Part No. 217468-C
February 2006

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.3.1

NORTEL

CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

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

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

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

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The 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

Introduction

These are the Release Notes for the Nortel* Ethernet Routing Switch 5500 Series, Software Release 4.3.1.

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

This line of switches was previously referred to as the Baystack 5500 Series.

These Release Notes provide the latest information about software release 4.3.1, as well as operational issues not included in the documentation suite.

Note: User instructions to configure the LAN component of the Nortel Secure Network Access (Nortel SNA) solution are included in these Release Notes. These instructions supplement the document titled, *Configuring and Managing Security for Nortel Ethernet Routing Switch 5500 Series*.

For a complete list of documentation in the 5500 Series suite, consult "Reading path" on page 100.

The following topics are discussed in this document:

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

File names for this release

Table 1 describes the Ethernet Routing Switch 5500 Series, Software Release 4.3.1 software files. File sizes are approximate.

Note: Only the SSH (security) runtime image is available for release 4.3.1; you must use this image.

Table 1 Ethernet Routing Switch 5500 Series, Software Release 4.3 files

Module or file type	Description	File name	File size (bytes)
Secure runtime image software version 4.3.1.0	Switch agent software	5530_43105s.img	4 373 720
Boot/diagnostic software version 4.2.0.11	Switch diagnostic software	5530_42011_diag.bin	808 960
Java Device Manager software version for Windows (5.9.5.0)	Device Manager software image for Windows NT, Windows XP, Windows 2003, Windows 2000	jdm_5950.exe	120 975 553
Java Device Manager software version for UNIX (5.9.5.0)	Device Manager software image for Solaris Device Manager software image for HP Unix	jdm_5950_solaris_sparc.sh jdm_5950_hpux_pa-risc.sh	139 137 432 168 038 808
Java Device Manager software version for Linux (5.9.5.0)	Device Manager software image for Linux	jdm_5950_linux.sh	141 562 264
Readme file	Device Manager readme file	readme_v5.9.5.0.txt	
Software Release 4.3.1 Management Information Base (MIB) definition files	MIB definition files	5530mibsv4.3.1.zip	1 048 576

Nortel Ethernet Routing Switch 5520 Phone Dongle

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

New software features in this release

Ethernet Routing Switch 5500 Series, Software Release 4.3.1 introduces features and commands to support the Nortel Secure Network Access (Nortel SNA) solution.

Antivirus software and intrusion protection systems are important features in protecting networks against viruses and worms. The goal of the Nortel SNA solution is to protect an enterprise network by providing a pre-defined level of clientless access to users based on credentials and security features.

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

Supported software and hardware capabilities

Table 2 lists the known limits for the Ethernet Routing Switch 5500 Series, Software Release 4.3.1 and Device Manager 5.9.5.0. These capabilities will be enhanced in subsequent software releases.

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

Table 2 Supported capabilities in the 5500 Series (Release 4.3.1)

Feature	Maximum number supported
VLANs	256
Protocol-based VLANs	7 HW entries. Depending on the protocol specified, the number of protocol VLANs supported at one time varies from 3–7.
Nortel SNA VLANs	1 Red VLAN per switch. Nortel recommends a maximum of 5 Yellow VLANs, 5 Green VLANs, and 5 VoIP VLANs per switch for release 4.3.1.
Nortel SNA ports	All ports. **Note:** The 5530 has two 10 Gigabit (Gb) ports. You can configure these as uplink ports only. You cannot configure these as dynamic ports.
ARP records	2 Kb
IP interfaces	256
Static routes	512
Spanning Tree groups	8
Aggregation groups (link aggregation)	6
Ports per aggregation group	4
IGMP maximum number of unique groups	240
EAPoL 802.1x supplicants	All ports

Issues resolved in release 4.3.1

Table 3 describes issues resolved in Ethernet Routing Switch 5500 Series, Software Release 4.3.1.

Table 3 Issues resolved in 5500 Series Software Release 4.3.1

Change Request Number	Issue
Q01104935	Under certain conditions, a switch may not age out all entries in the MAC Address Table.

Known limitations and considerations in this release

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

Table 4 describes additional issues known to exist in the 5500 Series Software Release 4.3.1.

Table 4 Ethernet Routing Switch 5500 Series known limitations

Change Request Number	Issue
Q01265045	If you delete a Nortel IP phone signature on the switch, that phone can still get an IP in the VoIP VLAN and connect to the call server.
Q01256947	To disable an MLT that is a Nortel SNA uplink, disable Nortel SNA on the MLT ports first: **`enable`** **`configure terminal`** **`no nsna port x`** (where **`x`** is an MLT port)
Q01252555	If you reset your stack, or any unit in the stack, the Nortel SNAS 4050 may require some time (up to several minutes) to get all port information. During this time, clients may experience a slow login time, and clients in the Yellow and Green VLANs attempting to log out receive the 'Cannot display this page' error message.
Q01249003	If you attempt to set a port as a Nortel SNA uplink or dynamic port, and that port is already configured as an uplink or dynamic port, the command fails if the VLAN list is different from the one used to configure that port originally. No meaningful message is displayed, in this case. Also, if you do not specify a VLAN list, the list you entered to configure that port originally is used (this applies to the dynamic port only).
Q01231314	After downloading the wrong SSH DSA Auth key five times, the TCP/UDP ports close, and you cannot open a Telnet/ SSH session. Workaround: Ensure you carefully look at the authentication keys downloaded to the switch. If the ports close, you must reset the switch.

Table 4 Ethernet Routing Switch 5500 Series known limitations (continued)

Change Request Number	Issue
Q01228894	When the switch is in Layer 3 mode, and a PC client is disconnected from a port and reconnected to a port in less than 10 seconds, the IP address can show as 0.0.0.0 and the VLAN ID can show as 1. Workaround: Enter the ipconfig/release command, followed by the ipconfig/renew command on the PC client (in the command line). Refer to *Release Notes for the Nortel Secure Network Access Solution, Software Release 1.0* (320850-A) for information on supported PC operating systems.
Q01217035	It can take 2–3 minutes to globally enable/disable Nortel SNA, especially on a fully populated stack with all ports Nortel SNA-enabled.
Q01186169	If a client is already connected to a port when you configure Nortel SNA on that port, the client does not do a “DHCP renew”, and so the client retains its old IP. This applies to Nortel SNA client ports only, and not to Nortel SNA uplink ports. Workaround: You must shut down the port and re-enable it to force the client to renew its IP using DHCP. You can shut down the port and re-enable it using the “shutdown/no shutdown” command sequence. Alternatively, you can unplug/plug in the client.
Q01185566	You can enter the Nortel SNA uplink port in a limited number of VLANs (that number is lower than the maximum number of the VLANs the switch supports) because CLI commands have a length limitation.

Note: The commands that configure Nortel SNA are not generated in the ASCII configuration file (`show running-config` or `copy running-config`).

Table 5 describes considerations for 5500 Series Software Release 4.3.1.

Table 5 Considerations for 5500 Series Release 4.3

Item	Description
1	When you enter the `show nsna client` command, the switch can sometimes show an IP address of 0.0.0.0 for an IP phone, and on the Nortel SNAS 4050 you see a dash (-) for the IP address. The phone is still working in this circumstances, and can connect to the call server (also see Change Request Number Q01228894). The following scenarios lead to this behavior (on a phone not powered from a PoE port): 1. You reset the switch. 2. You move the phone to a different port, or unplug and plug it in the same port.
2	Only one PC and one Nortel IP phone can be connected to a Nortel SNA port. Any additional PCs or phones are blocked.
3	If more than 10 devices come to the same Nortel SNA port, the switch shuts down that port. If this happens, you must enable the port manually from any interface (that is, from the CLI, Web, or Device Manager console interface). For example, use the following CLI commands: **`enable`** **`configure terminal`** **`interface fast x`** (where **`x`** is the port number) **`no shutdown`**
4	Nortel recommends that you avoid enabling Nortel SNA and IPFIX on the same port in release 4.3.1.

Nortel SNA mode to default mode – rollback instructions

When you enable Nortel SNA on a 5500 Series switch, 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: the Spanning Tree state (when Nortel SNA is enabled on a port, STP runs in FAST START mode to enable faster convergence) 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.

Deploying the Nortel SNA solution in an active network

You can deploy the Nortel SNA solution on an existing, active Ethernet Routing Switch 5500 Series. You must upgrade the switch to a minimum software release of 4.3.1, and you must understand how the implementation of Nortel SNA on the edge switch impacts the switch functions.

In this document, the term “network access device” is used to refer to the Ethernet Routing Switch 5500 Series edge switch once it is configured for the Nortel SNA environment. A port on the network access device can operate in one of two modes of operation:

- 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 that port:

- The port is removed from the existing VLAN and 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).

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

When Nortel SNA is disabled, the port returns to the pre-Nortel SNA state (see "Nortel SNA mode to default mode – rollback instructions" on page 18).

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" on page 47).

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 should be Fast Learning enabled on the router port, also).

You can configure multiple Nortel SNA uplink ports (see "Implementing the Nortel SNA solution" on page 24 and "Enabling Nortel SNA on ports" on page 45 for more information on uplink ports).

You can add/delete the uplink port to/from a non-Nortel SNA VLAN (see "Configuration example: Adding the uplink port" on page 47 for more information). 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.

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

Connect only PCs, devices that can run TunnelGuard, and Nortel IP phones to a Nortel SNA port. Refer to *Release Notes for the Nortel Secure Network Access Solution, Software Release 1.1* (320850-B) for a list of specific devices. Devices that cannot run TunnelGuard, or have static IP addresses must be in non-Nortel SNA VLANs. In addition, no non-Nortel SNA ports can be associated with Nortel SNA VLANs.

Nortel SNA VLANs 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 "Configuring QoS for the Nortel SNA solution" on page 52 and "Default Nortel SNA filters" on page 88 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 co-existing 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 4.3.1, Nortel recommends that you configure no more than five Yellow, five Green, and five VoIP VLANs on each switch.

Ensure you thoroughly plan your Nortel SNA deployment. For example, as part of the Nortel SNA configuration on the 5500 Series switch, you must configure the Nortel Secure Network Access Switch 4050 (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—see "Configuring Nortel SNA using the CLI" on page 39 for the Nortel SNA commands). 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 "Configuring QoS for the Nortel SNA solution" on page 52 and "Configuration example:

configuring the default Nortel SNA filters" on page 88 for specific information).

2 Remove the filters, and reconfigure:

a Disable Nortel SNA.

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:

— Delete all the filters at once:

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

— 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`—see "Removing the Nortel SNAS 4050 subnet" on page 41 for information on this command).

f Reconfigure Nortel SNA.

Documentation additions and corrections

Configuring the Ethernet Routing Switch 5500 Series for Nortel SNA

Documentation additions in this section are for the next full release of the book titled, *Configuring and Managing Security for Nortel Ethernet Routing Switch 5500 Series*.

These additions describe the configuration procedures for enabling the Ethernet Routing Switch 5500 Series to function as a network access device in the LAN component of the Nortel SNA solution.

The following sections will be added to Chapter 1 of the book titled, *Configuring and Managing Security for Nortel Ethernet Routing Switch 5500 Series*:

- "Implementing the Nortel SNA solution" on page 24
- "Configuring Nortel SNA using the CLI" on page 39

The section titled, "Configuring Nortel SNA using Device Manager" on page 63, will be added to Chapter 3 of the book titled, *Configuring and Managing Security for Nortel Ethernet Routing Switch 5500 Series*.

The section titled, "Configuration example" on page 83, will be added to the book titled, *Configuring and Managing Security for Nortel Ethernet Routing Switch 5500 Series*.

The section titled, "Default Nortel SNA filters" on page 88, will be added as an Appendix to the book titled, *Configuring and Managing Security for Nortel Ethernet Routing Switch 5500 Series.*

Managing the Ethernet Routing Switch 5500 Series for Nortel SNA

Documentation additions in the section titled, "New system messages for Nortel SNA" on page 99, are for the next full release of the book titled, *System Configuration Guide for Nortel Ethernet Routing Switch 5500 Series*.

Implementing the Nortel SNA solution

The Ethernet Routing Switch 5500 Series can be configured as a network access device for the Nortel SNA solution.

Nortel SNA is a protective framework to completely secure the network from endpoint vulnerability. The Nortel SNA solution addresses endpoint security and enforces policy compliance. Nortel SNA delivers endpoint security by enabling only trusted, role-based access privileges premised on the security level of the device, user identity, and session context. Nortel SNA enforces policy compliance, such as for Sarbanes-Oxley and COBIT, ensuring that the required anti-virus applications or software patches are installed before users are granted network access.

The Nortel SNA solution provides a policy-based, clientless approach to corporate network access. The Nortel SNA solution provides both authentication and enforcement (operating system/antivirus/firewall code revision enforcement, Windows ® registry content verification and enforcement, file system verification and enforcement).

A PC/desktop user gains access into the corporate network by passing through:

- authentication
- host integrity check & remediation (if needed)

Before authentication, the user is given restricted access within the whole network (Red VLAN). The restrictions, by default, allow access to the Nortel SNAS 4050 and to the Windows domain controller (or other network login controller, for example, Novell netware login) only (this is based on the default Nortel SNA Red filter set). This is necessary to allow the authentication traffic. You can customize the filter sets to allow greater access, if necessary.

After the client's credentials are checked with an authentication server, a TunnelGuard applet (the security agent) is downloaded to every PC client. TunnelGuard provides continual device integrity checking.

After password authentication, if the host integrity check fails, the user is given access to the remediation network only (Yellow VLAN).

After successful completion of all of these phases, the user is given full access to the network, depending on the user profile (Green VLAN).

Nortel IP phones are allowed access to one of the preconfigured VoIP subnets, 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 detailed information on the Nortel SNA solution and deployment scenarios, refer to *Nortel Secure Network Access Solution Guide* (320817-A). For information on configuring the Nortel SNAS 4050, refer to *Nortel Secure Network Access Switch 4050 User Guide* (320818-A).

Port modes

Nortel supports the following three 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 a RADIUS server. In this scenario, there is a client (for example, the EAP supplicant) present in the PC.

- Nortel SNA mode (Nortel SNA clientless dynamic IP [DHCP is necessary for both phone and PC]).

  A client receives a dynamic IP address and the PC client goes through authentication, and possibly remediation network, before it is allowed into the corporate network. No prior knowledge of the client PC is required on the switch, and the client does not require any pre-installed software to operate in the Nortel SNA solution.

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).

Using filters with the Nortel SNA solution

A corresponding Nortel SNA filter set is provisioned for Nortel SNA Red, Yellow, and Green VLANs. 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 once you have enabled them and assigned them to the Nortel SNA VLANs (see "Configuring QoS for the Nortel SNA solution" on page 52 for more information). For an example of the current default Nortel SNA filter set rules, refer to "Default Nortel SNA filters" on page 88.

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"Nortel SNA mode to default mode – rollback instructions" on page 18 and "Deploying the Nortel SNA solution in an active network" on page 19 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 are dependent 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 login. 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 co-existing on Nortel SNA ports.

Red, Yellow, and Green VLANs must be configured on the Nortel SNA uplink ports of the network access device according to the network topology using `nsna port <portlist> uplink vlans <vidlist>` (see "Enabling Nortel SNA on ports" on page 45). Only Nortel SNA ports (uplink or dynamic) can be in the

Red, Yellow, and Green VLANs. Nortel SNA ports become members of Nortel SNA VLANs 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 ports) 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 will be 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" on page 32 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 4.3.1, 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. 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—in the Green VLAN, all traffic is allowed by the default filter, therefore VoIP filters are not specifically added). 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 must use DHCP. If the device is configured to use a static IP address, the device cannot function on a Nortel SNA port.

Table 6 shows filter consumption when using the default Nortel SNA filters.

Table 6 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. Table 7 on page 29 describes the traffic allowed by each default Nortel SNA filter set.

Table 7 Traffic allowed in the default Nortel SNA filter sets

Filter set	DNS traffic	HTTP traffic	HTTPS traffic	ARP traffic	UDP traffic	ICMP traffic	Yellow subnet traffic	All traffic
*Red	Traffic to Nortel SNAS 4050 allowed	Traffic to Nortel SNAS 4050 allowed	Traffic to Nortel SNAS 4050 allowed	Yes		Yes		
Yellow	Traffic to Nortel SNAS 4050 allowed	Traffic to Nortel SNAS 4050 allowed	Traffic to Nortel SNAS 4050 allowed	Yes		Yes	Yes	
Green								Yes
VoIP					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 Table 6 on page 28).

Refer to "Configuring filters for Novell Netware login" on page 30 for information on configuring the filters for Novell Netware login. If you use any other login controller, you must modify the filter set to allow the login 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>` (refer to "Configuring Nortel SNA per VLAN" on page 41). You can enter the Remedial server IP/subnet as the Yellow subnet IP.

You can also add multiple IPs 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 "Configuring QoS for the Nortel SNA solution" on page 52 for more information on 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 login

If you use Novell Netware as your domain login, the following is one example of IPX filters for the Red VLAN. Note that these filters would 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
```

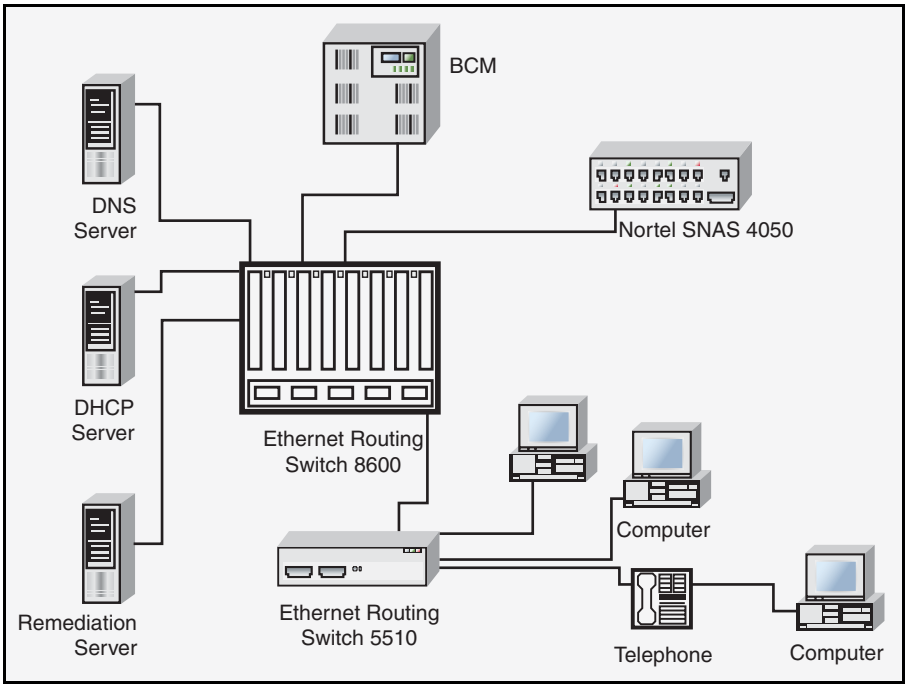
Topologies

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

Layer 2

In Layer 2 mode, DHCP-relay is done on a central router, or routing switch. Figure 1 on page 33 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.

Figure 1 Network access device—Layer 2 mode



Layer 3

In Layer 3 mode, DHCP-relay is enabled on the Ethernet Routing Switch 5500 Series switch. In the network setup shown in Figure 1, 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 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 Ethernet Routing Switch 8600 (that is, the core routing device) in your network, if it exists, before you configure the network access device.

Before you begin

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

- Generate the SSH keys on the Nortel SNAS 4050, and upload the public key to a TFTP server.
- Identify the Nortel SNAS 4050 pVIP address and mask.
- Identify VLAN IDs for Nortel SNA use (that is, for Red, Yellow, Green, and VoIP VLANs).
- Identify ports you will use for uplink ports (in Layer 2 mode only).
- Identify ports you will use for Nortel SNA client ports.

Configuring the network access device

To configure the 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. CLI commands for configuring the Nortel SNA solution on the switch are in the section, "Configuring Nortel SNA using the CLI" on page 39.

1. Configure static routes to all the networks behind the core routing device.
2. Configure the switch management VLAN, if necessary.
3. Configure SSH (see "Configuring SSH on the 5500 Series switch for Nortel SNA" on page 37):
   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 switch).

4 Configure the Nortel SNAS 4050 pVIP address/subnet.

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.

These VLANs are configured as VoIP, Red, Yellow, and Green VLANs in Step 9 and Step 10.

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 (see Step 9 and Step 10).

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

9 Configure the VoIP VLANs.

10 Configure the Red, Yellow, and Green VLANs, associating each with the applicable filters.

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.

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: If the Nortel SNA switch 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: You can configure Nortel SNA ports (both dynamic and uplink) after Nortel SNA is enabled globally.

12 Enable Nortel SNA globally.

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:

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:

```
5510-48T(config)# 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 in Step a.

2 On the 5500 Series switch, enable SSH using the following command from the Global configuration mode:

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

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

Configuring Nortel SNA using the CLI

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

Specifically, it includes the following topics:

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>).

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 (see "Configuration example: configuring the Nortel SNA VLANs" on page 43), you must manually update the Nortel SNAS 4050 subnet in the filters.

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 Communication Protocol (SSCP) server. Values are in the range 1024–65535. The default setting is 5000.

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 Nortel SNA per VLAN

Note: 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.

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:** This parameter is not allowed for configuration of a VoIP VLAN. VoIP filters are part of the Red/Yellow filter sets. **Note:** 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 on creating VLANs using the Ethernet Routing Switch 5500 Series, refer to *Configuring VLANs, Spanning Tree, and Multilink Trunking for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.2* (217464-A)).

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.

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
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 on port modes, refer to "Port modes" on page 25.

The uplink port is introduced for the Nortel SNA solution. These ports are members of the Nortel SNA VLANs. For more information on the uplink port, refer to *Nortel Secure Network Access Switch 4050 User Guide* (320818-A).

Note: The Ethernet Routing Switch 5530 has two 10 Gb 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 will fail because the two 10 Gb 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][,...]}.

nsna followed by:	
`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 "vlan members command" in *Configuring VLANs, Spanning Tree, and Multilink Trunking for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.2* (217464-A) 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.

Multiple Nortel SNA uplink ports are supported for Ethernet Routing Switch 5500 Series, Software Release 4.3.1.

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-if)#nsna uplink vlans 110,120,130,140
5510-48T(config-if)#show nsna interface 20
Port NSNA Mode Green VLAN ID VLAN IDs           State

DHCP State
-------------------------------------------------------------------------------------------
20   Uplink                   110,120,130,140  None

Unblocked
5510-48T(config-if)#exit
5510-48T(config)#
```

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-if)#nsna dynamic voip-vlans 140
5510-48T(config-if)#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-if)#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. It cannot be set to Normal Learning for Nortel SNA.

Viewing information on Nortel SNA clients

To view information on 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

For example, to view information about Nortel SNA clients, you can enter the following command:

```
5510-48T# show nsna client interface 5
Port Client MAC        Device Type Vlan Id  IP Address  Exp
-------------------------------------------------------------
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:

```
show nsna phone-signature [<LINE>]
```

where <LINE> is the phone signature string. The <LINE> parameter can contain an asterisk (*) at the end of the string to indicate that all signatures that start with the specified string will be displayed. 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. Refer to "Configuring SSH on the 5500 Series switch for Nortel SNA" on page 37 for detailed information.

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 on 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
```

Configuring QoS for the Nortel SNA solution

This section will be added to Chapter 2, "Configuring Quality of Service (QoS) with the CLI", of *Configuring Quality of Service and IP Filtering for Nortel Ethernet Routing Switch 5500 Series*.

When you assign a filter name using the `nsna vlan <vid> color <red|yellow|green> filter <name>` command (for example, `nsna vlan 110 color red filter redFilter`), the switch automatically creates all the necessary QoS classifiers with the name you assigned (in this case, redFilter) if that filter set does not already exist. If you had previously defined the filter (using the `qos nsna` command), then that pre-existent filter is used. Once a filter is created (either by you or automatically by the switch), it can be modified (that is, entries can be deleted or added) using the `qos nsna` command (see "Configuring Nortel SNA using Device Manager" on page 63 if you are using the Java Device Manager to modify 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).

There are eight policies available on the switch for Nortel SNA. The default Red filter set consumes four policies (two policies use classifier blocks, and two policies use classifiers (allowing ICMP and ARP)). The default Yellow filter set consumes five policies (two classifier blocks, and three classifiers). If you use the login filters (see Table 7 on page 29—these filters use classifier blocks), note that an additional precedence level is consumed.

See Table 6 on page 28 for information on filter consumption.

See "Default filter parameters" on page 90 for detailed information on the filter sets.

You can configure custom filters, but you must include them in the Nortel SNA filter set.

To configure QoS for Nortel SNA filters, use the following command from the Global configuration mode:

```
qos nsna
```

This command includes the following parameters:

qos nsna followed by:	
`classifier name [addr-type {ipv4|ipv6}] [block] [drop-action] [ds-field] [dst-ip] [dst-mac] [dst-port-min] [ethertype] [eval-order] [flow-id] [next-header] [priority] [protocol] [set-drop-prec] [src-ip] [src-mac] [src-port-min] [update-1p] [update-dscp] [vlan-min] [vlan-tag]`	Creates the QoS Nortel SNA classifier entry. Optional parameters: • addr-type {ipv4|ipv6} specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses. • block specifies the label to identify access list elements that are of the same block. • drop-action specifies whether or not to drop non-conforming traffic. • ds-field specifies the value for the DiffServ Codepoint (DSCP) in a packet. • dst-ip specifies the IP address to match against the destination IP address of a packet.

qos nsna followed by:	
	• dst-mac specifies the MAC address against which the MAC destination address of incoming packets is compared. • dst-port-min specifies the minimum value for the Layer 4 destination port number in a packet. • ethertype specifies a value indicating the version of Ethernet protocol being used. • eval-order specifies the evaluation order for all elements with the same name. • flow-id specifies the flow identifier for IPv6 packets. • next-header specifies the IPv6 next-header value. Values are in the range 0–255. • priority specifies a value for the 802.1p user priority. • protocol specifies the IPv4 protocol value. • set-drop-prec specifies automatic drop precedence (high-drop or low-drop). • src-ip specifies the IP address to match against the source IP address of a packet. • src-mac specifies the MAC source address of incoming packets. • src-port-min specifies the minimum value for the Layer 4 source port number in a packet. • update-1p specifies an 802.1p value used to update user priority. • update-dscp specifies a value used to update the DSCP field in an IPv4 packet • vlan-min specifies the minimum value for the VLAN ID in a packet. • vlan-tag specifies the type of VLAN tagging in a packet: tagged untagged

qos nsna followed by:	
`set name [committed-rate] [drop-nm-action] [drop-out-action] [max-burst-rate] [max-burst-duration]`	Creates the QoS Nortel SNA set. Optional parameters: • committed-rate specifies the committed rate in Kbps. • drop-nm-action specifies the action to take when a packet is non-matching. This action is applied to all traffic that was not previously matched by the specified filtering data. Options are the following: enable (the packet is dropped) disable (the packet is not dropped) • drop-out-action specifies the action to take when a packet is out-of-profile. This action is applied only if metering is being enforced, and if the traffic is deemed out-of-profile based on the level of traffic and the metering criteria. (Metering is applied only to traffic matching the filtering data.) Options are the following: enable (the packet is dropped) disable (the packet is not dropped) • max-burst-rate specifies the maximum number of bytes allowed in a single transmission burst. • max-burst-duration specifies the maximum burst duration in milliseconds.

Note: To modify an entry (corresponding to an evaluation order) in a filter set, you must delete that entry and add the new entry as desired.

For example:

```
no qos nsna eval-order 8

qos nsna classifier name red protocol 17 dst-port-min
427 dst-port-max 427 ethertype 0x0800 drop-action
disable block novell eval-order 8
```

Example: using qos nsna commands

The following command is an example of adding a classifier to an existing filter set (in this example, the ALPHAYELLOW filter set):

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

The following commands are an example of adding a classifier block (remedial) to an existing filter set (ALPHAYELLOW):

Note: To consume only one precedence level, group classifiers in a classifier block.

```
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
```

The following commands are an example of classifiers configured to allow various TCP/UDP destination ports in the red filter set, and configured as a classifier block (novell):

```
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
```

Deleting a classifier, classifier block, or an entire filter set

To delete an entire filter set, use the following command from the Global configuration mode:

```
no qos nsna name <filter name>
```

where `<filter name>` is the label used to reference the Nortel SNA entry.

To delete a classifier, use the following command from the Global configuration mode:

```
no qos nsna name <filter name> eval-order <value>
```

where:

- `<filter name>` is the label used to reference the Nortel SNA entry
- `<value>` is the evaluation order identifier that references the specific Nortel SNA entry

To delete a classifier block, use the command for deleting a classifier to delete all the classifier members in that block.

Note: You cannot delete all the classifiers in a filter set. There should always be at least one remaining.

Viewing filter descriptions

To view Nortel SNA filter parameters, use the following command from the Privileged EXEC configuration mode:

```
show qos nsna
```

To view the parameters for a specific filter set, use the following command from the Privileged EXEC configuration mode:

```
show qos nsna name <filter name>
```

To view ports and the filter sets assigned to those ports, use the following command from the Privileged EXEC configuration mode:

```
show qos nsna interface
```

To view classifier entries, use the following command from the Privileged EXEC configuration mode:

```
show qos nsna classifier
```

Refer to "Default filter parameters" on page 90 for Nortel SNA default filter parameters returned using the `show qos nsna` command.

Using the QoS Web-based Wizard for Nortel SNA

Refer to the *System Configuration Guide for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.2* (217462-A) for information on accessing the Web-based management interface for the 5500 Series switch.

You can use the Web-based management interface QoS Wizard for creating new Nortel SNA filters, or for viewing existing Nortel SNA filters. Only rate limit–related parameters can be modified from the Web interface on existing filters (and only if the filter is already configured for that):

- Meter Committed Rate
- Burst Size
- Out-Profile Action Drop

Use the CLI or Device Manager to make other changes to filters.

Using the web-based QoS Wizard to create new Nortel SNA filters

To create new Nortel SNA filters:

1. Open the Web-based management interface.
2. Select **Applications > QoS > QoS Wizard > QoS Wizard Config** from the menu (see Figure 2 on page 59).

Figure 2 Opening the QoS Configuration Wizard in the Web-based management interface

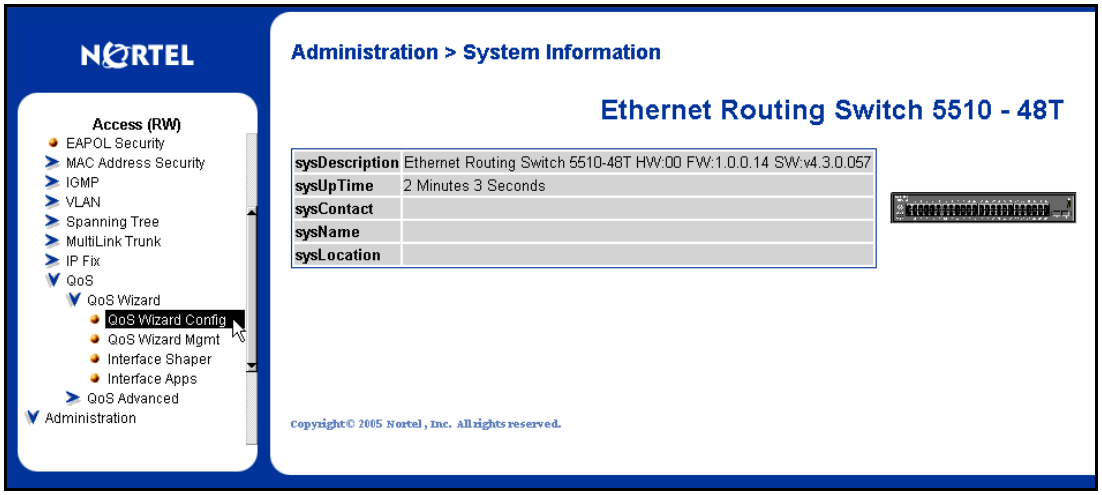
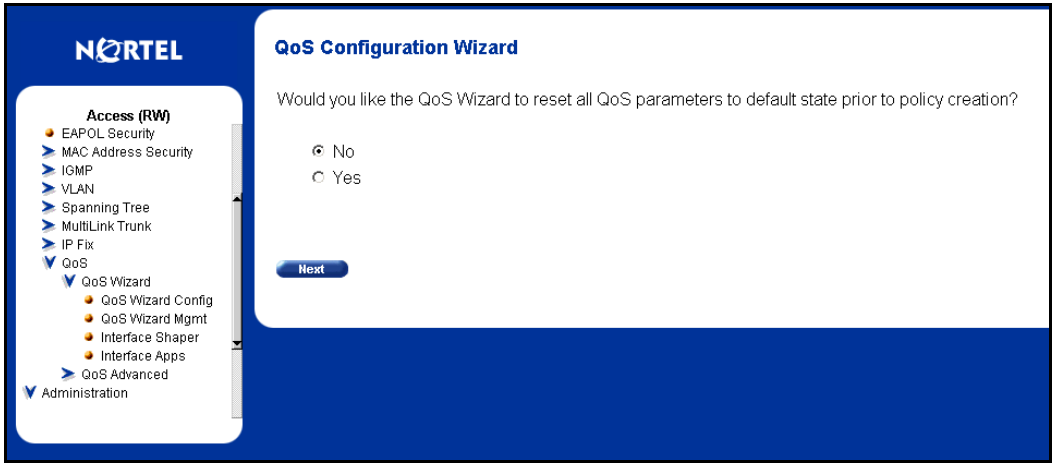


Figure 3 shows the first page of the QoS Configuration Wizard.

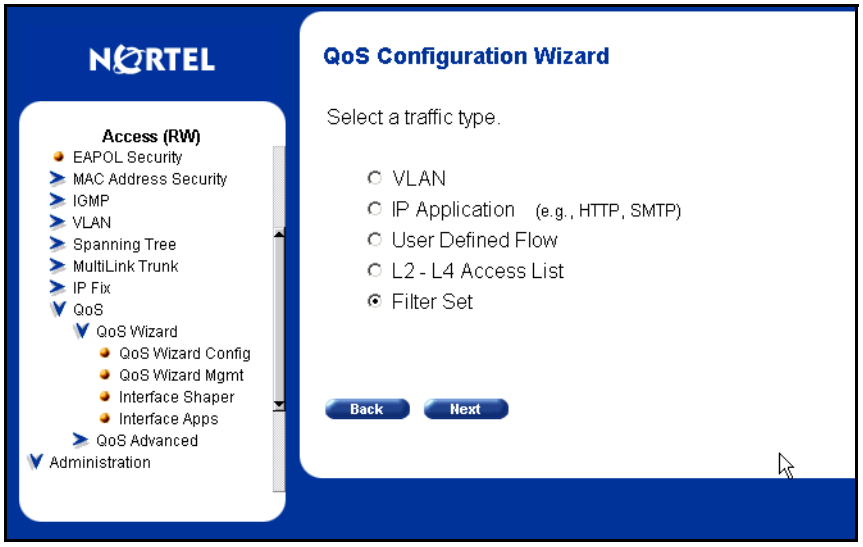
Figure 3 QoS Configuration Wizard



3 Click **Next**.

4 Select the **Filter Set** option button for the traffic type (see Figure 4 on page 60).

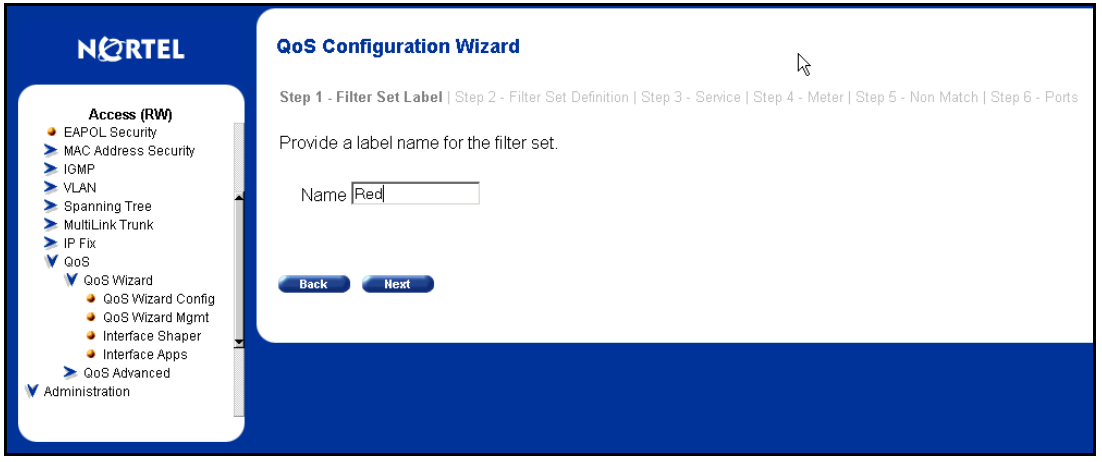
Figure 4 QoS Configuration Wizard: selecting the traffic type



5 Click **Next**.

6 Enter the name of the filter set you want to create (see Figure 5).

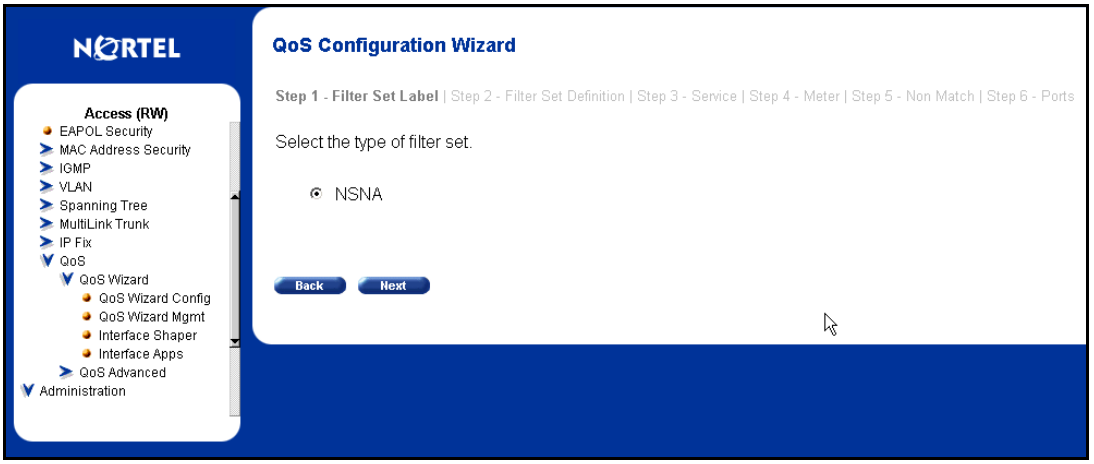
Figure 5 QoS Configuration Wizard: specifying the filter set name



7 Click **Next**.

8 Select the **NSNA** filter set option button, if not already selected (see Figure 6).

Figure 6 QoS Configuration Wizard: specifying the type of filter set



Use the pages that follow to configure your Nortel SNA filter set.

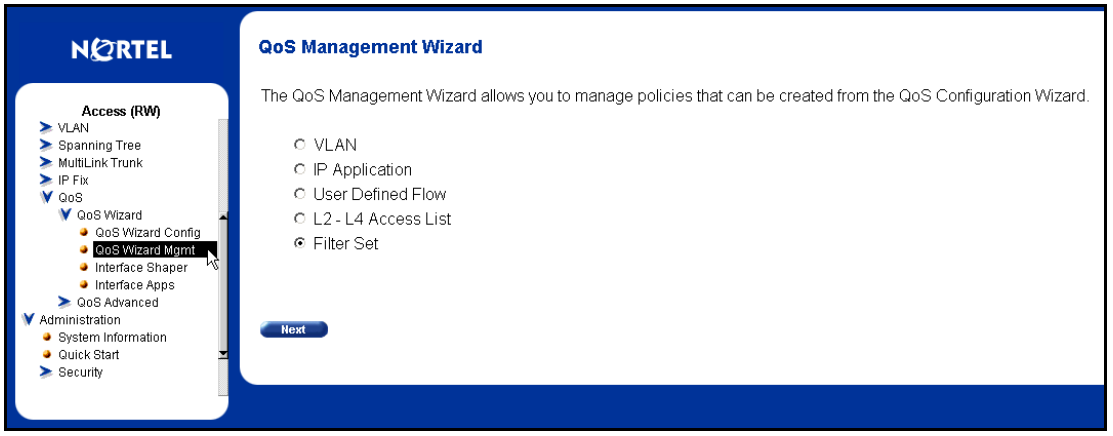
Using the web-based QoS Wizard to view or modify Nortel SNA filters

To view or modify existing Nortel SNA filter sets:

1 Select **Applications > QoS > QoS Wizard > QoS Wizard Mgmt** from the Web-based management interface menu.

2 Ensure you select the **Filter Set** option button (see Figure 7 on page 62).

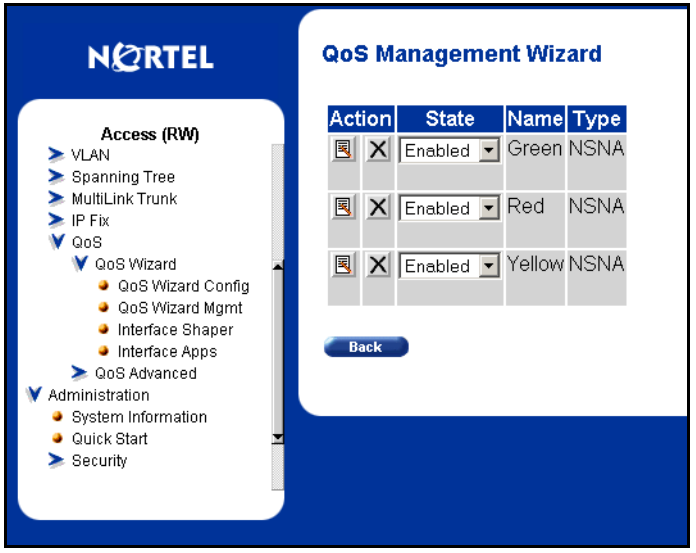
Figure 7 QoS Management Wizard: selecting the policies to manage



3 Click **Next**.

The page shows the current Nortel SNA filter sets (see Figure 8).

Figure 8 QoS Management Wizard: viewing or modifying the Nortel SNA filter sets



Configuring Nortel SNA using Device Manager

This section is added to Chapter 3, "Security Configuration and Management using the Java Device Manager", of the next full release of *Configuring and Managing Security for Nortel Ethernet Routing Switch 5500 Series*.

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

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

Specifically, it includes the following topics:

Configuring the Nortel SNAS 4050 subnet

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

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

The **NSNA** dialog box opens with the **NSNAS** tab selected (see Figure 9 on page 64).

Figure 9 The **NSNA** dialog box opens with the **NSNAS** tab selected.Security NSNA dialog box > NSNAS tab

Table 8 describes the **NSNAS** tab fields.

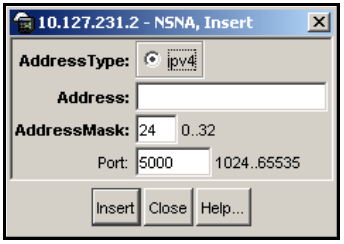
Table 8 NSNA NSNAS tab fields

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 Communication Protocol (SSCP) server. The default setting is 5000.

2 Click **Insert**.

The **NSNAS, Insert** dialog box opens (see Figure 10).

Figure 10 Security 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 (see "Configuration example: configuring the Nortel SNA VLANs" on page 43), 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.

Note: In Ethernet Routing Switch 5500 Series, Software Release 4.3.1, only one entry for the Nortel SNAS 4050 subnet can be configured.

Removing the Nortel SNAS 4050

To remove the currently configured Nortel SNAS 4050:

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

The **NSNA** dialog box opens with the **NSNAS** tab selected (see Figure 9 on page 64).

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.

Configuring QoS for the Nortel SNA solution

When you assign a filter name to a VLAN (for example, redFilter), the switch automatically creates all the necessary QoS classifiers with the name you assigned (in this case, redFilter) if that filter set does not already exist.

If you had previously defined the filter, then that pre-existent filter is used. Once a filter is created (either by you or automatically by the switch), it can be modified (that is, entries can be deleted or added) on the **QOS_NSNA** dialog box.

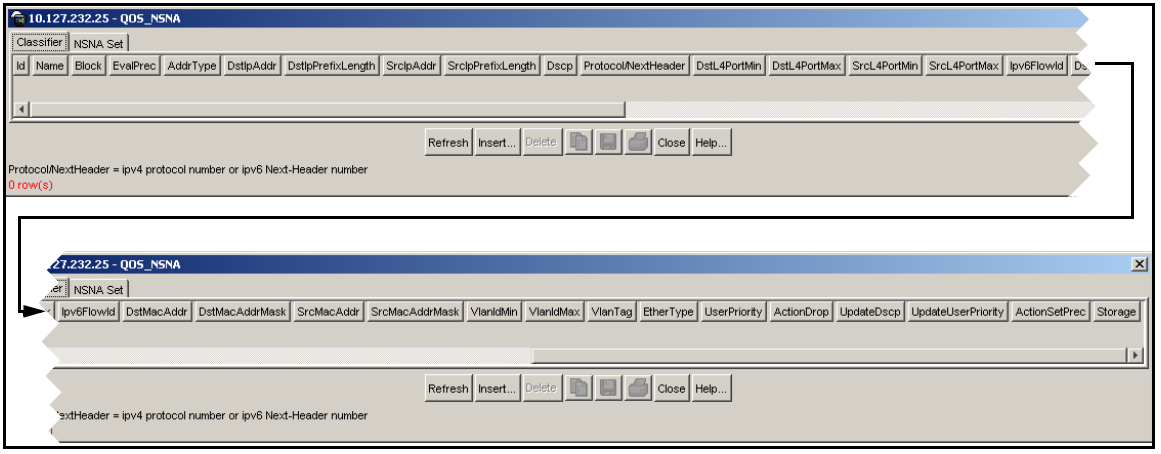
Inserting a Nortel SNA classifier

To configure a classifier for the Nortel SNA solution:

1 Select **QoS > QoS NSNA** from the Device Manager menu.

The **QOS_NSNA** dialog box opens with the **Classifier** tab selected (see Figure 11).

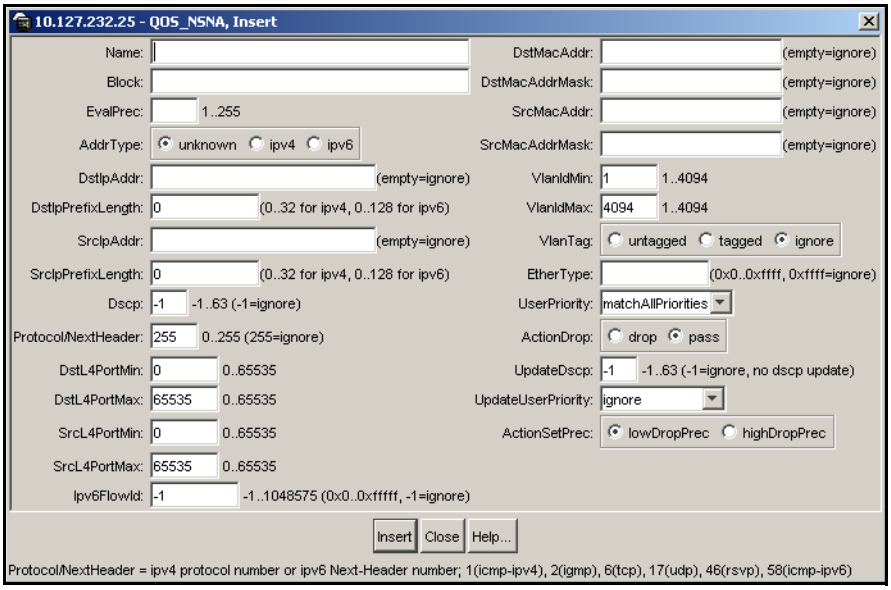
Figure 11 QOS_NSNA dialog box > Classifier tab



2 Click **Insert**.

The **QOS_NSNA, Insert** dialog box opens (see Figure 12 on page 67).

Figure 12 QOS_NSNA, Insert dialog box



3 Enter the classifier information in the fields.

4 Change values in any fields that present default values if you want to configure specific parameters.

5 Click **Insert**.

The information for the classifier appears in the **Classifier** tab of the **QOS_NSNA** dialog box.

Table 9 describes the **QOS_NSNA Classifier** tab fields.

Table 9 QOS_NSNA Classifier tab fields

Field	Description
Id	Specifies the ID number of the Nortel SNA classifier.
Name	Specifies the name of the Nortel SNA classifier. All classifiers with the same name are part of the same filter set. That filter set has the same name as the classifiers.
Block	Specifies the block name with which the classifier is associated.

Table 9 QOS_NSNA Classifier tab fields (continued)

Field	Description
EvalPrec	Specifies the evaluation order number of the classifier in that Nortel SNA filter set. Two classifiers in the same filter set cannot have the same evaluation order. A higher eval order means a lower precedence for the corresponding policy.
AddrType	Specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses.
DstIpAddr	Specifies the IP address to match against the destination IP address of a packet.
DstIpPrefixLength	Specifies the length of the destination address mask.
SrcIpAddr	Specifies the IP address to match against the source IP address of a packet.
SrcIpPrefixLength	Specifies the length of the source address mask.
Dscp	Specifies the value for the DiffServ Codepoint (DSCP) in a packet.
Protocol/NextHeader	Specifies the IPv4 protocol value, or the IPv6 next-header value. Values are the following: • 1 = ICMP-IPv4 • 2 = IGMP • 6 = TCP • 17 = UDP • 46 = RSVP • 58 = ICMP-IPv6
DstL4PortMin	Specifies the minimum value for the Layer 4 destination port number in a packet.
DstL4PortMax	Specifies the maximum value for the Layer 4 destination port number in a packet.
SrcL4PortMin	Specifies the minimum value for the Layer 4 source port number in a packet.
SrcL4PortMax	Specifies the maximum value for the Layer 4 source port number in a packet.
Ipv6FlowId	Specifies the flow identifier for IPv6 packets.
DstMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets is compared.
DstMacAddrMask	Specifies a mask identifying the destination MAC address.
SrcMacAddr	Specifies the MAC source address of incoming packets.
SrcMacAddrMask	Specifies a mask identifying the source MAC address.

Table 9 QOS_NSNA Classifier tab fields (continued)

Field	Description
VlanIdMin	Specifies the minimum value for the VLAN ID in a packet.
VlanIdMax	Specifies the maximum value for the VLAN ID in a packet.
VlanTag	Specifies the type of VLAN tagging in a packet: • untagged • tagged • ignore
EtherType	Specifies a value for the Ether type.
UserPriority	Specifies a value for the 802.1p user priority.
ActionDrop	Specifies whether or not to drop non-conforming traffic.
UpdateDscp	Specifies a value used to update the DSCP field in an IPv4 packet.
UpdateUserPriority	Specifies an 802.1p value used to update user priority.
ActionSetPrec	Specifies automatic drop precedence (high or low).
Storage	Specifies the type of storage: • volatile • nonVolatile (default) • readOnly

Deleting a Nortel SNA classifier

1 Select **QoS > QoS NSNA** from the Device Manager menu.

The **QOS_NSNA** dialog box opens with the **Classifier** tab selected (see Figure 11 on page 66).

2 Select the classifier you want to delete.

3 Click **Delete**.

Configuring a Nortel SNA set

To configure a Nortel SNA set:

1 Select **QoS > QoS NSNA** from the Device Manager menu.

The **QOS_NSNA** dialog box opens with the **Classifier** tab selected (see Figure 11 on page 66).

2 Click the **NSNA Set** tab.

The **NSNA Set** tab is selected (see Figure 13).

Figure 13 QOS_NSNA dialog box > NSNA Set tab

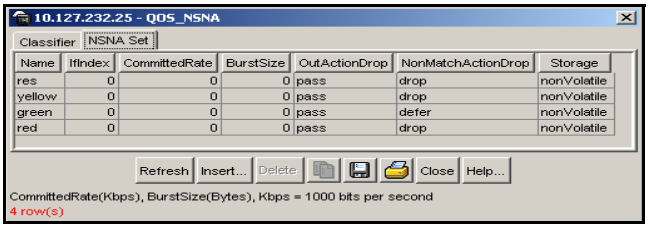


Table 10 describes the **QOS_NSNA NSNA Set** tab fields.

Table 10 QOS_NSNA NSNA Set tab fields

Field	Description
Name	Specifies a name for this entry. The name must be an existing classifier name. All classifiers with this name are part of this filter set. The filter set itself has this name.
IfIndex	Specifies the logical interface index assigned to the VLAN.
CommittedRate	Specifies the committed rate (in Kbps).
BurstSize	Specifies the maximum number of bytes in a single transmission burst.
OutActionDrop	Specifies the action to take when a packet is out-of-profile. This action is applied only if metering is being enforced, and if the traffic is deemed out-of-profile based on the level of traffic and the metering criteria. (Metering is applied only to traffic matching the filtering data.) Options are the following: • drop (the packet is dropped) • pass (the packet is not dropped) The default value is **pass**.

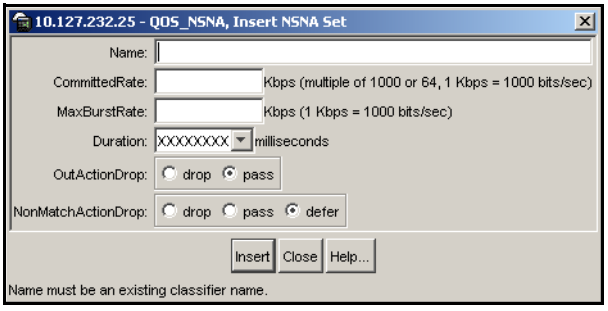
Table 10 QOS_NSNA NSNA Set tab fields (continued)

Field	Description
NonMatchActionDrop	Specifies the action to take when a packet is non-matching. This action is applied to all traffic that was not previously matched by the specified filtering data. Options are the following: • drop (the packet is dropped) • pass (the packet is not dropped) • defer (no explicit drop/pass action is specified; the decision is deferred) The default value is **defer**.
Storage	Specifies the type of storage.

3 Click **Insert**.

The **QOS_NSNA, Insert NSNA Set** dialog box opens (see Figure 14).

Figure 14 QOS_NSNA, Insert NSNA Set dialog box



4 Enter the Nortel SNA set information in the fields.

5 Click **Insert**.

The information for the Nortel SNA set appears in the **NSNA Set** tab of the **QOS_NSNA** dialog box.

Configuring Nortel SNA per VLAN

Note: 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:

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

The **VLAN** dialog box opens with the **Basic** tab selected (see Figure 15).

Figure 15 VLAN dialog box > Basic tab

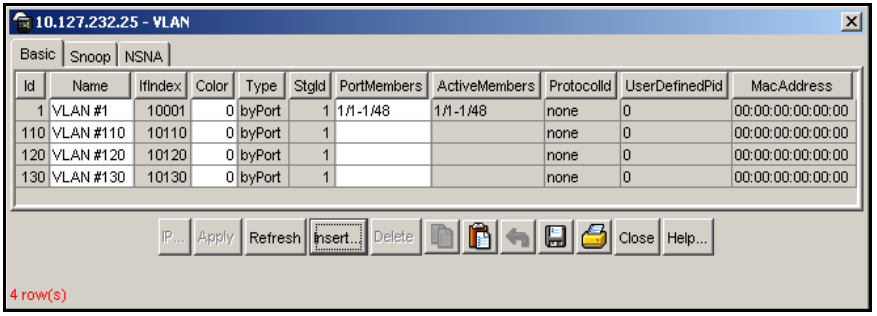


Table 11 describes the **VLAN Basic** tab fields.

Table 11 VLAN Basic tab fields

Field	Description
Id	Specifies the ID for the VLAN.
Name	Specifies the name of the VLAN.
IfIndex	Specifies the logical interface index assigned to the VLAN.
Color	A proprietary color scheme to associate a color with the VLAN. Color does not affect how frames are forwarded.
Type	Type of VLAN: • byPort • byProtocolId
StgId	The ID of the spanning tree group to which the VLAN belongs.

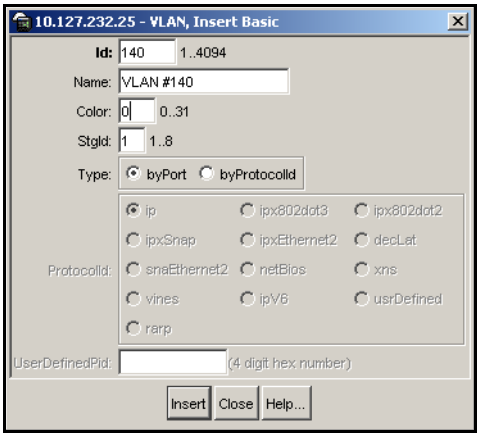
Table 11 VLAN Basic tab fields (continued)

Field	Description
PortMembers	The slot/port of each possible VLAN member.
ActiveMembers	The slot/port of each active VLAN member.
ProtocolId	Specifies the network protocol for protocol-based VLANs: • ip (IP version 4) • ipx802dot3 (Novell IPX on Ethernet 802.3 frames) • ipx802dot2 (Novell IPX on IEEE 802.2 frames) • ipxSnap (Novell IPX on Ethernet SNAP frames) • ipxEthernet2 (Novell IPX on Ethernet Type 2 frames) • decLat (DEC LAT protocol) • snaEthernet2 (IBM SNA on Ethernet Type 2 frames) • netBIOS (NetBIOS protocol) • xns (Xerox XNS) • vines (Banyan VINES) • ipv6 (IP version 6) • usrDefined (user-defined protocol) • RARP (Reverse Address Resolution protocol)
UserDefinedPid	Specifies the 16-bit user-defined network protocol identifier when the ProtocolId (above) is set to usrDefined for a protocol-based VLAN type.
MacAddress	The MAC address assigned to the virtual router interface for this VLAN. This field applies only when the VLAN is configured for routing. This MAC address is used as the Source MAC in routed frames and ARP replies.

2 Click **Insert**.

The **VLAN, Insert Basic** dialog box opens (see Figure 16 on page 74). Create the VLANs to be configured as Nortel SNA VLANs.

Figure 16 VLAN, Insert Basic dialog box



3 Enter the VLAN information in the **Id**, **Name**, **Color**, and **StgId** fields.

4 Select the **byPort** option button for VLAN type.

5 Click **Insert**.

The information for the VLAN appears in the **Basic** tab of the **VLAN** dialog box.

6 Click the **NSNA** tab.

The **NSNA** tab is selected (see Figure 17).

Figure 17 VLAN dialog box > NSNA tab

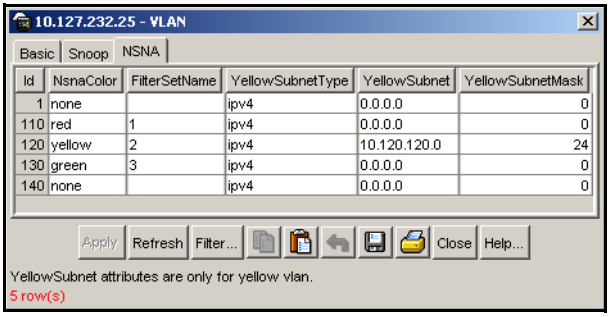


Table 12 describes the **VLAN NSNA** tab fields.

Table 12 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.

7 Double-click the **NsnaColor** field for each VLAN to select the color from the drop-down menu (input in Figure 17 on page 74 is for example purposes only—create, select, and configure the VLANs based on your network design).

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

9 Click **Apply**.

Note: Each switch 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 4.3.1, each switch supports up to five Yellow and five Green VLANs.

Removing a Nortel SNA VLAN

To remove a Nortel SNA VLAN:

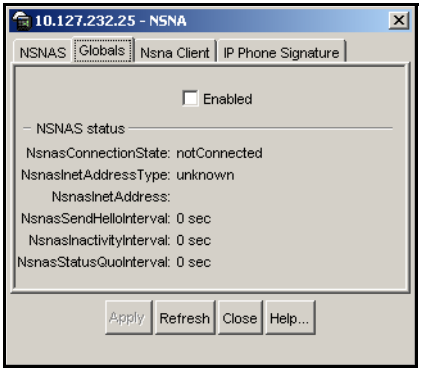
1 Select **Edit > Security > NSNA** from the Device Manager menu.

The **NSNA** dialog box opens with the **NSNAS** tab selected (see Figure 9 on page 64).

2 Click the **Globals** tab.

The **Globals** tab is selected (see Figure 18).

Figure 18 Security NSNA dialog box > Globals tab



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

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

4 Click **Close**.

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

The **VLAN** dialog box opens with the **Basic** tab selected (see Figure 15 on page 72).

6 Click the **NSNA** tab.

The **NSNA** tab is selected (see Figure 17 on page 74).

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

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

9 Click **Apply**.

10 Click the **Basics** tab.

The **Basics** tab is selected (see Figure 15 on page 72).

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

12 Click **Delete**.

Enabling Nortel SNA on ports

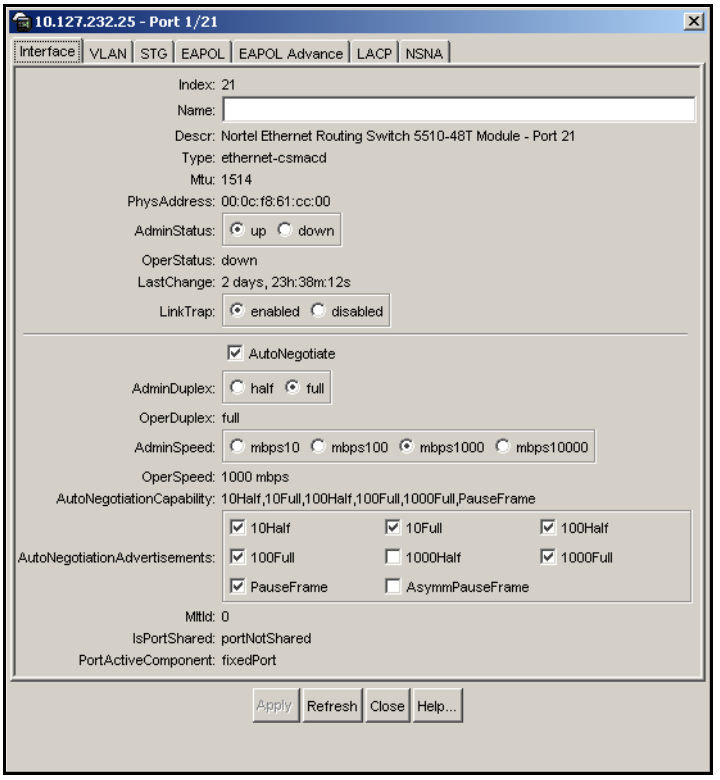
To enable Nortel SNA on ports:

1 Select a port that you want to add to the Nortel SNA solution.

2 Select **Edit > Port**.

The **Port** dialog box opens with the **Interface** tab selected (see Figure 19 on page 78).

Figure 19 Port dialog box > Interface tab



3 Click the **NSNA** tab.

The **NSNA** tab is selected (see Figure 20).

Figure 20 Port dialog box > NSNA tab

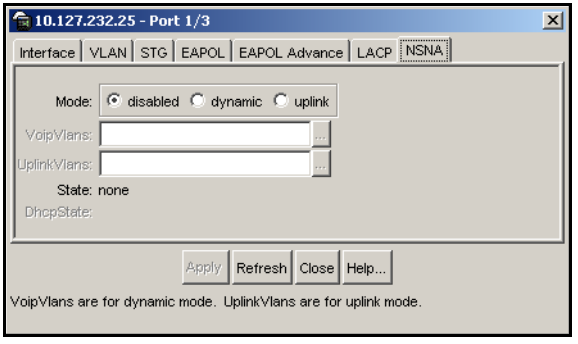


Table 13 describes the **NSNA** tab fields.

Table 13 Port NSNA tab fields

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

Viewing information on Nortel SNA clients

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

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

The **NSNA** dialog box opens with the **NSNAS** tab selected (see Figure 9 on page 64).

2 Click the **Nsna Client** tab.

The **Nsna Client** tab is selected (see Figure 21). Clients currently connected to the network access device display in this tab.

Figure 21 Security NSNA dialog box > Nsna Client tab

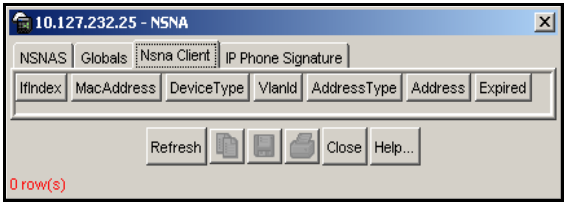


Table 14 describes the **NSNA Client** tab fields.

Table 14 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).
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.

Entering phone signatures for Nortel SNA

To specify IP phone signatures for Nortel SNA:

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

The **NSNA** dialog box opens with the **NSNAS** tab selected (see Figure 9 on page 64).

2 Click the **IP Phone Signature** tab.

The **IP Phone Signature** tab is selected (see Figure 22).

Figure 22 Security NSNA dialog box > IP Phone Signature tab

3 Click **Insert**.

The **NSNA, Insert IP Phone Signature** dialog box opens (see Figure 23).

Figure 23 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.

Removing Nortel SNA phone signatures

To remove a Nortel SNA phone signature:

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

   The **NSNA** dialog box opens with the **NSNAS** tab selected (see Figure 9 on page 64).

2. Click the **IP Phone Signature** tab.

   The **IP Phone Signature** tab is selected (see Figure 22 on page 81).

3. Select the row containing the IP phone signature you want to remove.
4. Click **Delete**.

Enabling Nortel SNA

Note: 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" on page 37 for detailed information.

To globally enable Nortel SNA:

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

   The **NSNA** dialog box opens with the **NSNAS** tab selected (see Figure 9 on page 64).

2. Click the **Globals** tab.

   The **Globals** tab is selected (see Figure 18 on page 76).

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.

Configuration example

The following 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 Software Release 4.3.1
- you have configured basic switch connectivity
- you have initialized the switch and it is ready to accept configuration

Configuring the 5500 Series switch for the Nortel SNA solution

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

Figure 24 on page 84 shows the basic network configuration used in this example. The Ethernet Routing Switch 8600 functions as the core router.

Table 15 describes the devices connected in this environment and their respective VLAN IDs and IP addresses.

Table 15 Network devices

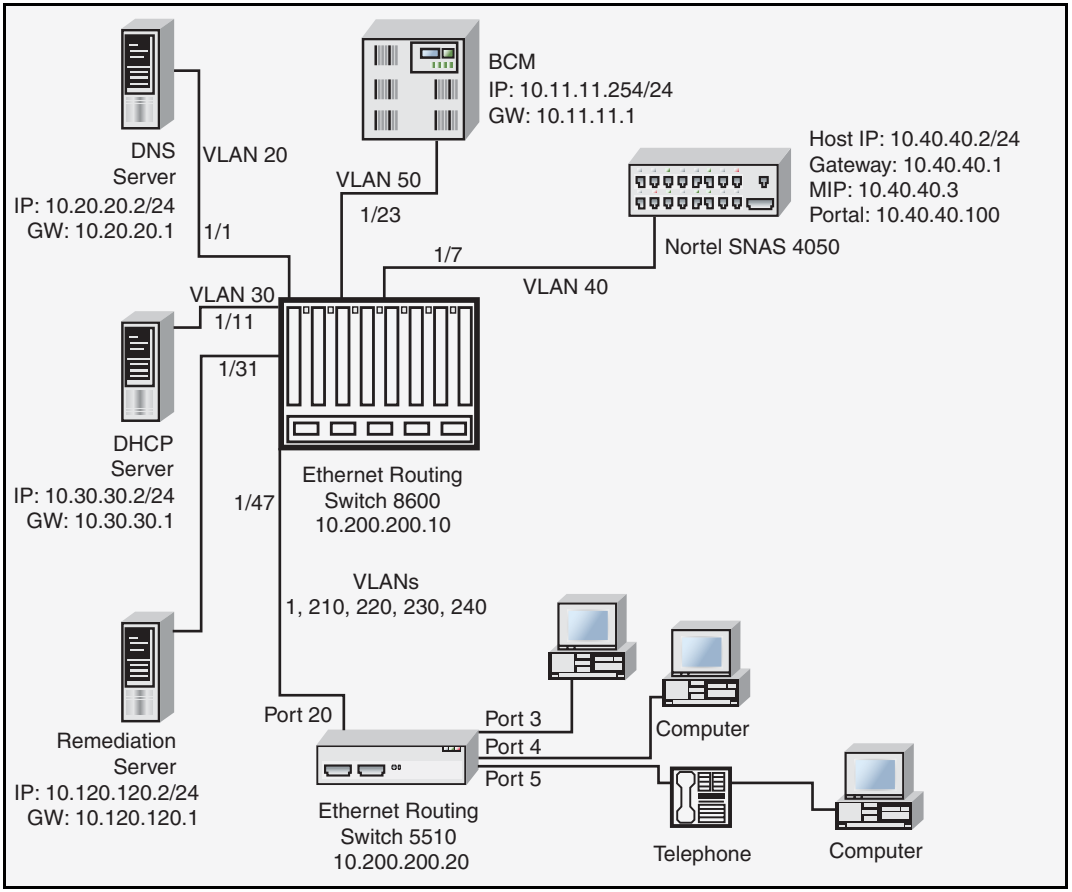
Device/Service	VLAN ID	VLAN IP	Device IP	Ethernet Routing Switch 8600 port
DNS	20	10.20.20.1	10.20.20.2	1/1
DHCP	30	10.30.30.1	10.30.30.2	1/11
Nortel SNAS 4050	40	10.40.40.1	10.40.40.2	1/7
Remediation server	120	10.120.120.1	10.120.120.2	1/31
Call server	50	10.11.11.1	10.11.11.254	1/23

Table 16 describes the VLANs for the Ethernet Routing Switch 5510.

Table 16 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

Figure 24 Basic network scenario



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

In this example, the assumption is 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 5500 Series switch. See "Configuring SSH on the 5500 Series switch for Nortel SNA" on page 37 for more information. Also, refer to *Nortel Secure Network Access Switch 4050 User Guide* (320818-A) for more information on 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 login domain controller filters

Note: This step is optional.

The PC client must be able to access the login domain controller you configure (that is, clients using the login 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
```

Default Nortel SNA filters

This section is added as an appendix to *Configuring and Managing Security for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.2* (217463-A).

The following example shows the default Nortel SNA filters that are created automatically by the switch. If you use the default filters created by the switch, ensure you configure the following settings in this order:

1. Configure the Nortel SNAS 4050 pVIP address.
2. Configure the VoIP VLANs (if VoIP is used).
3. Configure the Red, Yellow, and Green VLANs.

Configuration example: configuring the default Nortel SNA filters

You can use the following commands to manually replicate the default Nortel SNA filter sets.

Green Filter

The Green filter allows all traffic:

```
qos nsna classifier name GREENFILTER drop-action disable
eval-order 1

qos nsna set name GREENFILTER
```

Red Filter

HTTP traffic, HTTPS traffic, and DNS traffic for the Nortel SNAS 4050 portal VIP subnet

```
qos nsna classifier name REDFILTER dst-ip 10.40.40.0/24
protocol 6 dst-port-min 80 dst-port-max 80 ethertype 0x0800
drop-action disable block NsnaDefRedBlk1 eval-order 5
```

```
qos nsna classifier name REDFILTER dst-ip 10.40.40.0/24
protocol 6 dst-port-min 443 dst-port-max 443 ethertype
0x0800 drop-action disable block NsnaDefRedBlk1 eval-order 6

qos nsna classifier name REDFILTER dst-ip 10.40.40.0/24
protocol 17 dst-port-min 53 dst-port-max 53 ethertype 0x0800
drop-action disable block NsnaDefRedBlk1 eval-order 7
```

ARP traffic

```
qos nsna classifier name REDFILTER ethertype 0x0806
drop-action disable eval-order 12
```

UDP traffic and ICMP traffic for the VoIP VLAN

```
qos nsna classifier name REDFILTER protocol 17 vlan-min 540
vlan-max 540 ethertype 0x0800 drop-action disable block
NsnaDefRedBlk2 eval-order 17

qos nsna classifier name REDFILTER protocol 1 vlan-min 540
vlan-max 540 ethertype 0x0800 drop-action disable block
NsnaDefRedBlk2 eval-order 25
```

ICMP traffic

```
qos nsna classifier name REDFILTER protocol 1 ethertype
0x0800 drop-action disable eval-order 37
```

Enable Red filter set

```
qos nsna set name REDFILTER committed-rate 1000
max-burst-rate 4000 max-burst-duration 5 drop-out-action
enable drop-nm-action enable
```

Yellow Filter

HTTP traffic, HTTPS traffic, and DNS traffic for the Nortel SNAS 4050 portal VIP subnet

```
qos nsna classifier name YELLOWFILTER dst-ip 10.40.40.0/24
protocol 6 dst-port-min 80 dst-port-max 80 ethertype 0x0800
drop-action disable block NsnaDefYelBlk1 eval-order 5
```

```
qos nsna classifier name YELLOWFILTER dst-ip 10.40.40.0/24
protocol 6 dst-port-min 443 dst-port-max 443 ethertype
0x0800 drop-action disable block NsnaDefYelBlk1 eval-order 6

qos nsna classifier name YELLOWFILTER dst-ip 10.40.40.0/24
protocol 17 dst-port-min 53 dst-port-max 53 ethertype 0x0800
drop-action disable block NsnaDefYelBlk1 eval-order 7
```

ARP traffic

```
qos nsna classifier name YELLOWFILTER ethertype 0x0806
drop-action disable eval-order 12
```

Yellow subnet traffic

```
qos nsna classifier name YELLOWFILTER dst-ip 10.120.120.0/24
ethertype 0x0800 drop-action disable eval-order 17
```

UDP traffic and ICMP traffic for the VoIP VLAN

```
qos nsna classifier name YELLOWFILTER protocol 17 vlan-min
540 vlan-max 540 ethertype 0x0800 drop-action disable block
NsnaDefYelBlk2 eval-order 22

qos nsna classifier name YELLOWFILTER protocol 1 vlan-min
540 vlan-max 540 ethertype 0x0800 drop-action disable block
NsnaDefYelBlk2 eval-order 30
```

ICMP traffic

```
qos nsna classifier name YELLOWFILTER protocol 1 ethertype
0x0800 drop-action disable eval-order 42
```

Enable Yellow filter set

```
qos nsna set name YELLOWFILTER drop-nm-action enable
```

Default filter parameters

Table 17 on page 91 lists the default Nortel SNA filter set parameters. The filter set name will vary depending on configuration.

Table 17 Default Nortel SNA filter sets

Red filter set	Yellow filter set	Green filter set
Id: 1	Id: 2	Id: 3
Unit/Port: 0 (TEMPLATE)	Unit/Port: 0 (TEMPLATE)	Unit/Port: 0 (TEMPLATE)
Name: Red	Name: Yellow	Name: Green
Block: NsnaDefRedBlk1	Block: NsnaDefYelBlk1	Block:
Eval Order: 5	Eval Order: 5	Eval Order: 1
Address Type: IPv4	Address Type: IPv4	Address Type: Ignore
Destination Addr/Mask: 10.40.40.0/24	Destination Addr/Mask: 10.40.40.0/24	Destination Addr/Mask: Ignore
Source Addr/Mask: Ignore	Source Addr/Mask: Ignore	Source Addr/Mask: Ignore
DSCP: Ignore	DSCP: Ignore	DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: TCP	IPv4 Protocol / IPv6 Next Header: TCP	IPv4 Protocol / IPv6 Next Header: Ignore
Destination L4 Port Min: 80	Destination L4 Port Min: 80	Destination L4 Port Min: Ignore
Destination L4 Port Max: 80	Destination L4 Port Max: 80	Destination L4 Port Max: Ignore
Source L4 Port Min: Ignore	Source L4 Port Min: Ignore	Source L4 Port Min: Ignore
Source L4 Port Max: Ignore	Source L4 Port Max: Ignore	Source L4 Port Max: Ignore
IPv6 Flow Id: Ignore	IPv6 Flow Id: Ignore	IPv6 Flow Id: Ignore
Destination MAC Addr: Ignore	Destination MAC Addr: Ignore	Destination MAC Addr: Ignore
Destination MAC Mask: Ignore	Destination MAC Mask: Ignore	Destination MAC Mask: Ignore
Source MAC Addr: Ignore	Source MAC Addr: Ignore	Source MAC Addr: Ignore
Source MAC Mask: Ignore	Source MAC Mask: Ignore	Source MAC Mask: Ignore
VLAN: Ignore	VLAN: Ignore	VLAN: Ignore
VLAN Tag: Ignore	VLAN Tag: Ignore	VLAN Tag: Ignore
EtherType: 0x0800	EtherType: 0x0800	EtherType: Ignore
802.1p Priority: All	802.1p Priority: All	802.1p Priority: All
Action Drop: No	Action Drop: No	Action Drop: No
Action Update DSCP: Ignore	Action Update DSCP: Ignore	Action Update DSCP: Ignore
Action Update 802.1p Priority: Ignore	Action Update 802.1p Priority: Ignore	Action Update 802.1p Priority: Ignore
Action Set Drop Precedence: Low Drop	Action Set Drop Precedence: Low Drop	Action Set Drop Precedence: Low Drop
Commit Rate: 1000 Kbps	Commit Rate: 0 Kbps	Commit Rate: 0 Kbps
Commit Burst: 4096 Bytes	Commit Burst: 0 Bytes	Commit Burst: 0 Bytes
Out-Profile Action: Drop	Out-Profile Action: None	Out-Profile Action: None
Non-Match Action: Drop	Non-Match Action: Drop	Non-Match Action: Defer
Storage Type: NonVolatile	Storage Type: NonVolatile	Storage Type: NonVolatile

Table 17 Default Nortel SNA filter sets (continued)

Red filter set	Yellow filter set	Green filter set
Id: 1	Id: 2	
Unit/Port: 0 (TEMPLATE)	Unit/Port: 0 (TEMPLATE)	
Name: Red	Name: Yellow	
Block: NsnaDefRedBlk1	Block: NsnaDefYelBlk1	
Eval Order: 6	Eval Order: 6	
Address Type: IPv4	Address Type: IPv4	
Destination Addr/Mask: 10.40.40.0/24	Destination Addr/Mask: 10.40.40.0/24	
Source Addr/Mask: Ignore	Source Addr/Mask: Ignore	
DSCP: Ignore	DSCP: Ignore	
IPv4 Protocol / IPv6 Next Header: TCP	IPv4 Protocol / IPv6 Next Header: TCP	
Destination L4 Port Min: 443	Destination L4 Port Min: 443	
Destination L4 Port Max: 443	Destination L4 Port Max: 443	
Source L4 Port Min: Ignore	Source L4 Port Min: Ignore	
Source L4 Port Max: Ignore	Source L4 Port Max: Ignore	
IPv6 Flow Id: Ignore	IPv6 Flow Id: Ignore	
Destination MAC Addr: Ignore	Destination MAC Addr: Ignore	
Destination MAC Mask: Ignore	Destination MAC Mask: Ignore	
Source MAC Addr: Ignore	Source MAC Addr: Ignore	
Source MAC Mask: Ignore	Source MAC Mask: Ignore	
VLAN: Ignore	VLAN: Ignore	
VLAN Tag: Ignore	VLAN Tag: Ignore	
EtherType: 0x0800	EtherType: 0x0800	
802.1p Priority: All	802.1p Priority: All	
Action Drop: No	Action Drop: No	
Action Update DSCP: Ignore	Action Update DSCP: Ignore	
Action Update 802.1p Priority: Ignore	Action Update 802.1p Priority: Ignore	
Action Set Drop Precedence: Low Drop	Action Set Drop Precedence: Low Drop	
Commit Rate: 1000 Kbps	Commit Rate: 0 Kbps	
Commit Burst: 4096 Bytes	Commit Burst: 0 Bytes	
Out-Profile Action: Drop	Out-Profile Action: None	
Non-Match Action: Drop	Non-Match Action: Drop	
Storage Type: NonVolatile	Storage Type: NonVolatile	

Table 17 Default Nortel SNA filter sets (continued)

Red filter set	Yellow filter set	Green filter set
Id: 1	Id: 2	
Unit/Port: 0 (TEMPLATE)	Unit/Port: 0 (TEMPLATE)	
Name: Red	Name: Yellow	
Block: NsnaDefRedBlk1	Block: NsnaDefYelBlk1	
Eval Order: 7	Eval Order: 7	
Address Type: IPv4	Address Type: IPv4	
Destination Addr/Mask: 10.40.40.0/24	Destination Addr/Mask: 10.40.40.0/24	
Source Addr/Mask: Ignore	Source Addr/Mask: Ignore	
DSCP: Ignore	DSCP: Ignore	
IPv4 Protocol / IPv6 Next Header: UDP	IPv4 Protocol / IPv6 Next Header: UDP	
Destination L4 Port Min: 53	Destination L4 Port Min: 53	
Destination L4 Port Max: 53	Destination L4 Port Max: 53	
Source L4 Port Min: Ignore	Source L4 Port Min: Ignore	
Source L4 Port Max: Ignore	Source L4 Port Max: Ignore	
IPv6 Flow Id: Ignore	IPv6 Flow Id: Ignore	
Destination MAC Addr: Ignore	Destination MAC Addr: Ignore	
Destination MAC Mask: Ignore	Destination MAC Mask: Ignore	
Source MAC Addr: Ignore	Source MAC Addr: Ignore	
Source MAC Mask: Ignore	Source MAC Mask: Ignore	
VLAN: Ignore	VLAN: Ignore	
VLAN Tag: Ignore	VLAN Tag: Ignore	
EtherType: 0x0800	EtherType: 0x0800	
802.1p Priority: All	802.1p Priority: All	
Action Drop: No	Action Drop: No	
Action Update DSCP: Ignore	Action Update DSCP: Ignore	
Action Update 802.1p Priority: Ignore	Action Update 802.1p Priority: Ignore	
Action Set Drop Precedence: Low Drop	Action Set Drop Precedence: Low Drop	
Commit Rate: 1000 Kbps	Commit Rate: 0 Kbps	
Commit Burst: 4096 Bytes	Commit Burst: 0 Bytes	
Out-Profile Action: Drop	Out-Profile Action: None	
Non-Match Action: Drop	Non-Match Action: Drop	
Storage Type: NonVolatile	Storage Type: NonVolatile	

Table 17 Default Nortel SNA filter sets (continued)

Red filter set	Yellow filter set	Green filter set
Id: 1	Id: 2	
Unit/Port: 0 (TEMPLATE)	Unit/Port: 0 (TEMPLATE)	
Name: Red	Name: Yellow	
Block:	Block:	
Eval Order: 12	Eval Order: 12	
Address Type: Ignore	Address Type: Ignore	
Destination Addr/Mask: Ignore	Destination Addr/Mask: Ignore	
Source Addr/Mask: Ignore	Source Addr/Mask: Ignore	
DSCP: Ignore	DSCP: Ignore	
IPv4 Protocol / IPv6 Next Header: Ignore	IPv4 Protocol / IPv6 Next Header: Ignore	
Destination L4 Port Min: Ignore	Destination L4 Port Min: Ignore	
Destination L4 Port Max: Ignore	Destination L4 Port Max: Ignore	
Source L4 Port Min: Ignore	Source L4 Port Min: Ignore	
Source L4 Port Max: Ignore	Source L4 Port Max: Ignore	
IPv6 Flow Id: Ignore	IPv6 Flow Id: Ignore	
Destination MAC Addr: Ignore	Destination MAC Addr: Ignore	
Destination MAC Mask: Ignore	Destination MAC Mask: Ignore	
Source MAC Addr: Ignore	Source MAC Addr: Ignore	
Source MAC Mask: Ignore	Source MAC Mask: Ignore	
VLAN: Ignore	VLAN: Ignore	
VLAN Tag: Ignore	VLAN Tag: Ignore	
EtherType: 0x0806	EtherType: 0x0806	
802.1p Priority: All	802.1p Priority: All	
Action Drop: No	Action Drop: No	
Action Update DSCP: Ignore	Action Update DSCP: Ignore	
Action Update 802.1p Priority: Ignore	Action Update 802.1p Priority: Ignore	
Action Set Drop Precedence: Low Drop	Action Set Drop Precedence: Low Drop	
Commit Rate: 1000 Kbps	Commit Rate: 0 Kbps	
Commit Burst: 4096 Bytes	Commit Burst: 0 Bytes	
Out-Profile Action: Drop	Out-Profile Action: None	
Non-Match Action: Drop	Non-Match Action: Drop	
Storage Type: NonVolatile	Storage Type: NonVolatile	

Table 17 Default Nortel SNA filter sets (continued)

Red filter set	Yellow filter set	Green filter set
Id: 1 Unit/Port: 0 (TEMPLATE) Name: Red Block: NsnaDefRedBlk2 Eval Order: 17 Address Type: IPv4 Destination Addr/Mask: Ignore Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: UDP Destination L4 Port Min: Ignore Destination L4 Port Max: Ignore Source L4 Port Min: Ignore Source L4 Port Max: Ignore IPv6 Flow Id: Ignore Destination MAC Addr: Ignore Destination MAC Mask: Ignore Source MAC Addr: Ignore Source MAC Mask: Ignore VLAN: 140 VLAN Tag: Ignore EtherType: 0x0800 802.1p Priority: All Action Drop: No Action Update DSCP: Ignore Action Update 802.1p Priority: Ignore Action Set Drop Precedence: Low Drop Commit Rate: 1000 Kbps Commit Burst: 4096 Bytes Out-Profile Action: Drop Non-Match Action: Drop Storage Type: NonVolatile	Id: 2 Unit/Port: 0 (TEMPLATE) Name: Yellow Block: Eval Order: 17 Address Type: IPv4 Destination Addr/Mask: 10.120.120.0/24 Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: Ignore Destination L4 Port Min: Ignore Destination L4 Port Max: Ignore Source L4 Port Min: Ignore Source L4 Port Max: Ignore IPv6 Flow Id: Ignore Destination MAC Addr: Ignore Destination MAC Mask: Ignore Source MAC Addr: Ignore Source MAC Mask: Ignore VLAN: Ignore VLAN Tag: Ignore EtherType: 0x0800 802.1p Priority: All Action Drop: No Action Update DSCP: Ignore Action Update 802.1p Priority: Ignore Action Set Drop Precedence: Low Drop Commit Rate: 0 Kbps Commit Burst: 0 Bytes Out-Profile Action: None Non-Match Action: Drop Storage Type: NonVolatile	

Table 17 Default Nortel SNA filter sets (continued)

Red filter set	Yellow filter set	Green filter set
Id: 1	Id: 2	
Unit/Port: 0 (TEMPLATE)	Unit/Port: 0 (TEMPLATE)	
Name: Red	Name: Yellow	
Block: NsnaDefRedBlk2	Block: NsnaDefYelBlk2	
Eval Order: 25	Eval Order: 22	
Address Type: IPv4	Address Type: IPv4	
Destination Addr/Mask: Ignore	Destination Addr/Mask: Ignore	
Source Addr/Mask: Ignore	Source Addr/Mask: Ignore	
DSCP: Ignore	DSCP: Ignore	
IPv4 Protocol / IPv6 Next Header: ICMP	IPv4 Protocol / IPv6 Next Header: UDP	
Destination L4 Port Min: Ignore	Destination L4 Port Min: Ignore	
Destination L4 Port Max: Ignore	Destination L4 Port Max: Ignore	
Source L4 Port Min: Ignore	Source L4 Port Min: Ignore	
Source L4 Port Max: Ignore	Source L4 Port Max: Ignore	
IPv6 Flow Id: Ignore	IPv6 Flow Id: Ignore	
Destination MAC Addr: Ignore	Destination MAC Addr: Ignore	
Destination MAC Mask: Ignore	Destination MAC Mask: Ignore	
Source MAC Addr: Ignore	Source MAC Addr: Ignore	
Source MAC Mask: Ignore	Source MAC Mask: Ignore	
VLAN: 140	VLAN: 140	
VLAN Tag: Ignore	VLAN Tag: Ignore	
EtherType: 0x0800	EtherType: 0x0800	
802.1p Priority: All	802.1p Priority: All	
Action Drop: No	Action Drop: No	
Action Update DSCP: Ignore	Action Update DSCP: Ignore	
Action Update 802.1p Priority: Ignore	Action Update 802.1p Priority: Ignore	
Action Set Drop Precedence: Low Drop	Action Set Drop Precedence: Low Drop	
Commit Rate: 1000 Kbps	Commit Rate: 0 Kbps	
Commit Burst: 4096 Bytes	Commit Burst: 0 Bytes	
Out-Profile Action: Drop	Out-Profile Action: None	
Non-Match Action: Drop	Non-Match Action: Drop	
Storage Type: NonVolatile	Storage Type: NonVolatile	

Table 17 Default Nortel SNA filter sets (continued)

Red filter set	Yellow filter set	Green filter set
Id: 1	Id: 2	
Unit/Port: 0 (TEMPLATE)	Unit/Port: 0 (TEMPLATE)	
Name: Red	Name: Yellow	
Block:	Block: NsnaDefYelBlk2	
Eval Order: 37	Eval Order: 30	
Address Type: IPv4	Address Type: IPv4	
Destination Addr/Mask: Ignore	Destination Addr/Mask: Ignore	
Source Addr/Mask: Ignore	Source Addr/Mask: Ignore	
DSCP: Ignore	DSCP: Ignore	
IPv4 Protocol / IPv6 Next Header: ICMP	IPv4 Protocol / IPv6 Next Header: ICMP	
Destination L4 Port Min: Ignore	Destination L4 Port Min: Ignore	
Destination L4 Port Max: Ignore	Destination L4 Port Max: Ignore	
Source L4 Port Min: Ignore	Source L4 Port Min: Ignore	
Source L4 Port Max: Ignore	Source L4 Port Max: Ignore	
IPv6 Flow Id: Ignore	IPv6 Flow Id: Ignore	
Destination MAC Addr: Ignore	Destination MAC Addr: Ignore	
Destination MAC Mask: Ignore	Destination MAC Mask: Ignore	
Source MAC Addr: Ignore	Source MAC Addr: Ignore	
Source MAC Mask: Ignore	Source MAC Mask: Ignore	
VLAN: Ignore	VLAN: 140	
VLAN Tag: Ignore	VLAN Tag: Ignore	
EtherType: 0x0800	EtherType: 0x0800	
802.1p Priority: All	802.1p Priority: All	
Action Drop: No	Action Drop: No	
Action Update DSCP: Ignore	Action Update DSCP: Ignore	
Action Update 802.1p Priority: Ignore	Action Update 802.1p Priority: Ignore	
Action Set Drop Precedence: Low Drop	Action Set Drop Precedence: Low Drop	
Commit Rate: 1000 Kbps	Commit Rate: 0 Kbps	
Commit Burst: 4096 Bytes	Commit Burst: 0 Bytes	
Out-Profile Action: Drop	Out-Profile Action: None	
Non-Match Action: Drop	Non-Match Action: Drop	
Storage Type: NonVolatile	Storage Type: NonVolatile	

Table 17 Default Nortel SNA filter sets (continued)

Red filter set	Yellow filter set	Green filter set
	Id: 2 Unit/Port: 0 (TEMPLATE) Name: Yellow Block: Eval Order: 42 Address Type: IPv4 Destination Addr/Mask: Ignore Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: ICMP Destination L4 Port Min: Ignore Destination L4 Port Max: Ignore Source L4 Port Min: Ignore Source L4 Port Max: Ignore IPv6 Flow Id: Ignore Destination MAC Addr: Ignore Destination MAC Mask: Ignore Source MAC Addr: Ignore Source MAC Mask: Ignore VLAN: Ignore VLAN Tag: Ignore EtherType: 0x0800 802.1p Priority: All Action Drop: No Action Update DSCP: Ignore Action Update 802.1p Priority: Ignore Action Set Drop Precedence: Low Drop Commit Rate: 0 Kbps Commit Burst: 0 Bytes Out-Profile Action: None Non-Match Action: Drop Storage Type: NonVolatile	

New system messages for Nortel SNA

The following log messages will be added to *System Configuration Guide for Nortel Ethernet Routing Switch 5500 Series* (217462-x).

- `SSCP connection attempt failed, NSNAS already connected.`
- `SSCP connection attempt failed, incompatible SSCP versions`
- `SSCP connection attempt failed, NSNAS not configured.`
- `SSCP connection attempt failed, got bad interval values from NSNAS.`
- `SSCP connection attempt succeeded.`
- `SSCP connection lost, NSNAS closed the connection.`
- `SSCP connection lost, corrupt data stream.`
- `SSCP connection lost, memory allocation failure.`
- `SSCP connection lost, message processing failure.`
- `SSCP connection lost, inactivity timer expired.`
- `SSCP connection attempt failed, incompatible SSCP versions.`
- `SSCP connection attempt failed, got bad interval values from NSNAS.`
- `SSCP connection lost, corrupt data stream.`
- `SSCP connection lost, memory allocation failure.`
- `SSCP connection lost, message processing failure.`

Reading path

This section lists the documentation specific to the Nortel SNA solution. For information on finding and accessing up-to-date documentation, see "Online" on page 101.

Publications

Refer to the following publications for information on the Nortel SNA solution:

- *Nortel Secure Network Access Solution Guide* (320817-A)
- *Nortel Secure Network Access Switch 4050 Installation Guide* (320846-A)
- *Nortel Secure Network Access Switch 4050 User Guide* (320818-A)
- *Installing and Using the Security & Routing Element Manager (SREM)* (320199-B)
- *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.3.1* (217468-C)
- *Release Notes for the Ethernet Routing Switch 8300, Software Release 2.2.8.1* (316811-G)
- *Release Notes for the Nortel Secure Network Access Solution, Software Release 1.1* (320850-B)
- *Release Notes for Enterprise Switch Manager (ESM), Software Release 5.1* (209960-H)
- *Using Enterprise Switch Manager Release 5.1* (208963-F)

Online

To access Nortel technical documentation online, go to the Nortel web site:

www.nortel.com/support

You can download current versions of technical documentation. To locate documents, browse by category or search using the product name or number.

You can print the technical manuals and release notes free, directly from the Internet. Use Adobe* Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems site at www.adobe.com to download a free copy of Adobe Reader.

How to get help

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 for assistance.

If you purchased a Nortel service program, use the www.nortel.com/help web page to locate information to contact Nortel for assistance:

- To obtain Nortel Technical Support contact information, click the **CONTACT US** link on the left side of the page.
- To call a Nortel Technical Solutions Center for assistance, click the **CALL US** link on the left side of the page to find the telephone number for your region.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate the ERC for your product or service, go to the www.nortel.com/help web page and follow these links:

1. Click **CONTACT US** on the left side of the **HELP** web page.
2. Click **Technical Support** on the **CONTACT US** web page.
3. Click **Express Routing Codes** on the **TECHNICAL SUPPORT** web page.