attached.

The uplinks can be tagged or untagged. A typical uplink on the edge switch is one or more MLTs connected to two core Ethernet Routing Switches 8600 (to provide redundancy). The core routing switches implement SMLT, but that is transparent to the edge switch. In Layer 2, the Nortel SNA uplink is always tagged. In Layer 3, the uplink can be tagged or untagged (but you do not have to set that port as Nortel SNA uplink it is just an uplink to the router).

> ***Note:*** Nortel recommends that you set the Nortel SNA uplink port STP to either Fast Learning or disabled.

The Red, Yellow, and Green VLANs can be Layer 2 or Layer 3 (see "Topologies" (page 26) for more information).

You must have one, and only one, Red VLAN on each switch. You can, however, have multiple Yellow, Green, and VoIP VLANs on each switch.

Note: With Ethernet Routing Switch 5500 Series, Software Release 5.0.3, each switch can support five Yellow VLANs, five Green VLANs, and five VoIP VLANs.

The VoIP filters are part of the Red and Yellow filters by default, but you can define a separate set of VoIP filters (with different VoIP policing values), if necessary. In the Green enforcement zone, all traffic is allowed by the default filter, therefore VoIP filters are not specifically added.

You can create multiple Yellow and Green VLANs, as well as multiple VoIP filter sets. When you create the Red, Yellow, and Green VLANs, you attach the Red, Yellow, and Green filters (and a set of VoIP filters to the new Red and Yellow VLANs). For example, when the Nortel SNA software adds a port to the Yellow VLAN, it installs the Yellow filters and the VoIP filters that you attached to the Yellow VLAN.

Note: Manual configuration of filters is optional. If filters are not manually configured prior to configuring the Nortel SNA VLANs, the switch automatically generates default filters when you configure the Red, Yellow, Green, and VoIP VLANs.

The devices that connect to a Nortel SNA port can be DHCP PCs and dumb devices as well as static PCs and dumb devices. In order to have Green access, the MAC of the dumb device should be added to SNAS MAC address data base.

The following table shows filter consumption when using the default Nortel SNA filters.

Default Nortel SNA filter consumption

Filter set	Filters consumed	Precedence levels consumed
Red	5, plus 2 filters for each VoIP VLAN configured	3, *plus 1 precedence level for VoIP VLANs
Yellow	6, plus 2 filters for each VoIP VLAN configured	4, *plus 1 precedence level for VoIP VLANs
*Although each additional VoIP VLAN consumes two more filters, no additional precedence levels are consumed (that is, the first VoIP VLAN consumes one precedence level, but additional VoIP VLANs do not consume any more precedence levels).		

Filter parameters

Note: If you plan to use the default filters, it is not necessary to configure any filters before enabling Nortel SNA.

The default Nortel SNA filters protect the workstations. For a detailed listing of the parameters in the default filter sets, see Default Nortel SNA filters.

The following table describes the traffic allowed by each default Nortel SNA filter set.

Traffic allowed in the default Nortel SNA filter sets

Filter set	Traffic type								
	DNS	HTTP	HTTPS	ARP	DHCP	UDP	ICMP	Yellow subnet	All
*Red	Traffic to Nortel SNAS 4050 allowed	Traffic to Nortel SNAS 4050 allowed	Traffic to Nortel SNAS 4050 allowed	Yes	Yes		Yes		
Yellow	Traffic to Nortel SNAS 4050 allowed	Traffic to Nortel SNAS 4050 allowed	Traffic to Nortel SNAS 4050 allowed	Yes	Yes		Yes	Yes	
Green					Yes				Yes
VoIP				Yes	Yes	Yes	Yes		

* Note: Nortel recommends that you use filters to allow all traffic to your WINS domain controller in the Red VLAN. You must specify a destination IP address for all WINS domain controllers. For example, if you have two WINS domain controllers, use the following two commands:

```
qos nsna classifier name <Red VLAN name> dst-ip <win1-ipaddr/mask>
ethertype 0x0800 drop-action disable block wins-prim-sec eval-order 70

qos nsna classifier name <Red VLAN name> dst-ip <win2-ipaddr/mask>
ethertype 0x0800 drop-action disable block wins-prim-sec eval-order 71
```

Note that adding these two filters consumes another precedence level.

Refer to "Configuring filters for Novell Netware log on" (page 25) for information about configuring the filters for Novell Netware log on. If you use any other log on controller, you must modify the filter set to allow the log on to work

Note: In the Yellow VLAN, the default filters allow all IP traffic for the Yellow subnet. You specify the Yellow subnet in the command **`nsna vlan <vid> color yellow filter <filter name> yellow-subnet <ipaddr/mask>`** (see Configuring Nortel SNA per VLAN .

You can enter the remediation server IP/subnet as the Yellow subnet IP.

You can also add multiple IP addresses manually in the Yellow filter set. For example:

```
qos nsna classifier name ALPHAYELLOW dst-ip
10.80.22.25/32 ethertype 0x0800 drop-action disable
block remedial eval-order 70

qos nsna classifier name ALPHAYELLOW dst-ip
10.16.50.30/32 ethertype 0x0800 drop-action disable
block remedial eval-order 71

qos nsna classifier name ALPHAYELLOW dst-ip
10.81.2.21/32 ethertype 0x0800 drop-action disable
block remedial eval-order 72
```

Refer to *Nortel Ethernet Routing Switch 5500 Series Configuration - Quality of Service* (NN47200-504) for more information about the **qos nsna** commands.

Selective broadcast is allowed by the Red default filter set (DHCP broadcast (response) coming in on the uplink port goes out on the relevant Nortel SNA port only).

A rate-limiting rule applies to the Red filter set (committed rate = 1000 Kbps).

Configuring filters for Novell Netware log on If you use Novell Netware as your domain log on, the following is one example of IPX filters for the Red VLAN. Note that these filters require additional modification based on your specific configuration (the filter set name in this example is red; modify the command to use your actual Red filter set name):

```
qos nsna classifier name red protocol 17 dst-port-min 427
dst-port-max 427 ethertype 0x0800 drop-action disable block
novell eval-order 101

qos nsna classifier name red protocol 6 dst-port-min 524
dst-port-max 524 ethertype 0x0800 drop-action disable block
novell eval-order 102

qos nsna classifier name red protocol 6 dst-port-min 396
dst-port-max 396 ethertype 0x0800 drop-action disable block
novell eval-order 103

qos nsna classifier name red protocol 17 dst-port-min 396
dst-port-max 396 ethertype 0x0800 drop-action disable block
novell eval-order 104

qos nsna classifier name red protocol 6 dst-port-min 1366
dst-port-max 1366 ethertype 0x0800 drop-action disable block
novell eval-order 105
```

```
qos nsna classifier name red protocol 17 dst-port-min 1366
dst-port-max 1366 ethertype 0x0800 drop-action disable block
novell eval-order 106

qos nsna classifier name red protocol 6 dst-port-min 1416
dst-port-max 1416 ethertype 0x0800 drop-action disable block
novell eval-order 107

qos nsna classifier name red protocol 17 dst-port-min 1416
dst-port-max 1416 ethertype 0x0800 drop-action disable block
novell eval-order 108

qos nsna classifier name red protocol 6 dst-port-min 686
dst-port-max 686 ethertype 0x0800 drop-action disable block
novell eval-order 109

qos nsna classifier name red protocol 6 dst-port-min 389
dst-port-max 389 ethertype 0x0800 drop-action disable block
novell eval-order 110
```

If you want to open traffic to specific IP addresses (for example, IP address 1 - IP address 6), use the following commands:

```
qos nsna classifier name red dst-ip <ipaddr1> ethertype
0x0800 drop-action disable block novell-ips eval-order 111

qos nsna classifier name red dst-ip <ipaddr2> ethertype
0x0800 drop-action disable block novell-ips eval-order 112

qos nsna classifier name red dst-ip <ipaddr3> ethertype
0x0800 drop-action disable block novell-ips eval-order 113

qos nsna classifier name red dst-ip <ipaddr4> ethertype
0x0800 drop-action disable block novell-ips eval-order 114

qos nsna classifier name red dst-ip <ipaddr5> ethertype
0x0800 drop-action disable block novell-ips eval-order 115

qos nsna classifier name red dst-ip <ipaddr6> ethertype
0x0800 drop-action disable block novell-ips eval-order 116
```

Topologies

You can configure the Ethernet Routing Switch 5500 Series to function in either Layer 2 or Layer 3 for the Nortel SNA solution. In Layer 2, routing is disabled in the Nortel Ethernet Routing Switch 5500 Series switch. In Layer 3, routing is enabled in the switch.

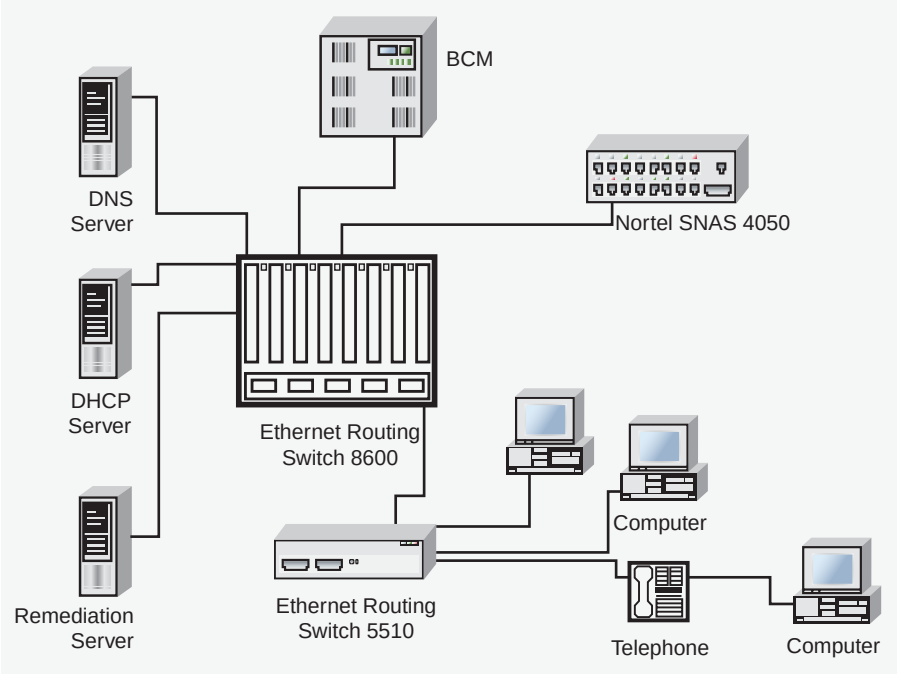
Layer 2

In Layer 2 mode, DHCP-relay is done on a central router or routing switch. The following figure shows a network where the Ethernet Routing Switch 8600 is the core routing device. The Ethernet Routing Switch 5510, the network access device in this case, functions in Layer 2 mode. All Nortel SNA VLANs (Red, Yellow, Green, and VoIP) are Layer 2.

There is a tagged uplink between the network access device and the routing device. You must configure this link as a Nortel SNA uplink port and specify all VLANs (Nortel SNA or non-Nortel SNA) in which it must be placed. When you do this, it is automatically tagged. This link can be MLT or LACP. You can configure multiple Nortel SNA uplink ports on the switch.

MLTs and LAGs must be configured before NSNA is globally enabled. After you globally enable NSNA, you cannot disable the MLT or LAG.

Network access device - Layer 2 mode



Layer 3

In Layer 3 mode, DHCP-relay is enabled on the Nortel Ethernet Routing Switch 5500 Series switch. In the network setup shown, the Ethernet Routing Switch 5510 can function in Layer 3 mode. The VLANs on the network access device are Layer 3 VLANs. The servers and Nortel SNAS 4050 are connected to the routing device. In this scenario, there is a tagged/untagged link between the Nortel Ethernet Routing Switch 5500 Series and the routing device, but you do not have to mark this link as an uplink port (that is, you do not need to specify any port as a Nortel SNA uplink while the switch is in Layer 3 mode).

Basic switch configuration for Nortel SNA

Note: Nortel recommends that you configure the core routing device, if it exists in your network, before you configure the network access device.

Before you begin

Before you begin configuration of the network access device, ensure you complete the following:

- Generate the SSH keys on the Nortel SNAS 4050, and upload the public key to a TFTP server.
- Identify the Nortel SNAS 4050 portal Virtual IP address (pVIP) and mask.
- Identify VLAN IDs for Nortel SNA use (that is, for Red and VoIP VLANs; plus Yellow and Green when enforcement zones are configured with VLANs and filters).
- Identify ports to use for uplink ports (in Layer 2 mode only).
- Identify ports to use for Nortel SNA client ports.

Note: Nortel SNA requires the secure runtime image of the Nortel Ethernet Routing Switch 5500 Series software.

Configuring the network access device

To configure the Nortel Ethernet Routing Switch 5500 Series to function as a network access device in the Nortel SNA solution, Nortel recommends following these steps in the order in which they are listed.

For information about the CLI commands to configure the Nortel SNA solution on the switch, see Configuring Nortel Secure Network Access using the CLI. For information about configuring the Nortel SNA solution using Device Manager, see Configuring Nortel Secure Network Access using Device Manager.

1. Configure static routes to all the networks behind the core routing device. This can be automated, as RIP and OSPF routing protocols are supported.
2. Configure the switch management VLAN, if necessary.
3. Configure SSH (see "Configuring SSH on the 5500 Series switch for Nortel SNA" (page 30)).
   a. Download the Nortel SNAS 4050 SSH public key to the switch.
   b. Enable SSH on the switch.

      Note: You must enable SSH before you enable Nortel SNA globally. The command to enable Nortel SNA fails if SSH is not enabled.

   c. Import the switch SSH public key on the Nortel SNAS 4050 (note that this step is performed on the Nortel SNAS 4050, not on the edge switch).

4. Configure the Nortel SNAS 4050 portal IP address (pVIP)/subnet (see Configuring the Nortel SNAS 4050 subnet for CLI, or Configuring the Nortel SNAS 4050 subnet for Device Manager).
5. Configure port tagging, if applicable.

   Note: For a Layer 2 switch, the uplink ports are tagged automatically to allow them to participate in multiple VLANs.

6. Create the port-based VLANs.

   The VLANs are configured as VoIP, Red, Yellow, and Green VLANs later.

7. Configure DHCP-relay and IP routing if the switch is used in Layer 3 mode.
8. (Optional) Configure the filters (Red, Yellow, Green, and VoIP).

   Note: Manual configuration of the filters is optional. The filters are configured automatically as predefined defaults when you configure the Red, Yellow, Green, and VoIP VLANs.

   You can modify default filter sets and manually created filter sets after Nortel SNA is enabled.

9. Configure the VoIP VLANs (see Configuring Nortel SNA per VLAN for CLI, or Configuring Nortel SNA per VLAN for Device Manager).
10. Configure the Red, Yellow, and Green VLANs, associating each with the applicable filters (see Configuring Nortel SNA per VLAN for CLI, or Configuring Nortel SNA per VLAN for Device Manager).

    When you configure the Yellow VLAN, you must configure the Yellow subnet. When a port is in the Yellow state, only traffic on the Yellow subnet is allowed (if you are using the default filters). Therefore, only devices in the Yellow subnet are accessible. Nortel recommends that you put the remediation server in the Yellow subnet.

11. Configure the Nortel SNA ports (see Enabling Nortel SNA on ports for CLI, or Enabling Nortel SNA on ports for Device Manager).

    Identify switch ports as uplink or dynamic. When you configure the uplink ports, you associate the Nortel SNA VLANs with those ports. Clients are connected on the dynamic ports.

    Note 1: If the network access device itself is the DHCP relay agent (that is, functioning in Layer 3 mode) for any of the Red, Yellow, Green, or VoIP VLANs, it is not necessary to configure an uplink port in that VLAN.

    Note 2: You can configure Nortel SNA ports (both dynamic and uplink) after Nortel SNA is enabled globally.

12. Enable Nortel SNA globally (see Enabling Nortel SNA for CLI, or Enabling Nortel SNA for Device Manager).

Configuring SSH on the 5500 Series switch for Nortel SNA

The Secure Shell (SSH) protocol provides secure and encrypted communication between the Nortel SNAS 4050 and the network access devices. For secure communication between the Nortel SNAS 4050 and the network access device, each must have knowledge of the other's public SSH key.

To configure SSH communication between the Ethernet Routing Switch 5500 Series and the Nortel SNAS 4050, use the following procedure:

Step	Action
1	Download the SSH public key from the Nortel SNAS 4050 to the switch: ***Note:*** Ensure you have generated the Nortel SNAS 4050 key. Use the following command on the Nortel SNAS 4050 to generate the SSH public and private keys for the Nortel SNAS 4050: **`cfg/domain #/sshkey/generate`** a. On the Nortel SNAS 4050, use the **`/cfg/domain #/sshkey/export`** command to upload the key to a TFTP server, for manual retrieval from the switch. b. On the 5500 Series switch, load the Nortel SNAS 4050 public key to the switch using the following commands from the Global configuration mode: **`ssh download-auth-key address <ipaddr> key-name <filename>`** where **`<ipaddr>`** is the IP address of the server (entered as A.B.C.D) where you placed the key.
2	On the 5500 Series switch, enable SSH using the following command from the Global configuration mode: **`ssh`**
3	On the Nortel SNAS 4050, import the 5500 Series switch public key: **`/cfg/domain #/switch #/sshkey/import`** **`apply`** For more information, refer to *Nortel Secure Network Access Switch 4050 User Guide (320818-A)*.

ATTENTION

If you subsequently reset the switch to factory defaults, a new public key is generated on the switch. Consequently, this procedure must be repeated each time the switch is set to factory default settings. Note that you must reimport the switch key on the Nortel SNAS 4050 and apply this change.

—End—

Deploying the Nortel SNA solution in an active network

You can deploy the Nortel SNA solution on an existing, active Nortel Ethernet Routing Switch 5500 Series switch. You must upgrade the switch to a minimum software release of 4.3, and you must understand how the implementation of Nortel SNA on the edge switch impacts the switch functions.

The term network access device is used to refer to the Nortel Ethernet Routing Switch 5500 Series edge switch when it is configured for the Nortel SNA environment.

About the ports

A port on the network access device can operate in one of two modes:

- Nortel SNA
- non-Nortel SNA

There are two kinds of Nortel SNA ports: dynamic and uplink.

When you configure a port as a dynamic Nortel SNA port and you enable Nortel SNA, the following properties are changed on the port:

- The port is removed from the existing VLAN. It is placed in the Red VLAN and in the VoIP VLAN that was configured for that port.
- The client port tagging behavior changes to untagpvidonly.
- The Port VLAN ID (PVID) of the port is changed to the Red PVID.
- If the port has existing QoS filters, they are replaced by the Nortel SNA filter set, and the port Spanning Tree state is changed to Fast Learning (if STP was set as Normal Learning before enabling Nortel SNA).

During runtime, Nortel SNA changes the port VLAN membership, the filters, and the PVID properties dynamically, based on the client authentication state.

If you subsequently disable Nortel SNA, the port returns to the pre-Nortel SNA state (see "Rolling back Nortel SNA mode to default mode" (page 33)).

When the port is a Nortel SNA uplink port and Nortel SNA is enabled, the port can be a member of Nortel SNA and non-Nortel SNA VLANs (see Configuration example: Adding the uplink port).

> ***Note:*** Nortel recommends that the Spanning Tree Protocol (STP) on the Nortel SNA uplink port and on the router port be either Fast Learning or disabled. Ensure STP is the same on both ports (that is, if STP is Fast Learning enabled on the Nortel SNA uplink port, it must be Fast Learning enabled on the router port, also).

You can configure multiple Nortel SNA uplink ports.

You can add the uplink port to a non-Nortel SNA VLAN or delete it from a non-Nortel SNA VLAN. The membership of the Nortel SNA uplink port in non-Nortel SNA VLANs is not affected by globally enabling or disabling Nortel SNA. No other Nortel SNA port can be a member of a non-Nortel SNA VLAN.

The PVID of the uplink port can be modified.

If a port is a Nortel SNA uplink port, enabling Nortel SNA changes the port to a tagall port.

About the VLANs and filters

VLANs that you plan to configure as Nortel SNA VLANs must be empty (that is, they have no port members assigned).

Nortel SNA enforcement zones have corresponding default Nortel SNA filter sets. Nortel recommends that you use the default filter sets. You can, however, create customized filters sets and attach these to the Nortel SNA VLANs. You can also modify the default filters, if necessary, after you have enabled them (see *Nortel Ethernet Routing Switch 5500 Series Configuration - Quality of Service (NN47200-504)* and Default Nortel SNA filters for more information).

When the Nortel SNA filters are applied to a port, any existing QoS filters on that port are disabled, and the Nortel SNA filters are applied (pre-existing policies are re-enabled when Nortel SNA is disabled).

Nortel does not support Nortel SNA filter sets and non-Nortel SNA filter sets coexisting on Nortel SNA ports. Nortel SNA VLANs are divided into four categories:

- Red
- Yellow
- Green
- VoIP

Each network access device must have one, and only one, Red VLAN. Each switch can, however, have multiple Yellow and multiple Green VLANs. In Ethernet Routing Switch 5500 Series, Software Release 5.0, you can configure no more than five Yellow, five Green, and five VoIP VLANs on each switch.

Updating the filter sets

Ensure you thoroughly plan your Nortel SNA deployment. For example, as part of the Nortel SNA configuration on the Nortel Ethernet Routing Switch 5500 Series switch, you must configure the Nortel SNAS 4050 portal Virtual IP (pVIP) address and mask. This address is added to the Nortel SNA filter sets only (this applies to VoIP VLAN IDs and the Yellow subnet, also).

If you change the Nortel SNAS 4050 pVIP subnet (or VoIP VLAN IDs, or the Yellow subnet), you must update the filter sets. You update the filter sets in one of two ways:

1. Manually update them using the **`qos nsna`** command (see *Nortel Ethernet Routing Switch 5500 Series Configuration - Quality of Service (NN47200-504)* and Configuration example: Configuring the default Nortel SNA filters for specific information).
2. Remove the filters and reconfigure:
   a. Disable Nortel SNA globally.
   b. Disable Nortel SNA on the ports.
   c. Mark the VLANs as non-Nortel SNA (mark VoIP VLANs last).
   d. Delete the filters using one of the following methods:
      i. Delete all the filters at once:

```
enable
con ter
qos agent reset-default
```

      ii. Delete the filters one by one:

```
no qos nsna name <filter-name-red>
no qos nsna name <filter-name-yellow>
no qos nsna name <filter-name-green>
```

   e. Remove the Nortel SNAS 4050 (**`no nsna nsnas`**).
   f. Reconfigure Nortel SNA.

Rolling back Nortel SNA mode to default mode

When you enable Nortel SNA on the Ethernet Routing Switch 5500 Series, Nortel SNA dynamically changes the following port settings:

- VLAN settings

- QoS parameters
- Spanning Tree configuration

When you disable Nortel SNA, the changes to those port settings are rolled back automatically, and pre-Nortel SNA settings are applied on the port.

There is, however, one exception: When Nortel SNA is enabled on a port, STP runs in FAST START mode to enable faster convergence. The Spanning Tree state of the LAN port can stay in FAST START mode when Nortel SNA is disabled if the client ports were set to Normal Learning in the pre-Nortel SNA state. If the pre-Nortel SNA Spanning Tree state was Fast Learning or disabled, the port rolls back correctly.

If you had physically moved existing users from a legacy switch to a Nortel SNA-enabled switch, the only task you must complete to roll back port settings is to physically reconnect the users to the legacy switch.

Configuring Nortel Secure Network Access using the CLI

This chapter describes how to configure the Nortel Ethernet Routing Switch 5500 Series as a network access device in the Nortel Secure Network Access (Nortel SNA) solution using the Command Line Interface (CLI).

This chapter includes the following topics:

For an overview of the steps required to configure a network access device in the Nortel SNA solution, see Basic switch configuration for Nortel SNA.

Configuring the Nortel SNAS 4050 subnet

To configure the Nortel SNAS 4050 subnet, use the following command from the Global configuration mode:

```
nsna nsnas <ipaddr/mask>
```

where

<ipaddr/mask> is the Nortel SNAS 4050 portal Virtual IP (pVIP) address and network mask (a.b.c.d./<0 - 32>)

This command includes the following parameters:

nsna nsnas <ipaddr/mask> followed by:	
port <value>	Defines the TCP port number for the Switch to Nortel SNAS 4050 Server Communication Protocol (SSCP). Values are in the range 1024 - 65535. The default setting is 5000.

Note: The pVIP address is used in the default Red filter set to restrict the communication of clients in the Red state to the Nortel SNAS 4050.

If you are using one Nortel SNAS 4050 in the network, you can use a 32-bit mask to further restrict traffic flow.

The subnet you specify is added to the filters (Red, Yellow, and VoIP). If you change the Nortel SNAS 4050 subnet after you have associated the filters with the Nortel SNA VLANs, you must manually update the Nortel SNAS 4050 subnet in the filters.

Configuration example: Adding a Nortel SNAS 4050 subnet

To configure the Nortel SNAS 4050 pVIP subnet of 10.40.40.0/24, enter the following command:

```
5510-48T(config)# nsna nsnas 10.40.40.0/24
```

Viewing Nortel SNAS 4050 subnet information

To view information related to the Nortel SNAS 4050 pVIP subnet you configured, enter the following command from the Privileged EXEC configuration mode:

```
5510-48T# show nsna nsnas 10.40.40.0/24
NSNAS IP Address     NSNAS NetMask     NSNAS Port
-------------------------------------------------------------
10.40.40.0           255.255.255.0     5000
```

Removing the Nortel SNAS 4050 subnet

To remove the Nortel SNAS 4050 pVIP subnet, enter the following command from Global configuration mode:

```
no nsna nsnas <ipaddr/mask>
```

where

<ipaddr/mask> is the pVIP address and network mask (a.b.c.d./<0 - 32>)

Configuring QoS for the Nortel SNA solution

For general information about configuring filters and Quality of Service (QoS) in the Nortel SNA solution, see Filters in the Nortel SNA solution. For detailed information about configuring the filters, see *Nortel Ethernet Routing Switch 5500 Series Configuration - Quality of Service (NN47200-504)*.

Configuring Nortel SNA per VLAN

Note 1: VLANs that you plan to configure as Nortel SNA VLANs must be empty (that is, they have no port members assigned).

No non-Nortel SNA ports can be associated with Nortel SNA VLANs.

Note 2: A filter name cannot begin with a number.

To configure the Nortel SNA VLANs, use the following command from the Global configuration mode:

```
nsna vlan <vid> color <red|yellow|green|voip>
```

where

<vid> is the VLAN ID in the range 1 - 4094. The Nortel SNA VLAN is given the color you specify in the command.

This command includes the following parameters:

nsna vlan <vid> color <red|yellow|green|voip> followed by:	
filter <filter name>	Sets the Nortel SNA filter set name. The string length is 0 - 255 characters. ***Note 1:*** This parameter is not allowed for configuration of a VoIP VLAN. VoIP filters are part of the Red/Yellow filter sets. ***Note 2:*** If the filter set with this name does not already exist, it is created when you specify it with this command. If a filter set with the name you specify does exist, that filter set is used.
yellow-subnet <ipaddr/mask>	Sets the Yellow VLAN subnet IP and mask (a.b.c.d/<0 - 32>). ***Note:*** This parameter is only allowed for configuration of the Yellow VLAN.

Viewing Nortel SNA VLAN information

To view information related to the Nortel SNA VLANs, use the following command from the Privileged EXEC configuration mode:

```
show nsna vlan <vid>
```

where

<vid> is the VLAN ID in the range 1-4094

Removing a Nortel SNA VLAN

To remove a Nortel SNA VLAN, use the following command from the Global configuration mode:

```
no nsna vlan <vid>
```

where

<vid> is the VLAN ID in the range 1-4094

Configuration example: Configuring the Nortel SNA VLANs

This example includes configuration of the VoIP, Red, Yellow, and Green VLANs. It is assumed that VLANs 110, 120, 130, and 140 (used in this example) were previously created as port-based VLANs. (For information about creating VLANs using the Nortel Ethernet Routing Switch 5500 Series, refer to *Nortel Ethernet Routing Switch 5500 Series Configuration - VLANs, Spanning Tree, and MultiLink Trunking (NN47200-502)* .

Note: You must configure the Nortel SNAS 4050 pVIP subnet before you configure the Nortel SNA VLANs.

VoIP VLANs are optional. If you are using VoIP VLANs, you must configure them before configuring the Red, Yellow, and Green VLANs.

It is recommended that the IP addresses of static devices be added to the Red subnet and the filter only enforcement type applied. With this configuration, static IP addresses cannot access the network prior to authentication but, once authenticated, the Green filter can be applied to the port, thus providing full network access even though the IP address is in the Red subnet.

In this example, the following parameters are used:

VLAN	Parameters
Red	VLAN ID: 110 Color: Red Filter name: red
Yellow	VLAN ID: 120 Color: Yellow Filter name: yellow Subnet IP: 10.120.120.0/24

VLAN	Parameters
Green	VLAN ID: 130 Color: Green Filter name: green
VoIP	VLAN ID: 140 Color: VoIP

Note: If filters are not manually configured prior to configuring the Nortel SNA VLANs, the switch automatically generates default filters when the Red, Yellow, and Green VLANs are configured.

Configuring the VoIP VLAN

To configure the VoIP VLAN, use the following command:

```
5510-48T(config)# nsna vlan 140 color voip
5510-48T(config)# show nsna vlan 140
VLAN ID     Color       Filter Set Name     Yellow Subnet
-------------------------------------------------------
140         VOIP                            0.0.0.0/0
```

Configuring the Red VLAN

To configure the Red VLAN, use the following command:

```
5510-48T(config)# nsna vlan 110 color red filter red
5510-48T(config)# show nsna vlan 110
VLAN ID     Color       Filter Set Name     Yellow Subnet
-------------------------------------------------------
110         Red         red                 0.0.0.0/0
```

Configuring the Yellow VLAN

To configure the Yellow VLAN, use the following command:

```
5510-48T(config)# nsna vlan 120 color yellow filter yellow
yellow-subnet 10.120.120.0/24
5510-48T(config)# show nsna vlan 120
VLAN ID     Color       Filter Set Name     Yellow Subnet
-------------------------------------------------------
120         Yellow      yellow              10.120.120.0/24
```

Configuring the Green VLAN

To configure the Green VLAN, use the following command:

```
5510-48T(config)# nsna vlan 130 color green filter green
5510-48T(config)# show nsna vlan 130
VLAN ID     Color       Filter Set Name     Yellow Subnet
-------------------------------------------------------
130         Green       green               0.0.0.0/0
```

Enabling Nortel SNA on ports

The following sections describe how to enable Nortel SNA on the ports. For information about port modes, refer to Port modes.

The Nortel SNA solution introduces the uplink port. Uplink ports are members of the Nortel SNA VLANs. For more information about the uplink port, refer to *Nortel Secure Network Access Solution Guide (320817-A)*.

> ***Note:*** The Ethernet Routing Switch 5530 has two 10-Gbit ports. You can configure these as uplink ports only. You cannot configure these as dynamic ports. Therefore, you must specify ports 1 - 24 in any Nortel SNA command where you configure dynamic ports. For example, if you enter the **`nsna port all dynamic voip-vlans <vidlist>`** command, it fails because the two 10-Gbit ports cannot be configured as dynamic ports.

To configure Nortel SNA on ports, use the following command from the Ethernet Interface configuration mode:

`nsna`

This command includes the following parameters:

`nsna` followed by:	
port <portlist>	Identifies a port other than that specified when entering the Ethernet Interface configuration mode. The parameter <portlist> uses the convention {port[port][,...]}.
dynamic voip-vlans <vidlist>	Sets the Nortel SNAS 4050 dynamic port configuration, where <vidlist> is the VoIP VLAN IDs (vlan-id[-vlan-id][,...]).
uplink vlans <vidlist>	Defines the Nortel SNAS 4050 uplink VLAN list, where <vidlist> is the Nortel SNA VLAN IDs (vlan-id[-vlan-id][,...]).

Viewing Nortel SNA port information

To view information related to the Nortel SNA interfaces, use the following command from the Privileged EXEC configuration mode:

```
show nsna interface [<interface-id>]
```

where

<interface-id> is the port number. Appropriate entries are {port[-port][,...]}, all, and none.

Removing a Nortel SNA port

To remove a Nortel SNA port, enter the following command from the Ethernet Interface configuration mode:

```
no nsna
```

Example: Removing Nortel SNA ports

To disable Nortel SNA on ports 20 - 24, enter the following commands:

```
5510-48T(config)#interface fastethernet 20-24
5510-48T(config-if)#no nsna
5510-48T(config-if)#exit
5510-48T(config)#
```

Configuration example: Adding the uplink port

To add the uplink port to the VLANs, use the following command from the Ethernet Interface configuration mode:

```
nsna uplink vlans <vidlist>
```

where

<vidlist> is the uplink VLAN IDs, entered using the convention {vlan-id[-vlan-id][,...]}

Note: All VLANs specified in the <vidlist> must be Nortel SNA VLANs. You can add the uplink port to or delete it from non-Nortel SNA VLANs (including the management VLAN) using the **vlan members add** command (see *Nortel Ethernet Routing Switch 5500 Series Configuration - VLANs, Spanning Tree, and MultiLink Trunking (NN47200-502)* for more information).

The membership of Nortel SNA uplink ports in non-Nortel SNA VLANs is not affected by globally enabling or disabling Nortel SNA. Nortel Ethernet Routing Switch 5500 Series Software Release 5.0 supports multiple Nortel SNA uplink ports.

In this example, the following parameters are used:

- uplink port is 20

- Nortel SNA VLAN IDs are 110, 120, 130, 140

```
5510-48T(config)# interface fastEthernet 20
5510-48T(config)# nsna uplink vlans 110,120,130,140
5510-48T(config)# show nsna interface 20
Port      NSNA Mode      Green VLAN ID   VLAN IDs             State
DHCP State
-------------------------------------------------------------------
-------
20        Uplink                         110,120,130,140      None
Unblocked
```

Configuration example: Adding client ports

In this example, the following parameters are used:

- Client ports are 3, 4, and 5.
- VoIP VLAN ID is 140.

```
5510-48T(config)# interface fastEthernet 3-5
5510-48T(config)# nsna dynamic voip-vlans 140
5510-48T(config)# show nsna interface 3-5
Port    NSNA Mode     Green VLAN ID    VLAN IDs      State       DHCP State
-------------------------------------------------------------------------
3       Dynamic       0                140           Red         Unblocked
4       Dynamic       0                140           Red         Unblocked
5       Dynamic       0                140           Red         Unblocked
5510-48T(config)# exit
5510-48T(config)#
```

Note: If the pre-Nortel SNA STP state of a port is Normal Learning, when you specify that port as a Nortel SNA dynamic port and you enable Nortel SNA, the STP state of the port is changed to Fast Learning automatically. You can change this to be disabled. You cannot set the state to Normal Learning for Nortel SNA.

Viewing information about Nortel SNA clients

To view information about Nortel SNA clients, enter the following command from the Privileged EXEC configuration mode:

```
show nsna client [interface [<interface-id>] | mac-address
<H.H.H.>]
```

where

<interface-id> is the port number
<H.H.H.> is the MAC address of the host

The following is an example of the command to view information about Nortel SNA clients:

```
5510-48T(config)# show nsna client interface 5
Por    Client MAC          Device Type    VLAN Id    IP Address      Exp
t
-------------------------------------------------------------------------
1/5    00:80:22:44:66:88   PC             110        10.11.12.13     No
1/5    00:08:11:22:33:44   IP-Phone       140        10.20.30.40     No
```

Entering phone signatures for Nortel SNA

To specify Nortel IP phone signatures for the Nortel SNA solution, enter the following command from the Global configuration mode:

nsna phone-signature <LINE>

where

<LINE> is the Nortel IP phone signature string (for example: Nortel-i2007-A)

Removing Nortel SNA phone signatures

To remove a Nortel SNA phone signature, enter the following command from the Global configuration mode:

no nsna phone-signature <LINE>

where

<LINE> is the phone signature string

Viewing Nortel SNA phone signatures

To view configured Nortel SNA phone signatures, enter the following command from the Privileged EXEC mode: where

show nsna phone-signature [<LINE>]

where

<LINE> is the phone signature string. Use an asterisk (*) at the end of the string to display all signatures that start with the specified string. For example, if you enter **Nort*** as the LINE parameter, output displays any signatures that start with the string `Nort`.

Enabling Nortel SNA

To enable Nortel SNA, use the following command from the Global configuration mode:

```
nsna enable
```

Note: You must enable SSH before you enable Nortel SNA globally. The command to enable Nortel SNA fails if SSH is not enabled. For more information, see Configuring SSH on the 5500 Series switch for Nortel SNA.

Disabling Nortel SNA

To disable Nortel SNA, use the following command from the Global configuration mode:

```
no nsna enable
```

Viewing the Nortel SNA state

Use the following command from the Privileged EXEC configuration mode for information about the state of Nortel SNA on the switch:

```
show nsna
```

Example: Viewing Nortel SNA and Nortel SNAS 4050 information

If the Nortel SNAS 4050 is connected, the output is the following:

```
5510-48T# show nsna
NSNA Enabled:  Yes
NSNAS Connection State:  Connected
NSNAS Address:  10.40.40.2
NSNAS Hello Interval:  60 seconds
NSNAS Inactivity Interval:  180 seconds
NSNAS Status-Quo Interval:  240 seconds
```

If the Nortel SNAS 4050 is not connected, the output is the following:

```
5510-48T# show nsna
NSNA Enabled:  No
NSNAS Connection State:  Not Connected
NSNAS Status-Quo Interval:  0 seconds
```

Configuration example

The configuration example is based on the following assumptions:

- You are starting with an installed switch that is not currently configured as part of the network.
- You have installed Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0.3.
- You have configured basic switch connectivity.
- You have initialized the switch and it is ready to accept configuration.

Note: Default Nortel SNA filters are used in this example.

Scenario

"Basic network scenario" (page 46) shows the basic network configuration used in this example. The Ethernet Routing Switch 8600 functions as the core router.

The following table describes the devices connected in this environment and their respective VLAN IDs and IP addresses.

Network devices

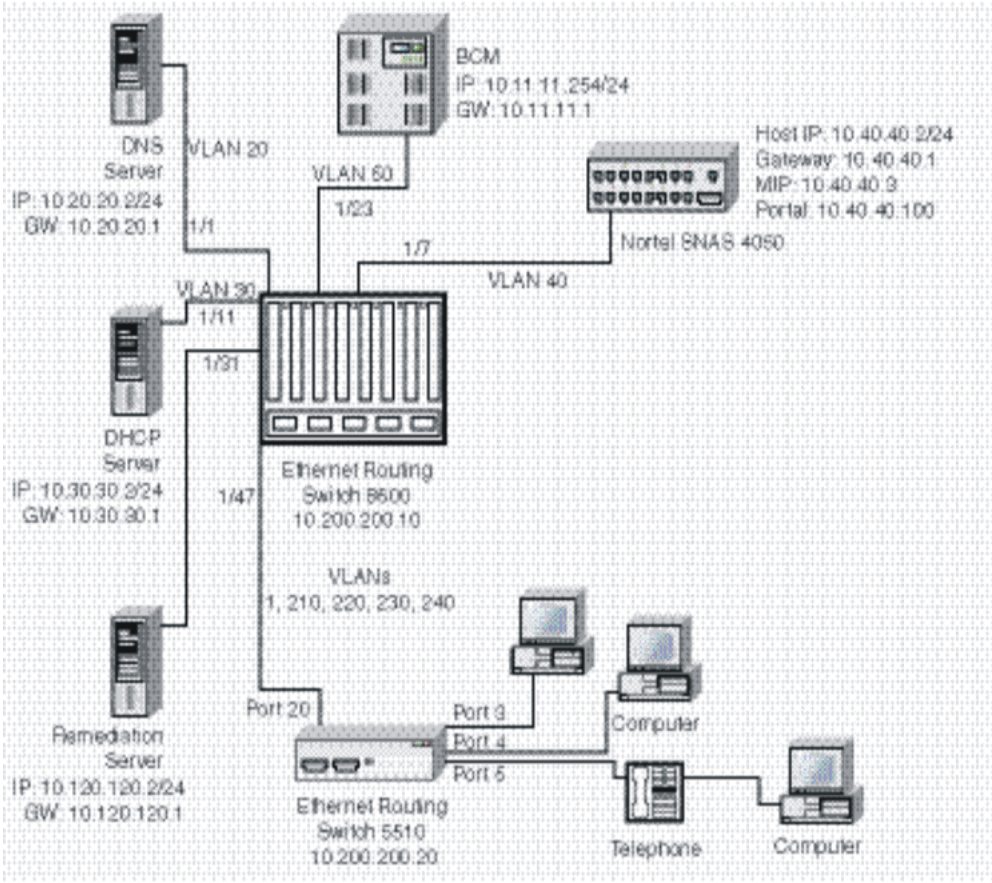
Device/Service	VLAN ID	VLAN IP	Device IP	Ethernet Routing Switch 8600 port
DNS	20	10.20.20.1	10.20.20.2	1/1
DHCP	30	10.30.30.1	10.30.30.2	1/11
Nortel SNAS 4050	40	10.40.40.1	10.40.40.2	1/7
Remediation server	120	10.120.120.1	10.120.120.2	1/31
Call server	50	10.11.11.1	10.11.11.254	1/23

The following table describes the VLANs for the Ethernet Routing Switch 5510.

VLANs for the Ethernet Routing Switch 5510

VLAN	VLAN ID	Yellow subnet
Management	1	N/A
Red	210	N/A
Yellow	220	10.120.120.0/24
Green	230	N/A
VoIP	240	N/A

Basic network scenario



Steps

The example illustrates the following required configuration steps:

1. "Setting the switch IP address" (page 46)
2. "Configuring SSH" (page 47)
3. "Configuring the Nortel SNAS 4050 pVIP subnet" (page 47)
4. "Creating port-based VLANs" (page 47)
5. "Configuring the VoIP VLANs" (page 47)
6. "Configuring the Red, Yellow, and Green VLANs" (page 47)
7. "Configuring the log on domain controller filters" (page 47)
8. "Configuring the Nortel SNA ports" (page 48)
9. "Enabling Nortel SNA globally" (page 48)

Setting the switch IP address

```
5510-48T(config)#ip address 10.200.200.20 netmask
255.255.255.0
```

```
5510-48T(config)# ip default-gateway 10.200.200.10
```

Configuring SSH

This example assumes that the Nortel SNAS 4050 public key has already been uploaded to the TFTP server (10.20.20.20).

```
5510-48T(config)# ssh download-auth-key address
10.20.20.20 key-name sac_key.1.pub

5510-48T(config)# ssh
```

Note: You must import the switch SSH key on the Nortel SNAS 4050 after enabling SSH on the Nortel Ethernet Routing Switch 5500 Series switch. For more information, see Configuring SSH on the 5500 Series switch for Nortel SNA. Also, refer to *Nortel Secure Network Access Switch 4050 User Guide (320818-A)* for more information about configuring SSH on the Nortel SNAS 4050.

Configuring the Nortel SNAS 4050 pVIP subnet

```
5510-48T(config)# nsna nsnas 10.40.40.0/24
```

Creating port-based VLANs

```
5510-48T(config)# vlan create 210 type port
5510-48T(config)# vlan create 220 type port
5510-48T(config)# vlan create 230 type port
5510-48T(config)# vlan create 240 type port
```

Configuring the VoIP VLANs

```
5510-48T(config)#nsna vlan 240 color voip
```

Configuring the Red, Yellow, and Green VLANs

```
5510-48T(config)#nsna vlan 210 color red filter red
5510-48T(config)#nsna vlan 220 color yellow filter
yellow yellow-subnet 10.120.120.0/24
5510-48T(config)#nsna vlan 230 color green filter green
```

Configuring the log on domain controller filters

Note: This step is optional.

The PC client must be able to access the log on domain controller you configure (that is, clients using the log on domain controller must be able to ping that controller).

```
5510-48T(config)# qos nsna classifier name red dst-ip
10.200.2.12/32 ethertype 0x0800 drop-action disable
block wins-prim-sec eval-order 70
```

```
5510-48T(config)# qos nsna classifier name red dst-ip
10.200.224.184/32 ethertype 0x0800 drop-action disable
block wins-prim-sec eval-order 71
```

Configuring the Nortel SNA ports

Add the uplink port:

```
5510-48T(config)#interface fastEthernet 20
5510-48T(config-if)#nsna uplink vlans 210,220,230,240
5510-48T(config-if)#exit
```

Add the client ports:

```
5510-48T(config)#interface fastEthernet 3-5
5510-48T(config-if)#nsna dynamic voip-vlans 240
5510-48T(config-if)#exit
```

Enabling Nortel SNA globally

```
5510-48T(config)#nsna enable
```

Configuring Nortel Secure Network Access using Device Manager

This chapter describes how to configure the Ethernet Routing Switch 5500 Series as a network access device in the Nortel Secure Network Access (Nortel SNA) solution using the Java Device Manager (Device Manager).

This chapter includes the following topics:

Note: The information in this section is available in the Device Manager online Help.

For an overview of the steps required to configure a network access device in the Nortel SNA solution, see Basic switch configuration for Nortel SNA.

Configuring the Nortel SNAS 4050 subnet

Note: In Ethernet Routing Switch 5500 Series, Software Release 5.0, only one entry for the Nortel SNAS 4050 subnet can be configured.

To configure the Nortel SNAS 4050 portal Virtual IP (pVIP) subnet:

Step	Action
1	Select **Edit > Security > NSNA** from the Device Manager menu.

The **NSNA** dialog box appears with the **NSNAS tab** selected (see the following figure).

NSNA -- NSNAS tab

The following table describes the NSNAS tab fields.

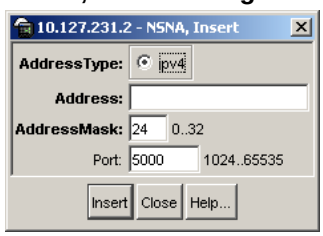
NSNA -- NSNAS tab fields

Field	Description
AddressType	Specifies the type of IP address used by the Nortel SNAS 4050. IPv4 is the only available option at this time.
Address	Specifies the pVIP address of the Nortel SNAS 4050.
AddressMask	Specifies the Nortel SNAS 4050 pVIP address subnet mask.
Port	Specifies the TCP port number for the Switch to Nortel SNAS 4050 Server Communication Protocol (SSCP). Values are in the range 1024 - 65535. The default setting is 5000.

2 Click **Insert**.

The **NSNA, Insert** dialog box appears (see the following figure).

NSNA, Insert dialog box



3 Enter the pVIP address and subnet mask of the Nortel SNAS 4050.

Note: The pVIP address is used in the default Red filter set to restrict the communication of clients in the Red state to the Nortel SNAS 4050. If you are using one Nortel SNAS 4050 in the network, you can use a 32-bit mask to further restrict traffic flow. The subnet you specify is added to the filters (Red, Yellow, and VoIP). If you change the Nortel SNAS 4050 subnet after you

have associated the filters with the Nortel SNA VLANs, you must manually update the Nortel SNAS 4050 subnet in the filters.

4 Enter the port number (if it is different than the default value).

5 Click **Insert**.

The information for the configured Nortel SNAS 4050 pVIP subnet appears in the NSNAS tab of the NSNA dialog box.

—End—

See also:

- "Removing the Nortel SNAS 4050 subnet" (page 51)
- "Configuring QoS for the Nortel SNA solution" (page 52)
- "Configuring Nortel SNA per VLAN" (page 52)
- "Enabling Nortel SNA on ports" (page 56)
- "Viewing Nortel SNA settings" (page 59)
- "Viewing information about Nortel SNA clients" (page 61)
- "Entering phone signatures for Nortel SNA" (page 62)
- "Enabling Nortel SNA" (page 64)

Removing the Nortel SNAS 4050 subnet

To remove the currently configured Nortel SNAS 4050:

Step	Action
1	Select **Edit > Security > NSNA** from the Device Manager menu. The **NSNA** dialog box appears with the **NSNAS** tab selected.
2	Select the row that contains the Nortel SNAS 4050 subnet information.
3	Click **Delete**. The Nortel SNAS 4050 pVIP subnet information is removed from the Nortel SNA configuration.

—End—

See also:

- "Configuring the Nortel SNAS 4050 subnet" (page 49)
- "Configuring QoS for the Nortel SNA solution" (page 52)
- "Configuring Nortel SNA per VLAN" (page 52)
- "Enabling Nortel SNA on ports" (page 56)
- "Viewing Nortel SNA settings" (page 59)
- "Viewing information about Nortel SNA clients" (page 61)
- "Entering phone signatures for Nortel SNA" (page 62)
- "Enabling Nortel SNA" (page 64)

Configuring QoS for the Nortel SNA solution

For general information about configuring filters and Quality of Service (QoS) in the Nortel SNA solution, see Filters in the Nortel SNA solution. For detailed information about configuring the filters, see *Nortel Ethernet Routing Switch 5500 Series Configuration - Quality of Service (NN47200-504).*

Configuring Nortel SNA per VLAN

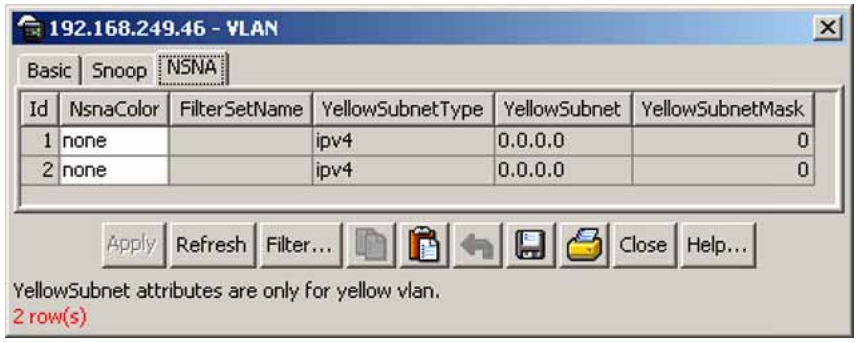
ATTENTION

VLANs that you plan to configure as Nortel SNA VLANs must be empty (that is, they have no port members assigned). Nortel SNA VLANs cannot be associated with non-Nortel SNA ports.

To configure the Nortel SNA VLANs:

Step	Action
1	Select **VLAN > VLANs** from the Device Manager menu.
2	Create the VLANs that you want to configure as Nortel SNA VLANs. For information about creating the VLANs, see *Nortel Ethernet Routing Switch 5500 Series Configuration - VLANs, Spanning Tree, and MultiLink Trunking (NN47200-502)* . After you have created a VLAN, the VLAN information appears in the **Basic** tab of the **VLAN** dialog box.
3	Click the **NSNA** tab. The following figure shows the NSNA tab selected.

VLAN -- NSNA tab



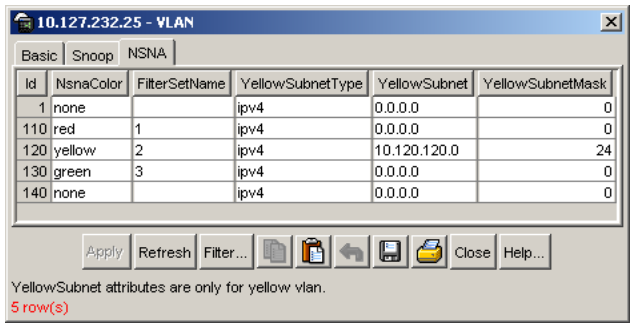
The following table describes the VLAN NSNA tab fields.

VLAN NSNA tab fields

Field	Description
Id	Specifies the VLAN ID.
NsnaColor	Specifies the color of the Nortel SNA VLAN (red, yellow, green, voip, or none).
FilterSetName	Specifies the name of the filter set. ***Note:*** This field is applicable only when the NsnaColor field is set to red, yellow, or green.
YellowSubnetType	Specifies the Ethernet type for the Yellow VLAN subnet (IPv4 is currently the only available option). ***Note:*** This field is applicable only when the NsnaColor field is set to yellow.
YellowSubnet	Specifies the subnet of the Yellow VLAN. ***Note:*** This field is applicable only when the NsnaColor field is set to yellow.
YellowSubnetMask	Specifies the mask for the Yellow VLAN subnet. ***Note:*** This field is applicable only when the NsnaColor field is set to yellow.

4 Double-click the **NsnaColor** field for each VLAN to select the color from the drop-down menu. The following figure illustrates the completed configuration. (Input in the following figure is for example purposes only - create, select, and configure the VLANs based on your network design.)

Example of configured VLAN -- NSNA tab



5 Double-click the **FilterSetName** field for each VLAN to enter the filter set name of your choice.

6 Click **Apply**.

ATTENTION

Each switch must have one, and only one, Red VLAN. Each switch can, however, have multiple Yellow, multiple Green, and multiple VoIP VLANs. In Ethernet Routing Switch 5500 Series, Software Release 5.0, each switch supports up to five Yellow, five Green, and five VoIP VLANs. If IP Phones are intended for use in the system, create the VoIP VLAN first, then create the Red, Yellow, and Green VLANs.

—End—

See also:

- "Removing a Nortel SNA VLAN" (page 54)
- "Configuring the Nortel SNAS 4050 subnet" (page 49)
- "Configuring QoS for the Nortel SNA solution" (page 52)
- "Enabling Nortel SNA on ports" (page 56)
- "Viewing Nortel SNA settings" (page 59)
- "Viewing information about Nortel SNA clients" (page 61)
- "Entering phone signatures for Nortel SNA" (page 62)
- "Enabling Nortel SNA" (page 64)

Removing a Nortel SNA VLAN

To remove a Nortel SNA VLAN:

Step	Action

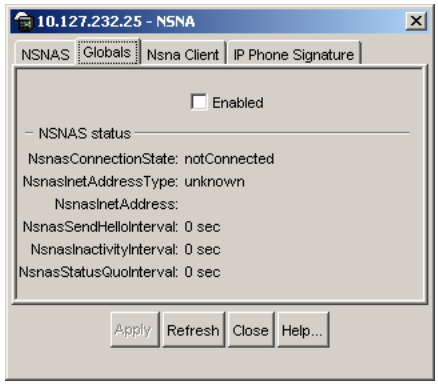
1 Select **Edit > Security > NSNA** from the Device Manager menu.

The **NSNA** dialog box appears with the **NSNAS** tab selected.

2 Click the **Globals** tab.

The **Globals** tab is selected (see the following figure).

NSNA -- Globals



3 Ensure the **Enabled** check box is cleared.

Nortel SNA must be globally disabled before deleting the Nortel SNA VLAN.

4 Click **Close**.

5 Open the **VLAN > VLANs > NSNA** tab:

a. Select **VLAN > VLANs** from the Device Manager menu.

The **VLAN** dialog box appears with the **Basic** tab selected.

b. Click the **NSNA** tab.

The **NSNA** tab is selected (see "VLAN -- NSNA tab" (page 53)).

6 Change the color of the Nortel SNA VLAN to none:

a. Double-click the **NsnaColor** field of the VLAN to be deleted.

b. Select the color **none** from the drop-down list.

7 Click **Apply**.

8 On the **VLAN > VLANs > Basic** tab, delete the VLAN from the list of configured VLANs:

a. Click the **Basics** tab.

The **Basics** tab is selected.

b. Select the row containing the VLAN for which you have changed the Nortel SNA color to none.

c. Click **Delete**.

—End—

See also:

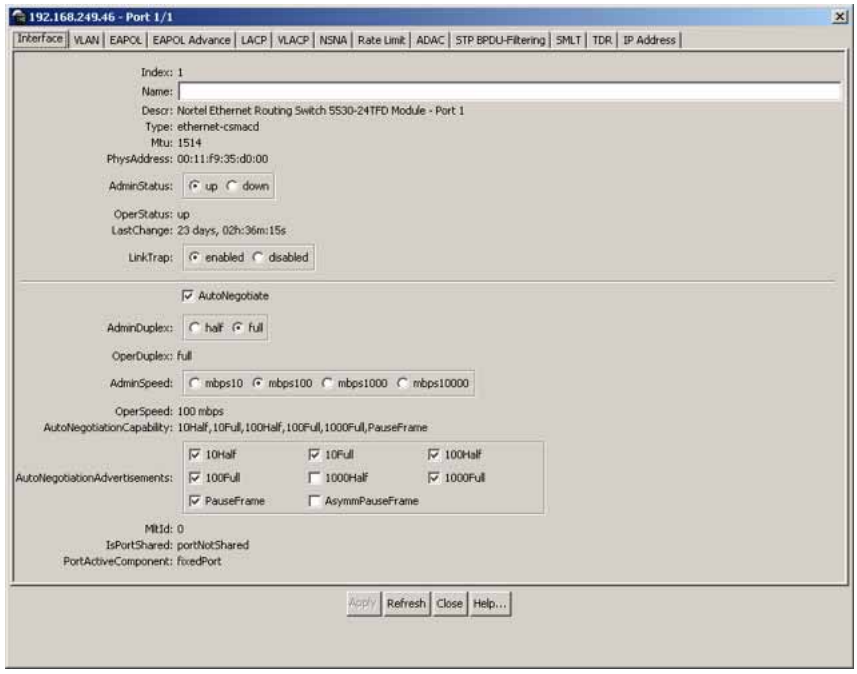
- "Configuring Nortel SNA per VLAN" (page 52)
- "Configuring the Nortel SNAS 4050 subnet" (page 49)
- "Configuring QoS for the Nortel SNA solution" (page 52)
- "Enabling Nortel SNA on ports" (page 56)
- "Viewing Nortel SNA settings" (page 59)
- "Viewing information about Nortel SNA clients" (page 61)
- "Entering phone signatures for Nortel SNA" (page 62)
- "Enabling Nortel SNA" (page 64)

Enabling Nortel SNA on ports

To enable Nortel SNA on ports:

Step	Action
1	Select a port that you want to add to the Nortel SNA solution.
2	Select **Edit > Port**. The **Port** dialog box appears with the **Interface** tab selected (see the following figure).

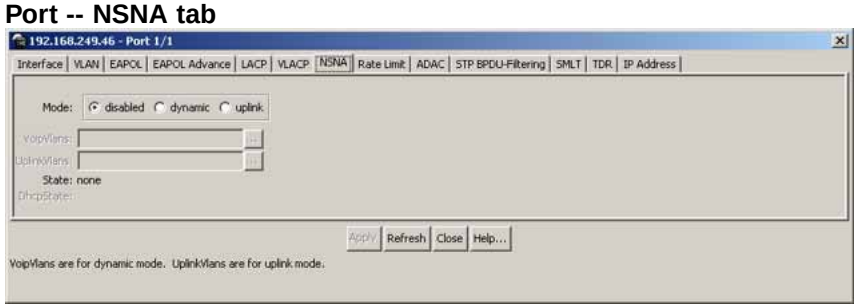
Port -- Interface tab



3 Click the **NSNA** tab.

The **NSNA** tab is selected (see the following figure).

Port -- NSNA tab



The following table describes the **NSNA** tab fields.

Port -- NSNA tab fields

Field	Description
Mode	Specifies the Nortel SNA mode for the port. Options are the following: • disabled • dynamic • uplink

Field	Description
	Note: When you specify a port as dynamic, it is changed to Spanning Tree Protocol (STP) Fast Learning automatically. You can change this to be disabled. It cannot be set to Normal Learning for Nortel SNA.
VoipVlans	Specifies the VoIP VLANs to which this port belongs. ***Note:*** This field is only available when the port mode is dynamic.
UplinkVlans	Specifies the Nortel SNA uplink VLANs to which this port belongs. ***Note:*** This field is only available when the port mode is uplink.
State	Specifies the current Nortel SNA color of the port. Possible states are the following: • none • red • yellow • green
DhcpState	Specifies the DHCP state of the port. Possible DHCP states are the following: • blocked • unblocked

4 Configure the port:

a. Select the port mode.

b. Enter the VoIP VLAN IDs if that field is available.

c. Enter the uplink VLANs if that field is available.

5 Click **Apply**.

—End—

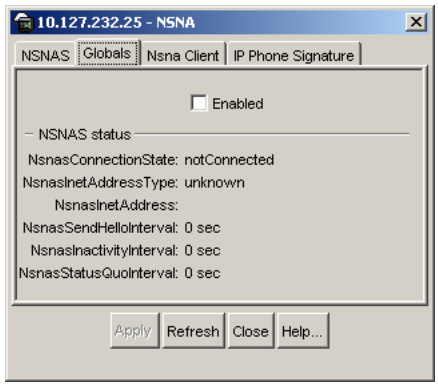
See also:

- "Configuring the Nortel SNAS 4050 subnet" (page 49)
- "Configuring QoS for the Nortel SNA solution" (page 52)

Viewing Nortel SNA settings

Step	Action
1	Select **Edit > Security > NSNA** from the Device Manager menu. The **NSNA** dialog box appears with the **NSNAS** tab selected.
2	Click the **Globals** tab. The **Globals** tab is selected (see the following figure).

NSNA -- Globals tab



The following table describes the **Globals** tab fields.

NSNA -- Globals tab fields

Field	Description
Enabled	When checked, enables Nortel SNA on the network access device (for more information, see "Enabling Nortel SNA" (page 64).
NsnasConnectionState	Displays the status of the connection between the network access device and the Nortel SNAS 4050.
NsnasInetAddressType	Displays the type of IP address used by the Nortel SNAS 4050.
NsnasInetAddress	Displays the pVIP of the Nortel SNAS 4050.

Field	Description
NsnasSendHelloInterval	Displays the time interval, in seconds (s), for the hello (healthcheck) messages sent by the Nortel SNAS 4050 to verify connectivity with the network access device. The interval is configured on the Nortel SNAS 4050. The valid configurable range for the interval is 60s (1m) to 64800s (18h). If there is no current connection between the network access device and the Nortel SNAS 4050, the field displays a value of zero.
NsnasInactivityInterval	Displays the switch inactivity interval, in seconds (s), after which the switch enters status-quo mode. The switch inactivity interval is the hello (healthcheck) interval x the number of retries (deadcount) configured on the Nortel SNAS 4050. If there is no current connection between the network access device and the Nortel SNAS 4050, the field displays a value of zero.
NsnasStatusQuoInterval	Displays the status-quo interval time, in seconds (s). The status-quo interval is configured on the Nortel SNAS 4050. If no activity is detected after the expiry of the switch inactivity interval, the status-quo interval timer starts. If no activity is detected after the expiry of the status-quo interval, the default behavior is for the network access device to move all ports to the Red VLAN. The valid configurable range for the status-quo interval is 0 to 64800s (18h). • If the connection between the Nortel SNAS 4050 and the network access device is active, the field displays the value of the status-quo interval configured on the Nortel SNAS 4050. • If the connection between the Nortel SNAS 4050 and the network access device has been interrupted and the switch inactivity interval has expired, the field displays the amount of time remaining in the status-quo interval. • If the solution has been configured so that no status-quo interval is used, the field displays a value of 65535. This means that the network access device does not move Nortel SNA-enabled ports to the Red VLAN even though the connection between the Nortel SNAS 4050 and the network access device may have been interrupted.

—End—

See also:

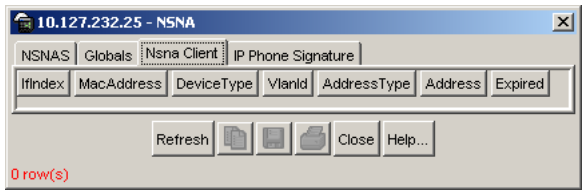
- "Configuring the Nortel SNAS 4050 subnet" (page 49)
- "Configuring QoS for the Nortel SNA solution" (page 52)
- "Configuring Nortel SNA per VLAN" (page 52)
- "Enabling Nortel SNA on ports" (page 56)
- "Viewing information about Nortel SNA clients" (page 61)
- "Entering phone signatures for Nortel SNA" (page 62)
- "Enabling Nortel SNA" (page 64)

Viewing information about Nortel SNA clients

To view information about Nortel SNA clients currently connected to the network access device:

Step	Action
1	Select **Edit > Security > NSNA** from the Device Manager menu. The **NSNA** dialog box appears with the **NSNAS** tab selected (see "NSNA -- NSNAS tab" (page 50)).
2	Click the **Nsna Client** tab. The **Nsna Client** tab is selected (see the following figure). Clients currently connected to the network access device display in this tab.

NSNA -- Nsna client tab



The following table describes the **Nsna Client** fields.

NSNA -- Nsna client tab fields

Field	Description
IfIndex	Specifies the logical interface index assigned to the VLAN.
MacAddress	Specifies the MAC address of the host.
Device Type	Specifies the type of client device (pc, ipPhone, or printer).

Field	Description
VlanId	Specifies the ID of the VLAN of which the client is a member.
AddressType	Specifies the type of IP address used by this client (IPv4 is currently the only option available).
Address	Specifies the IP address of the client.
Expired	Indicates whether this client has been aged-out.

—End—

See also:

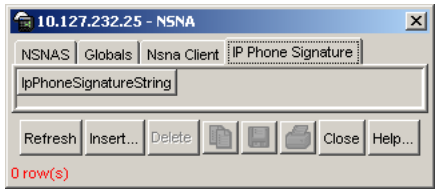
- "Configuring the Nortel SNAS 4050 subnet" (page 49)
- "Configuring QoS for the Nortel SNA solution" (page 52)
- "Configuring Nortel SNA per VLAN" (page 52)
- "Enabling Nortel SNA on ports" (page 56)
- "Viewing Nortel SNA settings" (page 59)
- "Entering phone signatures for Nortel SNA" (page 62)
- "Enabling Nortel SNA" (page 64)

Entering phone signatures for Nortel SNA

To specify IP phone signatures for Nortel SNA:

Step	Action
1	Select **Edit > Security > NSNA** from the Device Manager menu. The **NSNA** dialog box appears with the **NSNAS** tab selected.
2	Click the **IP Phone Signature** tab. The **IP Phone Signature** tab is selected (see the following figure).

NSNA -- IP Phone Signature tab



3 Click **Insert**.

The **NSNA, Insert IP Phone Signature** dialog box appears (see the following figure).

NSNA, Insert IP Phone Signature dialog box

4 Enter the IP phone signature string in the field (for example, Nortel-i2007-A).

5 Click **Insert**.

The IP phone signature you entered appears in the **IP Phone Signature** tab of the **NSNA** dialog box.

—End—

See also:

- "Removing Nortel SNA phone signatures" (page 63)
- "Configuring the Nortel SNAS 4050 subnet" (page 49)
- "Configuring QoS for the Nortel SNA solution" (page 52)
- "Configuring Nortel SNA per VLAN" (page 52)
- "Enabling Nortel SNA on ports" (page 56)
- "Viewing Nortel SNA settings" (page 59)
- "Viewing information about Nortel SNA clients" (page 61)
- "Enabling Nortel SNA" (page 64)

Removing Nortel SNA phone signatures

To remove a Nortel SNA phone signature:

Step	Action
1	Select **Edit > Security > NSNA** from the Device Manager menu. The **NSNA** dialog box appears with the **NSNAS** tab selected.
2	Click the **IP Phone Signature** tab. The **IP Phone Signature** tab is selected (see "NSNA -- IP Phone Signature tab" (page 62)).

3 Select the row containing the IP phone signature you want to remove.

4 Click **Delete**.

—End—

See also:

- "Entering phone signatures for Nortel SNA" (page 62)
- "Configuring the Nortel SNAS 4050 subnet" (page 49)
- "Configuring QoS for the Nortel SNA solution" (page 52)
- "Configuring Nortel SNA per VLAN" (page 52)
- "Enabling Nortel SNA on ports" (page 56)
- "Viewing Nortel SNA settings" (page 59)
- "Viewing information about Nortel SNA clients" (page 61)
- "Enabling Nortel SNA" (page 64)

Configuring Nortel SNA static clients

Static clients must have their MAC address registered in the Nortel SNAS 4050 MAC database and they must be members of a SNAS 4050 group that uses MAC authentication (mactrust set to bypass). For information, see *Nortel Secure Network Access Switch 4050 User Guide for the CLI, NN47230-100*.

Enabling Nortel SNA

ATTENTION

You must enable SSH before you enable Nortel SNA globally. The command to enable Nortel SNA fails if SSH is not enabled. Refer to Configuring SSH on the 5500 Series switch for Nortel SNA for detailed information.

To globally enable Nortel SNA:

Step	Action
1	Select **Edit > Security > NSNA** from the Device Manager menu. The **NSNA** dialog box appears with the **NSNAS** tab selected.
2	Click the **Globals** tab. The **Globals** tab is selected (see "NSNA -- Globals" (page 55)).
3	Select the **Enabled** check box.

4 Click **Apply**.

Note: It can take 2 - 3 minutes to globally enable/disable Nortel SNA, especially on a fully populated stack.

—End—

See also:

- "Configuring the Nortel SNAS 4050 subnet" (page 49)
- "Configuring QoS for the Nortel SNA solution" (page 52)
- "Configuring Nortel SNA per VLAN" (page 52)
- "Enabling Nortel SNA on ports" (page 56)
- "Viewing Nortel SNA settings" (page 59)
- "Viewing information about Nortel SNA clients" (page 61)
- "Entering phone signatures for Nortel SNA" (page 62)

Index

Nortel Ethernet Routing Switch 5500 Series

Ethernet Routing Switch 5500 Series: Release Notes for Software Release 5.0.3

Publication: NN47200-402
Document status: Standard
Document version: 01.01
Document date: 30 October 2006

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

Sourced in Canada and the United States of America