Part No. 316811-E
December 2005

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Ethernet Routing Switch 8300, Software Release 2.2.8

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 release notes for the Ethernet Routing Switch 8300 (formerly known as Passport 8300) Software Release 2.2.8 describe the hardware and software and any known issues that exist in this release. They are based on Ethernet Routing Switch 8300, Software Release 2.2.8 and Java Device Manager (Device Manager) 5.9.5.0.

For the list of related publications, see the "Reading path" on page 100. The Ethernet Routing Switch 8300, Software Release 2.2.8 documentation suite can be found on the Nortel technical documentation Web site, www.nortel.com/support.

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 8300, Software Release 2.2.8 software files. File sizes are approximate.

Table 1 Ethernet Routing Switch 8300, Software Release 2.2.8 files

Module or file type	Description	File name	File size (bytes)
Boot monitor image	CPU and switch fabric firmware for the Ethernet Routing Switch 8300. Supported on Ethernet Routing Switch 8393SF modules	p83b2280.img	1 072 128
Runtime image	The Ethernet Routing Switch 8300 image. Supported on Ethernet Routing Switch 8393SF modules	p83a2280.img	5 864 448
Pre-boot monitor image	Pre-boot monitor image	p83f2280.img	230 786
MIB (private)	Ethernet Routing Switch 8300 private MIB	p83a2280.mib	2 726 298
MIB zip file	Ethernet Routing Switch 8300 MIB	p83a2280.mib.zip	421 888
md5 checksum file	md5 checksums of all Release 2.2.8 software files	p83a2280.md5	
Input/output modules download file	Supported on Ethernet Routing Switch 8348TX, 8348TX-PWR, 8324FX, and 8324GTX	p83r2280.dld	1 665 024
Encryption module for SNMPv3 (includes DES and AES encryption capabilities) **Note:** Available only on the Nortel web site (www.nortel.com/support)	Supported on the Ethernet Routing Switch 8393SF modules	p83c2280.aes	27 648
Encryption module for SSH (includes 3DES and AES encryption capabilities) **Note:** Available only on the Nortel web site (www.nortel.com/support)	Supported on the Ethernet Routing Switch 8393SF modules	p83c2280.img (3DES) p83c2280.aes (AES)	53 248 27 648

Table 1 Ethernet Routing Switch 8300, Software Release 2.2.8 files (continued)

Module or file type	Description	File name	File size (bytes)
Java Device Manager software image for Windows (Version 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 image for UNIX (Version 5.9.5.0)	Device Manager software image for Solaris	jdm_5950_solaris_sparc.sh	139 137 432
	Device Manager software image for HP-UX	jdm_5950_hpux_pa-risc.sh	168 038 808
Java Device Manager software image for Linux (Version 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	

New software features in this release

Ethernet Routing Switch 8300, Software Release 2.2.8 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

Ethernet Routing Switch 8300, Software Release 2.2.8 is compatible with the Enterprise Switch Manager (ESM) version 5.1.

ESM is a Java-based network management application that lets you discover and view network nodes and their physical links on a topology map. Once your network is discovered, you can monitor, manage, and configure network settings for your devices.

With ESM 5.1, you can use an Upgrade Wizard to upgrade multiple Ethernet Routing Switch 8300 devices simultaneously through the same interface. For more information, refer to *Using Enterprise Switch Manager Release 5.1* (208963-F).

Table 2 lists the known limits for the Ethernet Routing Switch 8300, Software Release 2.2.8 and Device Manager 5.9.5.0. These capabilities will be enhanced in subsequent software releases.

Table 2 Supported capabilities in the 8300 Series (Release 2.2.8)

Feature	Maximum number supported
VLANs	Up to 2047 VLANs; 200 have been tested and are officially supported in Release 2.2.8 **Note:** The range of valid ID numbers is greater than the maximum number of supported VLANs. The range for VLAN IDs is 1-4000.
Protocol-based VLANs	12 records, 50 VLANs maximum
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 2.2.8.
Nortel SNA ports	All ports.
ARP records	2500
IP interfaces	Up to 512 IP interfaces; 200 have been tested and are officially supported in Release 2.2.8
Local next hops	500
Static routes	1000
Spanning Tree groups	Up to 64; groups 1 through 25 have been tested and are officially supported in Release 2.2.8

Table 2 Supported capabilities in the 8300 Series (Release 2.2.8) (continued)

Feature	Maximum number supported
Aggregation groups • 802.3ad static aggregation groups	31 • For 8348TX and 8324FX ports, you can use only Link Aggregation Groups 1-7 • For 8324GTX ports and CP I/O ports, you can use Link Aggregation Groups 1-31
Ports per aggregation group **Note**: All the ports MUST be of the same type (no mix of technology is supported)	4
IGMP maximum number of unique groups	2000
RIP scaling	• 8 routed VLANs • 750 RIP routes • 500 ARP entries • 1500 MAC entries • 8 STGs
EAPoL 802.1x supplicants	Up to 3072 supplicants; 128 have been tested and are officially supported in Release 2.2.8
RADIUS MAC centralization clients	Up to 3072 clients; 64 have been tested and are officially supported in Release 2.2.8

Note: Jumbo Frames are not supported in Release 2.2. Thus, you should not use the **`mtu`** command in the NNCLI Global configuration mode. (Q00876423)

Ethernet Routing Switch 8010/8006 chassis support

You can use Ethernet Routing Switch 8300 modules with the Ethernet Routing Switch 8010 and 8006 chassis. The following requirements must be adhered to:

1 The Ethernet Routing Switch 8010 and 8006 chassis require 4096 media access control (MAC) addresses to use the Ethernet Routing Switch 8300 modules. The upgrade kit (DS1411015) that allows you to increase the MAC addresses on your Ethernet Routing Switch 8300 to a total of 4096 MAC addresses is available for this purpose. For more information about this kit, see *Adding MAC Addresses to the Passport 8000 Series Chassis* (212486-B).

2 The Ethernet Routing Switch 8300 switch fabric modules (8393SF) are limited to one switch fabric per Ethernet Routing Switch 8010 or Ethernet Routing Switch 8006 chassis. This single switch fabric in the 8010 or 8006 chassis can be in either slot 5 or 6. Dual switch fabric modules in these chassis are not supported. Only Ethernet Routing Switch 8310 and 8306 (10-slot and 6-slot PoE chassis) support dual switch fabric configurations.

3 The Ethernet Routing Switch 8010 and 8006 chassis do not support Power over Ethernet (PoE) capabilities on the PoE module. Therefore, the PoE feature is not available in these chassis.

Note:

1. You can use the Ethernet Routing Switch 8348TX-PWR module in the 8010 or 8006 chassis. Be aware, however, that when the 8348TX-PWR module is operating in the 8010 or 8006 chassis, it operates as an Ethernet Routing Switch 8348TX module.

2. In an 8010 or 8006 chassis, you cannot mix Ethernet Routing Switch 8300 modules with Ethernet Routing Switch 8600 or 8100 modules.

3. The 8003 chassis is not supported.

Supported SFPs

Table 3 lists the transceivers supported by the Ethernet Routing Switch 8300.

Table 3 Supported SFP transceivers

Model	Product number
SFP transceivers:	
1000BASE-SX (LC Type)	AA1419013
1000BASE-SX (MT-RJ Type)	AA1419014
1000BASE-LX (LC Type)	AA1419015
1000 BaseT SFP (RJ-45)	AA1419043

Table 3 Supported SFP transceivers (continued)

Model	Product number
CWDM SFP GBICs:	
1470nm/Gray	AA1419025 AA1419033
1490nm/Violet	AA1419026 AA1419034
1510nm/Blue	AA1419027 AA1419035
1530nm/Green	AA1419028 AA1419036
1550nm/Yellow	AA1419029 AA1419037
1570nm/Orange	AA1419030 AA1419038
1590nm/Red	AA1419031 AA1419039
1610nm/Brown	AA1419032 AA1419040

Hot-removal/hot-insertion of Ethernet Routing Switch 8300 modules

In general, after you hot-insert or hot-remove an Ethernet Routing Switch 8300 module, you must wait 30 seconds before performing another hot-insertion or hot-removal of a module.

Hot-removal of master CPU

In a dual CPU configuration, both CPUs require the same set of images at all times. When you insert a new CPU in the Ethernet Routing Switch 8300, ensure that it has the same set of boot and runtime images as the existing CPU.

Removing the master CPU can result in a configuration loss for the removed CPU if it is replaced in the Ethernet Routing Switch 8300. To avoid this situation, follow these instructions if you need to remove a master CPU from an 8300 chassis:

1. Use the save to standby option to automatically save both the boot and the configuration files to both CPUs (master and standby).
2. If you are using the out-of-band Ethernet port of the 8393 SF module for management, add a virtual IP address. The virtual IP address will allow access to the master CPU whether the master CPU is in slot 5 or slot 6.
3. Perform a soft reset on the master CPU to cause failover to occur.
4. Wait until the new master comes up and the old master becomes the standby.
5. Remove the standby CPU. If you need to re-insert this CPU, you must wait at least 60 seconds.

Note that if you remove the master CPU without following this procedure and then save the configuration after removal, the new configuration will not contain the removed CPU configuration. You will then need to reconfigure the CPU ports.

To avoid this issue, back up the existing configuration file before saving any configuration. After you insert the removed CPU, you can then reboot the switch with the backup configuration file to restore the configuration. For more information, see the guidelines for warm standby in *Network Design Guidelines* (316809-C)

Known limitations and considerations in this release

Refer to *Release Notes for the Ethernet Routing Switch 8300 Software Release 2.2* (316811-D) for more information on known hardware and software limitations for the Ethernet Routing Switch 8300.

Table 4 describes additional issues known to exist in the 8300 Series, Software Release 2.2.8.

Table 4 Ethernet Routing Switch 8300 known limitations

Change Request Number	Issue
Q01217238	The switch crashes if you try to change the SSH mode to "secure" from the Java Device Manager (Device Manager). **Note:** This limitation exists in Ethernet Routing Switch 8300 Software Release 2.2. Workaround: Do not use Device Manager to change this parameter.
Q01264447	Do not disable the DSA key on the Ethernet Routing Switch 8300. If you must do so, first disable the switch from the Nortel SNAS 4050 (`/cfg domain 1 switch 1 disable`).
Q01233578	If all Red, Yellow, and Green VLANs are in STG 1, you can successfully modify STP parameters on a port and save the configuration (that is, it will be in effect across reboot). However, if the Nortel SNA VLANs are part of different STGs, you can modify STP parameters, but `save config` will not preserve the new STP parameters (that is, the default parameters for STP appear across reboot). Recommendation: Do not change the default STP values (Fast Start, STP enable) if your Nortel SNA VLANs are in different STGs.
Q01259808	Ensure you always execute `cd /flash` before saving your configuration (`save config`).

Table 4 Ethernet Routing Switch 8300 known limitations (continued)

Change Request Number	Issue
Q01225865	If you plan to use the default Nortel SNA filters, ensure you follow this configuration sequence: 1. Configure the Nortel Secure Network Access Switch 4050 (Nortel SNAS 4050) IP address. 2. Configure the VoIP VLAN(s). 3. Configure the Red, Yellow, and Green VLANs. The Nortel SNAS 4050 IP address, VoIP VLAN IDs, and Yellow subnet are used by the Red and Yellow filters. If the Nortel SNAS 4050 IP, VoIP VLAN, or Yellow subnet is changed, ensure you manually modify the filters—they are not updated automatically. To update the filters for these settings, you must disable Nortel SNA globally and manually delete Nortel SNA VLANs and QoS filters, then recreate them.
Q01260843	Only one port forwarding SSH connection is allowed from the Nortel SNAS 4050 subnet. Therefore, do not make any SSH connection from any clients in the Nortel SNAS 4050 subnet.
Q01256101	When Nortel SNA is globally disabled and enabled, licenses are not consumed for the IP phones since they do not do a DHCP because they are already in a VoIP VLAN. To make the phones consume licenses, the ports on the 8300 switch (to which the phones are connected) should be made admin down and up. When the ports are disabled and enabled, the switch sends the information about the phone clients to the Nortel SNAS 4050, and the licenses are consumed.
Q01187989	If you disconnect a client from a dynamic Nortel SNA port, or from a hub that is connected to a dynamic Nortel SNA port, you should wait for its fdb-entry to age out before reconnecting the client. If the fdb-entry is still available, the client does not get an IP.

Note: 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.

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.

Nortel SNA mode to default mode – rollback instructions

Although the Nortel SNA implementation changes port settings on edge switches, you can roll back edge switch settings to their pre-Nortel SNA states at any time.

There are two situations where a rollback procedure can apply:

1 You have upgraded an existing 8300 Series switch to the Nortel SNA software release (2.2.8)

2 You have physically moved existing users from a legacy switch to a Nortel SNA-enabled switch

If you have 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.

If the have you have upgraded an existing 8300 Series switch to the Nortel SNA software release (2.2.8), follow these steps to roll back port settings:

1 Disable Nortel SNA on the client's port (make the port a legacy port).

2 Add this port to your legacy VLAN (for example, VLAN 100).

3 Configure port parameters to your requirements (for example, STP, tagging, QoS, and so on).

When you enable Nortel SNA on a port, pre-existing parameters are not the parameters used by default (therefore, pre-Nortel SNA configuration can be lost when you disable Nortel SNA; see "Deploying the Nortel SNA solution in an active network"). One parameter, in particular, is important to consider: when Nortel SNA is enabled on a port, STP runs in FAST START mode to enable faster convergence.

Deploying the Nortel SNA solution in an active network

You can deploy the Nortel SNA solution on an existing, active Ethernet Routing Switch 8300. You must upgrade the switch to a minimum software release of 2.2.8, 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 8300 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 types of Nortel SNA ports: dynamic and uplink.

Dynamic ports that are configured to function in non-Nortel SNA VLANs cannot be used for Nortel SNA purposes unless they are first removed from those non-Nortel SNA VLANs.

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 Red filter is applied to the port.
- The client port becomes a tagged port.
- The port is configured to send untagged packets on the default VLAN.
- The Port VLAN ID (PVID) of the port is changed to the Red PVID.
- 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 default configuration:

- The port becomes part of Spanning Tree Group (STG) 1.
- The STG state is Normal.
- The port is untagged.
- No filters are applied to the port.

You can configure multiple Nortel SNA uplink ports (see "Implementing the Nortel SNA solution" on page 26 and "Enabling Nortel SNA on ports" on page 48 for more information on uplink ports).

Note: STP must be Fast Learning enabled on the 8300 uplink port and on the router. The 8300 is configured automatically when you configure a port to be an uplink. You must configure the router manually.

You can add/delete the uplink port to/from a non-Nortel SNA VLAN (see "Configuration example: Adding the uplink port" on page 50 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.

If a port is a member of an MLT, you cannot make it a Nortel SNA uplink port. You must use the following procedure to make an MLT an uplink:

- Add ports to the MLT.
- Attach the uplink filter to each port.
- Mark the port as uplink (you can select one port or all ports from the MLT—in either case the uplink configuration is applied to all MLT ports).

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

Printers and static devices must be in non-Nortel SNA VLANs. In addition, no non-Nortel SNA ports can be associated with Nortel SNA VLANs.

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 1.0* (320850-A) for a list of specific devices. Devices that cannot run TunnelGuard, or have static IP addresses must be in non-Nortel SNA VLANs.

When you create a Nortel SNA VLAN, you specify a filter ID ("Configuring Nortel SNA using the CLI" on page 39 for commands to configure a Nortel SNA VLAN). If no filter exists that has that ID, then a default filter with that ID is generated on the switch. If a filter exists with the ID you specify, that filter is used. Nortel recommends that you use the default filters. You can modify the default filters, if necessary, after you have enabled them.

Nortel does not support Nortel SNA filters and non-Nortel SNA filters co-existing on Nortel SNA ports.

Ensure you thoroughly plan your Nortel SNA deployment. For example, as part of the Nortel SNA configuration on the 8300 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 filters. If you change the Nortel SNAS 4050 subnet, you must manually update the Nortel SNA filters (Red, Yellow, Green, and VoIP filters). Refer to "Configuring Nortel SNA using the CLI", "Configuring Nortel SNA using the NNCLI", "Updates to the Bandwidth Management menu for Nortel SNA", and "Configuring Nortel SNA using Device Manager" for instructions and commands to configure the Nortel SNA solution.

You update the filters in one of two ways:

1. Configure a new filter (ACG)
2. Update the filter:
   - **a** Disable Nortel SNA globally.
   - **b** Ensure the filter is not attached to any port. If it is, you must manually detach it.
   - **c** Remove the ACL from the ACG.
   - **d** Modify the ACL/ACE.
   - **e** Put the ACL back in the ACG.

f Enable Nortel SNA.

g Re-attach the filter to the port if you removed it manually.

To update the uplink filter:

- Disable the Nortel SNA uplink configuration on the port.
- Detach the filter from the port.
- Change/update the filter.
- Attach the filter to the port (that is, reconfigure the port as an uplink port).

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 8300, Software Release 2.2.8, Nortel recommends that you configure no more than five Yellow, five Green, and five VoIP VLANs on each switch.

Documentation additions and corrections

Configuring the Ethernet Routing Switch 8300 for Nortel SNA

Documentation additions in this section are for the following books:

- *Configuring and Managing Security using the NNCLI and CLI* (316804-C)
- *Configuring and Managing Security using Device Manager* (317346-C)

These additions describe the configuration procedures for enabling the Ethernet Routing Switch 8300 to function as a network access device in the Nortel SNA solution.

The following sections will be added to the next full release of the book titled, *Configuring and Managing Security using the NNCLI and CLI*.

- "Implementing the Nortel SNA solution" on page 26
- "Configuring the Ethernet Routing Switch 8300 for Nortel SNA" on page 39
- "Configuring Nortel SNA using the CLI" on page 39
- "Configuring Nortel SNA using the NNCLI" on page 56

The section titled, "Updates to the Bandwidth Management menu for Nortel SNA" on page 71, will be added to the next full release of the book titled *Configuring QoS and Filters using Device Manager*.

The section titled, "Configuring Nortel SNA using Device Manager" on page 76, will be added as a new chapter to the book titled *Configuring and Managing Security using Device Manager*.

The section titled, "Configuration example" on page 90, will be added to the book titled, *Configuring and Managing Security using the NNCLI and CLI*.

The section titled, "Default Nortel SNA filters" on page 94, will be added as an Appendix to the book titled, *Configuring and Managing Security using Device Manager*.

Implementing the Nortel SNA solution

The Ethernet Routing Switch 8300 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 network (or other network login controller) only (this is based on the default Nortel SNA Red filter). This is necessary to allow the authentication traffic. You can customize the filters 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).

IP phones are allowed access to one of the pre-configured VoIP subnets, and are allowed a pre-specified type of communication. The VoIP filters are such that they do not allow the VoIP traffic to go to anywhere but 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, which allows you to configure a switch port in one of two ways:
  - — 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.

  - — Nortel SNA uplink

You do not attach clients to the uplink port. This port is physically connected to the uplink router. The purpose of the uplink port is provide a port that is configured statically in a Nortel SNA VLAN. This configuration is particularly necessary when the switch is not the DHCP relay agent in a Nortel SNA VLAN.

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 is provisioned for Nortel SNA Red, Yellow, and Green VLANs. Nortel recommends that you use these default Nortel SNA filters. You can modify the default filters once you have enabled them and assigned them to the Nortel SNA VLANs. For information on modifying filters on the Ethernet Routing Switch 8300, refer to *Configuring QoS and Filters using the CLI* (317339-B), *Configuring QoS and Filters using the NNCLI* (316801-B), and *Configuring QoS and Filters using Device Manager* (317340-B).

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 filters).

Note: Nortel does not support Nortel SNA filters and non-Nortel SNA filters 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. You must attach an uplink filter to the port before configuring it as uplink (refer to "Configuring the uplink filter" on page 32 for an example of the uplink VLAN

filter configuration). Nortel recommends that you add no other ports to the Red, Yellow, and Green VLANs. Nortel SNA ports become members of Nortel SNA VLANs when the VLANs are configured. Manually attaching ports to a non-Nortel SNA VLAN is not allowed.

The Nortel SNA software puts all user ports (dynamic Nortel SNA 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. The Red, Yellow, and Green VLANs can be Layer 2 or Layer 3 (see "Topologies" on page 34 for more information). You must have one, and only one Red VLAN on each switch. You can, however, have multiple Yellow and multiple Green VLANs on each switch.

Note: In Ethernet Routing Switch 8300, Software Release 2.2.8, Nortel recommends that you configure no more than five Yellow, five Green, and five VoIP VLANs on each switch.

The VoIP filters are part of the Red, Yellow, and Green 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 filters. 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, Yellow, and Green VLANs. For example, when the Nortel SNA software adds a port to the Yellow VLAN, it installs the Yellow filters and the VoIP filters that you attached to the Yellow VLAN.

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

On a dynamic Nortel SNA port, the first packet coming in from a client is assumed to be a DHCP packet. This packet contains information about the type of client, which tells the switch if the client is a PC or a phone. The tag for a phone is dynamically obtained using DHCP. Filters are used to forward the DHCP packets to the CPU.

Table 5 shows filter consumption when using the default Nortel SNA filters.

Table 5 Default Nortel SNA filter consumption

Filter	IP filters consumed	Non-IP filters consumed
Red	5, plus 1 filter for each VoIP VLAN configured, plus the default filter.	3 (includes the default filter)
Yellow	6, plus 1 filter for each VoIP VLAN configured, plus the default filter.	3 (includes the default filter)
Green	1 DHCP filter, plus the default filter.	1 (default filter)

Filter parameters

Note: If you plan to use the default filters, note that you must configure the uplink filter before enabling Nortel SNA (see "Configuring the uplink filter" on page 32).

If a port belongs to a range of VLANs, the hardware VLAN classification engine implicitly drops all traffic that is classified to be any VLAN other than those in the specified range. Therefore, put each Nortel SNA port in all the VoIP VLANs. Filters are used for the remaining requirements.

The default Nortel SNA filters protect the workstations. Table 6 describes the traffic allowed by each default Nortel SNA filter.

Table 6 Traffic allowed in the default Nortel SNA filters

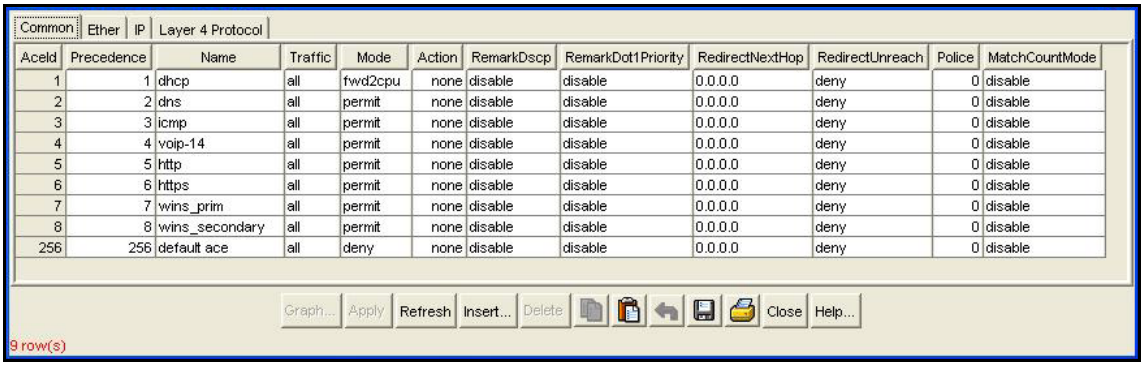
Filter	DHCP traffic	Yellow subnet traffic	DNS traffic	ICMP traffic	HTTP traffic	HTTPS traffic	ARP traffic	All traffic
Red	Forward traffic to CPU		Traffic to Nortel SNAS 4050 allowed	Permit	Traffic to Nortel SNAS 4050 allowed	Traffic to Nortel SNAS 4050 allowed	Permit	Denied
Yellow	Forward traffic to CPU	Permit	Permit	Permit	Traffic to Nortel SNAS 4050 allowed	Traffic to Nortel SNAS 4050 allowed	Permit	Denied
Green	Forward traffic to CPU							Permit

Note: When configuring the Nortel SNA Yellow VLAN, a Yellow subnet is specified (see the section "Configuring Nortel SNA per VLAN" on page 43 for the CLI command to configure the Yellow VLAN). The Yellow subnet is the Remediation server IP address/subnet.

Red VLANs allow selective broadcast (DHCP broadcast (response) coming in on the uplink port goes out on the relevant Nortel SNA port only).

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, configuration of the Red filter for two WINS domain controllers is shown in Figure 1 on page 32 and Figure 2 on page 32 (the **Common** and **IP** tabs for the Red filter ACEs as displayed in Device Manager [**Bandwidth Management > Filter > ACL > ACE**]).

Figure 1 Common tab: Red filter configuration



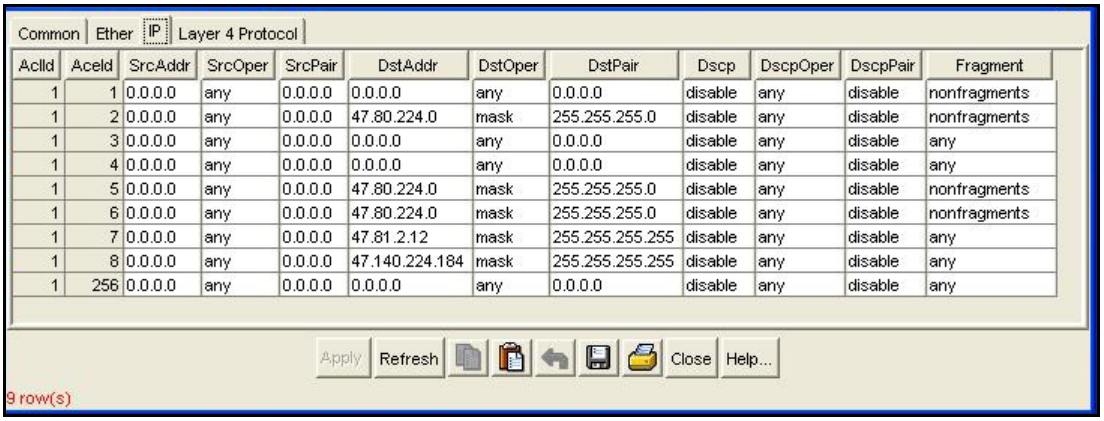
Common | Ether | IP | Layer 4 Protocol

AceId	Precedence	Name	Traffic	Mode	Action	RemarkDscp	RemarkDot1Priority	RedirectNextHop	RedirectUnreach	Police	MatchCountMode
1	1	dhcp	all	fwd2cpu	none	disable	disable	0.0.0.0	deny	0	disable
2	2	dns	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
3	3	icmp	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
4	4	voip-14	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
5	5	http	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
6	6	https	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
7	7	wins_prim	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
8	8	wins_secondary	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
256	256	default ace	all	deny	none	disable	disable	0.0.0.0	deny	0	disable

Graph... | Apply | Refresh | Insert... | Delete | Close | Help...

9 row(s)

Figure 2 IP tab: Red filter configuration



Common | Ether | IP | Layer 4 Protocol

AclId	AceId	SrcAddr	SrcOper	SrcPair	DstAddr	DstOper	DstPair	Dscp	DscpOper	DscpPair	Fragment
1	1	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	nonfragments
1	2	0.0.0.0	any	0.0.0.0	47.80.224.0	mask	255.255.255.0	disable	any	disable	nonfragments
1	3	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	any
1	4	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	any
1	5	0.0.0.0	any	0.0.0.0	47.80.224.0	mask	255.255.255.0	disable	any	disable	nonfragments
1	6	0.0.0.0	any	0.0.0.0	47.80.224.0	mask	255.255.255.0	disable	any	disable	nonfragments
1	7	0.0.0.0	any	0.0.0.0	47.81.2.12	mask	255.255.255.255	disable	any	disable	any
1	8	0.0.0.0	any	0.0.0.0	47.140.224.184	mask	255.255.255.255	disable	any	disable	any
1	256	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	any

Apply | Refresh | Close | Help...

9 row(s)

Configuring the uplink filter

The following is an example of the commands used to configure the uplink filter.

Using the CLI

1. Create the IP ACL that will forward DHCP traffic to the CPU:
   `Passport-8310:6/config#` **`filter acl 100 create ip acl-name "dhcp"`**
2. Create the first ACE in that ACL to forward DHCP traffic to the CPU:
   `Passport-8310:6/config#` **`filter acl 100 ace 1 create`**

```
Passport-8310:6/config# filter acl 100 ace 1 action
fwd2cpu precedence 1
Passport-8310:6/config# filter acl 100 ace 1 ip
ipfragment non-fragments
Passport-8310:6/config# filter acl 100 ace 1 protocol udp
eq any
Passport-8310:6/config# filter acl 100 ace 1 port
dst-port bootpd-dhcp
```

3. Configure other ACEs as needed, or modify the default ACE to permit all other traffic:
   ```
   Passport-8310:6/config# filter acl 100 ace default action
   permit
   ```
4. Put the ACL in an ACG:
   ```
   Passport-8310:6/config# filter acg 100 create 100
   acg-name "uplink"
   ```
5. Ensure you associate the filter with the uplink port using the following command:
   ```
   Passport-8310:6/config# ethernet <slot/port> filter
   create 100
   ```
   where `<slot/port>` indicates the location of the uplink port.

Using the NNCLI

Enter the commands from the Global configuration mode.

1. Create the IP ACL that will forward DHCP traffic to the CPU:
   ```
   Passport-8310:6/config# filter acl 100 ip acl-name "dhcp"
   ```
2. Create the first ACE in that ACL to forward DHCP traffic to the CPU:
   ```
   Passport-8310:6/config# filter acl 100 action 1 fwd2cpu
   precedence 1
   Passport-8310:6/config# filter acl 100 ip-hdr 1
   ipfragment non-fragments
   Passport-8310:6/config# filter acl 100 protocol 1 udp eq
   any
   Passport-8310:6/config# filter acl 100 port 1 dst-port
   bootpd-dhcp
   ```

3 Configure other ACEs as needed, or modify the default ACE to permit all other traffic:

```
Passport-8310:6/config# filter acl 100 action 1 permit
```

4 Put the ACL in an ACG:

```
Passport-8310:6/config# filter acg 100 100 acg-name
"uplink"
```

5 Ensure you associate the filter with the uplink port using the following command from the Ethernet Interface configuration mode:

```
Passport-8310:6(config)# interface fastethernet <slot/
port>
```

where `<slot/port>` indicates the location of the uplink port.

```
Passport-8310:6(config-if)# filter 100
```

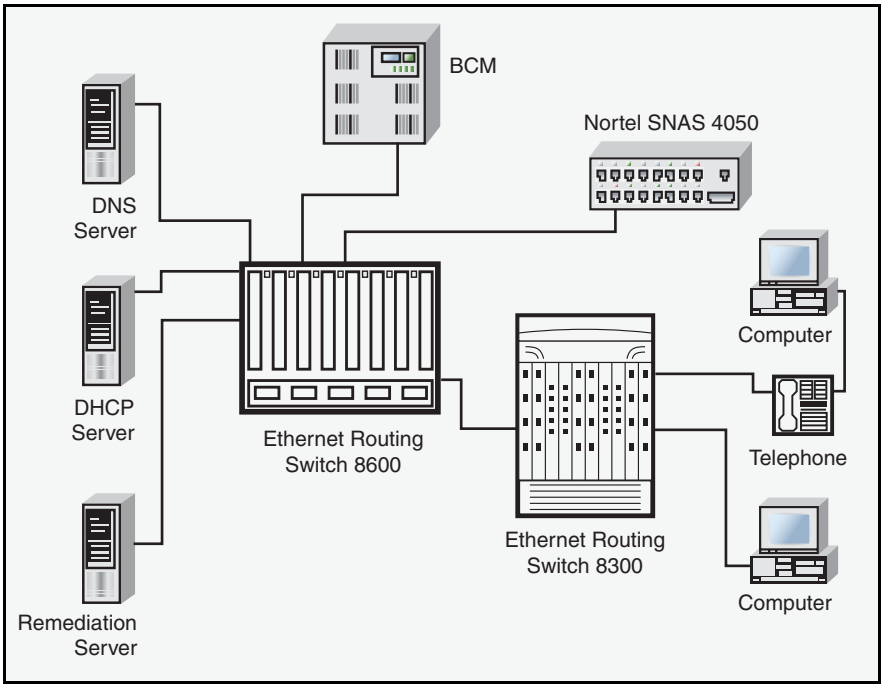
Topologies

You can configure the Ethernet Routing Switch 8300 switch to function in either Layer 2 or Layer 3 mode for the Nortel SNA solution.

Layer 2

In Layer 2 mode, DHCP-relay is done on a central router, or routing switch. Figure 3 on page 35 shows a network where the Ethernet Routing Switch 8600 is the core routing device. The Ethernet Routing Switch 8300, 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 link 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 needs to be placed. When you do this, it is automatically tagged.

Figure 3 Network access device—Layer 2 mode



Layer 3

In Layer 3 mode, DHCP-relay is enabled on the Ethernet Routing Switch 8300. In the network setup shown in Figure 3, the Ethernet Routing Switch 8300 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 8300 and the routing device.

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:

- Identify the Nortel SNAS 4050 pVIP address and mask.
- Identify VLAN IDs for Nortel SNA use.
- Identify ports you will use for uplink ports.
- Identify ports you will use for Nortel SNA client ports.

Configuring the network access device

To configure the Ethernet Routing Switch 8300 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:

1. Ensure the switch can communicate with the Nortel SNAS 4050 (try pinging the Nortel SNAS 4050).
2. Configure SSH on the switch if not already done.
   a. Load the particular encryption module needed (AES or 3DES).
   b. Enable sshd globally.

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

3. Configure the Nortel SNAS 4050 pVIP address/subnet.

4 (Optional) Configure the filters (Red, Yellow, and Green).

Note: Manual configuration of the filters is optional. The filters can be configured automatically as predefined defaults when you configure the Red, Yellow, and Green VLANs (see Step 9).

Default filters can be modified manually before Nortel SNA is enabled globally. After Nortel SNA is enabled globally, the filter (ACG) associated with a VLAN can be replaced with another one.

5 Create the port-based VLANs.

Existing VLANs can also be used.

These VLANs are configured as VoIP, Red, Yellow, and Green VLANs in Step 6 and Step 7.

6 Configure the VoIP VLANs.

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

Note: You must have previously created port-based VLANs (Step 5). You can also use an existing VLAN if it has no port members currently assigned.

8 Configure the Nortel SNA uplink filter, and attach it to the ports that are going to be configured as uplink ports.

9 Configure the Nortel SNA ports.

Identify switch ports as uplink or dynamic. Clients are connected on the dynamic ports.

Note: If the Nortel SNA switch itself is the DHCP relay agent 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.

10 Enable Nortel SNA globally.

Configuring the Ethernet Routing Switch 8300 for Nortel SNA

The following sections are added as new chapters to the next full release of *Configuring and Managing Security using the NNCLI and CLI*:

Configuring Nortel SNA using the CLI

This chapter describes how to configure the Ethernet Routing Switch 8300 as a network access device in the Nortel SNA solution using the CLI.

Specifically, it includes the following topics:

Roadmap of Nortel SNA CLI commands

The following roadmap lists the Nortel SNA CLI commands and their parameters. Use this list as a quick reference, or click on any entry for more information:

Command	Parameter
`config nsna nsnas <ipaddr/mask>`	`add`
	`delete`

Command	Parameter
	info
	nsna-port <value>
config vlan <vid> nsna color <red|green|yellow|voip|none>	filter-id <value>
	filter-name <value>
	yellow-subnet-ip <value>
config vlan <vid> nsna info	
config ethernet <ports> nsna	disable
	dynamic [voip-vlans <value>]
	info
	uplink uplink-vlans <value>
config nsna phone-signature	add <string>
	delete <string>
	info
config nsna state <enable|disable>	
config nsna info	
show commands	
show nsna nsnas [<ipaddr>]	
show nsna vlan [<vid>]	
show nsna interface [<ports>]	
show nsna client [ports <value>] [mac <value>]	
show nsna phone-signature [<string>]	
show nsna info	

Configuring the Nortel SNAS 4050 subnet

To configure the Nortel SNAS 4050 subnet, use the following command:

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

where `<ipaddr/mask>` is the Nortel SNAS 4050 pVIP address and network mask. Appropriate entries are **`a.b.c.d/x | a.b.c.d/x.x.x.x | default`**.

Note: The pVIP address is used in the default Red filter 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 45), you must manually update the Nortel SNAS 4050 subnet in the filters.

This command includes the following parameters:

`config nsna nsnas <ipaddr/mask>` followed by:	
`add`	Specifies the pVIP address of the Nortel SNAS 4050.
`delete`	Deletes the pVIP address of the Nortel SNAS 4050.
`info`	Shows the current level parameter settings and next level directories.
`nsna-port <value>`	Defines the TCP port number for the Switch to Nortel SNAS 4050 Communication Protocol (SSCP) server. The default setting is 5000.

Configuration example: adding a Nortel SNAS 4050 subnet

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

```
Passport-8310:5# config nsna nsnas 10.40.40.0/24 add
```

Viewing Nortel SNAS 4050 subnet information

To view information related to the Nortel SNAS 4050 subnet you configured, enter the following command:

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

where <ipaddr/mask> is the Nortel SNAS 4050 pVIP address and network mask (a.b.c.d./<0–32>).

Configuration example: viewing Nortel SNAS 4050 subnet information

```
Passport-8310:5# config nsna nsnas 10.40.40.0/24 info
                  Address : : 10.40.40.0
             Address Mask : : 255.255.255.0
                     Port : : 5000
Passport-8310:5#
```

Displaying Nortel SNAS 4050 information

To display the table of information related to the Nortel SNAS 4050, use the following command:

```
show nsna nsnas [<ipaddr>]
```

where <ipaddr> is the pVIP address for the Nortel SNAS 4050.

Example: displaying Nortel SNAS 4050 information

```
Passport-8310:5# show nsna nsnas

================================================================
                    NSNAS Info
================================================================
IP ADDRESS    NETMASK         PORT
----------------------------------------------------------------
10.40.40.0    255.255.255.0     5000
```

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).

You cannot manually assign dynamic ports to Nortel SNA VLANs. Printers and static devices must be in non-Nortel SNA VLANs.

To configure the Nortel SNA VLANs, use the following command:

```
config vlan <vid> nsna color <red|green|yellow|voip|none>
```

where `<vid>` is the VLAN ID in the range 1–4000.

This command includes the following parameters:

config vlan <vid> nsna color <red|yellow|green|voip|none> followed by:	
`filter-id <value>`	Sets the Nortel SNA filter ID. Values are in the range 1–1024.
`filter-name <value>`	Sets the Nortel SNA filter name. The string length 0–255.
`yellow-subnet-ip <value>`	Sets the Yellow VLAN subnet IP and mask. Appropriate entries are **`a.b.c.d/x`**, **`a.b.c.d/x.x.x.x`**, or **`default`**. **Note:** The Yellow subnet is the Remediation server IP address/subnet.

Viewing Nortel SNA VLAN information

To view information related to the Nortel SNA VLANs, use the following command:

```
config vlan <vid> nsna info
```

where <vid> is the VLAN ID in the range 1-4000.

Displaying Nortel SNA VLAN information in a table

To display the table of Nortel SNA VLAN information, use the following command:

```
show nsna vlan [<vid>]
```

where [<vid>] is the VLAN ID.

Example: displaying the Nortel SNA VLAN table

```
Passport-8310:5# show nsna vlan

=============================================================
                    NSNA VLAN Info
=============================================================
VLAN  VLAN   FILTER  FILTER-SET  YELLOW        YELLOW
ID    COLOR  ID      NAME        SUBNET-IP     SUBNET MASK
-------------------------------------------------------------
110   Red    310     acg-0310
120   Yellow 320     acg-0320    10.120.120.0  255.255.255.0
130   Green  330     acg-0330
140   Voip   0
```

Removing a Nortel SNA VLAN

To remove a Nortel SNA VLAN, use the following procedure:

1. Disable Nortel SNA globally.
2. Disable Nortel SNA on the uplink port.

3 Set the Nortel SNA VLAN color to **none** using the following command:

```
config vlan <vid> nsna color none
```

4 Delete the VLAN, if necessary, using the following command:

```
config vlan <vid> delete
```

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. VLANs 110, 120, 130, 140 were created as port-based VLANs to be used in the following configuration. For information on creating VLANs using the Ethernet Routing Switch 8300, refer to *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (317347-C))

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

VoIP VLANs are optional. Nortel recommends that you configure the VoIP VLANs before you configure the Red, Yellow, and Green VLANs, because the Red filters use the VoIP VLAN configuration. VoIP VLANs can be configured after you configure the other Nortel SNA VLANs, but in that case, you must modify the Red filter manually to update it.

In this example, the following parameters are used:

VLAN	Parameters
Red	VLAN ID: 110 Color: Red Filter ID: 310
Yellow	VLAN ID: 120 Color: Yellow Filter ID: 320 Subnet IP: 10.120.120.0/24

VLAN	Parameters
Green	VLAN ID: 130 Color: Green Filter ID: 330
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. The default filters are given the IDs you specify when you configure the Nortel SNA VLANs.

You can use pre-existing filters (using the IDs of those pre-existing filters when you configure the Nortel SNA VLANs), but you must ensure those filters are configured for Nortel SNA.

Configuring the VoIP VLAN

To configure the VoIP VLAN, use the following command:

```
Passport-8310:5# config vlan 140 nsna color voip

Passport-8310:5# config vlan 140 nsna info
            vlan Id : : 140
              color : : Voip
        filter-name : :
       YellowSubnet : : 0.0.0.0
   YellowSubnetMask : : 0.0.0.0
```

Configuring the Red VLAN

To configure the Red VLAN, use the following command:

```
Passport-8310:5# config vlan 110 nsna color red filter-id
310
```

```
Passport-8310:5# config vlan 110 nsna info
            vlan Id : : 110
              color : : Red
        filter-name : : acg-0310
       YellowSubnet : : 0.0.0.0
   YellowSubnetMask : : 0.0.0.0
```

Configuring the Yellow VLAN

To configure the Yellow VLAN, use the following command:

```
Passport-8310:5# config vlan 120 nsna color yellow filter-id
320 yellow-subnet-ip 10.120.120.0/24

Passport-8310:5# config vlan 120 nsna info
            vlan Id : 120
              color : Yellow
        filter-name : acg-0320
       YellowSubnet : 10.120.120.0
   YellowSubnetMask : 255.255.255.0
```

Configuring the Green VLAN

To configure the Green VLAN, use the following command:

```
Passport-8310:5# config vlan 130 nsna color green filter-id
330

Passport-8310:5# config vlan 130 nsna info
               vlan Id : 130
                 color : Green
           filter-name : acg-0330
          YellowSubnet : 0.0.0.0
      YellowSubnetMask : 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 27.

The uplink port is introduced for the Nortel SNA solution. You configure these ports to be 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).

To configure Nortel SNA on ports, use the following command:

```
config ethernet <ports> nsna
```

where `<ports>` uses the convention {slot/port[–slot/port][,...]}.

This command includes the following parameters:

config ethernet <ports> nsna followed by:	
`disable`	Enables/disables the Nortel SNA state of the port.
`dynamic [voip-vlans <value>]`	Sets the Nortel SNAS 4050 dynamic port configuration, where `<value>` is the VoIP VLAN IDs (vlan-id[-vlan-id][,...]).
`info`	Shows the current Nortel SNA settings for the port.
`uplink uplink-vlans <value>`	Defines the Nortel SNAS 4050 uplink VLAN list, where `<value>` is the Nortel SNA VLAN IDs (vlan-id[-vlan-id][,...]).

Viewing Nortel SNA port information

To view information related to the Nortel SNA ports, use the following command:

```
config ethernet <ports> nsna info
```

where <ports> uses the convention {slot/port[–slot/port][,...]}.

Displaying Nortel SNA interface information

To display the table of Nortel SNA interface information, use the following command:

```
show nsna interface [<ports>]
```

where [<ports>] uses the convention {slot/port[–slot/port][,...]}.

Example: displaying the Nortel SNA interface table

```
Passport-8310:5# show nsna interface 1/16-1/17

================================================================
                    NSNA Interface Info
================================================================
PORT  NSNA    GREEN    UPLINK    VOIP      PORT   DHCP
NUM   MODE    VLAN ID  VLAN IDS  VLAN IDS  STATE  STATE
----------------------------------------------------------------
1/16  DYNAMIC -                  140       None   UnBlocked
1/17  DYNAMIC -                  140       None   UnBlocked
```

Removing a Nortel SNA port

To remove a Nortel SNA port, use the following command:

```
config ethernet <ports> nsna disable
```

where <ports> uses the convention {slot/port[–slot/port][,...]}

Example: Removing Nortel SNA ports

To disable Nortel SNA on slot 1, ports 20–24, enter the following command:

```
Passport-8310:5# config ethernet 1/20-1/24 nsna disable
Passport-8310:5#
```

Configuration example: Adding the uplink port

Note: You must have the uplink filter configured before you can add the uplink port to the VLANs. Refer to "Configuring the uplink filter" on page 32 for an example.

To add the uplink port to the VLANs, use the following command:

```
config ethernet <ports> nsna uplink uplink-vlans <vidlist>
```

where:

- `<ports>` uses the convention {slot/port[–slot/port][,...]}
- `<vidlist>` is the Nortel SNA 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 `config vlan <vid> ports add` command (see "Adding ports to a VLAN" in *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (317347-C) for more information).

You cannot manually add a port to a Nortel SNA VLAN, and dynamic Nortel SNA ports cannot be added to non-Nortel SNA VLANs. Additionally, non-Nortel SNA ports cannot be associated with Nortel SNA VLANs.

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 8300, Software Release 2.2.8.

In this example, the following parameters are used:

- Uplink port is 1/48.
- Nortel SNA VLAN IDs are 110, 120, 130, 140.

```
Passport-8310:5# config ethernet 1/48 nsna uplink
uplink-vlans 110,120,130,140
Passport-8310:5# config ethernet 1/48 nsna info

Port : : 1/48
                Mode : : Uplink
          VoipVlanIds: :
        UplinkVlanIds: : 110 120 130 140
```

Configuration example: Adding client ports

In this example, client ports are 1/16–1/17.

```
Passport-8310:5# config ethernet 1/16-1/17 nsna dynamic
Passport-8310:5# config ethernet 1/16-1/17 nsna info

Port : : 1/16
              Mode : : Dynamic
        VoipVlanIds: :
      UplinkVlanIds: :

Port : : 1/17
              Mode : : Dynamic
       VoipVlanIds : :
     UplinkVlanIds : :
```

Note: When you configure a port as dynamic or uplink, 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.

Displaying information about Nortel SNA clients

To display the table of Nortel SNA clients currently connected to the switch, use the following command:

```
show nsna client [ports <value>] [mac <value>]
```

where:

- `[ports <value>]` is the slot/port number entered as {slot/port[-slot/port][,...]}
- `[mac <value>]` is the MAC address of the host

Example: show nsna client

```
Passport-8310:5# show nsna client

=============================================================
                       NSNA CLIENT INFO
=============================================================
PORT  CLIENT              DEVICE    VLAN  AGED    IP
NUM   MAC                 TYPE      ID     OUT   ADDRESS
-------------------------------------------------------------
1/5   00:80:22:44:66:88   PC        110     N    10.11.12.13
1/5   00:08:11:22:33:44   IP-Phone  140     N    10.20.30.40
```

Entering phone signatures for Nortel SNA

To specify IP phone signatures for the Nortel SNA solution, use the following command:

```
config nsna phone-signature
```

This command includes the following parameters:

config nsna phone-signature followed by:	
`add <string>`	Adds a phone signature. String length is in the range 1–64 characters.
`delete <string>`	Deletes a phone signature. String length is in the range 1–64 characters.
`info`	Displays information about currently configured phone signatures.

Example: adding Nortel SNA phone signatures

To add a phone signature of Nortel-i2007-A, use the following command:

```
Passport-8310:5# config nsna phone-signature add
Nortel-i2007-A
Passport-8310:5#
```

Example: viewing Nortel SNA phone signatures information

To view configured Nortel SNA phone signatures, use the following command:

```
Passport-8310:5# config nsna phone-signature info
           Nortel-i2004-A
           Nortel-i2007-A
Passport-8310:5#
```

Example: removing Nortel SNA phone signatures

To remove the Nortel SNA phone signature of Nortel-i2007-A, use the following command:

```
Passport-8310:5# config nsna phone-signature delete
Nortel-i2007-A
Passport-8310:5#
```

Displaying phone signatures in a table

To display the table of Nortel SNA phone signatures, use the following command:

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

where <string> is the phone signature string in the range of 1–64 characters.

Example: displaying the Nortel SNA IP phone signatures table

```
Passport-8310:5# show nsna phone-signature

================================================================
                NSNA IP PHONE SIGNATURE INFO
================================================================
--------------------------------
      Nortel-i2004-A
      Nortel-i2007-A

Passport-8310:5#
```

Enabling Nortel SNA

To enable Nortel SNA, use the following command:

```
config nsna state <enable|disable>
```

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

Viewing information about the Nortel SNA state

Use the following command for information on the state of Nortel SNA on the switch:

```
config nsna info
```

Displaying Nortel SNA information

To display information related specifically to Nortel SNA as it is currently configured, use the following command:

```
show nsna info
```

Example: displaying Nortel SNA information

```
Passport-8310:5# show nsna info
  nsnasConnectionState: :connected
      nsnasInetAddress: :10.40.40.0
                  nsna: :enable
   Send Hello Interval: :60
   Inactivity Interval: :180
            Status Quo: :240
Passport-8310:5#
```

Configuring Nortel SNA using the NNCLI

This section describes how to configure the Ethernet Routing Switch 8300 as a network access device in the Nortel SNA solution using the Nortel Command Line Interface (NNCLI).

Specifically, it includes the following topics:

Roadmap of Nortel SNA NNCLI commands

The following roadmap lists the Nortel SNA NNCLI commands and their parameters. Use this list as a quick reference, or click on any entry for more information.

Command	Parameter
nsna nsnas <ipaddr/mask>	port <value>
show nsna nsnas <ipaddr/mask>	
no nsna nsnas <ipaddr/mask>	
nsna vlan <vid> color <red|yellow|green|voip>	filter <filter id>
	yellow-subnet <ipaddr/mask>
show nsna vlan <vid>	
no nsna vlan <vid>	

Command	Parameter
nsna	port <portlist>
	dynamic voip-vlans <vidlist>
	uplink vlans <vidlist>
show nsna interface [<interface-type>] [<interface-id>]	
no nsna	
show nsna client [interface [<interface-type>] [<interface-id>] | mac-address <H.H.H.>]	
nsna phone-signature <LINE>	
no nsna phone-signature <LINE>	
show nsna phone-signature [<LINE>]	
nsna enable	
no nsna enable	
show nsna	

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 pVIP address and network mask (a.b.c.d./<0–32> | a.b.c.d/x.x.x.x | default).

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

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

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

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 subnet of 10.40.40.0/24, enter the following command:

```
Passport-8310:5(config)# nsna nsnas 10.40.40.0/24
```

Viewing Nortel SNAS 4050 subnet information

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

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

where <ipaddr/mask> is the Nortel SNAS 4050 pVIP address and network mask (a.b.c.d./<0–32>).

Configuration example: Viewing Nortel SNAS 4050 subnet information

```
Passport-8310:5# show nsna nsnas 10.40.40.0/24

=============================================================
                      NSNAS Info
=============================================================

IP ADDRESS    NETMASK         MGMT ADDRESS      MGMT MASK   Port
-------------------------------------------------------------
10.40.40.0    255.255.255.0                                 5000
```

Removing the Nortel SNAS 4050 subnet

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

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

where `<ipaddr/mask>` is the Nortel SNAS 4050 IP 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).

You cannot manually assign dynamic ports to Nortel SNA VLANs. Printers and static devices must be in non-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 2–4000.

This command includes the following parameters:

nsna vlan <vid> color <red|yellow|green|voip> followed by:	
filter <filter id>	Sets the NSNA filter ID. Values are in the range 1–1024. **Note:** This parameter is not allowed for configuration of a VoIP VLAN. VoIP filters are part of the Red/Yellow filters.
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. The Yellow subnet is the Remediation server IP address/subnet.

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 1-4000.

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 1-4000.

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, 140 (used in this example) were previously created as port-based VLANs (for information on creating VLANs using the Ethernet Routing Switch 8300, refer to *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI* (316805-C)).

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

VoIP VLANs are optional. Nortel recommends that you configure the VoIP VLANs before you configure the Red, Yellow, and Green VLANs, because the Red filters use the VoIP VLAN configuration. VoIP VLANs can be configured after you configure the other Nortel SNA VLANs, but in that case, you must modify the Red filter manually to update it.

In this example, the following parameters are used:

VLAN	Parameters
Red	VLAN ID: 110 Color: Red Filter name: 1
Yellow	VLAN ID: 120 Color: Yellow Filter name: 2 Subnet IP: 10.120.120.0/24
Green	VLAN ID: 130 Color: Green Filter name: 3
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. The default filters are given the IDs you specify when you configure the Nortel SNA VLANs.

You can use pre-existing filters (using the IDs of those pre-existing filters when you configure the Nortel SNA VLANs), but you must ensure those filters are configured for Nortel SNA.

Configuring the VoIP VLAN

To configure the VoIP VLAN, use the following command:

```
Passport-8310:5(config)# nsna vlan 140 color voip

Passport-8310:5(config)# show nsna vlan 140

============================================================
                        NSNA VLAN Info
============================================================
VLAN     VLAN    FILTER  FILTER-SET   YELLOW     YELLOW
ID       COLOR   ID       NAME       SUBNET-IP   SUBNET_MASK
------------------------------------------------------------
140      VOIP    0
```

Configuring the Red VLAN

To configure the Red VLAN, use the following command:

```
Passport-8310:5(config)# nsna vlan 110 color red filter 1

Passport-8310:5(config)# show nsna vlan 110

============================================================
                        NSNA VLAN Info
============================================================
VLAN     VLAN    FILTER  FILTER-SET   YELLOW     YELLOW
ID       COLOR   ID       NAME       SUBNET-IP   SUBNET_MASK
------------------------------------------------------------
110      Red     1       acg-0001
```

Configuring the Yellow VLAN

To configure the Yellow VLAN, use the following command:

```
Passport-8310:5(config)# nsna vlan 120 color yellow filter 2
yellow-subnet 10.120.120.0/24

Passport-8310:5# show nsna vlan 120

=============================================================
                          NSNA VLAN Info
=============================================================
VLAN  VLAN    FILTER  FILTER-SET  YELLOW        YELLOW
ID    COLOR   ID       NAME      SUBNET-IP     SUBNET-MASK
-------------------------------------------------------------
120   Yellow  2       acg-0002   10.120.120.0  255.255.255.0
```

Configuring the Green VLAN

To configure the Green VLAN, use the following command:

```
Passport-8310:5(config)# nsna vlan 130 color green filter 3

Passport-8310:5(config)# show nsna vlan 130

=============================================================
                          NSNA VLAN Info
=============================================================
VLAN      VLAN    FILTER  FILTER-SET   YELLOW      YELLOW
ID        COLOR   ID       NAME       SUBNET-IP   SUBNET_MASK
-------------------------------------------------------------
130       Green   3       acg-0003
```

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 27.

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).

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

```
nsna
```

This command includes the following parameters:

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

Viewing Nortel SNA port information

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

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

where:

- `<interface-type>` is the port type (for example, FastEthernet)
- `<interface-id>` is the slot/port number entered as {slot/port[-slot/port][,...]}

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 slot 1, ports 20–24, enter the following commands:

```
Passport-8310:5(config)#interface fastethernet 1/20-1/24
Passport-8310:5(config-if)#no nsna
Passport-8310:5(config-if)#exit
Passport-8310:5(config)#
```

Configuration example: Adding the uplink port

Note: You must have the uplink filter configured before you add the uplink port to the VLANs. Refer to "Configuring the uplink filter" on page 32 for an example.

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 Nortel SNA 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 ports add` command (see "Adding ports to a VLAN" in *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (317347-C) for more information).

You cannot manually add a port to a Nortel SNA VLAN, and dynamic Nortel SNA ports cannot be added to non-Nortel SNA VLANs. Additionally, non-Nortel SNA ports cannot be associated with Nortel SNA VLANs.

Multiple Nortel SNA uplink ports are supported for Ethernet Routing Switch 8300, Software Release 2.2.8.

In this example, the following parameters are used:

- uplink ports are slot 1, ports 20-24
- Nortel SNA VLAN IDs are 110, 120, 130, 140

```
Passport-8310:5(config)#interface fastEthernet 1/20-1/24
Passport-8310:5(config-if)#nsna uplink vlans 110,120,130,140
Passport-8310:5(config-if)#show nsna interface 1/20-1/24

================================================================
                    NSNA Interface Info
================================================================
PORT  NSNA  GREEN    UPLINK      VOIP        PORT    DHCP
NUM   MODE  VLAN ID  VLAN IDS    VLAN IDS    STATE   STATE
----------------------------------------------------------------
1/20   Uplink        110 120 130 140       None    Unblocked
1/20   Uplink        110 120 130 140       None    Unblocked
1/20   Uplink        110 120 130 140       None    Unblocked
1/20   Uplink        110 120 130 140       None    Unblocked
Passport-8310:5(config-if)#exit
Passport-8310:5(config)#
```

Configuration example: Adding client ports

In this example, the following parameters are used:

- Client ports are slot 1, ports 3, 4, and 5.
- VoIP VLAN ID is 140.

```
Passport-8310:5(config)#interface fastEthernet 1/3-1/5
Passport-8310:5(config-if)#nsna dynamic voip-vlans 140
Passport-8310:5(config-if)#show nsna interface 1/3-1/5
==========================================================
                    NSNA Interface Info
==========================================================
PORT  NSNA  GREEN    UPLINK    VOIP       PORT    DHCP
NUM   MODE  VLAN ID  VLAN IDS  VLAN IDS   STATE   STATE
----------------------------------------------------------------------------------------------
1/3   Dynamic                  140        None    UnBlocked
1/4   Dynamic                  140        None    UnBlocked
1/5   Dynamic                  140        None    UnBlocked
Passport-8310:5(config-if)#exit
Passport-8310:5(config)#
```

Viewing information on Nortel SNA clients

To view information on Nortel SNA clients currently connected to the switch, enter the following command from the Privileged EXEC configuration mode:

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

where:

- `<interface-type>` is the port type (for example, FastEthernet)
- `<interface-id>` is the slot/port number entered as {slot/port[-slot/port][,...]}
- `<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:

```
Passport-8310:5# show nsna client interface 1/5

================================================================
                        NSNA CLIENT INFO
================================================================
PORT  CLIENT              DEVICE    VLAN   AGED    IP
NUM   MAC                 TYPE      ID     OUT   ADDRESS
----------------------------------------------------------------
1/5   00:08:11:22:33:44   IP-Phone  140     N    10.20.30.40
```

Entering phone signatures for Nortel SNA

To specify 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 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.

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:

```
Passport-8310:5# show nsna
  nsnasConnectionState: :connected
      nsnasInetAddress: :10.40.40.0
                  nsna: :enable
   Send Hello Interval: :60
   Inactivity Interval: :180
            Status Quo: :240
```

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

```
Passport-8310:5# show nsna
nsnasConnectionState : : not connected
    nsnasInetAddress : :
                nsna : : enable
  Send Hello Interval: : 0
  Inactivity Interval: : 0
           Status Quo: : 0
```

Updates to the Bandwidth Management menu for Nortel SNA

The following sections describe updates to the **Bandwidth Management** menu:

Additions to field entries for the ACE Common tab

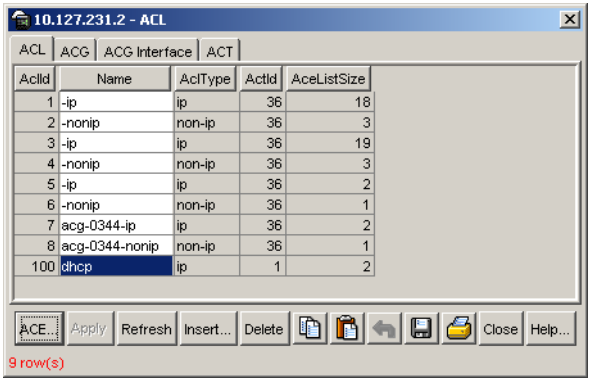
You can now set the operating mode for an ACE to **fwd2cpu**, which is necessary when configuring the Nortel SNA uplink filter.

To configure the uplink filter:

1 Select **Bandwidth Management > Filter > ACL** from the Device Manager menu.

The **ACL** dialog box opens with the **ACL** tab selected (see Figure 4).

Figure 4 ACL dialog box > ACL tab



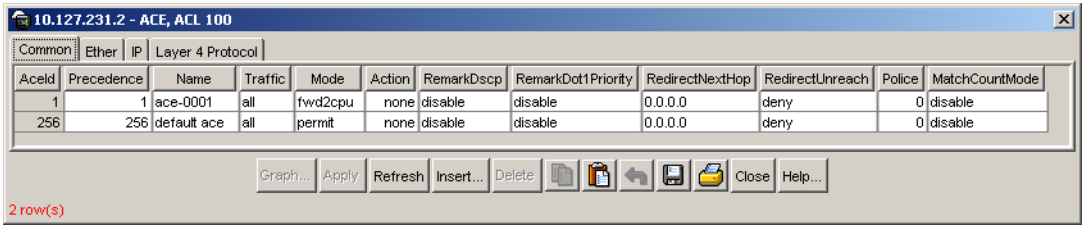
2 Select an ACL.

The **ACE** button is activated.

3 Click the **ACE** button.

The **ACE, ACL** dialog box opens with the **Common** tab selected (see Figure 5).

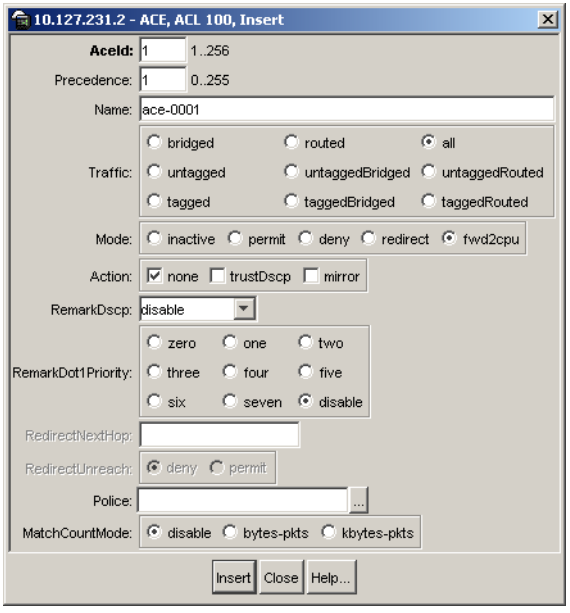
Figure 5 ACE, ACL dialog box > Common tab



4 Click **Insert**.

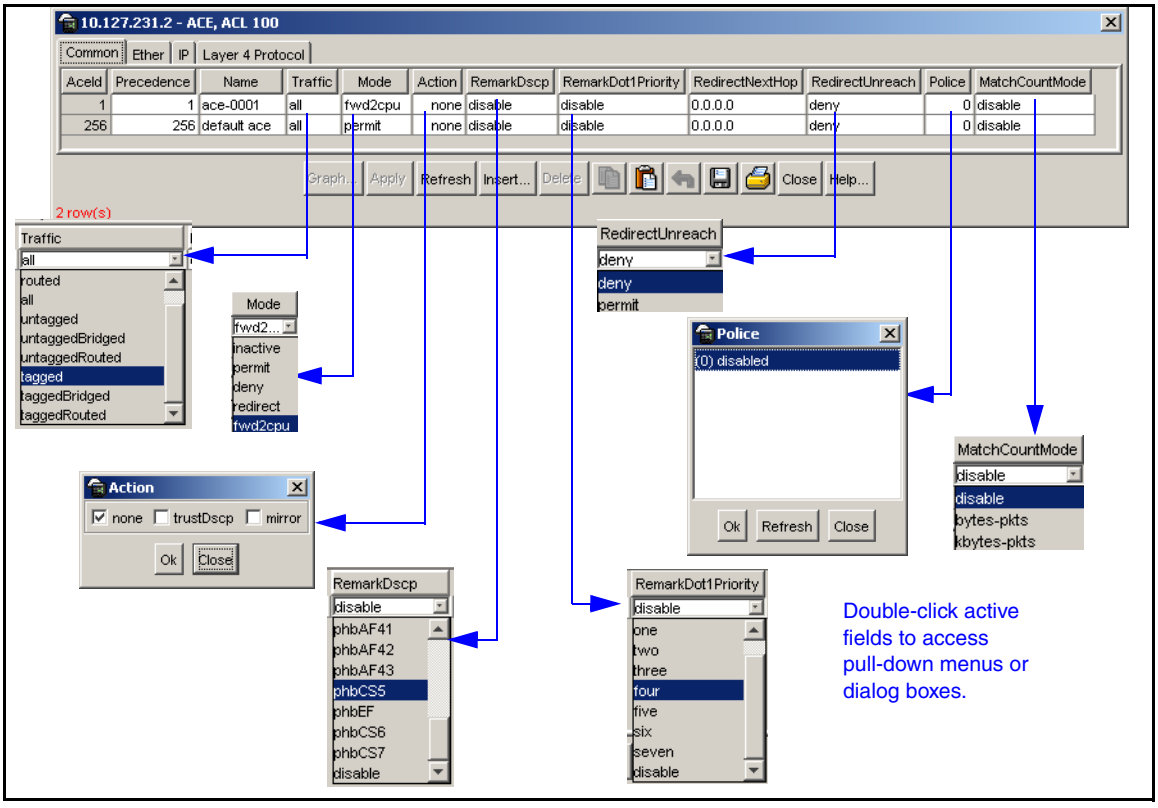
The **ACE, ACL, Insert Common** dialog box opens (see Figure 6).

Figure 6 ACE, ACL, Insert Common dialog box



Mode options now include **fwd2cpu**. When selected, the **fwd2cpu** option forwards traffic to the CPU (used for the Nortel SNA uplink filter).

Figure 14 in Chapter 3 of *Configuring QoS and Filters using Device Manager* (317340-B), page 58, is updated:



The **Mode** field description in Table 6, page 59, Chapter 3 of *Configuring QoS and Filters using Device Manager* (317340-B), is updated as follows:

Field	Description
Mode	Specifies the operating mode associated with this ACE. The following modes determine what action is taken when the ACE matches a packet: • inactive - no affect on traffic • permit - permits traffic • deny - denies traffic • redirect - redirects traffic • fwd2cpu - forwards traffic to the CPU (used for the Nortel SNA uplink filter) The default setting is deny.

Additions to field entries for the ACE Ether tab

For additions to the **ACE, ACL Ether** tab for Nortel SNA:

1 Select **Bandwidth Management > Filter > ACL** from the Device Manager menu.

The **ACL** dialog box opens with the **ACL** tab selected (see Figure 4 on page 71).

2 Click the **ACE** button.

The **ACE, ACL** dialog box opens with the **Common** tab selected (see Figure 5 on page 72).

3 Click the **Ether** tab.

The **Ether** tab is selected (see Figure 7 on page 75).

Figure 7 ACE, ACL dialog box > Ether tab

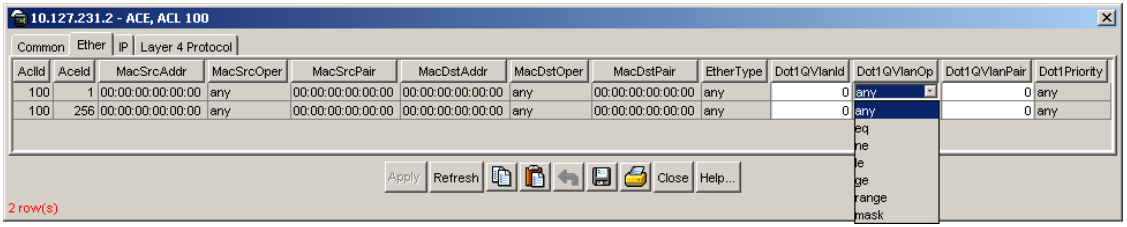


Table 7 describes the **ACE, ACL Ether** tab field additions.

Table 7 ACE, ACL Common tab fields

Field	Description
Dot1QVlanOp	Specifies the logical operator. Options are the following: • any • eq • ne • le • ge • range • mask
Dot1QVlanPair	Defines a set of VLAN IDs in the context of the Dot1qVlanId and the Dot1qVlanOp fields. This field specifies the second value when the operator is mask or range.

Configuring Nortel SNA using Device Manager

This section describes how to configure the Ethernet Routing Switch 8300 as a network access device in the Nortel SNA solution using the Java Device Manager (Device Manager).

Specifically, it includes the following topics:

Configuring the Nortel SNAS 4050 subnet

To configure the Nortel SNAS 4050 subnet:

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

The **NSNA** dialog box opens with the **NSNAS** tab selected (see Figure 8).

Figure 8 Security NSNA dialog box > NSNAS tab

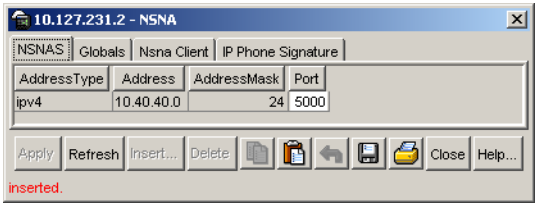


Table 8 describes the **NSNAS** tab fields.

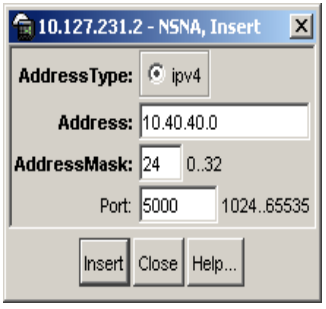
Table 8 NSNA NSNAS tab fields

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 portal Virtual IP (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 SSCP server. The default setting is 5000.

2 Click **Insert**.

The **NSNAS, Insert** dialog box opens (see Figure 9).

Figure 9 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 to restrict the communication of clients in the Red state to the Nortel SNAS 4050.

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

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

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

5 Click **Insert**.

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

Note: In Ethernet Routing Switch 8300, Software Release 2.2.8, you can configure only one entry for the Nortel SNAS 4050 subnet.

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 8 on page 76).

2 Select the row that contains the Nortel SNAS 4050 subnet information.

3 Click **Delete**.

The Nortel SNAS 4050 subnet information is removed from the Nortel SNA configuration.

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).

Ports that are configured to function in non-Nortel SNA VLANs cannot be used for Nortel SNA purposes unless they are first removed from those non-Nortel SNA VLANs.

You cannot manually assign dynamic ports to Nortel SNA VLANs.

Printers and static devices must be in non-Nortel SNA VLANs.

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 10).

Figure 10 VLAN dialog box > Basic tab

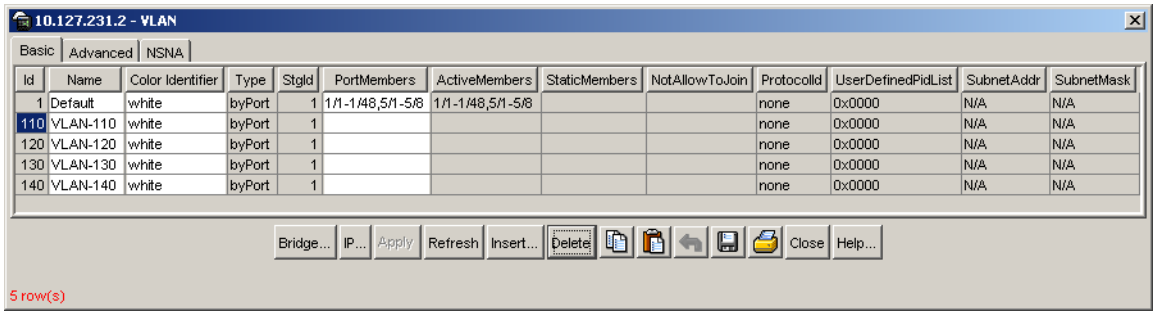


Table 9 describes the **VLAN Basic** tab fields.

Table 9 VLAN Basic tab fields

Field	Description
Id	Specifies the ID for the VLAN.
Name	Specifies the name of the VLAN.
Color Identifier	A proprietary color scheme to associate a color with the VLAN. Color does not affect how frames are forwarded.
Type	Specifies the type of VLAN: • byPort • byProtocolId
StgId	Specifies the ID of the spanning tree group to which the VLAN belongs.
PortMembers	Specifies the slot/port of each possible VLAN member.
ActiveMembers	Specifies the slot/port of each active VLAN member.
StaticMembers	Specifies the slot/port of each static member of a protocol-based VLAN.
NotAllowToJoin	Specifies the slot/ports that are never allowed to become a member of the protocol-based VLAN.

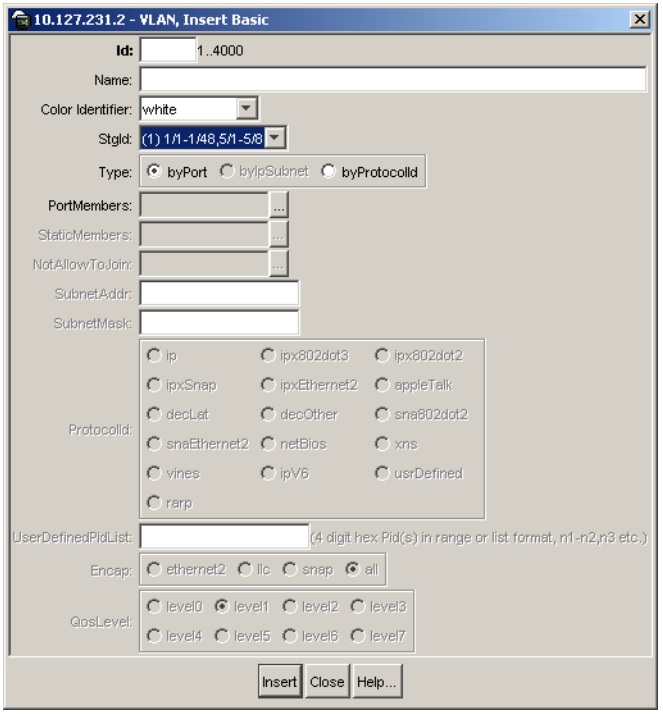
Table 9 VLAN Basic tab fields (continued)

Field	Description
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)
UserDefinedPidList	Specifies the 16-bit user-defined network protocol identifier when the ProtocolId (above) is set to usrDefined for a protocol-based VLAN type.

2 Click **Insert**.

The **VLAN, Insert Basic** dialog box opens (see Figure 11 on page 81). Create the VLANs to be configured as Nortel SNA VLANs.

Figure 11 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 12 on page 82).

Figure 12 VLAN dialog box > NSNA tab

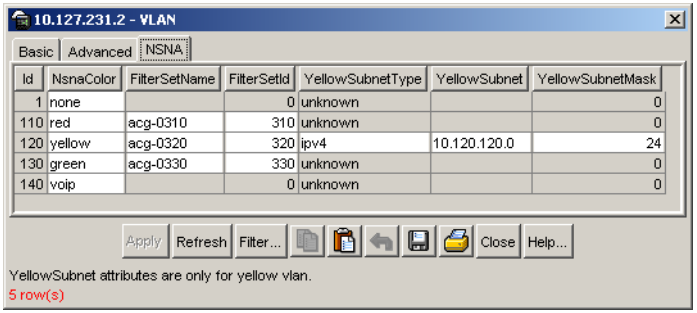


Table 10 describes the **VLAN NSNA** tab fields.

Table 10 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. The string length 0–255. **Note:** This field is applicable only when the **NsnaColor** field is set to red, yellow, or green.
FilterSetId	Specifies the Nortel SNA filter ID. Values are in the range 1–1024. **Note:** This parameter is not allowed for configuration of a VoIP VLAN. VoIP filters are part of the Red/Yellow filters.
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. The Yellow subnet is the Remediation server IP address/subnet. **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 12 on page 82 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 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 8300, Software Release 2.2.8, Nortel recommends that you configure no more than five Yellow, five Green, and five VoIP VLANs on each switch.

Removing a Nortel SNA VLAN

To remove a Nortel SNA VLAN:

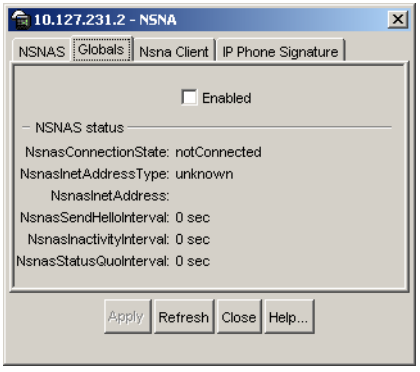
1 Select **Edit > Security > NSNA** from the Device Manager menu.

The **NSNA** dialog box opens with the **NSNAS** tab selected (see Figure 8 on page 76).

2 Click the **Globals** tab.

The **Globals** tab is selected (see Figure 13).

Figure 13 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 10 on page 79).

6 Click the **NSNA** tab.

The **NSNA** tab is selected (see Figure 12 on page 82).

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 10 on page 79).

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

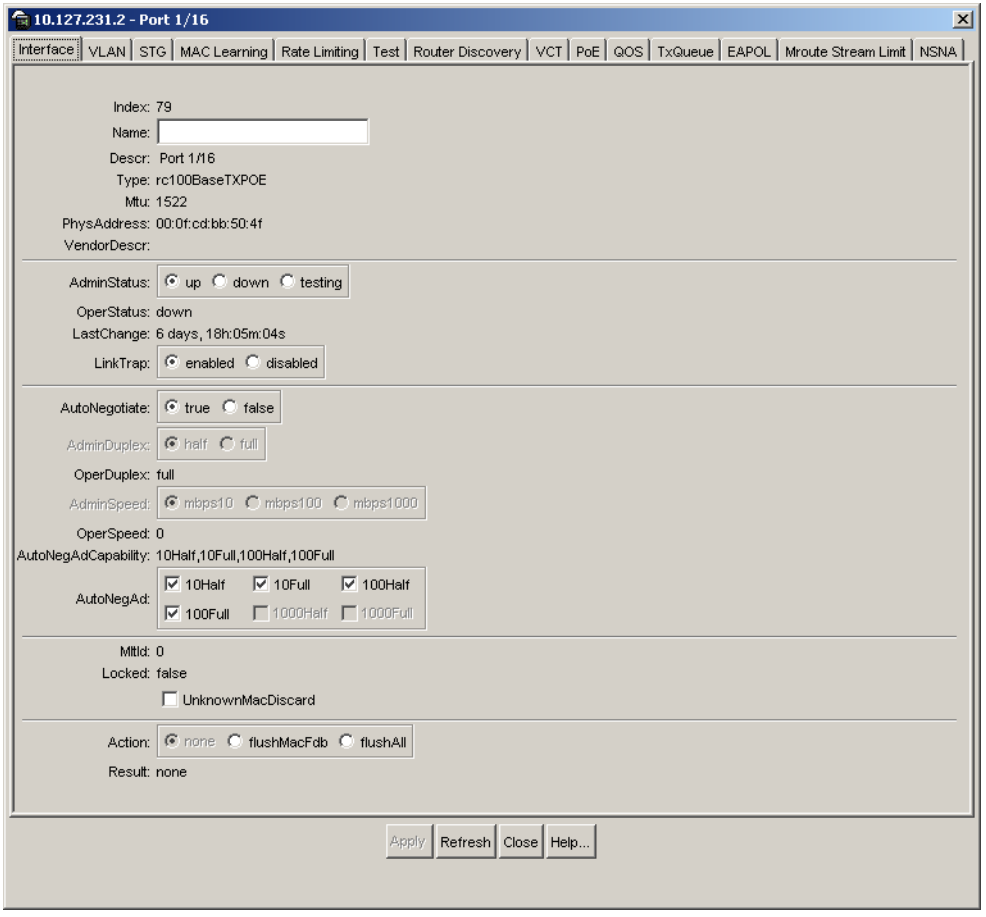
To enable Nortel SNA on ports:

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 14 on page 85).

Figure 14 Port dialog box > Interface tab



3 Click the **NSNA** tab.

The **NSNA** tab is selected (see Figure 15 on page 86).

Figure 15 Port dialog box > NSNA tab

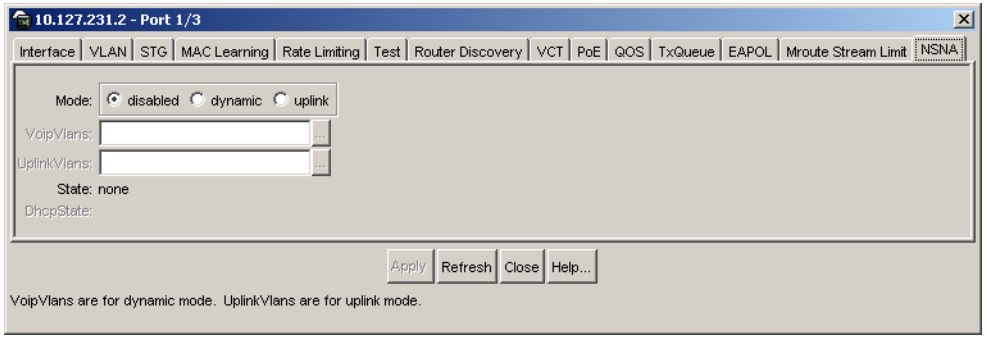


Table 11 describes the **NSNA** tab fields.

Table 11 Port NSNA tab fields

Field	Description
Mode	Specifies the Nortel SNA mode for the port. Options are the following: • disabled • dynamic • uplink
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 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 8 on page 76).

2 Click the **Nsna Client** tab.

The **Nsna Client** tab is selected (see Figure 16). Clients currently connected to the network access device display in this tab.

Figure 16 Security NSNA dialog box > Nsna Client tab

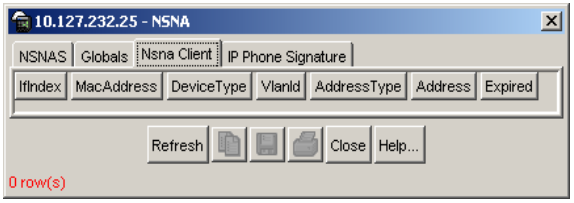


Table 12 describes the **NSNA Client** tab fields.

Table 12 NSNA NSNA Client tab fields

Field	Description
IfIndex	Specifies the logical interface index of the port to which the client is attached.
MacAddress	Specifies the MAC address of the client.
Device Type	Specifies the type of client device (pc, ipPhone, or printer).

Table 12 NSNA NSNA Client tab fields (continued)

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

Entering phone signatures for Nortel SNA

To specify IP phone signatures for Nortel SNA:

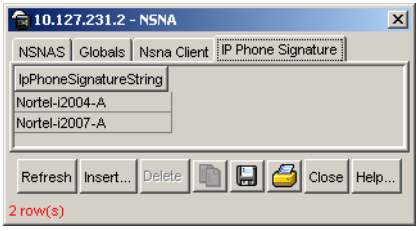
1 Select **Edit > Security > NSNA** from the Device Manager menu.

The **NSNA** dialog box opens with the **NSNAS** tab selected (see Figure 8 on page 76)).

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

The **IP Phone Signature** tab is selected (see Figure 17).

Figure 17 Security NSNA dialog box > IP Phone Signature tab



3 Click **Insert**.

The **NSNA, Insert IP Phone Signature** dialog box opens (see Figure 18).

Figure 18 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 8 on page 76).

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

The **IP Phone Signature** tab is selected (see Figure 17 on page 88).

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.

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 8 on page 76).

2 Click the **Globals** tab.

The **Globals** tab is selected (see Figure 13 on page 83).

3 Select the **Enabled** check box.

4 Click **Apply**.

Configuration example

The following configuration procedure 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 2.2.8
- you have configured basic switch connectivity
- you have initialized the switch and it is ready to accept configuration

Configuring the Ethernet Routing Switch 8300 for the Nortel SNA solution using the CLI

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

Figure 19 on page 91 shows the basic network configuration used in this example. The Ethernet Routing Switch 8600 functions as the core router.

Table 13 describes the devices connected in this environment and their respective VLAN IDs and IP addresses.

Table 13 Network devices

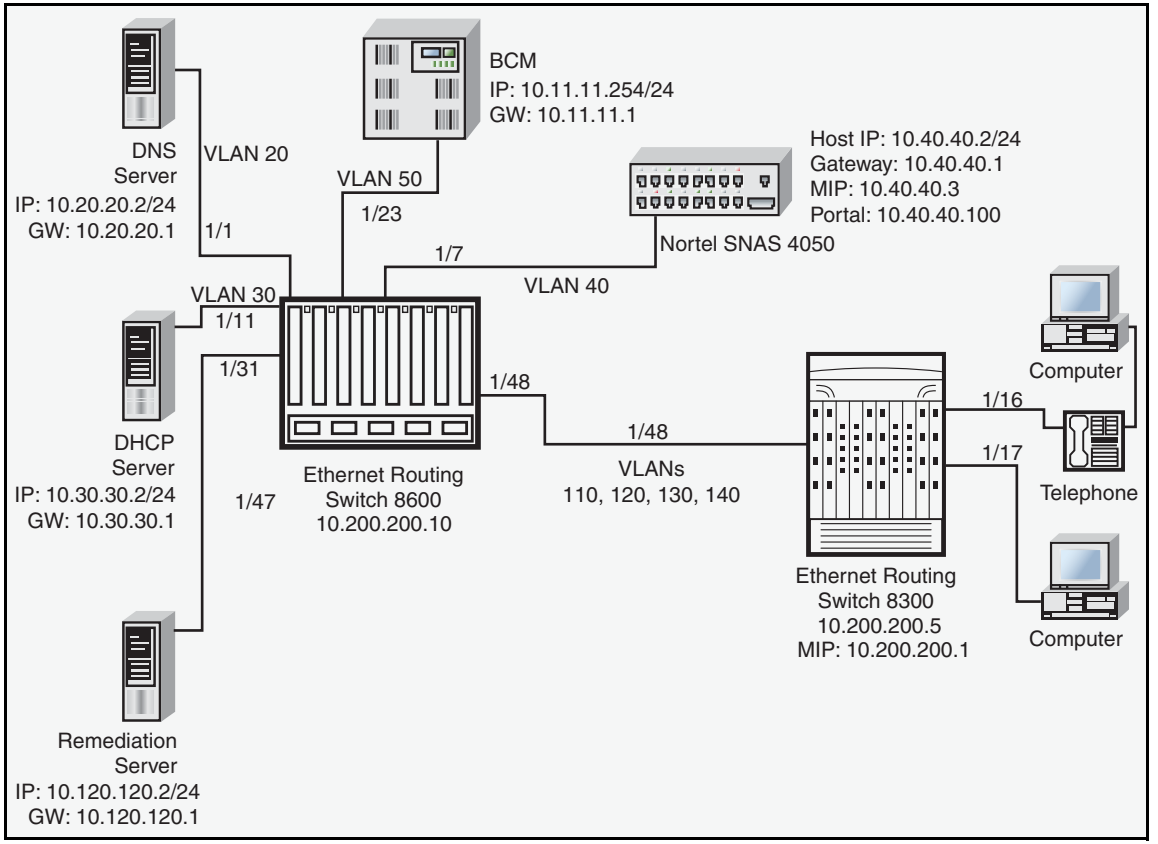
Device/Service	VLAN ID	VLAN IP	Device IP	Ethernet Routing Switch 8600 port
DNS	20	10.20.20.1	10.20.20.2	1/1
DHCP	30	10.30.30.1	10.30.30.2	1/11
Nortel SNAS 4050	40	10.40.40.1	10.40.40.2	1/7
Remediation server	120	10.120.120.1	10.120.120.2	1/31
Call server	50	10.11.11.1	10.11.11.254	1/23

Table 14 describes the VLANs for the Ethernet Routing Switch 8300.

Table 14 VLANs for the Ethernet Routing Switch 8300

VLAN	VLAN ID	Yellow subnet
Red	110	N/A
Yellow	120	10.120.120.0/24
Green	130	N/A
VoIP	140	N/A

Figure 19 Basic network scenario



Enabling SSH

```
Passport-8310:5# config bootconfig flags ssh true
Passport-8310:5# config sys set ssh enable true
Passport-8310:5# config load-module 3DES /flash/P83C2280.IMG
```

Note: You have the option of using the AES encryption module, instead of the 3DES module.

Configuring the Nortel SNAS 4050 pVIP subnet

```
Passport-8310:5# config nsna nsnas 10.40.40.0/24 add
```

Creating port-based VLANs

```
Passport-8310:5# config vlan 110 create byport 1
Passport-8310:5# config vlan 120 create byport 1
Passport-8310:5# config vlan 130 create byport 1
Passport-8310:5# config vlan 140 create byport 1
```

Configuring the VoIP VLANs

```
Passport-8310:5# config vlan 140 nsna color voip
```

Configuring the Red, Yellow, and Green VLANs

```
Passport-8310:5# config vlan 110 nsna color red filter-id
310
Passport-8310:5# config vlan 120 nsna color yellow filter-id
320 yellow-subnet-ip 10.120.120.0/24
Passport-8310:5# config vlan 130 nsna color green filter-id
330
```

Configuring the Nortel SNA uplink filter

```
Passport-8310:6# config filter acl 100 create ip acl-name
"dhcp"
Passport-8310:6/config# filter acl 100 ace 1 create
Passport-8310:6# config filter acl 100 ace 1 action fwd2cpu
precedence 1
Passport-8310:6# config filter acl 100 ace 1 ip ipfragment
```

```
non-fragments
Passport-8310:6# config filter acl 100 ace 1 protocol udp eq
any
Passport-8310:6# config filter acl 100 ace 1 port dst-port
bootpd-dhcp
Passport-8310:6# config filter acl 100 ace default action
permit
Passport-8310:6# config filter acg 100 create 100 acg-name
"uplink"

Passport-8310:6# config ethernet <slot/port> filter create
100
```

Configuring the Nortel SNA ports

Add the uplink port:

```
Passport-8310:6# config ethernet 1/48 nsna uplink
uplink-vlans 110,120,130,140
```

Add the client ports:

```
Passport-8310:5# config ethernet 1/16-1/17 nsna dynamic
```

Enabling Nortel SNA globally

```
Passport-8310:5# config nsna state enable
```

Default Nortel SNA filters

This section is added as an appendix to *Configuring and Managing Security using Device Manager* (317346-C) and *Configuring and Managing Security using the NNCLI and CLI* (316804-C).

The following example shows the default Nortel SNA filters that are generated automatically by the switch. For this example, the Nortel SNAS 4050 portal VIP address is 10.40.40.0/24, and VLAN IDs are the following:

- VoIP = 140
- Red = 110
- Yellow = 120
- Green = 130

If you use the default filters generated 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.

Default filter parameters

Figure 20 on page 95–Figure 31 on page 99 show the default (Red, Yellow, and Green) Nortel SNA filter parameters as they appear in Device Manager. The filter ID can vary depending on configuration.

Click on an entry in the following table to view the Device Manager tab and the default filter parameters on that tab.

Figure 20 Red default filter: Common tab

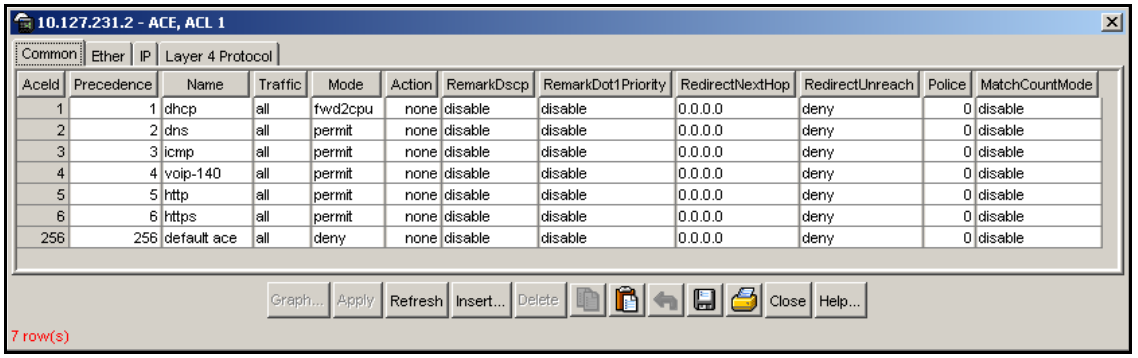


Figure 21 Red default filter: Ether tab

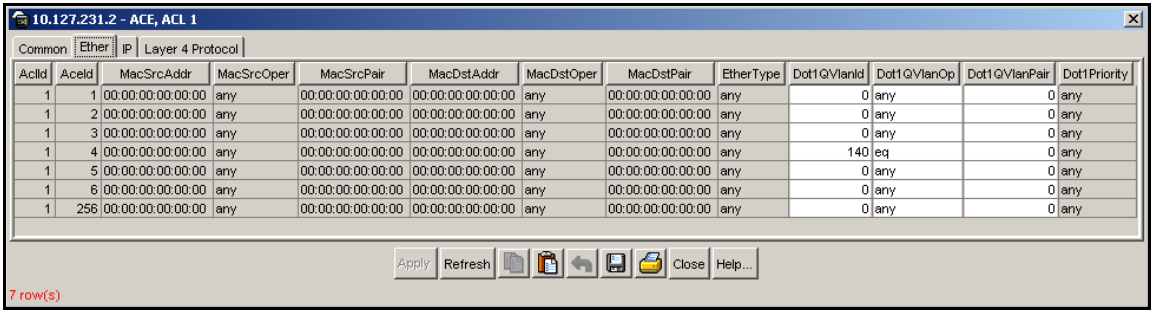
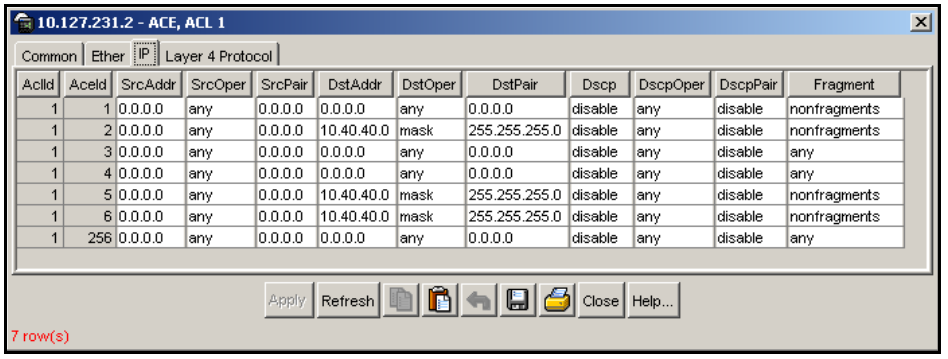
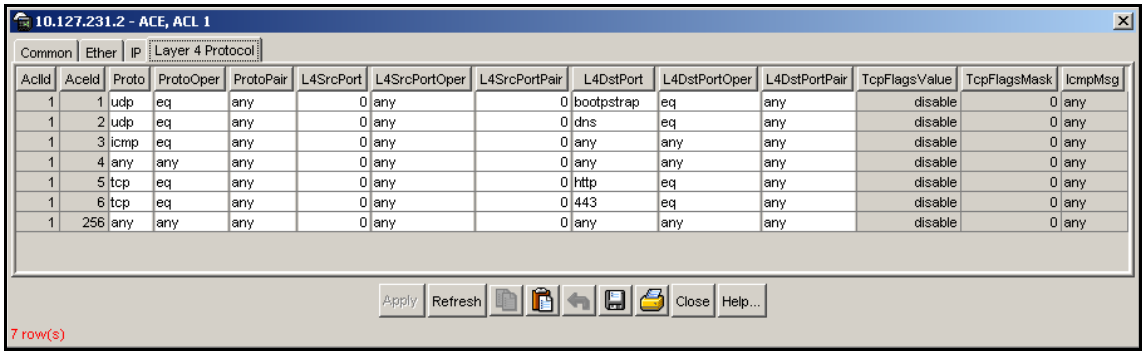


Figure 22 Red default filter: IP tab



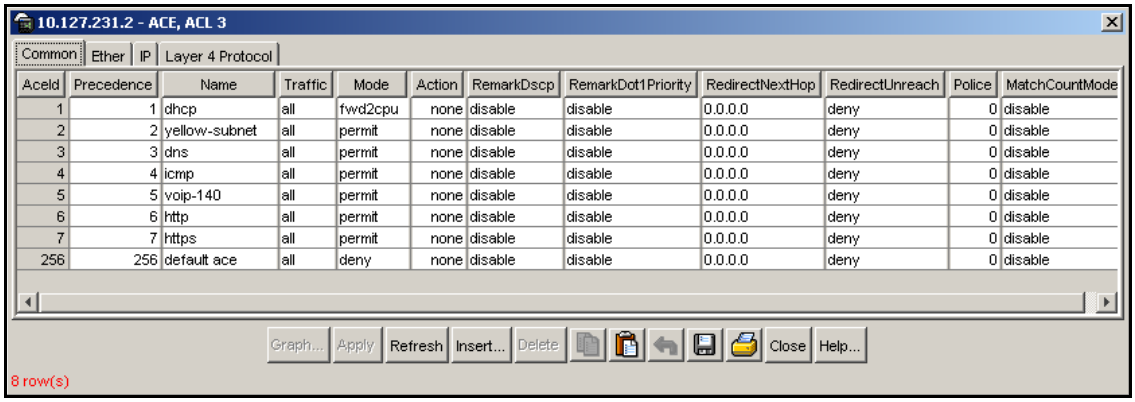
AclId	AceId	SrcAddr	SrcOper	SrcPair	DstAddr	DstOper	DstPair	Dscp	DscpOper	DscpPair	Fragment
1	1	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	nonfragments
1	2	0.0.0.0	any	0.0.0.0	10.40.40.0	mask	255.255.255.0	disable	any	disable	nonfragments
1	3	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	any
1	4	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	any
1	5	0.0.0.0	any	0.0.0.0	10.40.40.0	mask	255.255.255.0	disable	any	disable	nonfragments
1	6	0.0.0.0	any	0.0.0.0	10.40.40.0	mask	255.255.255.0	disable	any	disable	nonfragments
1	256	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	any

Figure 23 Red default filter: Layer 4 Protocol tab



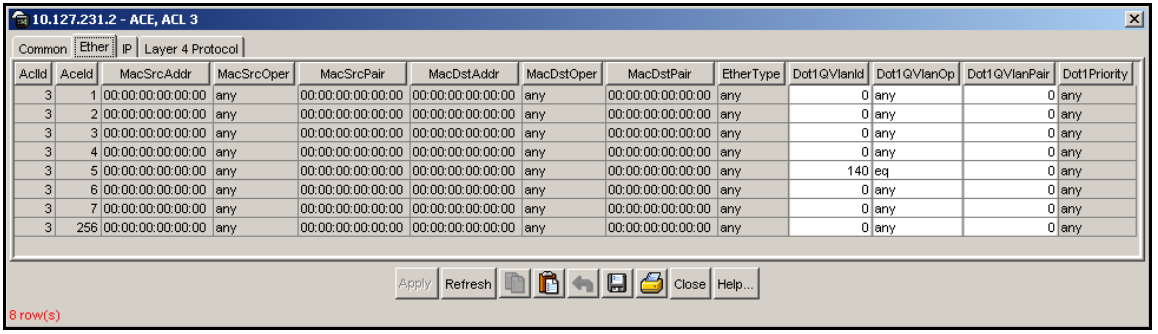
AclId	AceId	Proto	ProtoOper	ProtoPair	L4SrcPort	L4SrcPortOper	L4SrcPortPair	L4DstPort	L4DstPortOper	L4DstPortPair	TcpFlagsValue	TcpFlagsMask	IcmpMsg
1	1	udp	eq	any	0	any	0	bootpstrap	eq	any	disable	0	any
1	2	udp	eq	any	0	any	0	dns	eq	any	disable	0	any
1	3	icmp	eq	any	0	any	0	any	any	any	disable	0	any
1	4	any	any	any	0	any	0	any	any	any	disable	0	any
1	5	tcp	eq	any	0	any	0	http	eq	any	disable	0	any
1	6	tcp	eq	any	0	any	0	443	eq	any	disable	0	any
1	256	any	any	any	0	any	0	any	any	any	disable	0	any

Figure 24 Yellow default filter: Common tab



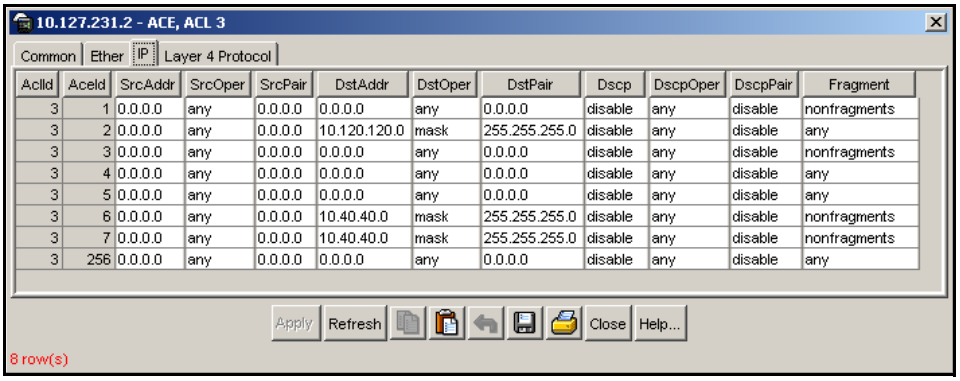
AceId	Precedence	Name	Traffic	Mode	Action	RemarkDscp	RemarkDot1Priority	RedirectNextHop	RedirectUnreach	Police	MatchCountMode
1	1	dhcp	all	fwd2cpu	none	disable	disable	0.0.0.0	deny	0	disable
2	2	yellow-subnet	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
3	3	dns	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
4	4	icmp	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
5	5	voip-140	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
6	6	http	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
7	7	https	all	permit	none	disable	disable	0.0.0.0	deny	0	disable
256	256	default ace	all	deny	none	disable	disable	0.0.0.0	deny	0	disable

Figure 25 Yellow default filter: Ether tab



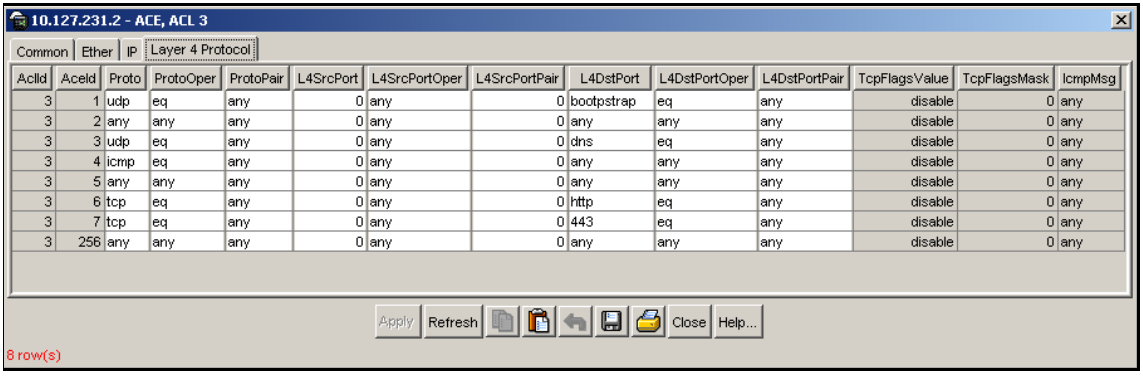
AclId	AceId	MacSrcAddr	MacSrcOper	MacSrcPair	MacDstAddr	MacDstOper	MacDstPair	EtherType	Dot1QVlanId	Dot1QVlanOp	Dot1QVlanPair	Dot1Priority
3	1	00:00:00:00:00:00	any	00:00:00:00:00:00	00:00:00:00:00:00	any	00:00:00:00:00:00	any	0	any	0	any
3	2	00:00:00:00:00:00	any	00:00:00:00:00:00	00:00:00:00:00:00	any	00:00:00:00:00:00	any	0	any	0	any
3	3	00:00:00:00:00:00	any	00:00:00:00:00:00	00:00:00:00:00:00	any	00:00:00:00:00:00	any	0	any	0	any
3	4	00:00:00:00:00:00	any	00:00:00:00:00:00	00:00:00:00:00:00	any	00:00:00:00:00:00	any	0	any	0	any
3	5	00:00:00:00:00:00	any	00:00:00:00:00:00	00:00:00:00:00:00	any	00:00:00:00:00:00	any	140	eq	0	any
3	6	00:00:00:00:00:00	any	00:00:00:00:00:00	00:00:00:00:00:00	any	00:00:00:00:00:00	any	0	any	0	any
3	7	00:00:00:00:00:00	any	00:00:00:00:00:00	00:00:00:00:00:00	any	00:00:00:00:00:00	any	0	any	0	any
3	256	00:00:00:00:00:00	any	00:00:00:00:00:00	00:00:00:00:00:00	any	00:00:00:00:00:00	any	0	any	0	any

Figure 26 Yellow default filter: IP tab



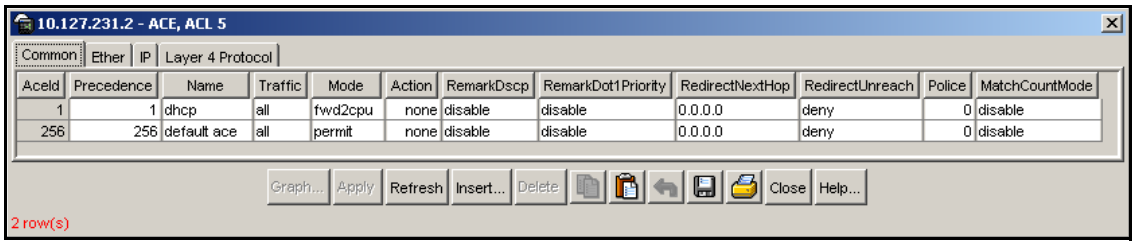
AclId	AceId	SrcAddr	SrcOper	SrcPair	DstAddr	DstOper	DstPair	Dscp	DscpOper	DscpPair	Fragment
3	1	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	nonfragments
3	2	0.0.0.0	any	0.0.0.0	10.120.120.0	mask	255.255.255.0	disable	any	disable	any
3	3	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	nonfragments
3	4	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	any
3	5	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	any
3	6	0.0.0.0	any	0.0.0.0	10.40.40.0	mask	255.255.255.0	disable	any	disable	nonfragments
3	7	0.0.0.0	any	0.0.0.0	10.40.40.0	mask	255.255.255.0	disable	any	disable	nonfragments
3	256	0.0.0.0	any	0.0.0.0	0.0.0.0	any	0.0.0.0	disable	any	disable	any

Figure 27 Yellow default filter: Layer 4 Protocol tab



AclId	AceId	Proto	ProtoOper	ProtoPair	L4SrcPort	L4SrcPortOper	L4SrcPortPair	L4DstPort	L4DstPortOper	L4DstPortPair	TcpFlagsValue	TcpFlagsMask	IcmpMsg
3	1	udp	eq	any	0	any	0	bootpstrap	eq	any	disable	0	any
3	2	any	any	any	0	any	0	any	any	any	disable	0	any
3	3	udp	eq	any	0	any	0	dns	eq	any	disable	0	any
3	4	icmp	eq	any	0	any	0	any	any	any	disable	0	any
3	5	any	any	any	0	any	0	any	any	any	disable	0	any
3	6	tcp	eq	any	0	any	0	http	eq	any	disable	0	any
3	7	tcp	eq	any	0	any	0	443	eq	any	disable	0	any
3	256	any	any	any	0	any	0	any	any	any	disable	0	any

Figure 28 Green default filter: Common tab



AceId	Precedence	Name	Traffic	Mode	Action	RemarkDscp	RemarkDot1Priority	RedirectNextHop	RedirectUnreach	Police	MatchCountMode
1	1	dhcp	all	fwd2cpu	none	disable	disable	0.0.0.0	deny	0	disable
256	256	default ace	all	permit	none	disable	disable	0.0.0.0	deny	0	disable

Figure 29 Green default filter: Ether tab

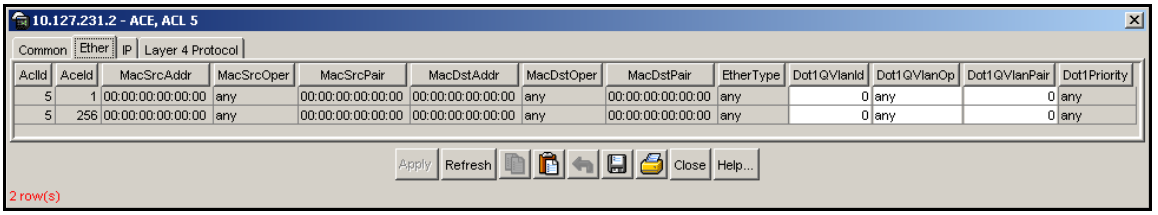


Figure 30 Green default filter: IP tab

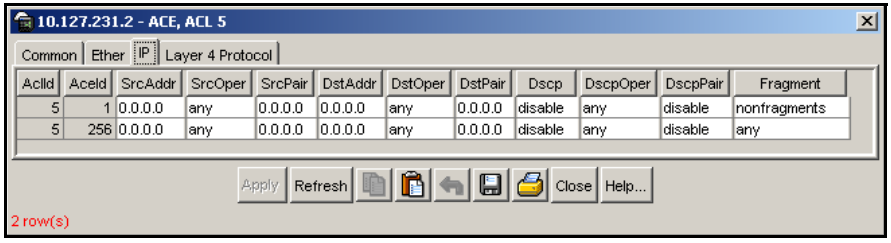
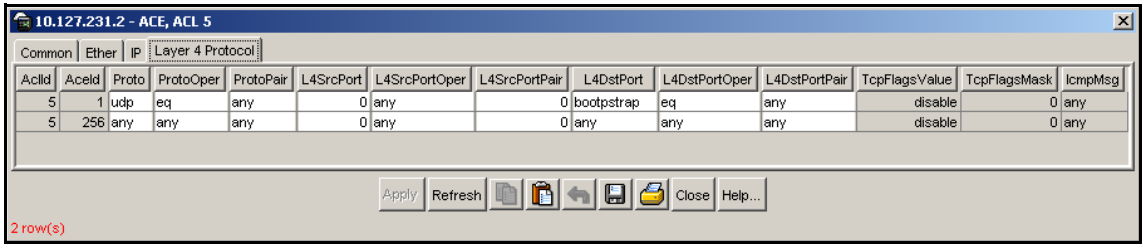


Figure 31 Green default filter: Layer 4 Protocol tab



Reading path

This section lists the documentation specific to the Ethernet Routing Switch 8300 platform. 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* (217468-B)
- *Release Notes for the Ethernet Routing Switch 8300, Software Release 2.2.8* (316811-E)
- *Release Notes for the Nortel Secure Network Access Solution, Software Release 1.0* (320850-A)
- *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.