Nortel Ethernet Routing Switch 5500 Series

Configuration — Security

NN47200-501 (217463-C)

Document status: Standard
Document version: 03.01
Document date: 27 August 2007

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

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

Trademarks

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

Restricted rights legend

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

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

Statement of conditions

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

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

Revision History

Date Revised	Version	Reason for revision
July 2005	1.00	New document for Software Release 4.2.
June 2006	2.00	Document updated for Software Release 5.0.
June 2006	2.01	Minor revision for Software Release 5.0.
June 2006	2.02	Minor revision for Software Release 5.0.
July 2006	2.03	Minor revision for Software Release 5.0.
July 2007	3.01	New document for Software Release 5.1.
August 2007	3.01	Updated for Software Release 5.1.

Contents

Preface

This guide provides information and instructions on the configuration and management of security on the 5500 Series Nortel Ethernet Routing Switch. Please consult any documentation included with the switch and the product release notes (see "Nortel Ethernet Routing Switch 5500 Series Documentation" (page 14)) for any errata before beginning the configuration process.

Nortel Ethernet Routing Switch 5500 Series

"5500 Series Switch Platforms" (page 13) outlines the switches that are part of the 5500 Series of Nortel Ethernet Routing Switches

5500 Series Switch Platforms

5500 Series Switch Model	Key Features
Nortel Ethernet Routing Switch 5510-24T	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains two shared SFP ports.
Nortel Ethernet Routing Switch 5510-48T	A 48 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains two shared SFP ports.
Nortel Ethernet Routing Switch 5520-24T-PWR	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch with full Power over Ethernet (PoE) capability on all copper ports. This switch contains four shared SFP ports.
Nortel Ethernet Routing Switch 5520-48T-PWR	A 48 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch with full Power over Ethernet (PoE) capability on all copper ports. This switch contains four shared SFP ports.
Nortel Ethernet Routing Switch 5530-24TFD	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains twelve shared SFP ports and two XFP ports.

Related Publications

For more information about the management, configuration, and usage of the Nortel Ethernet Routing Switch 5500 Series, refer to the publications listed in "Nortel Ethernet Routing Switch 5500 Series Documentation" (page 14).

Nortel Ethernet Routing Switch 5500 Series Documentation

Title	Description	Part Number
Nortel Ethernet Routing Switch 5500 Series Installation	Instructions for the installation of a switch in the Nortel Ethernet Routing Switch 5500 Series. It also provides an overview of hardware key to the installation, configuration, and maintenance of the switch.	NN47200-300
Nortel Ethernet Routing Switch 5500 Series Overview — System Configuration	Instructions for the general configuration of switches in the 5500 Series that are not covered by the other documentation.	NN47200-500
Nortel Ethernet Routing Switch 5500 Series Security — Configuration	Instructions for the configuration and management of security for switches in the 5500 Series.	NN47200-501
Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking	Instructions for the configuration of spanning and trunking protocols on 5500 Series switches	NN47200-502
Nortel Ethernet Routing Switch 5500 Series Configuration — IP Routing Protocols	Instructions on the configuration of IP routing protocols on 5500 Series switches.	NN47200-503
Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service	Instructions on the configuration and implementation of QoS on 5500 Series switches.	NN47200-504
Nortel Ethernet Routing Switch 5500 Series Configuration — System Monitoring	Instructions on the configuration, implementation, and usage of system monitoring on 5500 Series switches.	NN47200-505

Title	Description	Part Number
Nortel Ethernet Routing Switch 5500 Series Release Notes — Software Release 5.1	Provides an overview of new features, fixes, and limitations of the 5500 Series switches. Also included are any supplementary documentation and document errata.	NN47200-400
Installing the Nortel Ethernet Redundant Power Supply Unit 15	Instructions to install and use the Nortel Ethernet RPSU 15.	217070-A
DC-DC Converter Module for the Baystack 5000 Series Switch	Instructions to install and use the DC-DC power converter.	215081-A
Installing SFP and XFP Transceivers and GBICs	Instructions to install and use small form-factor pluggable transceivers and gigabit interface converters.	318034-C

Finding the latest updates on the Nortel Website

The content of this documentation was current at the time of release. To check for updates to the documentation and software for the Nortel Ethernet Routing Switch 4500 Series, go to www.nortel.com/support and use the following procedure.

Step Action

1 Select **Ethernet Routing Switches**from the Product Categories list in section 1.

2 Select **Ethernet Routing Switch 5500** from section 2.

3 Select one of the following from section 3.

- **Documentation**
- **Product**

4 Click **Go**

—End—

How to get help

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

Getting help from the Nortel web site

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

www.nortel.com/support

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

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

Getting help over the phone from a Nortel Solutions Center

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

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

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

www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Security in the Nortel Ethernet Routing Switch 5500 Series

This chapter includes the following topics:

Overview

The following table describes types of security provided by the Nortel Ethernet Routing Switch 5500 Series.

Security in the Nortel Ethernet Routing Switch 5500 Series

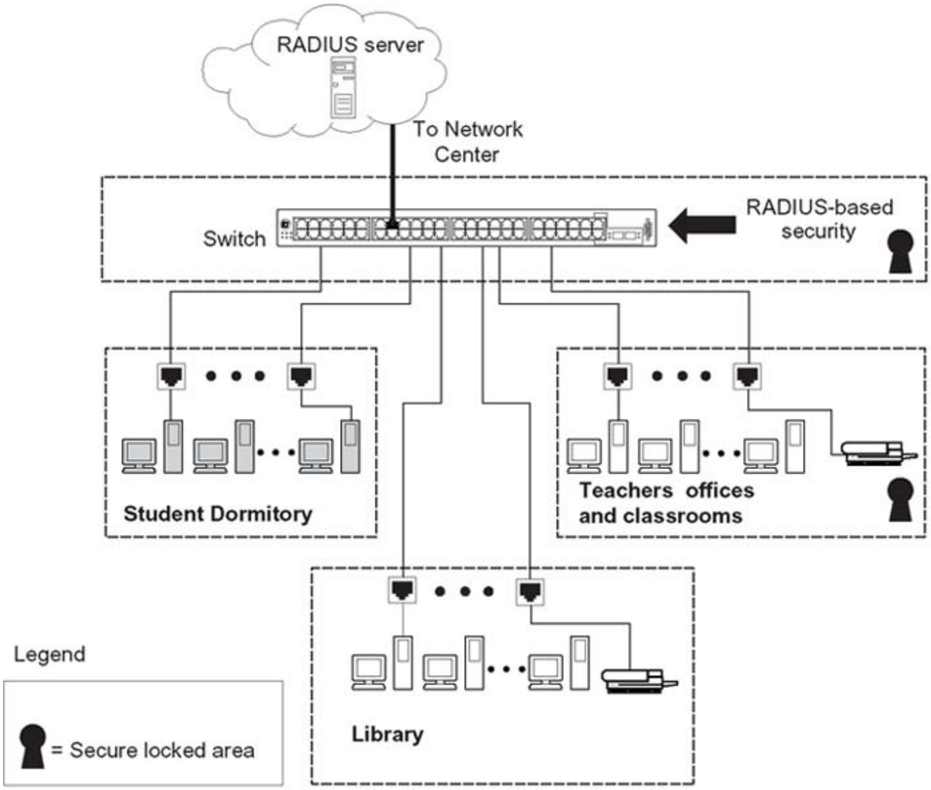
Security Type	Description
MAC address-based security	Limits access to the switch based on allowed source and destination MAC addresses.
RADIUS-based security	Limits administrative access to the switch through user authentication.
EAPOL-based security (IEEE 802.1X)	Allows the exchange of authentication information between any end station or server connected to the switch and an authentication server, such as a RADIUS server.
TACACS+	Provides centralized validation of users attempting to gain access to the switch. Authentication, authorization, and accounting services are separate.
IP Manager list	Limits access to management features of the switch based on the management station IP address.
SNMPv3	Allows access to the various services by using password authentication (MD5), secure-hash algorithm (SHA), and encryption using the Advanced Encryption Standard (AES) or Data Encryption Standard (DES).
SSL	Provides a secure Web management interface.
SSH	Replaces Telnet and provides a secure access to the user console menu and CLI interface.
DHCP snooping	Filters untrusted DHCP messages and verifies the source of DHCP messages to prevent DHCP spoofing.
Dynamic ARP inspection	Validates ARP packets in the network to protect against “man-in-the-middle” attacks.
Nortel Secure Network Access	A protective framework to completely secure the network from endpoint vulnerability. The Nortel Secure Network Access (Nortel SNA) solution addresses endpoint security and enforces policy compliance. Nortel SNA provides a policy-based, clientless approach to corporate network access.
IP Source Guard	Sets up filters for IP addresses, based on information stored in the corresponding DHCP snooping Binding Table entry.

Campus security example

The following figure shows a typical campus configuration using the RADIUS-based and MAC address-based security features for the Nortel Ethernet Routing Switch 5500 Series.

This example assumes that the switch, the teachers’ offices, classrooms, and the library are physically secured. The student dormitory can also be physically secured.

Nortel Ethernet Routing Switch 5500 Series security features



In the given configuration example, the security measures are implemented in the following locations, as follows:

- The switch

  RADIUS-based security is used to limit administrative access to the switch through user authentication. See "RADIUS-based network security" (page 22).

  MAC address-based security is used to allow up to 448 authorized stations access to one or more switch ports. See "MAC address-based security" (page 20).

  The switch is located in a locked closet, accessible only by authorized Technical Services personnel.

- Student dormitory

  Dormitory rooms are typically occupied by two students and are prewired with two RJ-45 jacks.

  As specified by the MAC address-based security feature, only students who are authorized can access the switch on the secured ports.

- Teachers' offices and classrooms

The PCs that are located in the teachers' offices and in the classrooms are assigned MAC address-based security, which is specific for each classroom and office location.

The security feature logically locks each wall jack to the specified station, thereby preventing unauthorized access to the switch.

The printer is assigned to a single station and is allowed full bandwidth on that switch port.

It is also assumed that all PCs are password protected and that the classrooms and offices are physically secured.

- Library

  The PCs can be connected to any wall jack in the room. However, the printer is assigned to a single station with full bandwidth to that port.

  It is assumed that all PCs are password protected and that access to the library is physically secured.

MAC address-based security

The MAC address-based security feature is based on Nortel Networks BaySecure* LAN Access for Ethernet, a real-time security system that safeguards Ethernet networks from unauthorized surveillance and intrusion.

The MAC address-based security feature allows you to set up network access control, based on source MAC addresses of authorized stations.

MAC address-based security allows you to do the following:

- Create a list of up to 10 MAC addresses that you want to filter
  - as destination addresses (DA)—all packets with one of the specified MAC addresses as the DA will be dropped, regardless of the ingress port, source address intrusion, or VLAN membership
  - as source addresses (SA)—all packets with one of the specified MAC addresses as the SA will be dropped

    Note: Ensure that you do not enter the MAC address for the stack or any of the units you are using.

- Create a list of up to 448 MAC source addresses (SA) and specify SAs that are authorized to connect to the switch or stack configuration. Up to 32 MAC source addresses (SA) per-port can be configured for the Nortel Ethernet Routing Switch 5520 and 5530 switches and up to 448 MAC source addresses per-port can be configured for the Nortel Ethernet Routing Switch 5510 switches.

  The 448 MAC SAs can be configured within a single stand-alone switch, or they can be distributed in any order among the units in a single stack configuration.

At the time of configuring MAC-based security, you must specify the following:

- Switch ports that can be accessed by each MAC SA.

  The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1/1-4,1/6,2/9.

- Optional actions to be performed by your switch, if the software detects an SA security violation.

  The response can be to send a trap, turn on destination address (DA) filtering for the specified SAs, disable the specific port, or any combination of these three options.

Use either the CLI or the Web-based management system to configure MAC address-based security features.

MAC address-based security auto-learning

The MAC address-based security auto-learning feature provides the ability to add allowed MAC addresses to the MAC Security Address Table automatically without user intervention.

MAC address-based security auto-learning includes the following features:

- You specify the number of addresses that can be learned on the ports, to a maximum of 25 addresses per-port. The switch forwards traffic only for those MAC addresses statically associated with a port or auto-learned on the port.
- You can configure an aging time period in minutes, after which auto-learned entries are refreshed in the MAC Security Address Table. If you set the aging time value to 0, the entries never age out; you need to reset the MAC Security Address Table for the specified port to force new addresses to be learned.
- Auto-learned entries associated in the MAC Security Address Table with a particular port are deleted from the table if a link down event occurs for the port.
- You cannot modify auto-learned MAC addresses in the MAC Security Address Table.
- Auto-learned addresses are not saved in NVRAM but learned after the bootup sequence. The aging time and the allowed number of auto-learned MAC addresses per-port are saved in non-volatile memory.
- You can reset the MAC address table for a port by disabling the security on the port and then re-enabling it.
- If a MAC address is already learned on a port (port x) and the address migrates to another port (port y), the entry in the MAC Security Address

Table is modified to associate that MAC address with the new port (port y). The aging timer for the entry is reset.

- If you disable auto-learning on a port, all the auto-learned MAC entries associated with that port in the MAC Security Address Table are removed.
- If a static MAC address is associated with a port (which may or may not be configured with the auto-learning feature) and the same MAC address is learned on a different port, an auto-learn entry associating that MAC address with the second port is not created in the MAC Security Address Table. In other words, user settings have priority over auto-learning.

RADIUS-based network security

Remote Access Dial-In User Services (RADIUS) is a distributed client/server system that assists in securing networks against unauthorized access, allowing a number of communication servers and clients to authenticate user identities through a central database. The database within the RADIUS server stores information about clients, users, passwords, and access privileges, protected with a shared secret.

RADIUS authentication is a fully open and standard protocol defined by RFC 2865.

How RADIUS works

A RADIUS application has two components:

- RADIUS server—a computer equipped with server software (for example, a UNIX workstation) that is located at a central office or campus. It has authentication and access information in a form that is compatible with the client. Typically, the database in the RADIUS server stores client information, user information, password, and access privileges, protected with a shared secret.
- RADIUS client—a switch, router, or a remote access server equipped with client software, that typically resides on the same LAN segment as the server. The client is the network access point between the remote users and the server.

RADIUS authentication allows a remote server to authenticate users attempting to log on to the switch from the local console or Telnet.

Nortel recommends including two RADIUS servers in the Ethernet Routing Switch 5500 Series network: a primary RADIUS server and a secondary RADIUS server for backup. The secondary server is used only if the primary server is unavailable or unreachable. You identify which server functions as the primary and secondary, respectively, when you configure the RADIUS servers on the switch.

RADIUS allows three retries for service requests to each RADIUS server in the network. The timeout interval between each retry is configurable.

RADIUS server configuration

You must set up specific user accounts on the RADIUS server before you can use RADIUS authentication in the Ethernet Routing Switch 5500 Series network. User account information about the RADIUS server includes user names, passwords, and Service-Type attributes.

To provide each user with the appropriate level of access to the switch, ensure that you set the following user name attributes:

- for read-write access, set the Service-Type field value to `Administrative`
- for read-only access, set the Service-Type field value to `NAS-Prompt`

The maximum length of user name and password is 32 characters.

For detailed information about configuring the RADIUS server, refer to the documentation that came with the server software.

RADIUS password fallback

The RADIUS password fallback feature allows the user to log on to the switch or stack by using the local password if the RADIUS server is unavailable or unreachable for authentication.

RADIUS password fallback is disabled by default.

Configuring RADIUS authentication

Configure and manage RADIUS authentication using the CLI, Web-based Management interface or Java Device Manager (JDM).

For information about configuring RADIUS authentication using the CLI, see "Configuring RADIUS authentication" (page 74). For information about configuring RADIUS authentication using Web-based management, see "Configuring RADIUS security" (page 148). For information about configuring RADIUS authentication using the JDM, see "Radius Server tab" (page 182).

EAPOL-based security

The Nortel Ethernet Routing Switch 5500 Series uses an encapsulation mechanism to provide security. This is referred to as the Extensible Authentication Protocol over LAN (EAPOL). This concept uses the Extensible Authentication Protocol (EAP) as described in the IEEE 802.1X to allow you to set up network access control on internal LANs.

EAP allows the exchange of authentication information between any end station or server connected to the switch and an authentication server, such as a RADIUS server. The EAPOL-based security feature operates in conjunction with a RADIUS-based server to extend the benefits of remote authentication to internal LAN clients.

The following example illustrates how the Nortel Ethernet Routing Switch 5500 Series, configured with the EAPOL-based security feature, react to a new network connection:

- The switch detects a new connection on one of its ports.
  - — The switch requests a user ID from the new client.
  - — EAPOL encapsulates the user ID and forwards it to the RADIUS server.
  - — The RADIUS server responds with a request for the user’s password.
- The new client forwards a password to the switch, within the EAPOL packet.
  - — The switch relays the EAPOL packet to the RADIUS server.
  - — If the RADIUS server validates the password, the new client is allowed access to the switch and the network.

Some components and terms used with EAPOL-based security are:

- Supplicant: Refers to the device applying for access to the network.
- Authenticator: Refers to the software that authorizes a supplicant attached to the other end of a LAN segment.
- Authentication Server: Refers to the RADIUS server that provides authorization services to the Authenticator.
- Port Access Entity (PAE): Refers to the software entity that is associated with each port that supports the Authenticator or Supplicant functionality.
- Controlled Port: Refers to any switch port with EAPOL-based security enabled.

The Authenticator communicates with the Supplicant using an encapsulation mechanism known as EAP over LANs (EAPOL).

The Authenticator PAE encapsulates the EAP message into a RADIUS packet before sending the packet to the Authentication Server. The Authenticator facilitates the authentication exchanges that occur between the Supplicant and the Authentication Server by encapsulating the EAP message to make it suitable for the packet destination.

The Authenticator PAE functionality is implemented for each controlled port on the switch. At system initialization, or when a supplicant is initially connected to the switch's controlled port, the controlled port's state is set to Unauthorized. During this time, EAP packets are processed by the authenticator.

When the Authentication server returns a "success" or "failure" message, the controlled port's state is changed accordingly. If the authorization is successful, the controlled port's operational state is set to Authorized. The blocked traffic direction on the controlled port depends on the Operational Traffic Control field value in the EAPOL Security Configuration screen.

The Operational Traffic Control field can have one of the following two values:

- Incoming and Outgoing: If the controlled port is unauthorized, frames are not transmitted through the port. All frames received on the controlled port are discarded.
- Incoming: If the controlled port is unauthorized, frames received on the port are discarded, but the transmit frames are forwarded through the port.

EAPOL dynamic VLAN assignment

If EAPOL-based security is enabled on an authorized port, the EAPOL feature dynamically changes the port's VLAN configuration and assigns a new VLAN. The new VLAN configuration values are applied according to previously stored parameters in the Authentication server.

The following VLAN configuration values are affected:

- port membership
- PVID
- port priority

When EAPOL-based security is disabled on a port that was previously authorized, the port VLAN configuration values are restored directly from the switch non-volatile random access memory (NVRAM).

The following exceptions apply to dynamic VLAN assignments:

- The dynamic VLAN configuration values assigned by EAPOL are *not* stored in the switch's NVRAM.
- If an EAPOL connection is active on a port, any changes to the port membership, PVID, or port priority are not saved to NVRAM.
- When EAPOL is enabled on a port, and you configure values other than VLAN configuration values, these values are applied and stored in NVRAM.

You can set up your Authentication server (RADIUS server) for EAPOL dynamic VLAN assignments. The Authentication server allows you to configure user-specific settings for VLAN memberships and port priority.

When you log on to a system that has been configured for EAPOL authentication, the Authentication server recognizes your user ID and notifies the switch to assign preconfigured (user-specific) VLAN membership and port priorities to the switch. The configuration settings are based on configuration parameters that were customized for your user ID and previously stored on the Authentication server.

To set up the Authentication server, set the following "Return List" attributes for all user configurations. For more information, refer to your Authentication server documentation:

- VLAN membership attributes (automatically configures PVID)
  - Tunnel-Type: value 13, Tunnel-Type-VLAN
  - Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
  - Tunnel-Private-Group-Id: ASCII value 1 to 4094 (this value is used to identify the specified VLAN)
- Port priority (vendor-specific) attributes
  - Vendor Id: value 562, Nortel Networks vendor Id
  - Attribute Number: value 1, Port Priority
  - Attribute Value: value 0 (zero) to 7 (this value is used to indicate the port priority value assigned to the specified user)

System requirements

The following are the minimum system requirements for the EAPOL-based security feature:

- at least one Nortel Ethernet Routing Switch 5500 Series switch
- RADIUS server (Microsoft Windows 2003 Server or other RADIUS server with EAPOL support)
- client software that supports EAPOL (Microsoft Windows XP Client)

You must configure the Nortel devices with the RADIUS server IP address for the Primary RADIUS server.

EAPOL-based security configuration rules

The following configuration rules apply to the Nortel Ethernet Routing Switch 5500 Series when using EAPOL-based security:

- Before configuring your switch, you must configure the Primary RADIUS Server and Shared Secret fields.

- You cannot configure EAPOL-based security on ports that are currently configured for:
  - Shared segments
  - MultiLink Trunking
  - MAC address-based security
  - IGMP (Static Router Ports)
  - Port mirroring
  - IP Source Guard
- With EAPOL SHSA (the simplest EAPOL port operating mode), you can connect only a single client on each port that is configured for EAPOL-based security. If you attempt to add additional clients to a port, that port state is modified to Unauthorized.

RADIUS-based security uses the RADIUS protocol to authenticate local console, Telnet, and EAPOL-authorized log ons.

Advanced EAPOL features

EAPOL supports the following advanced features:

- Single Host with Single Authentication (SHSA) and Guest VLAN (see "Single Host with Single Authentication and Guest VLAN" (page 27))
- Multihost (MH) support:
  - Multiple Host with Multiple Authentication (MHMA) (see "Multiple Host with Multiple Authentication" (page 29))
  - Non-EAP hosts on EAP-enabled ports (see "Non-EAP hosts on EAP-enabled ports" (page 33))
  - Multiple Host with Single Authentication (MHSA) (see "Multiple Host with Single Authentication" (page 36))

Single Host with Single Authentication and Guest VLAN

Single Host with Single Authentication (SHSA) support is the default configuration for an EAP-enabled port. At any time, only one MAC user is authenticated on a port, and the port is assigned to only one port-based VLAN.

If no guest VLAN is configured, only the particular device or user that completes EAP negotiations on the port is allowed to access that port for traffic. Tagged ingress packets are sent to the PVID of that port. The only exceptions are reserved addresses.

You can configure a guest VLAN to allow non-authenticated users to access the port. Any active VLAN can be made a guest VLAN.

The following rules apply for SHSA:

- When the port is EAP enabled:
  - If Guest VLAN is enabled, the port is put in a Guest VLAN.

    PVID of the port = Guest VLAN ID
  - If Guest VLAN is not enabled, the port services EAPOL packets only, until successful authentication.
- During EAP authentication:
  - If Guest VLAN is enabled, the port is put in a Guest VLAN.
  - If Guest VLAN is not enabled, the port services EAPOL packets only.
- If authentication succeeds:
  - The port is put in a preconfigured VLAN or a RADIUS-assigned VLAN. Only packets with the authenticated MAC (authMAC) are allowed on that port. Any other packets are dropped.
- If authentication fails:
  - If Guest VLAN is enabled, the port is put in a Guest VLAN.
  - If Guest VLAN is not enabled, the port services EAPOL packets only.
- Reauthentication can be enabled for the authenticated MAC address. If reauthentication fails, the port is put back in the Guest VLAN.

The EAP-enabled port belongs to the Guest VLAN, Radius-assigned VLAN, or configured VLANs.

Guest VLAN

A global default Guest VLAN ID can be configured for the stack or the switch. Set the VLAN ID as Valid when you configure the switch or the stack.

Guest VLAN support includes the following features:

- Guest VLAN support is on a per-port basis. Guest VLANs can be enabled with a valid Guest VLAN ID on each port. If a Guest VLAN ID is not specified for a port, the global default value is used. This feature cannot be enabled on a particular port, if the global default value or the local Guest VLAN ID is invalid.
- The Guest VLAN chosen must be an active VLAN configured on the switch. EAP registers with the VLAN module, so that it can be recovered in the event of a VLAN delete.

When a VLAN that is in use by EAP is deleted, the following actions are performed:

— A message is sent to the syslog.

— The port is blocked.

- When an authentication failure occurs, a port is put back in the Guest VLAN.
- This feature affects ports that have EAP-Auto enabled. Therefore, the port must always be in a forwarding mode. It does not affect ports with administrative state, force-authorized or force-unauthorized.
- This feature uses Enterprise Specific MIBs.
- The Guest VLAN configuration settings are saved across resets.

Multiple Host with Multiple Authentication

For an EAP-enabled port configured for Multiple Host with Multiple Authentication (MHMA), a finite number of EAP users or devices with unique MAC addresses are allowed on the port.

Each user must complete EAP authentication before the port allows traffic from the corresponding MAC address. Only traffic from the authorized hosts is allowed on that port.

Radius-assigned VLAN values are allowed in the MHMA mode. For information on Radius-assigned VLANs in the MHMA mode, see "Radius-assigned VLAN use in MHMA mode" (page 30).

MHMA support is on a per-port basis for an EAP-enabled port.

The following are some of the concepts associated with MHMA:

- Logical and physical ports

  Each unique port and MAC address combination is treated as a logical port. MAX_MAC_PER_PORT defines the maximum number of MAC addresses that can perform EAP authentication on a port at any given time. Each logical port is treated as if it is in the SHSA mode.

- Indexing for MIBs

  Logical ports are indexed by a port and source MAC address (src-mac) combination. Enterprise-specific MIBs are defined for state machine-related MIB information for individual MACs.

- Transmitting EAPOL packets

  Only unicast packets are sent to a specific port so that the packets reach the correct destination.

- Receiving EAPOL packets

The EAPOL packets are directed to the correct logical port for state machine action.

- Traffic on an authorized port

  Only a set of authorized MAC addresses is allowed access to a port.

MHMA support for EAP clients includes the following features:

- A port remains on the Guest VLAN when no authenticated hosts exist on it. Until the first authenticated host, both EAP and non EAP clients are allowed on the port.
- After the first successful authentication, only EAPOL packets and data from the authenticated MAC addresses are allowed on a particular port.
- Only a predefined number of authenticated MAC users are allowed on a port.
- RADIUS VLAN assignment is enabled for ports in MHMA mode. Upon successful RADIUS authentication, the port gets a VLAN value in a RADIUS Attribute with EAP success. The port is added and the PVID is set to the first such VLAN value from the RADIUS server.
- Configuration of timer parameters is per physical port, not per user session. However, the timers are used by the individual sessions on the port.
- Reauthenticate Now, when enabled, causes all sessions on the port to reauthenticate.
- Reauthentication timers are used to determine when a MAC is disconnected so as to enable another MAC to log in to the port.
- EAP accounting, when enabled, displays the octet and packet counts per physical port.
- Configuration settings are saved across resets.

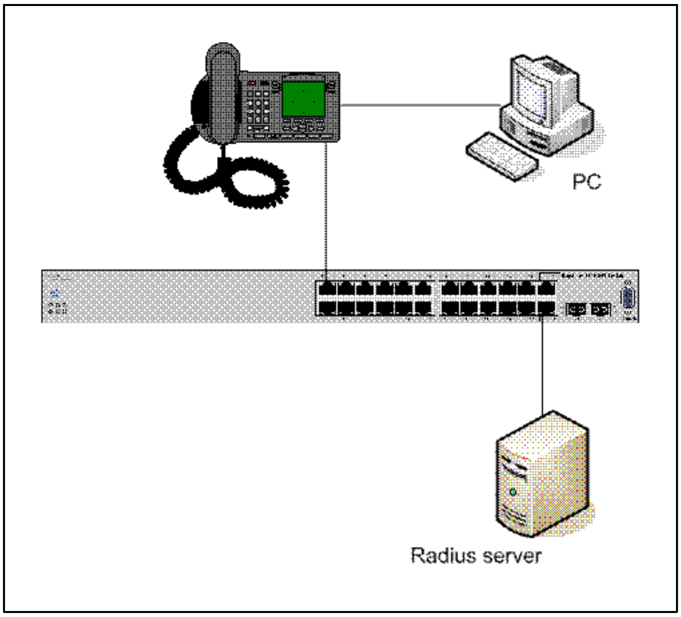
Radius-assigned VLAN use in MHMA mode

Radius-assigned VLAN use in the MHMA mode is allowed to give you greater flexibility and a more centralized assignment than existed. This feature is also useful in an IP Phone set up, when the phone traffic can be directed to the Voice over IP (VoIP) VLAN and the PC Data traffic can be directed to the assigned VLAN. When Radius-assigned VLAN values are allowed, the port behaves as follows: the first authenticated EAP MAC address may not have a Radius-assigned VLAN value. At this point, the port is moved to a configured VLAN. A later authenticated EAP MAC address (for instance, the third one on the port) may get a Radius-assigned VLAN value. This port is then added, and the port VLAN ID (PVID) is set to the first such VLAN value from the Radius server. The VLAN remains the same irrespective of which MAC leaves, and a change in the VLAN takes place only when there are no authenticated hosts on the port.

> ***Note:*** All VLAN movement in an EAP-enabled state is dynamic and is not saved across resets.

Consider the following setup in the figure:

- ERS 5510-24T standalone switch with default settings
- IP Phone connected to the switch in port 1
- PC connected to the PC port of the IP Phone
- Radius server connected to switch port 24 (directly or through a network)



Before getting to the details regarding the EAP enhancements configuration, EAP multihost mode needs to be configured on the switch (global settings and local settings for switch port 1/1):

1. Put a valid IP address on the switch
2. Configure at least the Primary Radius server IP address (we could also fill the IP address of the Secondary one)
3. Enable EAP globally
4. Enable EAP (status Auto) for switch port 1
5. Enable EAP multihost mode for switch port 1

   The EAP clients will authenticate using MD5 credentials, but any other available type of authentication could be used (TLS, PEAP-MSCHAPv2, PEAP-TLS, TTLS and so on). The Radius server should be properly configured to authenticate the EAP users with at least MD5 authentication

a. Non-EAP IP Phone authentication :

   This enhancement is useful mainly for the IP Phones which are not able to authenticate themselves with EAP. As for the Local and Radius Non-EAP authentications, EAP Guest VLAN needs to be disabled (Guest VLAN and Non-EAP are mutually exclusive features). On an EAP capable IP Phone, EAP has to be disabled if the user specifically wants to use the Non-EAP IP Phone authentication. DHCP has to be enabled on the phone, because the switch will examine the phone signature contained in the DHCP Discover packet sent by the phone.

   Following are the steps to enable the enhancement :

6. Enable Non-EAP IP Phone authentication in global config mode

   ```
   5510-24T(config)#eapol multihost non-eap-phone-enable
   ```

7. Enable Non-EAP IP Phone authentication in interface mode for switch port 1

   ```
   5510-24T(config-if)#eapol multihost port 1 non-eap-phone-
   enable
   ```

   The switch will wait for DHCP Discover packets on port 1. Once a DHCP Discover packet is received on port 1, the switch will look for the phone signature (e.g. Nortel-i2004-A), which should be enclosed in the DHCP Discover packet. If the proper signature is found, the switch will register the MAC address of the IP Phone as an authenticated MAC address and will let the phone traffic pass through the port.

   By default, the Non-EAP IP Phone authentication enhancement is disabled in both global config and interface modes, for all switch ports.

   a. Unicast EAP Requests in MHMA :

      With this enhancement enabled, the switch no longer periodically queries the connected MAC addresses to a port with EAP Request Identity packets. So the clients must be able to initiate for themselves the EAP authentication sessions (send EAP Start packets to the switch). Note that not all EAP supplicants might be able to support this operating mode.

      Following are the steps to enable the enhancement :

      - Enable unicast EAP requests in global config mode:

      ```
      5510-24T(config)#eapol multihost eap-packet-mode
      unicast
      ```

      - enable Unicast EAP Requests in interface mode for switch port 1:

```
5510-24T(config-if)#eapol multihost port 1 eap-packet-
mode unicast
```

By default, multicast mode is selected in both global config and interface modes, for all switch ports. Note that you need to set the EAP packet mode to "Unicast" in both global an interface modes, for a given switch port, in order to enable this feature. Any other combination (e.g. multicast in global, unicast in interface mode) will select the multicast operating mode.

Radius Assigned VLANs in MHMA

This enhancement works in a very similar manner with the already existing Radius assigned VLANs feature in SHSA mode. It is basically an extension of that feature which gives the user the ability to move a port to a specific VLAN, even if that switch port operates in EAP MHMA mode.

The only restriction of this enhancement is that if you have multiple EAP clients authenticating on a given switch port (as you normally would in MHMA mode), each one configured with a different VLAN ID on the Radius server, the switch will move the port to the VLAN of the first authenticated client. In this way, a permanent bounce between different VLANs of the switch port is avoided.

Following are the steps to enable the enhancement :

- Enable Radius assigned VLANs in global config mode:

```
5510-24T(config)#eapol multihost use-radius-assigned-vlan
```

- Enable Radius assigned VLANs in interface mode for switch port 1:

```
5510-24T(config-if)#eapol multihost port 1 use-radius-
assigned-vlan
```

By default, the Radius assigned VLANs in MHMA enhancement is disabled in global config and interface modes, for all switch ports.

Non-EAP hosts on EAP-enabled ports

For an EAPOL-enabled port configured for non-EAPOL host support, a finite number of non-EAPOL users or devices with unique MAC addresses are allowed access to the port.

The following types of non-EAPOL users are allowed:

- Hosts that match entries in a local list of allowed MAC addresses. You can specify the allowed MAC addresses when you configure the port to allow non-EAPOL access. These hosts are allowed on the port without authentication.
- Non-EAPOL hosts whose MAC addresses are authenticated by RADIUS.

- IP Phones configured for Auto-Detection and Auto-Configuration (ADAC).
- Nortel IP Phones.

Support for non-EAPOL hosts on EAPOL-enabled ports is primarily intended to accommodate printers and other dumb devices sharing a hub with EAPOL clients.

Support for non-EAPOL hosts on EAPOL-enabled ports includes the following features:

- EAPOL and authenticated non-EAPOL clients are allowed on the port at the same time. Authenticated non-EAPOL clients are hosts that satisfy one of the following criteria:
  - — Host MAC address matches an entry in an allowed list preconfigured for the port.
  - — Host MAC address is authenticated by RADIUS.
- Non-EAPOL hosts are allowed even if no authenticated EAPOL hosts exist on the port.
- When a new host is seen on the port, non-EAPOL authentication is performed as follows:
  - — If the MAC address matches an entry in the preconfigured allowed MAC list, the host is allowed.
  - — If the MAC address does not match an entry in the preconfigured allowed MAC list, the switch generates a <username, password> pair, which it forwards to the network RADIUS server for authentication. For more information about the generated credentials, see "Non-EAPOL MAC RADIUS authentication" (page 35).

    If the MAC address is authenticated by RADIUS, the host is allowed.
  - — If the MAC address does not match an entry in the preconfigured allowed MAC list, fails RADIUS authentication, and is not an allowed IP Phone, the host is counted as an intruder. Data packets from that MAC address are dropped.

  EAPOL authentication is not affected.
- For RADIUS-authenticated non-EAPOL hosts, VLAN information from RADIUS is ignored. Upon successful authentication, untagged traffic is put in a VLAN preconfigured for the port.
- For RADIUS-authenticated non-EAPOL hosts, VLAN information from RADIUS is ignored. Upon successful authentication, untagged traffic follows the PVID of the port.

- Non-EAPOL hosts continue to be allowed on the port until the maximum number of non-EAPOL hosts is reached. The maximum number of non-EAPOL hosts allowed is configurable.
- After the maximum number of allowed non-EAPOL hosts has been reached, any data packets received from additional non-EAPOL hosts are dropped. The additional non-EAPOL hosts are counted as intruders. New EAPOL hosts can continue to negotiate EAPOL authentication.
- When the intruder count reaches 25, a SNMP trap and system message are generated. The port shuts down, and you must reset the port administrative status (from force-unauthorized to auto) to allow new EAPOL and non-EAPOL negotiations on the port. The intruder counter is reset to zero.
- The feature uses enterprise-specific MIBs.
- Configuration settings are saved across resets.

  Note: Guest VLAN and non-EAPOL host support on a port are mutually exclusive. If you have configured a port to support Guest VLAN, you cannot enable support for non-EAPOL hosts on that port. Similarly, if you have configured an EAPOL-enabled port to support non-EAPOL hosts, you cannot enable Guest VLAN on that port. Also, you cannot enable non-EAPOL support on uplink or call server ports.

For information about configuring non-EAPOL host support, see "Configuring support for non-EAPOL hosts on EAPOL-enabled ports" (page 92).

Non-EAPOL MAC RADIUS authentication

For RADIUS authentication of a non-EAPOL host MAC address, the switch generates a <username, password> pair as follows:

- The username is the non-EAPOL MAC address in string format.
- The password is a string that combines the MAC address, switch IP address, unit, and port.

  > ***Note:*** Follow theses global configuration examples, to select a password format that combines one or more of these 3 elements:
  >
  > password = 010010011253..0305 (when the switch IP address, unit and port are used).
  >
  > password = 010010011253.. (when only the switch IP address is used).

The following example illustrates the <username, password> pair format:

switch IP address = 10.10.11.253
non-EAP host MAC address = 00 C0 C1 C2 C3 C4

unit = 3
port = 25

- username = 00C0C1C2C3C4
- password = 010010011253.00C0C1C2C3C4.0325

Multiple Host with Single Authentication

Multiple Host with Single Authentication (MHSA) is a more restrictive implementation of support for non-EAPOL hosts on EAPOL-enabled ports.

For an EAPOL-enabled port configured for MHSA, one EAPOL user must successfully authenticate before a finite number of non-EAPOL users or devices with unique MAC addresses are allowed to access the port without authentication.

The MHSA feature is intended primarily to accommodate printers and other dumb devices sharing a hub with EAPOL clients.

MHSA support is on a per-port basis for an EAPOL-enabled port.

MHSA support for non-EAPOL hosts includes the following features:

- The port remains unauthorized when no authenticated hosts exist on it. Before the first successful authentication occurs, both EAPOL and non-EAPOL clients are allowed on the port to negotiate access, but at any time, only one host can negotiate EAPOL authentication.
- After the first EAPOL client successfully authenticates, EAPOL packets and data from that client are allowed on the port. No other clients are allowed to negotiate EAPOL authentication. The port is set to preconfigured VLAN assignments and priority values or to values obtained from RADIUS for the authenticated user.
- After the first successful authentication, any new hosts, up to a configured maximum number, are automatically allowed on the port, without authentication.
- After the maximum number of allowed non-EAPOL hosts has been reached, any data packets received from additional non-EAPOL hosts are dropped. The additional non-EAPOL hosts are counted as intruders.
- When the intruder count reaches 25, a SNMP trap and system message are generated. The port shuts down, and you must reset the port administrative status (from force-unauthorized to auto) to allow new EAPOL negotiations on the port. The intruder counter is reset to zero.
- If the EAPOL-authenticated user logs off, the port returns to an unauthorized state and non-EAPOL hosts are not allowed.
- This feature uses enterprise-specific MIBs.

The maximum value for the maximum number of non-EAPOL hosts allowed on an MHSA-enabled port is 32. However, Nortel expects that the usual maximum value configured for a port is 2. This translates to around 200 for a box and 800 for a stack.

Summary of multiple host access on EAPOL-enabled ports

The following table summarizes the order of the checks performed by the switch when a new host is seen on an EAPOL multihost port. If all the checks fail, the new host is counted as an intruder.

EAPOL Multihost access

Scenario	Action
• No authenticated hosts on the port. • Guest VLAN is enabled.	Allow
• New host MAC address is authenticated.	Allow
• Port is configured for MHSA. • One EAPOL-authenticated host already exists on the port. • The number of existing non-EAPOL hosts on the port is less than the configured maximum number allowed.	Allow
• Host is an IP Phone. • Port is configured for ADAC (allowed PhoneMac, not callSvr, not Uplink).	Allow
• Port is configured for non-EAPOL host support. • Host MAC address is in a preconfigured list of allowed MAC addresses. • The number of existing non-EAPOL hosts on the port is less than the configured maximum number allowed.	Allow
• Port is configured for non-EAPOL host support. • Host MAC address is authenticated by RADIUS. • The number of existing non-EAPOL hosts on the port is less than the configured maximum number allowed.	Disallow pending RADIUS authentication; allow when authentication succeeds.

EAP (802.1x) accounting

EAP accounting provides RADIUS accounting for EAP-authenticated clients in the network.

The RADIUS accounting protocol is defined in RFC 2866.

RADIUS accounting in the current Ethernet Routing Switch 5500 Series implementation utilizes the same RADIUS server used for RADIUS authentication. The RADIUS Accounting UDP port is the RADIUS authentication port + 1.

Feature operation

RADIUS accounting logs all of the activity of each remote user in a session on the centralized RADIUS accounting server.

Session IDs for each RADIUS account are generated as 12-character strings. The first four characters in the string form a random number in hexadecimal format. The last eight characters in the string indicate, in hexadecimal format, the number of user sessions started since reboot.

The Network Access Server (NAS) IP address for a session is the IP address of the switch management VLAN.

The following table summarizes the events and associated accounting information logged at the RADIUS accounting server.

Accounting events and logged information

Event	Accounting information logged at server
Accounting is turned on at the router	`Accounting on` request: NAS IP address
Accounting is turned off at the router	`Accounting off` request: NAS IP address
User logs on	`Account start` request: • NAS IP address • NAS port • Account session ID • Account status type • User name
User logs off or port is forced to unauthorized state	`Account stop` request: • NAS IP address • NAS port • Account session ID • Account status type • User name • Account session time • Account terminate cause

Event	Accounting information logged at server
	• Input octet count for the session* • Output octet count for the session* • Input packet count for the session* • Output packet count for the session* *Note: Octet and packet counts are by port and therefore provide useful information only when ports operate in the SHSA mode.

The following table summarizes the accounting termination causes supported.

Supported Account Terminate causes

Cause	Cause ID	When logged at server
ACCT_TERM_USER_REQUEST	1	on User LogOff
ACCT_TERM_LOST_CARRIER	2	on Port Link Down/Failure
ACCT_TERM_ADMIN_RESET	6	on Authorised to ForceUnAuthorised
ACCT_TERM_SUPP_RESTART	19	on EapStart on Authenticated Port
ACCT_TERM_REAUTH_FAIL	20	on ReAuth Failure
ACCT_TERM_PORT_INIT	21	on Port ReInitialization
ACCT_TERM_PORT_ADMIN_DISABLE	22	on Port Administratively Shutdown

For information about configuring RADIUS accounting using the CLI, see "Configuring RADIUS accounting" (page 102).

TACACS+

Ethernet Routing Switch 5500 Series supports the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ is a security application implemented as a client/server-based protocol that provides centralized validation of users attempting to gain access to a router or network access server.

TACACS+ differs from RADIUS in two important ways:

- TACACS+ is a TCP-based protocol.
- TACACS+ uses full packet encryption, rather than just encrypting the password (RADIUS authentication request).

> ***Note:*** TACACS+ encrypts the entire body of the packet but uses a standard TACACS+ header.

TACACS+ separates authentication, authorization, and accounting services. This means that you can selectively implement one or more TACACS+ services.

TACACS+ provides management of users who access the switch through Telnet, serial, and SSH v2 connections. TACACS+ supports users only on the CLI.

Access to the console interface, SNMP, and Web management are disabled when TACACS+ is enabled.

The TACACS+ protocol is a draft standard available at: ftp://ietf.org/internet-drafts/draft-grant-tacacs-02

> ***Note:*** TACACS+ is not compatible with any previous versions of TACACS.

Terminology

The following terms are used in connection with TACACS+:

- AAA—Authentication, Authorization, Accounting
  - *Authentication* is the action of determining who a user (or entity) is, before allowing the user to access the network and network services.
  - *Authorization* is the action of determining what an authenticated user is allowed to do.
  - *Accounting* is the action of recording what a user is doing or has done.
- Network Access Server (NAS)—any client, such as an Ethernet Routing Switch 5500 Series box, that makes TACACS+ authentication and authorization requests, or generates TACACS+ accounting packets.
- daemon/server—a program that services network requests for authentication and authorization, verifies identities, grants or denies authorizations, and logs accounting records.
- AV pairs—strings of text in the form "attribute=value" sent between a NAS and a TACACS+ daemon as part of the TACACS+ protocol.

TACACS+ architecture

You can configure TACACS+ on the Ethernet Routing Switch 5500 Series using the following methods:

- Connect the TACACS+ server through a local interface. Management PCs can reside on an out-of-band management port or serial port, or on the corporate network. The TACACS+ server is placed on the corporate network so that it can be routed to the Ethernet Routing Switch 5500 Series.
- Connect the TACACS+ server through the management interface using an out-of-band management network.

You can configure a secondary TACACS+ server for backup authentication. You specify the primary authentication server when you configure the switch for TACACS+.

Feature operation

During the log on process, the TACACS+ client initiates the TACACS+ authentication session with the server. After successful authentication, if TACACS+ authorization is enabled, the TACACS+ client initiates the TACACS+ authorization session with the server. After successful authentication, if TACACS+ accounting is enabled, the TACACS+ client sends accounting information to the TACACS+ server.

TACACS+ authentication

TACACS + authentication offers complete control of authentication through log on/password dialog and response. The authentication session provides username/password functionality.

You cannot enable both RADIUS and TACACS+ authentication on the same interface. However, you can enable RADIUS and TACACS+ on different interfaces; for example, RADIUS on the serial connection and TACACS+ on the Telnet connection.

> ***Note:*** Prompts for log on and password occur prior to the authentication process. If TACACS+ fails because there are no valid servers, then the username and password are used for the local database. If TACACS+ or the local database return an access denied packet, then the authentication process stops. No other authentication methods are attempted.

TACACS+ authorization

The transition from TACACS+ authentication to the authorization phase is transparent to the user. Upon successful completion of the authentication session, an authorization session starts with the authenticated username. The authorization session provides access level functionality.

TACACS+ authorization enables you to limit the switch commands available to a user. When TACACS+ authorization is enabled, the NAS uses information retrieved from the user profile, which is located either in the local user database or on the security server, to configure the user's session. The user is granted access to a requested command only if the information in the user profile allows it.

TACACS+ authorization is not mandatory for all privilege levels.

When authorization is requested by the NAS, the entire command is sent to the TACACS+ daemon for authorization. You preconfigure command authorization on the TACACS+ server by specifying a list of regular expressions that match command arguments, and associating each command with an action to deny or permit. For an example of the configuration required on the TACACS+ server, see "TACACS+ server configuration example" (page 43).

Authorization is recursive over groups. Thus, if you place a user in a group, the daemon looks in the group for authorization parameters if it cannot find them in the user declaration.

> ***Note:*** If authorization is enabled for a privilege level to which a user is assigned, the TACACS+ server denies any commands for which access is not explicitly granted for the specific user or for the user's group. On the daemon, ensure that each group is authorized to access basic commands such as **`enable`** or **`logout`**.

If the TACACS+ server is not available or an error occurs during the authorization process, the only command available is **`logout`**.

In the TACACS+ server configuration, if no privilege level is defined for a user but the user is allowed to execute at least one command, the user defaults to privilege level 0. If all commands are explicitly denied for a user, the user cannot access the switch at all.

Changing privilege levels at runtime Users can change their privilege levels at runtime by using the following command on the switch:

```
tacacs switch level [<level>]
```

where **`<level>`** is the privilege level the user wants to access. The user is prompted to provide the required password. If the user does not specify a level in the command, the administration level (15) is selected by default.

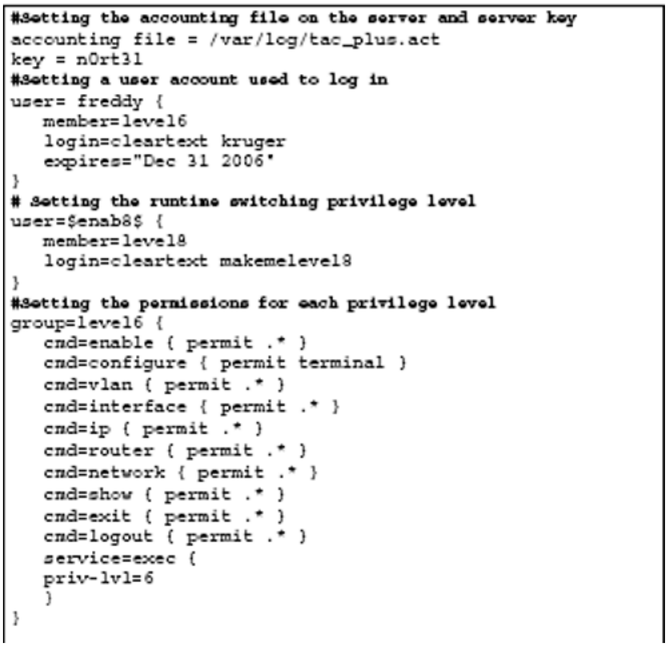
To return to the original privilege level, the user uses the following command on the switch:

`tacacs switch back`

To support runtime switching of users to a particular privilege level, you must preconfigure a dummy user for that level on the daemon. The format of the user name for the dummy user is `$enab<n>$`, where **`<n>`** is the privilege level to which you want to allow access. For an example of the configuration required on the TACACS+ server, see "TACACS+ server configuration example" (page 43).

TACACS+ server configuration example The following example shows a sample configuration for a Linux TACACS+ server. In this example, the privilege level is defined for the group, not the individual user. Note the dummy user created to support runtime switching of privilege levels.

Sample TACACS+ server configuration



```
#Setting the accounting file on the server and server key
accounting file = /var/log/tac_plus.act
key = n0rt31
#Setting a user account used to log in
user= freddy {
   member=level6
   login=cleartext kruger
   expires="Dec 31 2006"
}
# Setting the runtime switching privilege level
user=$enab8$ {
   member=level8
   login=cleartext makemelevel8
}
#Setting the permissions for each privilege level
group=level6 {
   cmd=enable { permit .* }
   cmd=configure { permit terminal }
   cmd=vlan { permit .* }
   cmd=interface { permit .* }
   cmd=ip { permit .* }
   cmd=router { permit .* }
   cmd=network { permit .* }
   cmd=show { permit .* }
   cmd=exit { permit .* }
   cmd=logout { permit .* }
   service=exec {
   priv-lvl=6
   }
}
```

For more information about configuring Linux and other types of TACACS+ servers, see "TACACS+ server configuration examples" (page 315).

TACACS+ accounting

TACACS+ accounting enables you to track:

- the services accessed by users
- the amount of network resources consumed by users

When accounting is enabled, the NAS reports user activity to the TACACS+ server in the form of accounting records. Each accounting record contains accounting AV pairs. The accounting records are stored on the security server. The accounting data can then be analyzed for network management and auditing.

TACACS+ accounting provides information about user CLI terminal sessions within serial, Telnet, or SSH shells (in other words, from the CLI management interface).

The accounting record includes the following information:

- user name
- date
- start/stop/elapsed time
- access server IP address
- reason

You cannot customize the set of events that are monitored and logged by TACACS+ accounting. TACACS+ accounting logs the following events:

- user log on and logoff
- logoff generated because of activity timeout
- unauthorized command
- Telnet session closed (not logged off)

Feature limitations

The following features are not supported in the current implementation of TACACS+ in the Ethernet Routing Switch 5500 Series:

- S/KEY (One Time Password) authentication.
- PPP/PAP/CHAP/MSCHAP authentication methods.
- The FOLLOW response of a TACACS+ server, in which the AAA services are redirected to another server. The response is interpreted as an authentication failure.
- User capability to change passwords at runtime over the network. The system administrator must change user passwords locally, on the server.

TACACS+ configuration

You must use the CLI to configure TACACS+ on the Ethernet Routing Switch 5500 Series. You cannot configure TACACS+ using Device Manager or Web-based management.

For information about configuring TACACS+ server information and TACACS+ authentication, authorization, and accounting using the CLI, see "Configuring TACACS+" (page 102).

You can also use the console interface to enable or disable TACACS+ authentication on serial and Telnet connections: On the Console/Comm Port Configuration menu, select **Telnet/WEB Switch Password Type** or **Telnet/WEB Stack Password Type**, and then select **TACACS+ Authentication**.

IP Manager

You can limit access to the management features of the Nortel Ethernet Routing Switch 5500 Series by defining the IP addresses that are allowed access to the switch.

The IP Manager allows you to do the following:

- Define up to 50 IP addresses and masks that are allowed to access the switch. No other source IP addresses have management access to the switches.
- Enable or disable access to Telnet, SNMP, and the Web-based management system.

You cannot change the Telnet access field if you are connected to the switch through Telnet. Use a non-Telnet connection to modify the Telnet access field.

> ***Note:*** To avoid locking a user out of the switch, Nortel recommends that you configure *ranges* of IP addresses that are allowed to access the switch.

Changes you make to the IP Manager list are reflected only after you restart the system. The sessions that were open at the time of configuring the IP Manager list remain unaffected.

Password security

The Nortel Ethernet Routing Switch 5500 Series provides enhanced password security for the following passwords:

- Switch RO password
- Switch RW password
- Stack RO password
- Stack RW password
- RADIUS Shared Secret (display limitation feature only)
- Read-Only community string (display limitation feature only)

- Read-Write community string (display limitation feature only)

Password security features

The following enhanced password security features are available:

Password length and valid characters

Valid passwords are between 10 and 15 characters long. The password must contain a minimum of the following:

- 2 lower-case letters
- 2 capital letters
- 2 numbers
- 2 special symbols, such as:!@#$%^&*()

The password is case sensitive.

Password retry

If the user fails to provide the correct password after a number of consecutive retries, the switch resets the log on process. The number of allowed retries is configurable. The default is three.

You can configure the allowed number of retries using the Console Interface (**TELNET/SNMP/Web Access > Login Retries** field) or the CLI (see "Configuring the number of retries" (page 107)).

Password history

The Nortel Ethernet Routing Switch 5500 Series keeps a history of the last three passwords. You cannot reuse a password stored in history. When you set the password for the fourth time, you can reuse the password that you used the first time.

Password display

The password is not displayed as clear text. Each character of the password is substituted with an asterisk (*).

Password verification

When you provide a new password, you must retype the same to confirm it. If the two passwords do not match, the password update process fails. In this case, you must try to update the password once again. There is no limit on the number of times you are allowed to update the password.

Password aging time

Passwords expire after a specified aging period. The aging period is configurable, with a range of 1 day to approximately 7.5 years (2730 days). The default is 180 days. When a password has aged out, the user is prompted to create a new password. Only users with a valid RW password can create a new RW or RO password.

Read-Only and Read-Write passwords

The RO and RW passwords cannot be the same.

Default password and default password security

For the non-SSH image, the default password for RO is "user" and "secure" for RW. For the SSH software image, the default password for RO is "userpasswd" and "securepasswd" for RW.

Password security enabled or disabled

By default, password security is disabled for the non-SSH software image and enabled for the SSH software image.

Password security can be enabled from the CLI only. When it is enabled, the following happens:

- Current passwords remain unchanged if they meet the required specifications. If they do not meet the required specifications, the user is prompted to change them to passwords that do meet the requirements.
- An empty password history *bank* is established. The password bank stores three used passwords.
- Password verification is required.

Password security can be disabled from the CLI only. When it is disabled, the following happens:

- Current passwords remain valid.
- Password history bank is removed.
- Password verification is not required.

Password security commands

For information about the CLI commands to enable or disable password security, see "Configuring password security" (page 107).

Password security features and requirements

The following table describes the password security features and requirements in place when password security is enabled.

Summary of password security features and requirements

Feature/Requirement	Description
Password composition	The password must contain a minimum of 2 of each of the following types of characters: lower-case letters, capital letters, numbers, and special symbols such as !@#$%^&*().
Password length	The password must consist of between 10 and 15 characters.
Login attempts	The switch allows only a specified maximum number of consecutive failed log on attempts. The number of allowed retries is configurable. The default is three.
Password history	The previous three passwords used are saved on the switch and cannot be reused until they pass out of the history table.
Password update verification	Any password change must be verified by typing the new password twice.
Password aging time	Passwords expire after a specified period. The aging time is configurable. The default is 180 days.
Password display masking	Any time a password is displayed or entered in the CLI, each character of the password is displayed as an asterisk (*).
Password security factory default	By default, password security is enabled on the SSH software image and disabled on the non SSH software image.

CLI audit

CLI audit provides a means for tracking CLI commands.

The command history is stored in a special area of flash reserved for CLI audit. Access to this area is read-only. If remote logging is enabled, the audit message is also forwarded to a remote syslog server, no matter the logging level.

Every time a CLI command is issued, an audit message is generated. Each log entry consists of the following information:

- timestamp
- fixed priority setting of 30 (= informational message)
- command source
  - — serial console and the unit connected
  - — Telnet or SSH connection and the IP address

- command status (success or failure)
- the CLI command itself

CLI audit is enabled by default and cannot be disabled.

For information on displaying the CLI audit log, refer to "Displaying CLI Audit log" (page 107).

Simple Network Management Protocol

The Nortel Ethernet Routing Switch 5500 Series supports Simple Network Management Protocol (SNMP).

SNMP is traditionally used to monitor Unix systems, Windows systems, printers, modem racks, switches, routers, power supplies, Web servers, and databases. Any device running software that allows the retrieval of SNMP information can be monitored.

You can also use SNMP to change the state of SNMP-based devices. For example, you can use SNMP to shut down an interface on your device.

SNMP versions

SNMP Version 1 (SNMPv1)

SNMP Version 1 (SNMPv1) is a historic version of the SNMP protocol. It is defined in RFC 1157 and is an Internet Engineering Task Force (IETF) standard.

SNMPv1 security is based on communities, which are nothing more than passwords: plain-text strings that allow any SNMP-based application that knows the strings to gain access to a device’s management information. There are typically three communities in SNMPv1: read-only, read-write, and trap.

SNMP Version 2 (SNMPv2)

SNMP Version 2 (SNMPv2) is another historic version of SNMP, and is often referred to as community string-based SNMPv2. This version of SNMP is technically called SNMPv2c. It is defined in RFC 1905, RFC 1906, and RFC 1907.

SNMP Version 3 (SNMPv3)

SNMP Version 3 (SNMPv3) is the current formal SNMP standard, defined in RFCs 3410 through 3419, and in RFC 3584. It provides support for strong authentication and private communication between managed entities.

Nortel Ethernet Routing Switch 5500 Series support for SNMP

The SNMP agent in the Nortel Ethernet Routing Switch 5500 Series supports SNMPv1, SNMPv2c, and SNMPv3. Support for SNMPv2c introduces a standards-based GetBulk retrieval capability using SNMPv1 communities.

SNMPv3 support in the Nortel Ethernet Routing Switch 5500 Series introduces industrial-grade user authentication and message security. This includes MD5- and SHA-based user authentication and message integrity verification, as well as AES- and DES-based privacy encryption.

The Nortel Ethernet Routing Switch 5500 Series allows you to configure SNMPv3 using the Device Manager, Web-based management, or CLI.

SNMP MIB support

The Nortel Ethernet Routing Switch 5500 Series supports an SNMP agent with industry-standard Management Information Bases (MIB) as well as private MIB extensions, which ensures compatibility with existing network management tools.

The IETF standard MIBS supported on the switch include MIB-II (originally published as RFC 1213, then split into separate MIBs as described in RFCs 4293, 4022, and 4113), Bridge MIB (RFC 4188), and the RMON MIB (RFC 2819), which provides access to detailed management statistics.

For information about the MIBs supported by the Nortel Ethernet Routing Switch 5500 Series, see "Supported SNMP MIBs and traps" (page 329).

SNMP trap support

With SNMP management, you can configure SNMP traps (on individual ports) to generate automatically for conditions such as an unauthorized access attempt or changes in port operating status.

The Nortel Ethernet Routing Switch 5500 Series supports both industry-standard SNMP traps, as well as private Nortel enterprise traps.

For information about the MIBs and traps supported by the Nortel Ethernet Routing Switch 5500 Series, see "Supported SNMP MIBs and traps" (page 329).

Secure Socket Layer protocol

Secure Socket Layer (SSL) deployment provides a secure Web management interface.

The SSL server has the following features:

- SSLv3-compliant

- Supports PKI key exchange
- Uses key size of 1024-bit encryption
- Supports RC4 and 3DES cryptography
- Supports MAC algorithms MD5 and SHA-1

Generally, an SSL certificate is generated when:

1. The system is powered on for the first time and the NVRAM does not contain a certificate that can be used to initialize the SSL server.
2. The management interface (CLI/SNMP) requests that a new certificate to be generated. A certificate cannot be used until the next system reset or SSL server reset.

Secure versus Non-secure mode

The management interfaces (CLI/SNMP) can configure the Web server to operate in a secure or non-secure mode. The SSL Management Library interacts with the Web server to this effect.

In the secure mode, the Web server listens on TCP port 443 and responds only to HTTPS client browser requests. All existing non-secure connections with the browser are closed down.

In the non-secure mode, the Web server listens on TCP port 80 and responds only to HTTP client browser requests. All existing secure connections with the browser are closed down.

SSL Certificate Authority

Generally, an SSL certificate is issued and signed by a Certificate Authority (CA), such as VeriSign. Because the management and cost of purchasing a certificate from the CA is a concern, Nortel issues and signs the SSL certificate, with the understanding that it is not a recognized Certificate Authority. Ensure that client browsers that connect to the Nortel Ethernet Routing Switch 5500 Series SSL-enabled Web management interface are aware of this fact.

The SSL certificate contains the information shown as follows. The first three lines are constant. The rest is derived from the RSA host key associated with the certificate.

```
Issuer       : Nortel Networks
Start Date : May 26 2003, 00:01:26
End  Date : May 24 2033, 23:01:26
SHA1 Finger Print:
d6:b3:31:0b:ed:e2:6e:75:80:02:f2:fd:77:cf:a5:fe:9d:6d:6b:e0
MD5 Finger Print:
fe:a8:41:11:f7:26:69:e2:5b:16:8b:d9:fc:56:ff:cc
RSA Host Key (length= 1024 bits):
```

```
40e04e564bcfe8b7febf1f7139b0fde9f5289f01020d5a59b66ce7207895545f
b3abd694f836a9243651fd8cee502f665f47de8da44786e0ef292a3309862273
d36644561472bb8eac4d1db9047c35ad40c930961b343dd03f77cd88e8ddd3dd
a02ae29189b4690a1f47a5fa71b75ffcac305fae37c56ca87696dd9986aa7d19
```

SSL configuration and management

For information about configuring and managing SSL services, see "Secure Socket Layer services" (page 108)

Secure Shell protocol

Secure Shell (SSH) protocol replaces Telnet to provide secure access to the user console menu and CLI interface.

There are two versions of the SSH protocol: SSH1 and SSH2. The SSH implementation in the Nortel Ethernet Routing Switch 5500 Series supports SSH2.

Components of SSH2

SSH2 is used for secure remote log on and other secure network services over an insecure network. SSH2 consists of three major components:

- The Transport Layer Protocol (SSH-TRANS): SSH-TRANS is one of the fundamental building blocks, providing the initial connection, packet protocol, server authentication, and basic encryption and integrity services. After establishing an SSH-TRANS connection, an application has a single, secure, full-duplex byte streak to an authenticated peer. The protocol can also provide compression. The transport layer is used over a TCP/IP connection, but can also be used on top of any other reliable data stream.
- The User Authentication Protocol (SSH-USERAUTH) authenticates the client-side user to the server. It runs over the transport layer protocol. SSH-AUTH supports two methods: public key and password authentication. To authenticate, an SSH2 client tries a sequence of authentication methods chosen from the set allowed by the server (public key, password, and so on) until one succeeds or all fail.
- The Connection Protocol [SSH-CONNECT] multiplexes the encrypted tunnel into several logical channels. This protocol runs over the user authentication protocol.

SSH service configuration

The SSH service engine allows you to configure the SSH service. You can configure SSH through the CLI interface and the SNMP interface.

The management objects are:

- SSH enable or disable

When SSH is enabled, you can configure the SSH server to disable other non-secured interfaces. This is referred to as the SSH secured mode. Otherwise, when you enable SSH, it operates in unsecured mode.

- DSA authentication enable or disable

  You can configure the SSH server to allow or disallow DSA authentication. The other authentication method supported by the Nortel Ethernet Routing Switch 5500 Series is password authentication.

- Password authentication enable or disable

  If password authentication is not enabled, you are not allowed to initiate any connections. After you have access, you cannot disable both DSA and password authentication.

- DSA public key upload/download
- SSH information dump -- shows all the SSH-related information

SSH clients

The following SSH clients are supported by the Nortel Ethernet Routing Switch 5500 Series:

- Putty SSH (Windows 2000)
- F-secure SSH, v5.3 (Windows 2000)
- SSH Secure Shell 3.2.9 (Windows 2000)
- SecureCRT 4.1
- Cygwin OpenSSH (Windows 2000)
- AxeSSH (Windows 2000)
- SSHPro (Windows 2000)
- Solaris SSH (Solaris)
- Mac OS X OpenSSH (Mac OS X)

IP Source Guard

IP Source Guard provides security to the network by filtering clients with invalid IP addresses. It is an L2, per-port feature that works closely with information in the Dynamic Host Control Protocol (DHCP) snooping Binding Table. For information on DHCP snooping, see "DHCP snooping" (page 55). When IP Source Guard is enabled on an untrusted port with DHCP snooping enabled, an IP filter entry is created or deleted for that port automatically, based on IP information stored in the corresponding DHCP snooping Binding Table entry. When a connecting client receives a valid IP address from the DHCP server, a filter is installed on the port to allow traffic only from the assigned IP address. A maximum of 10 IP addresses is allowed on each IP Source Guard-enabled port. When this number is reached, no more filter is set up and traffic is dropped. When IP Source Guard is enabled without DHCP snooping enabled, a default filter is installed and IP traffic for the port is dropped.

IP Source Guard is available to the ERS 55xx Series utilizing Broadcom 569x ASICs, and is implemented with the facility provided by the per-port Fast Filter Processor (FFP) in the ASIC .

ATTENTION
Enable IP Source Guard only on an untrusted DHCP snooping port.

The following table shows you how IP Source Guard works with DHCP snooping:

IP Source Guard and DHCP snooping

IP Source Guard configuration state	DHCP snooping configuration state	DHCP snooping Binding Entry action (untrusted ports)	IP Source Guard action
disabled or enabled	enabled	creates a binding entry.	creates a filter for the IP address using the IP address from the Binding Table entry.
enabled	enabled	creates a binding entry.	creates a filter for the IP address using the IP address from the Binding Table entry.
enabled	enabled	deletes a binding entry.	deletes the IP filter and installs a default filter to block all IP traffic on the port.
enabled	enabled or disabled	deletes binding entries when one of the following conditions occurs: • DHCP is released. • the port link is down, or the administrator is disabled. • the lease time has expired.	deletes the corresponding IP Filter and installs a default filter to block all IP traffic.
enabled or disabled	enabled	not applicable.	deletes the installed IP filter for the port.

disabled	enabled	creates a binding entry.	not applicable.
disabled	enabled	deletes a binding entry.	not applicable.

IP Source Guard does not support the following features:

- Manual assignment of IP addresses.

  This is because DHCP snooping does not support static binding entries.
- IP and MAC address filter.

IP Source Guard can be configured through the Nortel Networks Command Line Interface (NNCLI), Java Device Manager (JDM) and SNMP. For information on configuring IP Source Guard through the NNCLI, , see "IP Source Guard Configuration" (page 133). For information on configuring IP Source Guard through the JDM, see "Configuring IP Source Guard using the Java Device Manager" (page 184)

DHCP snooping

Dynamic Host Configuration Protocol (DHCP) snooping provides security to the network by preventing DHCP spoofing. DHCP spoofing refers to an attacker’s ability to respond to DHCP requests with false IP information. DHCP snooping acts like a firewall between untrusted hosts and the DHCP servers, so that DHCP spoofing cannot occur.

DHCP snooping classifies ports into two types:

- untrusted—ports that are configured to receive messages from outside the network or firewall. Only DHCP requests are allowed.
- trusted—ports that are configured to receive messages only from within the network, such as switch-to-switch and DHCP server ports. All types of DHCP messages are allowed.

DHCP snooping operates as follows to eliminate the “man-in-the-middle” attack capability to set up rogue DHCP servers on untrusted ports:

- DHCP snooping allows only DHCP requests from untrusted ports. DHCP replies and all other types of DHCP messages from untrusted ports are dropped.
- DHCP snooping verifies the source of DHCP packets.
  - — When the switch receives a DHCP request on an untrusted port, DHCP snooping compares the source MAC address and the DHCP client hardware address. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

    Note: This verification is applicable only in Layer 2 mode.

— When the switch receives a DHCP release or DHCP decline broadcast message from a client, DHCP snooping verifies that the port on which the message was received matches the port information for the client MAC address in the DHCP binding table. If the port information matches, the switch forwards the DHCP packet.

WARNING
If the DHCP snooping application drops violating DHCP packets, in rare instances, some PCs may reuse old IP addresses, even the PC cannot obtain one.

Note: DHCP snooping is also available as a Quality of Service (QoS) feature. The QoS application provides basic DHCP snooping that filters DHCP traffic on untrusted interfaces. For information about the QoS DHCP snooping application, see *Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service* (NN47200-504).

DHCP binding table

DHCP snooping dynamically creates and maintains a binding table. The DHCP binding table includes the following information about DHCP leases on untrusted interfaces:

- source MAC address
- IP address
- lease duration
- VLAN ID
- port

The maximum size of the DHCP binding table is 512 entries.

You can view the DHCP binding table during runtime, but you cannot modify it manually. In particular, you cannot configure static entries.

The DHCP binding table is stored in RAM, and therefore is not saved across reboots.

Release 5.1 introduces IP Source Guard, which works closely with DHCP Snooping. IP Source Guard can be enabled per port and is used to prevent IP spoofing. This feature uses the data in the DHCP Snooping binding table to filter traffic. If the sending station is not in the binding table, no IP traffic is allowed to pass. When a connecting client receives a valid IP address from the DHCP server, IP Source Guard installs a filter on the port to only allow traffic from the assigned IP address.

DHCP snooping configuration and management

DHCP snooping is configured on a per VLAN basis.

Configure and manage DHCP snooping using the Nortel Networks Command Line Interface (NNCLI), Java Device Manager (JDM), and SNMP. For information on configuring DHCP snooping through the NNCLI, see "Configuring DHCP snooping" (page 115). For information on configuring DHCP snooping through JDM, see "Configuring DHCP snooping using the Java Device Manager" (page 191).

Feature limitations

Be aware of the following limitations:

- Routed, tagged DHCP packets can bypass DHCP Snooping filters due to the VLAN changes when a packet is rerouted in Layer 3 mode. This limitation does not apply to Layer 2 VLANs.
- Routed DHCP packets bypass source MAC address and client hardware address verification because this type of verification is not applicable in Layer 3 mode.

  Note: Violating DHCP Release or Decline packets may interrupt communication between the server and the client. Nortel recommends restarting the communication or clearing the ARP cache on the server, after the violating traffic is stopped.

Dynamic ARP inspection

Dynamic Address Resolution Protocol (Dynamic ARP) inspection is a security feature that validates ARP packets in the network.

Without dynamic ARP inspection, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Dynamic ARP inspection prevents this type of *man-in-the-middle* attack. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings.

The address binding table is dynamically built from information gathered in the DHCP request and reply when DHCP snooping is enabled. The MAC address from the DHCP request is paired with the IP address from the DHCP reply to create an entry in the DHCP binding table. (For more information about the DHCP binding table, see "DHCP binding table" (page 56).)

When Dynamic ARP inspection is enabled, ARP packets on *untrusted* ports are filtered based on the source MAC and IP addresses seen on the switch port. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the address binding table. Otherwise, the ARP packet is dropped.

For dynamic ARP inspection to function, DHCP snooping must be globally enabled. For more information about DHCP snooping, see "DHCP snooping" (page 55)and "Configuring DHCP snooping" (page 115).

Dynamic ARP inspection is configured on a per VLAN basis.

Configure and manage dynamic ARP inspection using the CLI. For information about configuring this feature with the CLI, see "Configuring dynamic ARP inspection" (page 124). For information about configuring this feature with Web-based management or the JDM, see *Nortel Ethernet Routing Switch 5500 Series Configuration — IP Routing Protocols* (NN47200-503).

Feature limitations

Be aware of the following limitations:

- Dynamic ARP inspection does not operate during the BootP process. BootP occurs after the switch initializes if the unit does not have an IP address and the BootP mode is set to BootP When Needed or Bootp Always.
- Routed, tagged ARP packets can bypass Dynamic ARP Inspection filters due to the VLAN changes when a packet is rerouted in Layer 3 mode. This limitation does not apply to Layer 2 VLANs.

Nortel Secure Network Access

The Nortel Secure Network Access (Nortel SNA) solution 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, and file system verification and enforcement).

In a Nortel SNA network, Nortel Ethernet Routing Switch 5500 Series switches can function as network access devices.

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

For information about configuring the Nortel Ethernet Routing Switch 5500 Series switches in the Nortel SNA solution, see "Implementing the Nortel Secure Network Access solution" (page 265).

Summary of security features

"MAC security" (page 59) through "SNMPv3 security" (page 61) provide an overview of some of the security features available on the Nortel Ethernet Routing Switch 5500 Series.

MAC security

MAC Security	Description
Description	Use the MAC address-based security feature to set up network access control based on source MAC addresses of authorized stations.
What is being secured	Access to the network or specific subnets or hosts.
Per-Port or Per Switch	Per-Port.
Layer	Layer 2.
Level of Security	Forwarding.
Violations	SA filtering, DA filtering, Port Partitioning, SNMP Trap.
Requirements for Setup	Not applicable.
Configuring using interfaces	Web, Console, NNCLI, ASCII configuration file, SNMP.
Restrictions and Limitations	
Reference	s5sbs103 MIB
Comments	

Password Authentication security

Password Authentication	Description
Description	Security feature.
What is being secured	User access to a switch or stack.

Password Authentication	Description
Per-Port or Per Switch	For Radius authentication: • The Radius server needs to be accessible from switch. • The Radius client from the switch must be provided with the Radius server IP and UDP Port and a shared secret.
Layer	Not applicable.
Level of Security	Provides Read Only/Read Write access. The access rights are checked against Local Password/Radius Server.
Violations	Not applicable.
Requirements for Setup	For Radius authentication: • The Radius server needs to be accessible from the switch. • The Radius client from the switch must be provisioned with the Radius server IP, the UDP Port, and a shared secret.
Configuring using interfaces	Console, web, NNCLI, ASCII configuration file.
Restrictions and Limitations	Not applicable.

EAPOL security

EAPOL	Description
Description	Extensible Authentication Protocol Over LAN (Ethernet) You can use this to set up network access control on internal LANs.
What is being secured	User access to the network.
Per-Port or Per Switch	User authentication per-port.
Layer	Layer 2.
Level of Security	Network access encryption.
Violations	The switch blocks a port if intruder is seen on that port. Admin has to re-enable port.
Requirements for Setup	Radius Server configuration on the switch. EAP-Radius server needs to be accessible from the switch.
Configuring using interfaces	Device Manger (DM), Nortel Networks Command Line (NNCLI), Web-based management system.
Restrictions and Limitations	Not allowed--Shared segments and ports configured for Nortel Secure Network Access (NSNA), MultiLink Trunking, MAC address-based security, IGMP (static router ports), or port mirroring.
Reference	IEEE802.1X, RFC 2284.

IP Manager security

IP Manager	Description
Description	IP Manager is an extension of Telnet. It provides an option to enable/disable access for TELNET (Telnet On/Off), SNMP (SNMP On/Off) and Web Page Access (Web On/Off) with or without a list of 50 IP Addresses and masks.
What is being secured	User access to the switch through telnet, SNMP, or Web.
Per-Port or Per Switch	Per switch.
Layer	IP.
Level of Security	Access.
Violations	User is not allowed to access the switch.
Requirements for Setup	Optional IP Addresses/Masks, Individual Access (enable/disable) for TELNET, SNMP or Web Page.
Configuring using interfaces	Web, console, and CLI.
Restrictions and Limitations	Not applicable.

SNMPv3 security

SNMPv3	Description
Description	The latest version of SNMP provides strong authentication and privacy for Simple Network Management Protocol (SNMP)--using hash message authentication codes message digest 5 (HMAC-MD5), HMAC-secure hash algorithm (SHA), and cipher block chaining Data Encryption Standard (CSCDES)--plus access control of Management Information Base (MIB) objects based on usernames.
What is being secured	Access to MIBs using SNMPv3 is secured. Access to MIBs using SNMPv1/v2c can be restricted.
Per-Port or Per Switch	Per switch.
Layer	SNMP Port 161, 162.
Level of Security	Access/Encryption.
Violations	Received SNMPv3 packets that cannot be authenticated are discarded. For authenticated packets that try to access MIB objects in an unauthorized manner, an error is returned to the sender. In any case, various MIB counters is incremented when any kind of violation occurs. (These can be monitored to detect intrusions, for example, by using RMON alarms.)

SNMPv3	Description
Requirements for Setup	For maximum security, initial configuration of views, users, and keys must be done through the console port or over a physical network connection. Subsequent secure configuration changes can be accomplished using SNMPv3 using a secure SHA/DES connection.
Configuring using interfaces	Device Manger (DM), Nortel Networks Command Line Interface (NNCLI), Web-based management system, ASCII config file, and SNMP Set requests.

DHCP Snooping security

DHCP Snooping	Description
Description	Use the Dynamic Host Control Protocol (DHCP) snooping security feature to provide security to the network by filtering un-trusted DHCP messages to prevent DHCP spoofing.
What is being secured	Access to the network.
Per port or per switch	Per port.
Layer	Layer 2 and 3.
Level of security	Forwarding.
Violations	Allows only DHCP requests from untrusted ports. DHCP replies and all other types of DHCP messages are dropped. If the source MAC address and the DHCP client hardware address do not match, the switch drops the packet.
Requirements for setup	Not applicable.
Configuring using interfaces	Nortel Networks Command Line Interface (NNCLI) and Java Device Manager (JDM).
Restrictions and limitations	Routed, tagged DHCP packets can bypass filters due to VLAN changes, when a packet is rerouted in the Layer 3 mode. Routed DHCP packets can bypass source MAC address and client hardware address verification because this type of verification is not applicable in the Layer 3 mode.

Dynamic ARP Inspection security

Dynamic ARP Inspection	Description
Description	Use the dynamic Address Resolution Protocol (ARP) Inspection to validate ARP packets in a network.
What is being secured	Access to the network.
Per port or per switch	Per port.

Layer	Layer 2 and 3.
Level of security	Forwarding.
Violations	Dynamic ARP Inspection intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings.
Requirements for setup	DHCP snooping must be globally enabled.
Configuring using interfaces	Nortel Networks Command Line Interface (NNCLI) and Java Device Manager (JDM).
Restrictions and limitations	Dynamic ARP inspection does not operate during the BootP process. Routed, tagged ARP packets can bypass dynamic ARP Inspection filters due to VLAN changes, when a packet is rerouted in the Layer 3 mode.

IP Source Guard security

IP Source Guard	**Description**
Description	Use IP Source Guard to prevent IP spoofing by creating a filter entry based on information in the Dynamic Host Control Protocol (DHCP) snooping Binding Table.
What is being secured	Access to the port.
Per port or per switch	Per port.
Layer	Layer 2.
Level of security	IP address filtering.
Violations	IP Source Guard filters IP addresses based on the port's DHCP snooping Binding Table entry and prevents invalid IP traffic from going through.
Requirements for setup	Ensure that: • the port has DHCP snooping globally enabled. • the port is a member of a VLAN configured for DHCP snooping and dynamic ARP Inspection. • the port is a DHCP snooping and dynamic ARP Inspection untrusted port. • the port has a minimum of ten available rules.

Configuring using interfaces	Nortel Networks Command Line Interface (NNCLI), SNMP and Java Device Manager (JDM).
Restrictions and limitations	IP Source Guard allows up to ten IP addresses on each port. Traffic is dropped for entries created after this number is reached. Manual IP assignment is not supported because DHCP snooping does not support static binding entries. IP and MAC address filter is not supported.

NSNA security

NSNA	Description
Description	Use the Nortel Secure Network Access (NSNA) feature to protect the network from DoS attacks and endpoint vulnerability.
What is being secured	Access to devices that are not compliant with network policies is restricted.
Per-Port or Per Switch	per port.
Layer	Layer 2-7
Level of Security	Network access
Violations	For non-authenticated clients, the switch keeps the ports in RED VLAN (restricted access zone). For authenticated clients that are not compliant with network policies, the ports are kept in YELLOW LAN (remediation zone).
Requirements for setup	SNAS server IP address/port and NSNA VLANs must be configured on the switch. SNAS server needs to be accessible from the switch and Switch to SNAS Communication Protocol (SSCP) must be up.
Configuring using interfaces	Nortel Networks Command Line Interface (NNCLI) and Device Manger (DM).
Restrictions and Limitations	Not allowed on ports configured for EAP, MAC address-based security, port mirroring (monitor port), BRouter port, ADAC and VLACP.

Configuring and managing security using the Command Line Interface

This chapter describes the methods and procedures necessary to configure security on the Nortel Ethernet Routing Switch 5500 Series using the Command Line Interface (CLI).

Depending on the scope and usage of the commands listed in this chapter, different command modes can be needed to execute them.

This chapter includes the following topics:

Setting user access limitations

For a complete explanation of the configuration and management of user access limitations using the CLI, refer to the *Nortel Ethernet Routing Switch 5500 Series Overview – System Configuration* (NN47200-500).

Configuring MAC address-based security

The following CLI commands allow for the configuration of the BaySecure* application using Media Access Control (MAC) addresses.

> ***Note:*** The MAC Security feature on the Nortel Ethernet Routing Switch 5530-24TFD shares resources with QoS. Precedence values for non-QoS features are allocated dynamically in descending order of availability. Therefore, the precedence value used depends on the order in which features are configured. With DHCP Relay enabled by default and assigned the highest precedence value (15), a QoS policy with a precedence value of 15 cannot be installed. If the MAC Security feature is also enabled, it is assigned a precedence value of 14. Therefore, a QoS policy with a precedence value of 14 cannot be installed.
>
> For further information about QoS policies, refer to *Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service* (NN47200-504))

CLI commands for MAC address security

The CLI commands in this section are used to configure and manage MAC address security.

show mac-security command

The **`show mac-security`** command displays configuration information for the BaySecure application.

The syntax for the **`show mac-security`** command is:

```
show mac-security {config|mac-address-table [address
<macaddr>]|port|security-lists}
```

The following table outlines the parameters for this command.

show mac-security parameters

Parameter	Description
config	Displays general BaySecure configuration.
mac-address-table [address <macaddr>]	Displays contents of BaySecure table of allowed MAC addresses: • address - specifies a single MAC address to display; enter the MAC address
port	Displays the BaySecure status of all ports.
security-lists	Displays port membership of all security lists.

The **show mac-security** command is executed in the Privileged EXEC command mode.

show mac-security mac-da-filter command

The **show mac-security mac-da-filter** command displays configuration information for filtering MAC destination addresses (DA). Packets can be filtered from up to 10 MAC DAs.

The syntax for the **show mac-security mac-da-filter** command is:

```
show mac-security mac-da-filter
```

The **show mac-security mac-da-filter** command is executed in the Privileged EXEC command mode.

The **show mac-security mac-da-filter** command has no parameters or variables.

mac-security command

The **mac-security** command modifies the BaySecure configuration.

The syntax for the **mac-security** command is:

```
mac-security [disable|enable] [filtering {enable|disable}]
[intrusion-detect {enable|disable|forever}] [intrusion-timer
<1-65535>] [learning-ports  <portlist>] [learning
{enable|disable}] [snmp-lock {enable|disable}]
[snmp-trap {enable|disable}]
```

The following table outlines the parameters for this command.

mac-security parameters

Parameter	Description
disable|enable	Disables or enables MAC address-based security.
filtering {enable|disable}	Enables or disables destination address (DA) filtering on intrusion detected.
intrusion-detect {enable|disable|forever}	Specifies partitioning of a port when an intrusion is detected: • enable - port is partitioned for a period of time • disabled - port is not partitioned on detection • forever - port is partitioned until manually changed

Parameter	Description
intrusion-timer <1-65535>	Specifies, in seconds, length of time a port is partitioned when an intrusion is detected; enter the number of seconds desired.
learning-ports <portlist>	Specifies MAC address learning. Learned addresses are added to the table of allowed MAC addresses. Enter the ports to learn; a single port, a range of ports, several ranges, all ports, or no ports can be entered.
learning {enable|disable}	Specifies MAC address learning: • enable - enables learning by ports • disable - disables learning by ports
snmp-lock {enable|disable}	Enables or disables a lock on SNMP write-access to the BaySecure MIBs.
snmp-trap {enable|disable}	Enables or disables trap generation upon intrusion detection.

The **`mac-security`** command is executed in the Global Configuration command mode.

mac-security mac-address-table address command

The **`mac-security mac-address-table address`** command assigns either a specific port or a security list to the MAC address. This removes any previous assignment to the specified MAC address and creates an entry in the BaySecure table of allowed MAC addresses.

The syntax for the **`mac-security mac-address-table address`** command is:

```
mac-security mac-address-table address  <H.H.H.>  {port
<portlist>| security-list  <1-32>}
```

The following table outlines the parameters for this command.

mac-security mac-address-table address parameters

Parameter	Description
<H.H.H>	Enter the MAC address in the form of H.H.H.
port <portlist>|security-list <1-32>	Enter the port number or the security list number. In this command the port list must be a single port.

The **`mac-security mac-address-table address`** command is executed in the Global Configuration command mode.

no mac-security mac-address-table command

The **`no mac-security mac-address-table`** command clears static entries from the MAC address security table. MAC addresses auto-learned on ports are not deleted.

The syntax for the **`no mac-security mac-address-table`** command is:

```
no mac-security mac-address-table {address  <H.H.H.>
|port <portlist> |security-list  <1-32>}
```

The following table outlines the parameters for this command.

no mac-security mac-address-table parameters

Parameter	Description
address <H.H.H>	Enter the MAC address in the form of H.H.H.
port <portlist>	Enter the port number.
security-list <1-32>	Enter the security list number.

The **`no mac-security mac-address-table`** command is executed in the Global Configuration command mode.

show mac-security mac-address-table command

The **`show mac-security mac-address-table`** command displays the current global MAC Address security table. The syntax for this command is:

```
show mac-security mac-address-table.
```

This command is executed in the Privileged EXEC command mode.

mac-security security-list command

The **`mac-security security-list`** command assigns a list of ports to a security list.

The syntax for the **`mac-security security-list`** command is:

```
mac-security security-list  <1-32> <portlist>
```

The following table outlines the parameters for this command.

mac-security security-list parameters

Parameter	Description
<1-32>	Enter the number of the security list you want to use.
<portlist>	Enter the port number.

The `mac-security security-list` command is executed in the Global Configuration command mode.

no mac-security security-list command

The `no mac-security security-list` command clears the port membership of a security list.

The syntax for the `no mac-security security-list` command is:

```
no mac-security security-list  <1-32>
```

Substitute the `<1-32>` with the number of the security list to be cleared.

The `no mac-security security-list` command is executed in the Global Configuration command mode.

mac-security command for specific ports

The `mac-security` command for specific ports configures the BaySecure status of specific ports.

The syntax for the `mac-security` command for specific ports is:

```
mac-security [port <portlist>] {disable|enable|learning}
```

The following table outlines the parameters for this command.

mac-security parameters

Parameter	Description
port <portlist>	Enter the port numbers.
disable|enable|learning	Directs the specific port: • disable - disables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is being performed • enable - enables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is being performed

Parameter	Description
	• learning - disables BaySecure on the specified port and adds these port to the list of ports for which MAC address learning is being performed

The **mac-security** command for specific ports is executed in the Interface Configuration command mode.

show mac-security command

The **show mac-security** command displays the current MAC Address security table for the ports entered. The syntax for this command is:

```
show mac-security port <portlist>.
```

Substitute **<portlist>** with the ports to be displayed.

This command is executed in the Privileged EXEC command mode.

mac-security mac-da-filter command

The **mac-security mac-da-filter** command allows packets to be filtered from up to ten specified MAC DAs. This command is also used to delete such a filter and then receive packets from the specified MAC DA.

The syntax for the **mac-security mac-da-filter** command is:

```
mac-security mac-da-filter {add|delete} <H.H.H.>
```

Substitute the **{add|delete} <H.H.H.>** with either the command to add or delete a MAC address and the MAC address in the form of H.H.H.

The **mac-security mac-da-filter** command is executed in the Global Configuration command mode.

CLI commands for MAC address auto-learning

The CLI commands in this section are used to configure and manage MAC auto-learning.

mac-security auto-learning aging-time command

The **mac-security auto-learning aging-time** command sets the aging time for the auto-learned addresses in the MAC Security Table.

The syntax for the command is:

```
mac-security auto-learning aging-time  <0-65535>
```

Substitute **<0-65535>** with the aging time in minutes. An aging time of 0 means that the learned addresses never age out. The default is 60 minutes.

The **mac-security auto-learning aging-time** command is executed in the Global Configuration command mode.

no mac-security auto-learning aging-time command

The **no mac-security auto-learning aging-time** command sets the aging time for the auto-learned addresses in the MAC Security Table to 0. In this way, it disables the removal of auto-learned MAC addresses.

The syntax for the command is:

```
no mac-security auto-learning aging-time
```

The **no mac-security aging-time** command is executed in the Global Configuration command mode.

default mac-security auto-learning aging-time command

The default **mac-security auto-learning aging-time** command sets the aging time for the auto-learned addresses in the MAC Security Table to the default of 60 minutes.

The syntax for the command is:

```
default mac-security auto-learning aging-time
```

The **default mac-security auto-learning aging-time** command is executed in the Global Configuration command mode.

mac-security auto-learning port command

The **mac-security auto-learning port** command configures MAC security auto-learning on the ports.

The syntax for the command is:

```
mac-security auto-learning port  <portlist>  disable|{enable
[max-addrs  <1-25>]}
```

The following table outlines the parameters for this command.

mac-security auto-learning parameters

Parameter	Description
<portlist>	The ports to configure for auto-learning.

Parameter	Description
disable|enable	Disables or enables auto-learning on the specified ports. The default is disabled.
max-addrs <1 - 25>	Sets the maximum number of addresses the port will learn. The default is 2.

The **`mac-security auto-learning`** command is executed in the Interface Configuration command mode.

no mac-security auto-learning command

This command disables MAC security auto-learning for the specified ports on the switch. The syntax for this command is:

```
no mac-security auto-learning port  <portlist>
```

where

`<portlist>` is the list of port numbers on which you want to disable MAC address auto-learning

The **`no mac-security auto-learning`** command is executed in the Interface Configuration command mode.

default mac-security auto-learning command

The **`default mac-security auto-learning`** command sets the default MAC security auto-learning on the switch.

The syntax for the command is:

```
default mac-security auto-learning port  <portlist>
[enable]  [max-addrs]
```

The following table outlines the parameters for this command.

default mac-security auto-learning parameters

Parameter	Description
<portlist>	The ports to configure for auto-learning.
enable	Sets to default the auto-learning status for the port. The default is disabled.
max-addrs	Sets to default the maximum number of addresses the port will learn. The default is 2.

The **`default mac-security auto-learning`** command is executed in the Interface Configuration command mode.

Configuring RADIUS authentication

For information about the function and operation of RADIUS in a Nortel Ethernet Routing Switch 5500 Series network, see "RADIUS-based network security" (page 22).

To configure RADIUS to perform authentication services for system users, do the following:

- Configure the RADIUS server itself. Refer to the vendor documentation for your server for specific configuration procedures. In particular, ensure that you set the appropriate Service-Type attribute in the user accounts:
  - for read-write access, Service-Type = Administrative
  - for read-only access, Service-Type = NAS-Prompt
- Configure RADIUS server settings on the switch (see "Configuring RADIUS server settings" (page 74)).
- (Optional) Enable the RADIUS password fallback feature (see "Enabling RADIUS password fallback" (page 75)).

Configuring RADIUS server settings

To add a RADIUS server, use the following command in Global or Interface configuration mode:

```
radius-server
```

This command includes the following parameters:

radius-server followed by:	
host <IPaddr>	Specifies the IP address of the primary server you want to add or configure.
key <key>	Specifies the secret authentication and encryption key used for all communications between the NAS and the RADIUS server. The key, also referred to as the *shared secret*, must be the same as the one defined on the server. You are prompted to enter and confirm the key.
[port <port>]	Specifies the UDP port for RADIUS. • <port> is an integer in the range 0–65535. The default port number is 1812.

[secondary-host <IPaddr>]	Specifies the IP address of the secondary server. The secondary server is used only if the primary server does not respond.
[timeout <timeout>]	Specifies the number of seconds before the service request times out. RADIUS allows three retries for each server (primary and secondary). **`<timeout>`** is an integer in the range 1–60. The default timeout interval is 2 seconds.

To delete a RADIUS server and restore default RADIUS settings, use one of the following commands in Global or Interface configuration mode:

```
no radius-server
```

```
default radius-server
```

Enabling RADIUS password fallback

To enable the RADIUS password fallback feature, use the following command in Global or Interface configuration mode:

```
radius-server password fallback
```

When RADIUS password fallback is enabled, users can log on to the switch or the stack using the local password if the RADIUS server is unavailable or unreachable.The default is disabled.

After it has been enabled, you cannot disable RADIUS password fallback without erasing all other RADIUS server settings.

> ***Note:*** You can use the Console Interface to disable the RADIUS password fallback without erasing other RADIUS server settings. From the main menu, choose **Console/Comm Port Configuration**, then toggle the **RADIUS Password Fallback** field to **No**.

To disable the RADIUS password fallback feature, use one of the following commands in Global or Interface configuration mode:

```
no radius-server
```

```
default radius-server
```

The command erases settings for the RADIUS primary and secondary servers and secret key, and restores default RADIUS settings.

Viewing RADIUS information

To display RADIUS configuration status, enter the following command from any mode:

```
show radius-server
```

The following example shows sample output for the command.

```
5530-24TFD(config)#show radius-server
Password Fallback:  Disabled
Primary Host:  10.10.10.5
Secondary Host:  0.0.0.0
Port:  1812
Time-out:  2
Key:  ***************
Radius Accounting is  Disabled
AcctPort:  1813
```

Configuring Extensible Authentication Protocol security

The following CLI commands are used to configure and manage Extensible Authentication Protocol over LAN (EAPOL) security.

eapol command

The **eapol** command enables or disables EAPOL-based security.

The syntax for the eapol command is:

```
eapol {disable|enable}
```

Use either **disable** or **enable** to enable or disable EAPOL-based security.

The **eapol** command is executed in the Global Configuration command mode.

eapol command for modifying parameters

The **eapol** command for modifying parameters modifies EAPOL-based security parameters for a specific port.

The syntax for the **eapol** command for modifying parameters is:

```
eapol [port <portlist>] [init] [status
authorized|unauthorized|auto] [traffic-control in-out|in]
[re-authentication enable|disable] [re-authentication-period
<1-604800>] [re-authenticate] [quiet-interval <num>]
[transmit-interval  <num>] [supplicant-timeout <num>]
[server-timeout  <num>] [max-request  <num>]
```

The following table outlines the parameters for this command.

eapol parameters

Parameter	Description
port <portllist>	Specifies the ports to configure for EAPOL; enter the desired port numbers ***Note:*** If this parameter is omitted, the system uses the port number specified when the interface command was issued.
init	Re-initiates EAP authentication.
status authorized|unauthorized|auto	Specifies the EAP status of the port: • authorized - port is always authorized • unauthorized - port is always unauthorized • auto - port authorization status depends on the result of the EAP authentication
traffic-control in-out I in	Sets the level of traffic control: • in-out - if EAP authentication fails, both ingressing and egressing traffic are blocked • in - if EAP authentication fails, only ingressing traffic is blocked
re-authentication enable|disable	Enables or disables re-authentication.
re-authentication-period <1-604800>	Enter the desired number of seconds between re-authentication attempts.
re-authenticate	Specifies an immediate re-authentication.
quiet-interval <num>	Enter the desired number of seconds between an authentication failure and the start of a new authentication attempt; range is 1 to 65535.
transmit-interval <num>	Specifies a waiting period for response from supplicant for EAP Request/Identity packets. Enter the number of seconds to wait; range is 1-65535.
supplicant-timeout <num>	Specifies a waiting period for response from supplicant for all EAP packets except EAP Request/Identity packets. Enter the number of seconds to wait; range is 1-65535.

Parameter	Description
server-timeout <num>	Specifies a waiting period for response from the server. Enter the number of seconds to wait; range is 1-65535
max-request <num>	Enter the number of times to retry sending packets to supplicant.

The **eapol** command for modifying parameters is executed in the Interface Configuration command mode.

show eapol command

The **show eapol** command displays the EAPOL-based security.

The syntax for the **show eapol** command is:

```
show eapol [<portlist>] [multihost {interface|status}]
[guest-vlan {interface}] [auth-diags {interface}] [auth-stats
{interface}]
```

The following table outlines the parameters for this command.

show eapol parameters

Parameter	Description
portlist	The list of ports that EAPOL security is to be displayed for.
multihost {interface|status}	Displays EAPOL multihost configuration. Select interface to display multihost port configuration and status to display multihost port status.
guest-vlan {interface}	Displays EAPOL per-port Guest VLAN settings.
auth-diags {interface}	Displays the EAPOL authentication diagnostics interface.
auth-stats {interface}	Dispays the authentication statistics interface.

The **show eapol** command is executed in the Privileged EXEC command mode.

show eapol multihost status command

The **show eapol multihost status** command displays the multihost status of eapol clients on EAPOL-enabled ports.

The syntax for the **show eapol multihost status** command is:

```
show eapol multihost status [<interface-type>] [<interface-
id>]
```

The following table outlines the parameters for this command:

show eapol multihost status parameters

Parameter	Description
<interface-id>	displays the interface ID.
<interface-type>	displays the type of interface used.

The **`show eapol multihost status`** command is executed in the Privileged Exec command mode.

eapol user-based-policies command

The **`eapol user-based-policies`** command configures 802.1x (Radius server accounting) user-based policies settings.

The syntax for the **`eapol user-based-policies`** command is:

```
eapol user-based-policies { [enable] [filter-on-mac enable] }
```

The **`eapol user-based-policies`** command is executed in the Global Configuration command mode.

The following table outlines the parameters for this command:

eapol user-based-policies parameters

Parameter	Description
enable	configures 802.1x user-based policies settings.
filter-on-mac enable	enables filtering on MAC addresses.

no eapol user-based-policies command

The **`no eapol user-based-policies`** command disables configuration of 802.1x (Radius server accounting) user-based policies settings.

The syntax for the **`no eapol user-based-policies`** command is:

```
no eapol user-based-policies { [enable] [filter-on-mac
enable] }
```

The **`no eapol user-based-policies`** command is executed in the Global Configuration command mode.

The following table outlines the parameters for this command:

no eapol user-based-policies parameters

Parameter	Description
enable	disables configuration of 802.1x (Radius server accounting) user-based policies settings.
filter-on-mac enable	disables filtering on MAC addresses.

default eapol user-based-policies command

The **`default eapol user-based-policies`** command sets the default configuration of 802.1x (Radius server accounting) user-based policies.

The syntax for the **`default eapol user-based-policies`** command is:

```
default eapol user-based-policies { [enable] [filter-on-mac
enable] }
```

The **`default eapol user-based-policies`** command is executed in the Global Configuration command mode.

The following table outlines the parameters for this command:

default eapol user-based-policies parameters

Parameter	Description
enable	sets the default configuration of 802.1x user-based policies.
filter-on-mac enable	sets the default configuration for filtering on MAC addresses.

eapol multihost non-eap-user-based-policies command

The **`eapol multihost non-eap-user-based-policies`** command sets the default configuration of 802.1x (Radius server accounting) multihost non-EAP user-based policies.

The syntax for the **`eapol multihost non-eap-user-based-policies`** command is:

```
eapol multihost non-eap-user-based-policies { [enable]
[filter-on-mac enable] }
```

The **`eapol multihost non-eap-user-based-policies`** command is executed in the Global Configuration command mode.

The following table outlines the parameters for this command:

eapol multihost non-eap-user-based-policies parameters

Parameter	Description
enable	configures the multihost non-EAP user-based policies settings.
filter-on-mac enable	configures settings for the multihost non-EAP filtering on MAC addresses.

no eapol multihost non-eap-user-based-policies command

The **`no eapol multihost non-eap-user-based-policies`** command disables configuration of the 802.1x (Radius server accounting) multihost non-EAP user-based policies.

The syntax for the **`no eapol multihost non-eap-user-based-policies`** command is:

```
no eapol multihost non-eap-user-based-policies { [enable]
[filter-on-mac enable] }
```

The **`no eapol multihost non-eap-user-based-policies`** command is executed in the Global Configuration command mode.

The following table outlines the parameters for this command:

no eapol multihost non-eap-user-based-policies parameters

Parameter	Description
enable	disables non-EAP user-based policies settings.
filter-on-mac enable	disables settings for the multihost non-EAP filtering on MAC addresses.

default eapol multihost non-eap-user-based-policies command

The **`default eapol multihost non-eap-user-based-policies`** command sets the default configuration of 802.1x (Radius server accounting) multihost non-EAP user-based policies.

The syntax for the **`default eapol multihost non-eap-user-based-policies`** command is:

```
default eapol multihost non-eap-user-based-policies {
[enable] [filter-on-mac enable] }
```

The **`default eapol multihost non-eap-user-based-policies`** command is executed in the Global Configuration command mode.

The following table outlines the parameters for this command:

default eapol multihost non-eap-user-based-policies parameters

Parameter	Description
enable	sets the default multihost non-EAP user-based policies settings.
filter-on-mac enable	sets the default multihost non-EAP settings for filtering on MAC addresses.

show interface FastEthernet eapol auth-diags command

This command displays the eapol authentication diagnostics for the desired FastEthernet ports.

The syntax for the **`show interface FastEthernet eapol auth-diags`** command is:

```
show interface FastEthernet eapol auth-diags [<portlist>]
```

where **`FastEthernet`** is one of the keywords in the <portType> parameter used in the ’show’ commands. (The other keywords are: **`Ethernet`** and **`GigabitEthernet`**).

The **`show interface FastEthernet eapol auth-diags`** command is executed in the Privileged Exec command mode.

The following table outlines the parameters for this command:

show interface FastEthernet eapol auth-diags parameters

Parameter	Description
auth-diags	the authentication diagnostics for the desired FastEthernet ports.
<portlist>	a list of ports (of the FastEthernet type) for which you want the eapol authentication diagnostics displayed.

Configuring advanced EAPOL features

Ethernet Routing Switch 5500 Series, Software Release 5.1 supports advanced EAPOL features that allow multiple hosts and non-EAPOL clients on a port. For more information about the advanced EAPOL features, see "Advanced EAPOL features" (page 27).

This section provides information about configuring the following features:

- Single Host with Single Authentication (SHSA) and Guest VLAN (see "Configuring guest VLANs" (page 83))
- Multiple Host with Multiple Authentication (MHMA) (see "Configuring multihost support" (page 84))

- Non-EAPOL hosts on EAPOL-enabled ports (see "Configuring support for non-EAPOL hosts on EAPOL-enabled ports" (page 92))
- Multiple Host with Single Authentication (MHSA) (see "Configuring MHSA" (page 100))

SHSA is the default configuration.

Configuring guest VLANs

To configure guest VLAN support, do the following:

1. Enable guest VLAN globally and set the guest VLAN ID.
2. Enable guest VLAN on specific ports on an interface.

eapol guest-vlan command

The **`eapol guest-vlan`** command sets the guest VLAN for EAP-controlled ports.

The syntax for the **`eapol guest-vlan`** command is:

```
eapol guest-vlan enable vid  <1-4094>
```

The following table outlines the parameters for this command.

eapol guest-vlan parameters

Parameter	Description
enable	Enable Guest VLAN.
<vid>	Guest VLAN ID.

The **`eapol guest-vlan`** command is executed in the Global Configuration command mode.

no eapol guest-vlan command

The **`no eapol guest-vlan`** command disables the guest VLAN.

The syntax for the **`no eapol guest-vlan`** command is:

```
no eapol guest-vlan [enable]
```

The **`no eapol guest-vlan`** command is executed in the Global Configuration command mode.

default eapol guest-vlan command

The **`default eapol guest-vlan`** command disables the guest VLAN.

The syntax for the **`default eapol guest-vlan`** command is:

```
default eapol guest-vlan
```

The **default eapol guest-vlan** command is executed in the Global Configuration command mode.

The **default eapol guest-vlan** command has no parameters or variables.

Configuring multihost support

To configure multihost support, do the following:

1. Enable multihost support for the interface. The relevant command is executed in Interface Configuration mode. You can issue the command for the interface selected when you enter the Interface Configuration mode (so that all ports have the same setting), or you can issue the command for specific ports on the interface.
2. Specify the maximum number of EAP clients allowed on each multihost port. You can issue the command for the interface selected when you enter the Interface Configuration mode (so that all ports have the same setting), or you can issue the command for specific ports on the interface.

eapol multihost command

This command controls the global multihost settings.

The syntax for the **eapol multihost** command is:

```
eapol multihost { [enable] [eap-mac-max
<1-800>] [non-eap-mac-max <1-800>]
[allow-non-eap-enable] [radius-non-eap-enable]
[auto-non-eap-mhsa-enable] [non-eap-phone-enable]
[use-radius-assigned-vlan] [eap-packet-mode {multicast
| unicast}]                    [eap-reauth-sec-mode
{fail | do-not-fail}] }
```

The following table outlines the parameters for this command:

eapol multihost parameters

Parameter	Description
enable	globally enables EAPoL.
eap-mac-max	specifies the maximum number of EAP MAC addresses allowed.
non-eap-mac-max	specifies the maximum number of non-EAP MAC addresses allowed.
allow-non-eap-enable	enables MAC addresses of non-EAP clients.
radius-non-eap-enable	enables Radius authentication of non-EAP clients.

auto-non-eap-mhsa-enable	enables auto-authentication of non-EAP clients in the Multiple Host with Single Authentication (MHSA) mode.
non-eap-phone-enable	enables Nortel IP Phone clients as another non-EAP type.
use-radius-assigned-vlan	enables use of Radius-assigned VLAN values in the multihost mode.
eap-packet-mode {multicast | unicast}	enables the packet mode (multicast or unicast) for EAP requests.
eap-reauth-sec-mode {fail | do-not-fail}	enables reauthentication of the secondary mode (fail or do not fail) for EAP requests.

no eapol multihost command

The **`no eapol multihost`** command disables EAPOL multihost . This command is executed in the global configuration mode.

The syntax for the **`no eapol multihost`** command is:

```
no eapol multihost [enable] [eap-mac-max] [non-eap-mac-max]
[allow-non-eap-enable] [radius-non-eap-enable]
[auto-non-eap-mhsa-enable] [non-eap-phone-enable]
[use-radius-assigned-vlan] [eap-packet-mode]
[eap-reauth-sec-mode]
```

The following table outlines the parameters for this command. If you do not specify any parameters, the command resets all EAPOL multihost settings to the defaults.

no eapol multihost parameters

Parameter	Description
eap-mac-max	specifies the maximum number of EAP clients allowed on the port.
non-eap-mac-max	specifies the maximum number of non-EAP authenticated MAC addresses allowed.
non-eap-mac	disables allowing a non-EAPOL MAC address.
allow-non-eap-enable	disables MAC addresses of non-EAP clients.
radius-non-eap-enable	disables RADIUS authentication of non-EAP clients.
auto-non-eap-mhsa-enable	disables auto-authentication of non-EAP clients.
non-eap-phone-enable	disables authentication of Nortel IP Phone clients as another non-EAP type.
use-radius-assigned-vlan	disables use of RADIUS-assigned VLAN values in the MHMA mode.

Parameter	Description
eap-packet-mode	disables the EAP packet mode request feature.
eap-reauth-sec-mode	disables reauthentication of the secondary mode.

default eapol multihost command

The **default eapol multihost** command sets the EAPoL multihost feature to the defaults.

The syntax for the default EAPoL multihost command is:

```
default eapol multihost [enable]
[eap-mac-max] [non-eap-mac-max]
[allow-non-eap-enable] [radius-non-eap-enable]
[auto-non-eap-mhsa-enable] [non-eap-phone-enable]
[use-radius-assigned-vlan] [eap-packet-mode]
[eap-reauth-sec-mode]
```

The following table outlines the parameters for this command. If you do not specify any parameters, the command resets all EAPoL multihost settings to the defaults.

default eapol multihost parameters

Parameter	Description
enable	restores EAPoL multihost support status to the default value (disabled).
eap-mac-max	resets the maximum number of EAP clients allowed on the port to the default value (1).
non-eap-mac-max	resets the maximum number of non-EAP authenticated MAC addresses allowed to the default value (1).
non-eap-mac	resets the non-EAP MAC addresses to the default.
allow-non-eap-enable	resets control of non-EAP clients (MAC addresses) to the default (disabled).
radius-non-eap-enable	disables RADIUS authentication of non-EAP clients.
auto-non-eap-mhsa-enable	disables auto-authentication of non-EAP clients.
non-eap-phone-enable	disables authentication of Nortel IP Phone clients as non-EAP type.
use-radius-assigned-vlan	disables use of RADIUS-assigned VLAN values in the MHMA mode.

Parameter	Description
eap-packet-mode	Resets the EAP packet mode to the default (multicast).
eap-reauth-sec-mode	Resets reauthentication of the secondary mode to the default (disabled).

eapol multihost enable command

The **`eapol multihost enable`** command enables multihost support for EAPOL.

The syntax for the **`eapol multihost enable`** command is:

```
eapol multihost [port <portlist>] enable
```

where

`<portlist>` is the list of ports on which you want to enable EAPOL support. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies to all ports on the interface.

The default is disabled.

The **`eapol multihost [port <portlist>] enable`** command is executed in the Interface Configuration mode.

no eapol multihost enable command

The **`no eapol multihost enable`** command disables the EAPoL multihost.

The syntax for the **`no eapol multihost enable`** command is:

```
no eapol multihost [<portlist>] [enable]
[allow-non-eap-enable] [radius-non-eap-enable]
[auto-non-eap-mhsa-enable] [non-eap-phone-enable]
[use-radius-assigned-vlan]
```

no eapol multihost command parameters

Variable	Description
<portlist>	is the list of ports on which you want to disable EAPOL support. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies to all ports on the interface
enable	Disables eapol on the desired port(s).

radius-non-eap-enable	Disables RADIUS authentication of non-EAP clients.
allow-non-eap-enable	Disables control of non-EAP clients (MAC addresses).
auto-non-eap-mhsa-enable	Disables auto-authentication of non-EAP clients.
non-eap-phone-enable	Disables Nortel IP Phone clients.
use-radius-assigned-vlan	Disables use of RADIUS-assigned VLAN.

where

`<portlist>` is the list of ports on which you want to disable EAPoL support. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies to all ports on the interface.

The **`no eapol multihost enable`** command is executed in the Interface Configuration mode.

eapol multihost eap-mac-max command

The **`eapol multihost eap-mac-max`** command sets the maximum number of EAP clients.

The syntax for the **`eapol multihost eap-mac-max`** command is:

```
eapol multihost [port <portlist>] eap-mac-max <num>
```

where

`<portlist>` is the list of ports for which you are setting the maximum number of EAP clients. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies to all ports on the interface.
`<num>` is an integer in the range 1–32 that specifies the maximum number of EAP clients allowed. The default is 1.

The **`eapol multihost [port <portlist>] eap-mac-max`** command is executed in the Interface Configuration mode.

eapol multihost use radius-assigned-vlan command

To enable RADIUS-assigned VLAN use in the MHMA mode, use the following command in the global configuration mode:

```
eapol multihost [use-radius-assigned-vlan]
```

The following table outlines the parameters for this command:

eapol multihost [use-radius-assigned-vlan] parameters

Parameter	Description
use-radius-assigned-vlan	globally enables RADIUS-assigned VLAN use in the MHMA mode.

To enable RADIUS-assigned VLAN use in the MHMA mode for the desired interface, use the following command:

```
eapol multihost [port <portlist>] [use-radius-assigned-vlan]
```

The following table outlines the parameters for this command:

eapol multihost [use-radius-assigned-vlan] parameters: Interface mode

Parameter	Description
<portlist>	the port on which you want RADIUS-assigned VLAN use configured in the MHMA mode. You can enter a single port, several ports or a range of ports.
use-radius-assigned-vlan	enables RADIUS-assigned VLAN use on the desired interface.

no eapol multihost use radius-assigned-vlan command

To globally disable RADIUS-assigned VLAN use in MHMA mode, use one of the following commands in the global configuration mode:

```
no eapol multihost [use-radius-assigned-vlan]
```

or

```
default eapol multihost [use-radius-assigned-vlan]
```

The following tables outline the parameters for the **no** and **default** versions of this command respectively:

no eapol multihost [use-radius-assigned-vlan] parameters

Parameter	Description
use-radius-assigned-vlan	globally disables RADIUS-assigned VLAN use in the MHMA mode.

default eapol multihost [use-radius-assigned-vlan] parameters

Parameter	Description
use-radius-assigned-vlan	globally sets the default (disable) for RADIUS-assigned VLAN use in the MHMA mode.

To disable RADIUS-assigned VLAN use in the MHMA mode for the desired interface, use one of the following commands:

```
no eapol multihost [port <portlist>] [use-radius-assigned-
vlan]
```

or

```
default eapol multihost [port <portlist>] [use-radius-
assigned-vlan]
```

The following tables outline the parameters for the `no` and `default` versions of this command respectively:

no eapol multihost [use-radius-assigned-vlan] parameters: Interface mode

Parameter	Description
<portlist>	specifies the port on which you want RADIUS-assigned VLAN use disabled in the MHMA mode. You can enter a port, several ports or a range of ports.
use-radius-assigned-vlan	disables RADIUS-assigned VLAN use in the MHMA mode, on the desired interface.

default eapol multihost [use-radius-assigned-vlan] parameters: Interface mode

Parameter	Description
<portlist>	specifies the port on which you want RADIUS-assigned VLAN use disabled in the MHMA mode. You can enter a port, several ports or a range of ports.
use-radius-assigned-vlan	sets the default (disable) for RADIUS-assigned VLAN use in the MHMA mode, on the desired port.

Selecting the packet mode for EAP requests

With EAP support up to release 5.0.3, the switch transmits multicast packets at defined intervals (the default interval time is 30 seconds) to solicit potential EAP-capable devices. The PC then sends an EAP response and unicast transactions begin. Release 5.1 allows you to select the packet mode. This feature prevents repeated EAP responses from an EAP-capable device that has already been authenticated.

Use the following command to globally select the packet mode for EAP requests:

```
eapol multihost [eap-packet-mode {multicast | unicast}]
```

The following table outlines the parameters for this command:

eapol multihost [eap-packet-mode {multicast | unicast}] parameters

Parameter	Description
[eap-packet-mode {multicast | unicast}]	globally enables the desired packet mode (multicast or unicast) for EAP requests.

Use the following command to select the packet mode on the desired interface or on specific ports:

```
eapol multihost [port <portlist>] [eap-packet-mode {multicast
| unicast}]
```

The following table outlines the parameters for this command:

eapol multihost [eap-packet-mode {multicast | unicast}] parameters: Interface mode

Parameter	Description
<portlist>	the port or ports for which you want to select the packet mode. You can enter a single port, several ports or a range of ports.
[eap-packet-mode {multicast | unicast}]	enables the desired packet mode (multicast or unicast) on the desired port or ports.

Use one of the following commands to globally disable the selection of packet mode:

```
no eapol multihost [eap-packet-mode {multicast | unicast}]
```

or

```
default eapol multihost [eap-packet-mode {multicast |
unicast}]
```

The following tables outline the parameters for the **no** and **default** versions of this command, respectively:

no eapol multihost [eap-packet-mode {multicast | unicast}] parameters

Parameter	Description
[eap-packet-mode {multicast | unicast}]	globally disables selection of the packet mode.

default eapol multihost [eap-packet-mode {multicast | unicast}] parameters

Parameter	Description
[eap-packet-mode {multicast | unicast}]	globally sets the default (disable) for the selection of packet mode.

Use one of the following commands to disable the selection of packet mode on the desired interface:

```
no eapol multihost [port <portlist>][[eap-packet-mode
{multicast | unicast}]
```

or

```
default eapol multihost [<portlist>][eap-packet-mode
{multicast | unicast}]
```

The following tables outline the parameters for the **no** and **default** versions of this command, respectively:

no eapol multihost [eap-packet-mode {multicast | unicast}] command parameters

Parameter	Description
[eap-packet-mode {multicast | unicast}]	disables selection of packet mode on the desired interface.

default eapol multihost [eap-packet-mode {multicast | unicast}] command parameters

Parameter	Description
[eap-packet-mode {multicast | unicast}]	sets the default (disable) for the selection of packet mode on the desired interface.

Configuring support for non-EAPOL hosts on EAPOL-enabled ports

To configure support for non-EAPOL hosts on EAPOL-enabled ports, do the following:

1. Ensure that:

   a. EAPOL is enabled globally and locally (for the desired interface ports) (see "Configuring Extensible Authentication Protocol security" (page 76))

   b. the desired ports have been enabled for multihost mode (see "Configuring multihost support" (page 84))

   c. guest VLAN is disabled locally (for the desired interface ports) (see "Configuring guest VLANs" (page 83))

2. Enable non-EAPOL support globally on the switch and locally (for the desired interface ports), using one or both of the following authentication methods:

   a. local authentication (see "Enabling local authentication of non-EAPOL hosts on EAPOL-enabled ports" (page 93))

   b. RADIUS authentication (see "Enabling RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports" (page 93))

3. Configure
4. Specify the maximum number of non-EAPOL MAC addresses allowed on a port (see "Specifying the maximum number of non-EAPOL hosts allowed" (page 95)).
5. For local authentication only, identify the MAC addresses of non-EAPOL hosts allowed on the ports (see "Creating the allowed non-EAPOL MAC address list" (page 95)).

By default, support for non-EAPOL hosts on EAPOL-enabled ports is disabled.

Enabling local authentication of non-EAPOL hosts on EAPOL-enabled ports

For local authentication of non-EAPOL hosts on EAPOL-enabled ports, you must enable the feature globally on the switch and locally for ports on the interface.

To enable local authentication of non-EAPOL hosts globally on the switch, use the following command in Global configuration mode:

```
eapol multihost allow-non-eap-enable
```

To enable local authentication of non-EAPOL hosts for a specific port or for all ports on an interface, use the following command in Interface configuration mode:

```
eapol multihost [port <portlist>] allow-non-eap-enable
```

where

`<portlist>` is the list of ports on which you want to enable non-EAPOL hosts using local authentication. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies to all ports on the interface.

To discontinue local authentication of non-EAPOL hosts on EAPOL-enabled ports, use the **`no`** or **`default`** keywords at the start of the commands in both the Global and Interface configuration modes.

Enabling RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports

For RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports, you must enable the feature globally on the switch and locally for ports on the interface.

To enable RADIUS authentication of non-EAPOL hosts globally on the switch, use the following command in Global configuration mode:

```
eapol multihost radius-non-eap-enable
```

The following table outlines the parameters for this command:

eapol multihost radius-non-eap-enable command

Parameter	Description
radius-non-eap-enable	globally enables RADIUS authentication for non-EAPOL hosts.

To enable RADIUS authentication of non-EAPOL hosts for a specific port or for all ports on an interface, use the following command in Interface configuration mode:

```
eapol multihost [port <portlist>] radius-non-eap-enable
```

The following table outlines the parameters for this command:

eapol multihost radius-non-eap-enable command: Interface mode

Parameter	Description
<portlist>	the port or ports on which you want RADIUS authentication enabled. You can enter a single port, several ports or a range of ports. If you do not specify a port parameter, the command enables RADIUS authentication of non-EAP hosts on all ports on the interface.
radius-non-eap-enable	enables RADIUS authentication on the desired interface or on a specific port, for non-EAPOL hosts.

The default for this fature is ’disabled’.

To discontinue RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports, use the `no` or `default` keywords at the start of the commands in both the Global and Interface configuration modes.

Configuring the format of the RADIUS password attribute when authenticating non-EAP MAC addresses using RADIUS

To configure the format of the RADIUS password when authenticating non-EAP MAC addresses using RADIUS, use the following command in the Global configuration mode:

```
eapol multihost non-eap-pwd-fmt
```

The syntax for the `eapol multihost non-eap-pwd-fmt` command is:

```
eapol multihost non-eap-pwd-fmt { [ip-addr] [mac-addr]
[port-number] }
```

The following table outlines the parameters for this command:

eapol multihost non-eap-pwd-fmt parameters

Parameter	Description
<ip-addr>	the IP address of the non-EAP client.
<mac-addr>	the MAC address of the non-EAP client.
<port-number>	the port number for which you want the RADIUS password attribute configured.

To discontinue configuration of the RADIUS password attribute format, use the `no` or `default` keywords at the start of the commands, in the Global configuration mode.

Specifying the maximum number of non-EAPOL hosts allowed

To configure the maximum number of non-EAPOL hosts allowed for a specific port or for all ports on an interface, use the following command in Interface configuration mode:

```
eapol multihost [port <portlist>] non-eap-mac-max <value>
```

where

`<portlist>` is the list of ports to which you want the setting to apply. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command sets the value for all ports on the interface.
`<value>` is an integer in the range 1–32 that specifies the maximum number of non-EAPOL clients allowed on the port at any one time. The default is 1.

> ***Note:*** The configurable maximum number of non-EAPOL clients for each port is 32, but Nortel expects that the usual maximum allowed for each port will be lower. Nortel expects that the combined maximum will be approximately 200 for each box and 800 for a stack.

Creating the allowed non-EAPOL MAC address list

To specify the MAC addresses of non-EAPOL hosts allowed on a specific port or on all ports on an interface, for local authentication, use the following command in Interface configuration mode:

```
eapol multihost non-eap-mac [port <portlist>] <H.H.H>
```

where

`<portlist>` is the list of ports on which you want to allow the specified non-EAPOL hosts. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies to all ports on the interface.

`<H.H.H>` is the MAC address of the allowed non-EAPOL host.

Viewing non-EAPOL host settings and activity

Various show commands allow you to view:

- global settings (see "Viewing global settings for non-EAPOL hosts" (page 96))
- port settings (see "Viewing port settings for non-EAPOL hosts" (page 96))
- allowed MAC addresses, for local authentication (see "Viewing allowed MAC addresses" (page 96))
- current non-EAPOL hosts active on the switch (see "Viewing current non-EAPOL host activity" (page 97))
- status in the Privilege Exec mode (see "show eapol multihost status command" (page 78)).

Viewing global settings for non-EAPOL hosts To view global settings for non-EAPOL hosts on EAPOL-enabled ports, use the following command in Privileged Exec, Global configuration, or Interface configuration mode:

```
show eapol multihost
```

The display shows whether local and RADIUS authentication of non-EAPOL clients is enabled or disabled.

Viewing port settings for non-EAPOL hosts To view non-EAPOL support settings for each port, use the following command in Privileged Exec, Global configuration, or Interface configuration mode:

```
show eapol multihost interface [<portlist>]
```

where

`<portlist>` is the list of ports you want to view. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command displays all ports.

For each port, the display shows whether local and RADIUS authentication of non-EAPOL clients is enabled or disabled, and the maximum number of non-EAPOL clients allowed at a time.

Viewing allowed MAC addresses To view the MAC addresses of non-EAPOL hosts allowed to access ports on an interface, use the following command in Privileged Exec, Global configuration, or Interface configuration mode:

```
show eapol multihost non-eap-mac interface [<portlist>]
```

where

`<portlist>` is the list of ports you want to view. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command displays all ports.

The display lists the ports and the associated allowed MAC addresses.

Viewing current non-EAPOL host activity To view information about non-EAPOL hosts currently active on the switch, use the following command in Privileged Exec, Global configuration, or Interface configuration mode:

```
show eapol multihost non-eap-mac status [<portlist>]
```

where

`<portlist>` is the list of ports you want to view. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command displays all ports.

The following example shows sample output for the command.

```
5530-24TFD#show eapol multihost non-eap-mac status
Unit/Port Client MAC Address State
--------- --------------------------- -----------------------
1/5 00:01:00:07:00:01 Authenticated By RADIUS
1/7 00:02:B3:BC:AF:6E Authenticated By RADIUS
1/7 00:C0:C1:C2:C3:C4 Authenticated Locally
1/7 00:C0:C1:C2:C3:C7 Authenticated Locally
2/21 00:02:00:21:00:80 Authenticated By RADIUS
3/12 00:03:12:21:00:82 Auto-Learned For MHSA
3/15 00:0A:E4:01:10:21 Authenticated For IP Telephony
3/15 00:0A:E4:01:10:22 Authenticated For IP Telephony

----------------------------------------------------------------
5530-24TFD#
```

Enabling Nortel IP Phone clients on an EAP-enabled port

Enable this feature to allow a Nortel IP Phone client and an EAP PC to exist together on a port. To enable Nortel IP Phone clients on an EAP-enabled port, do the following:

1. Ensure that:
   - EAP is enabled globally and locally (on the desired interface ports). (See "Configuring Extensible Authentication Protocol security" (page 76)).
   - Multihost is enabled on the desired ports. (See "Configuring multihost support" (page 84)).
   - NonEAP is enabled globally and locally (on the desired interface ports). (See "Configuring support for non-EAPOL hosts on EAPOL-enabled ports" (page 92)).

- Filtering is enabled (to capture DHCP packets and to look for the Nortel Phone Signature).

> **ATTENTION**
>
> Nortel recommends that the following two features not be enabled at the same time:
>
> - Guest VLAN.
>
>   This is to ensure that the Call server and VoIP information packets the phone receives from the DHCP server are sent on the configured VLAN, so correct information (such as the IP address) is obtained.
>
> - EAP at the phone.

2. Enable Nortel IP Phone clients globally on the switch. (See "Globally enabling Nortel IP Phone clients as a non-EAP type" (page 98)).
3. Enable Nortel IP Phone clients locally or for specific ports on the interface. (See "Enabling Nortel IP Phone clients in the interface mode" (page 99)).
4. Specify the maximum number of non-EAPoL MAC addresses allowed: the maximum number allowed is 32.

Globally enabling Nortel IP Phone clients as a non-EAP type

To globally enable Nortel IP Phone clients as a non-EAP type, use the following command in the global configuration mode:

```
eapol multihost {[non-eap-phone-enable]}
```

The following table outlines the parameters for this command:

eapol multihost non-eap-phone-enable parameters

Parameter	Description
non-eap-phone-enable	globally enables Nortel IP Phone clients as a non-EAP type.

To globally disable Nortel IP Phone clients as a non-EAP type, use one of the following commands in the global configuration mode:

```
no eapol multihost {[non-eap-phone-enable]}
```

or

```
default eapol multihost {[non-eap-phone-enable]}
```

The following tables outline the parameters for the **`no`** and **`default`** versions of this command respectively:

no eapol multihost non-eap-phone-enable parameters

Parameter	Description
non-eap-phone-enable	globally disables Nortel IP Phone clients as a non-EAP type.

default eapol multihost non-eap-phone-enable parameters

Parameter	Description
non-eap-phone-enable	globally sets the default (disable) for Nortel IP Phone clients as a non-EAP type.

Enabling Nortel IP Phone clients in the interface mode

To enable Nortel IP Phone clients in the interface mode, use the following command:

```
eapol multihost [port <portlist>] [non-eap-phone-enable]
```

eapol multihost non-eap-phone-enable parameters: Interface mode

Parameter	Description
<portlist>	the port or ports on which you want Nortel IP Phone clients enabled as a non-EAP type. You can enter a single port, several ports or a range of ports.
non-eap-phone-enable	enables Nortel IP Phone clients as a non-EAP type, on the desired port or ports.

To disable Nortel IP Phone clients in the interface mode, use one of the following commands:

```
no eapol multihost [port <portlist>] [non-eap-phone-enable]
```

or

```
default eapol multihost [port <portlist>] [non-eap-phone-
enable]
```

The following tables outline the parameters for the **`no`** and **`default`** versions of this command respectively:

no eapol multihost non-eap-phone-enable parameters: Interface mode

Parameter	Description
<portlist>	the port or ports on which you want Nortel IP Phone clients disabled as a non-EAP type. You can enter a single port, several ports or a range of ports.
non-eap-phone-enable	disables Nortel IP Phone clients as a non-EAP type, on the desired port or ports.

default eapol multihost non-eap-phone-enable parameters: Interface mode

Parameter	Description
<portlist>	the port or ports on which you want the defaults for Nortel IP Phone clients set. You can enter a single port, several ports or a range of ports.
non-eap-phone-enable	sets the default (disable) for Nortel IP Phone clients, on the desired port or ports.

Configuring MHSA

To configure MHSA support, do the following:

1. Ensure that:
   a. EAP is enabled globally and locally (for the desired interface ports) (see "Configuring Extensible Authentication Protocol security" (page 76))
   b. the desired ports have been enabled for Multihost (see "Configuring multihost support" (page 84))
   c. guest VLAN is disabled locally (for the desired interface ports) (see "Configuring guest VLANs" (page 83))
2. Enable MHSA globally on the switch (see "Globally enabling support for MHSA" (page 101)).
3. Configure MHSA settings for the interface or for specific ports on the interface (see "Configuring interface and port settings for MHSA" (page 101)):
   a. Enable MHSA support.
   b. Specify the maximum number of non-EAPOL MAC addresses allowed.

By default, MHSA support on EAP-enabled ports is disabled.

Globally enabling support for MHSA

To enable support for MHSA globally on the switch, use the following command in Global configuration mode:

```
eapol multihost auto-non-eap-mhsa-enable
```

To discontinue support for MHSA globally on the switch, use one of the following commands in Global configuration mode:

```
no eapol multihost auto-non-eap-mhsa-enable
```

```
default eapol multihost auto-non-eap-mhsa-enable
```

Configuring interface and port settings for MHSA

To configure MHSA settings for a specific port or for all ports on an interface, use the following command in Interface configuration mode:

```
eapol multihost [port <portlist>]
```

where

<portlist> is the list of ports to which you want the settings to apply. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies the settings to all ports on the interface.

This command includes the following parameters for configuring MHSA:

eapol multihost [port <portlist> followed by:	
auto-non-eap-mhsa-enable	Enables MHSA on the port. The default is disabled. To disable MHSA, use the **no** or **default** keywords at the start of the command.
non-eap-mac-max <value>	Sets the maximum number of non-EAPOL clients allowed on the port at any one time. • <value> is an integer in the range 1 to 32. The default is 1. ***Note:*** The configurable maximum number of non-EAPOL clients for each port is 32, but Nortel expects that the usual maximum allowed for each port will be lower. Nortel expects that the combined maximum will be approximately 200 for each box and 800 for a stack.

Viewing MHSA settings and activity

For information about the commands to view MHSA settings and non-EAPOL host activity, see "Viewing non-EAPOL host settings and activity" (page 96).

Configuring RADIUS accounting

RADIUS accounting utilizes the same network server settings used for RADIUS authentication. For information about the commands to configure the RADIUS server settings for the Nortel Ethernet Routing Switch 5500 Series, see "Configuring RADIUS server settings" (page 74).

The RADIUS accounting UDP port is the RADIUS authentication port +1. By default, therefore, the RADIUS accounting UDP port is port 1813.

By default, RADIUS accounting is disabled.

To enable RADIUS accounting, use the following command in Global or Interface configuration mode:

```
radius accounting enable
```

To discontinue RADIUS accounting, use the following command in Global or Interface configuration mode:

```
no radius accounting enable
```

To view RADIUS accounting settings, use the following command in Global or Interface configuration mode:

```
show radius-server
```

For a sample of the command output, see "Viewing RADIUS information" (page 75).

Configuring TACACS+

For information about the function and operation of TACACS+ in a Nortel Ethernet Routing Switch 5500 Series network, see "TACACS+" (page 39).

To configure TACACS+ to perform AAA services for system users, do the following:

1. Configure the TACACS+ server itself. Refer to the vendor documentation for your server for specific configuration procedures. For sample configurations, see "TACACS+ server configuration examples" (page 315).
2. Configure TACACS+ server settings on the switch (see "Configuring TACACS+ server settings" (page 103)).
3. Enable TACACS+ services over serial or Telnet connections (see "Enabling remote TACACS+ services" (page 104).
4. Enable TACACS+ authorization and specify privilege levels (see "Enabling TACACS+ authorization" (page 104)).

5. Enable TACACS+ accounting (see "Enabling TACACS+ accounting" (page 105)).

   Note: You can enable TACACS+ authorization without enabling TACACS+ accounting, and vice versa.

Configuring TACACS+ server settings

To add a TACACS+ server, use the following command in Global or Interface configuration mode:

```
tacacs server
```

The **`tacacs server`** command includes the following parameters:

Parameter	Description
host <IPaddr>	Specifies the IP address of the primary server you want to add or configure.
key <key>	Specifies the secret authentication and encryption key used for all communications between the NAS and the TACACS+ server. The key, also referred to as the *shared secret*, must be the same as the one defined on the server. You are prompted to confirm the key when you enter it. ***Note:*** The key parameter is a required parameter when you create a new server entry. The parameter is optional when you are modifying an existing entry.
[secondary host <IPaddr>]	Specifies the IP address of the secondary server. The secondary server is used only if the primary server does not respond.
[port <port>]	Specifies the TCP port for TACACS+ where **`port`** is an integer in the range 0–65535 The default port number is 49.

To delete a TACACS+ server, use one of the following commands in Global or Interface configuration mode:

```
no tacacs
```

```
default tacacs
```

The commands erase settings for the TACACS+ primary and secondary servers and secret key, and restore default port settings.

Enabling remote TACACS+ services

To enable TACACS+ to provide services to remote users over serial or Telnet connections, use the following commands in Global or Interface configuration mode.

For serial connections:

```
cli password serial tacacs
```

For Telnet connections:

```
cli password telnet tacacs
```

You must configure a TACACS+ server on the switch before you can enable remote TACACS+ services. For information about configuring the primary TACACS+ server and shared secret, see "Configuring TACACS+ server settings" (page 103).

Enabling TACACS+ authorization

To enable TACACS+ authorization globally on the switch, use the following command in Global or Interface configuration mode:

```
tacacs authorization enable
```

To disable TACACS+ authorization globally on the switch, use the following command in Global or Interface configuration mode:

```
tacacs authorization disable
```

The default is disabled.

Setting authorization privilege levels

The preconfigured privilege levels control which commands can be executed. If a user has been assigned a privilege level for which authorization has been enabled, TACACS+ authorizes the authenticated user to execute a specific command only if the command is allowed for that privilege level.

To specify the privilege levels to which authorization applies, use the following command in Global or Interface configuration mode:

```
tacacs authorization level all|<level>|none
```

where

all = authorization is enabled for all privilege levels.
<level> = an integer in the range 0–15 that specifies the privilege levels for which authorization is enabled. You can enter a single level, a range of levels, or several levels. For any levels you do not specify,

authorization does not apply, and users assigned to these levels can execute all commands.
`none` = authorization is not enabled for any privilege level. All users can execute any command available on the switch.

The default is none.

Enabling TACACS+ accounting

To enable TACACS+ accounting globally on the switch, use the following command in Global or Interface configuration mode:

```
tacacs accounting enable
```

To disable TACACS+ accounting globally on the switch, use the following command in Global or Interface configuration mode:

```
tacacs accounting disable
```

The default is disabled.

Viewing TACACS+ information

To display TACACS+ configuration status, enter the following command from any mode:

```
show tacacs
```

The following is an example of sample output for the command.

```
5530-24TFD(config)#show tacacs
Primary Host:  10.10.10.20
Secondary Host:  0.0.0.0
Port:  49
Key:  ***************
TACACS+ authorization is enabled
Authorization is enabled on levels : 1-6
TACACS+ accounting is disabled
5530-24TFD(config)#
```

Configuring IP Manager

To configure the IP Manager to control management access to the switch, do the following:

- Enable IP Manager.
- Configure the IP Manager list.

Enabling IP Manager

To enable IP Manager to control Telnet, SNMP, or HTTP access, use the following command in Global configuration mode:

```
ipmgr {telnet|snmp|web}
```

where

telnet enables the IP Manager list check for Telnet access
snmp enables the IP Manager list check for SNMP, including Device Manager
web enables the IP Manager list check for the Web-based management system

To disable IP Manager for a management system, use the **no** keyword at the start of the command.

Configuring the IP Manager list

To specify the source IP addresses or address ranges that have access the switch or the stack when IP Manager is enabled, use the following command in Global configuration mode:

```
ipmgr source-ip  <list ID>  <IPaddr>  [mask  <mask>]
```

where

<list ID> is an integer in the range 1-50 that uniquely identifies the entry in the IP Manager list

The **ipmgr source-ip <list ID>** command includes the following parameters for configuring the IP Manager list:

Parameter	Description
<IPaddr>	Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation.
[mask <mask>]	Specifies the subnet mask from which access is allowed. Enter the IP mask in dotted-decimal notation.

Removing IP Manager list entries

To deny access to the switch or stack for specified source IP addresses or address ranges, use the following command in Global configuration mode:

```
no ipmgr source-ip [<list ID>]
```

where

<list ID> is an integer in the range 1-50 that uniquely identifies the entry in the IP Manager list

The command sets both the IP address and mask for the specified entry to 255.255.255.255. If you do not specify a **<list ID>** value, the command resets the whole list to factory defaults.

Viewing IP Manager settings

To view IP Manager settings, use the following command in any mode:

```
show ipmgr
```

The command displays:

- whether Telnet, SNMP, and Web access are enabled
- whether the IP Manager list is being used to control access to Telnet, SNMP, and the Web-based management system
- the current IP Manager list configuration

Configuring password security

The CLI commands detailed in this section are used to manage password security features. These commands can be used in the Global Configuration and Interface Configuration command modes.

password security command

The **password security** command enables the Password Security feature on the Nortel Ethernet Routing Switch 5500 Series.

The syntax of the **password security** command is:

```
password security
```

no password security command

The **no password security** command disables the Password Security feature on the Nortel Ethernet Routing Switch 5500 Series.

The syntax for the **no password security** command is:

```
no password security
```

Configuring the number of retries

To configure the number of times a user can retry a password, use the following command in Global or Interface Configuration mode:

```
telnet-access retry <number>
```

where

number is an integer in the range 1-100 that specifies the allowed number of failed log on attempts. The default is 3.

Displaying CLI Audit log

The CLI audit provides a means for tracking CLI commands. The **show audit log** command displays the command history audit log stored in NVRAM. The syntax for the **show audit log** command is:

```
show audit log [asccfg | serial | telnet]
```

The **show audit log** command is in the Privileged EXEC mode.

The following table describes the parameters and variables for the **`show audit log`** command.

Parameter	Description
asccfg	Displays the audit log for ASCII configuration.
serial	Displays the audit log for serial connections.
telnet	Displays the audit log for Telnet and SSH connections.

Secure Socket Layer services

The following table lists the CLI commands available for working with Secure Socket Layer (SSL).

SSL commands

Command	Description
[no] ssl	Enables or disables SSL. The Web server operates in a secure mode when SSL is enabled and in non-secure mode when the SSL server is disabled.
[no] ssl certificate	Creates or deletes a certificate. The new certificate is used only on the next system reset or SSL server reset. The new certificate is stored in the NVRAM with the file name SSLCERT.DAT. The new certificate file replaces the existing file. On deletion, the certificate in NVRAM is also deleted. The current SSL server operation is not affected by the create or delete operation.
ssl reset	Resets the SSL server. If SSL is enabled, the SSL server is restarted and initialized with the certificate that is stored in the NVRAM. Any existing SSL connections are closed. If SSL is not enabled, the existing non-secure connection is also closed and the non-secure operation resumes.
show ssl	Shows the SSL server configuration and SSL server state. Refer to "Server state information" (page 109) for more information.
show ssl certificate	Displays the certificate which is stored in the NVRAM and is used by the SSL server.

The following table describes the output for the **`show ssl`** command.

Server state information

Field	Description
WEB Server SSL secured	Shows whether the Web server is using an SSL connection.
SSL server state	Displays one of the following states: • Un-initialized: The server is not running. • Certificate Initialization: The server is generating a certificate during its initialization phase. • Active: The server is initialized and running.
SSL Certificate: Generation in progress	Shows whether SSL is in the process of generating a certificate. The SSL server generates a certificate during server startup initialization, or the CLI user can regenerate a new certificate.
SSL Certificate: Saved in NVRAM	Shows whether an SSL certificate exists in the NVRAM. The SSL certificate is not present if the system is being initialized for the first time or the CLI user has deleted the certificate.

Secure Shell protocol

Secure Shell protocol is used to improve Telnet and provide a secure access to the CLI interface. There are two versions of the SSH Protocol. The Nortel Ethernet Routing Switch 5500 Series SSH supports SSH2.

The following CLI commands are used in the configuration and management of SSH.

show ssh command

This command displays information about all active SSH sessions and on other general SSH settings.

The syntax for the **show ssh** command is:

```
show ssh {global|session|download-auth-key}
```

"show ssh parameters" (page 109) outlines the parameters for this command.

show ssh parameters

Parameter	Description
download-auth-key	Display authorization key and TFTP server IP address

Parameter	Description
global	Display general SSH settings
session	Display SSH session info

The **show ssh global** command is executed in the Privileged EXEC command mode.

ssh dsa-host-key command

The **ssh dsa-host-key** command triggers the DSA key regeneration.

The syntax for the **ssh dsa-host-key** command is:

```
ssh dsa-host-key
```

The command is executed in the Global Configuration command mode.

The **ssh dsa-host-key** command has no parameters or variables.

no ssh dsa-host-key command

The **no ssh dsa-host-key** command deletes the DSA keys in the switch. A new DSA key can be generated by executing **dsa-host-key** or **SSH enable** commands.

The syntax for the **no ssh dsa-host-key** command is:

```
no ssh dsa-host-key
```

The **no ssh dsa-host-key** command is executed in the Global Configuration command mode.

The **no ssh dsa-host-key** command has no parameters or variables.

ssh download-auth-key command

The **ssh download-auth-key** command downloads the DSA authentication key into the switch from the specified TFTP server or from the USB stick, if available.

The syntax for the **ssh download-auth-key** command is:

```
ssh download-auth-key [<ip>] [<key-name>] [usb]
```

"ssh download-auth-key parameters" (page 111) outlines the parameters for this command.

ssh download-auth-key parameters

Parameter	Description
<ip>	Specify the TFTP server IP address
key-name	Specify the TFTP/USB filename
usb	Specify whether download SSH auth key from the USB stick Available only if the device has USB port.

The **ssh download-auth-key** command is executed in the Global Configuration command mode.

no ssh dsa-auth-key command

The **no ssh dsa-auth-key** command deletes the DSA authentication key stored in the switch.

The syntax for the **no ssh dsa-auth-key** command is:

```
no ssh dsa-auth-key
```

The **no ssh dsa-auth-key** command is executed in the Global Configuration command mode.

ssh command

The **ssh** command enables SSH in a non secure mode. If the host keys do not exist, they are generated.

The syntax for the **ssh** command is:

```
ssh
```

The **ssh** command is executed in the Global Configuration command mode.

This command has no parameters.

no ssh command

The **no ssh** command disables SSH.

The syntax for the **no ssh** command is:

```
no ssh {dsa-auth|dsa-auth-key|dsa-host-key|pass-auth}
```

"no ssh parameters" (page 111) outlines the parameters for this command.

no ssh parameters

Parameter	Description
dsa-auth	Disable SSH DSA authentication

Parameter	Description
dsa-auth-key	Delete SSH DSA auth key
dsa-host-key	Delete SSH DSA host key
pass-auth	Disable SSH password authentication

The **`no ssh`** command is executed in the Global Configuration command mode.

ssh secure command

The **`ssh secure`** command disables web, SNMP, and Telnet management interfaces permanently.

The **`no ssh`** command does NOT turn them back on; they must be re-enabled manually. A warning message is issued to the user to re-enable one of the other interfaces before turning off SSH secure mode.

The syntax for the **`ssh secure`** command is:

```
ssh secure
```

The **`ssh secure`** command is executed in the Global Configuration command mode.

ssh dsa-auth command

The **`ssh dsa-auth`** command enables the user log on using DSA key authentication.

The syntax for the command is:

```
ssh dsa-auth
```

The **`ssh dsa-auth`** command is executed in the Global Configuration command mode.

no ssh dsa-auth

The **`no ssh dsa-auth`** command disables user log on using DSA key authentication.

The syntax for the **`no ssh dsa-auth`** command is:

```
no ssh dsa-auth
```

The **`no ssh dsa-auth`** command is executed in the Global Configuration command mode.

default ssh dsa-auth command

The **`default ssh dsa-auth`** command enables the user log on using the DSA key authentication.

The syntax for the **`default ssh dsa-auth`** command is:

```
default ssh dsa-auth
```

The **`default ssh dsa-auth`** command is executed in the Global Configuration command mode.

ssh pass-auth command

The **`ssh pass-auth`** command enables user log on using the password authentication method.

The syntax for the **`ssh pass-auth`** command is:

```
ssh pass-auth
```

The **`ssh pass-auth`** command is executed in the Global Configuration command mode.

no ssh pass-auth command

The **`no ssh pass-auth`** command disables user log on using password authentication.

The syntax for the **`no ssh pass-auth`** command is:

```
no ssh pass-auth
```

The **`no ssh pass-auth`** command is executed in the Global Configuration command mode.

default ssh pass-auth command

The **`default ssh pass-auth`** command enables user log on using password authentication.

The syntax for the **`default ssh pass-auth`** command is:

```
default ssh pass-auth
```

The **`default ssh pass-auth`** command is executed in the Global Configuration command mode.

ssh port command

The **`ssh port`** command sets the TCP port for the SSH daemon.

The syntax for the **`ssh port`** command is:

```
ssh port  <1-65535>
```

Substitute the**<1-65535>** with the number of the TCP port to be used.

The **ssh port** command is executed in the Global Configuration command mode.

default ssh port command

The **default ssh port** command sets the default TCP port for the SSH daemon.

The syntax for the **default ssh port** command is:

```
default ssh port
```

The **default ssh port** command is executed in the Global Configuration command mode.

ssh timeout command

The **ssh timeout** command sets the authentication timeout, in seconds.

The syntax of the **ssh timeout** command is:

```
ssh timeout  <1-120>
```

Substitute **<1-120>** with the desired number of seconds.

The **ssh timeout** command is executed in the Global Configuration command mode.

default ssh timeout command

The **default ssh timeout** command sets the default authentication timeout to 60 seconds.

The syntax for the **default ssh timeout** command is:

```
default ssh timeout
```

The **default ssh timeout** command is executed in the Global Configuration command mode.

Configuring IP Source Guard

For information about the function and operation of IP Source Guard in a Nortel Ethernet Routing Switch 5500 Series network, see "IP Source Guard" (page 53).

For information about configuring IP Source Guard through the Nortel Networks Command Line Interface (NNCLI), see "IP Source Guard Configuration" (page 133).

For information about configuring IP Source Guard through the Java Device Manager (JDM), see "Configuring IP Source Guard using the Java Device Manager" (page 184).

Configuring DHCP snooping

For information about the function and operation of DHCP snooping in a Nortel Ethernet Routing Switch 5500 Series network, see "DHCP snooping" (page 55).

To configure DHCP snooping, do the following:

1. Enable DHCP snooping globally (see "Enabling DHCP snooping globally" (page 115)).
2. Enable DHCP snooping on the VLANs (see "Enabling DHCP snooping on the VLANs" (page 115)).
3. Identify the ports as trusted (DHCP packets are forwarded automatically) or untrusted (DHCP packets are filtered through DHCP snooping) (see "Configuring trusted and untrusted ports" (page 116)).

Enabling DHCP snooping globally

Before DHCP snooping can function on a VLAN or port, you must enable DHCP snooping globally. If DHCP snooping is disabled globally, the switch forwards DHCP reply packets to all applicable ports, regardless of whether the port is trusted or untrusted.

To enable DHCP snooping globally, use the following command in Global configuration mode:

```
ip dhcp-snooping [enable]
```

The default is disabled.

To disable DHCP snooping globally, use one of the following commands in Global configuration mode:

```
no ip dhcp-snooping
```

```
default ip dhcp-snooping [enable]
```

Enabling DHCP snooping on the VLANs

You must enable DHCP snooping separately for each VLAN. If DHCP snooping is disabled on a VLAN, the switch forwards DHCP reply packets to all applicable ports, regardless of whether the port is trusted or untrusted.

To enable DHCP snooping on a VLAN, use the following command in Global configuration mode:

```
ip dhcp-snooping vlan <vlanID>
```

where

`<vlanID>` is an integer in the range 1–4094 specifying the preconfigured VLAN on which you want to enable DHCP snooping

The default is disabled.

To disable DHCP snooping on a VLAN, use the following command in Global configuration mode:

```
no ip dhcp-snooping vlan <vlanID>
```

where

`<vlanID>` is an integer in the range 1–4094 specifying the preconfigured VLAN on which you want to disable DHCP snooping. If you do not specify a VLAN ID, DHCP snooping is disabled on all VLANs.

Configuring trusted and untrusted ports

To specify whether a particular port or range of ports is trusted (DHCP replies are forwarded automatically) or untrusted (DHCP replies are filtered through DHCP snooping), use the following command in Interface configuration mode:

```
ip dhcp-snooping [port <portlist>] <trusted|untrusted>
```

where

`<portlist>` is the physical port number of the port you want to configure. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port number, the command applies to the ports specified upon entering the Interface configuration mode.

The default is untrusted.

To return a port or range of ports to default values, use the following command in Interface configuration mode:

```
default ip dhcp-snooping <portlist>
```

where

`<portlist>` is the physical port number of the port you want to configure. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port number, the command applies to the ports specified upon entering the Interface configuration mode.

To return all ports in the interface to default values, use the following command in Interface configuration mode:

```
default ip dhcp-snooping port ALL
```

Viewing DHCP snooping settings

To view the global DHCP snooping state and the VLANs on which DHCP snooping has been enabled, use the following command in Global or Interface configuration mode:

```
show ip dhcp-snooping
```

To view only the VLANs on which DHCP snooping has been enabled, use the following command in Global or Interface configuration mode:

```
show ip dhcp-snooping vlan
```

The output lists only the VLANs enabled for DHCP snooping.

To view port settings, use the following command in Global or Interface configuration mode:

```
show ip dchp-snooping interface [<interface type>] [<port>]
```

The output lists the ports and their associated DHCP snooping status (trusted or untrusted). If you specify the interface type or port as part of the command, the output includes only the ports specified. If you do not specify the interface type or port as part of the command, the output displays all ports.

Viewing the DHCP binding table

To view the DHCP binding table, use the following command in Global or Interface configuration mode:

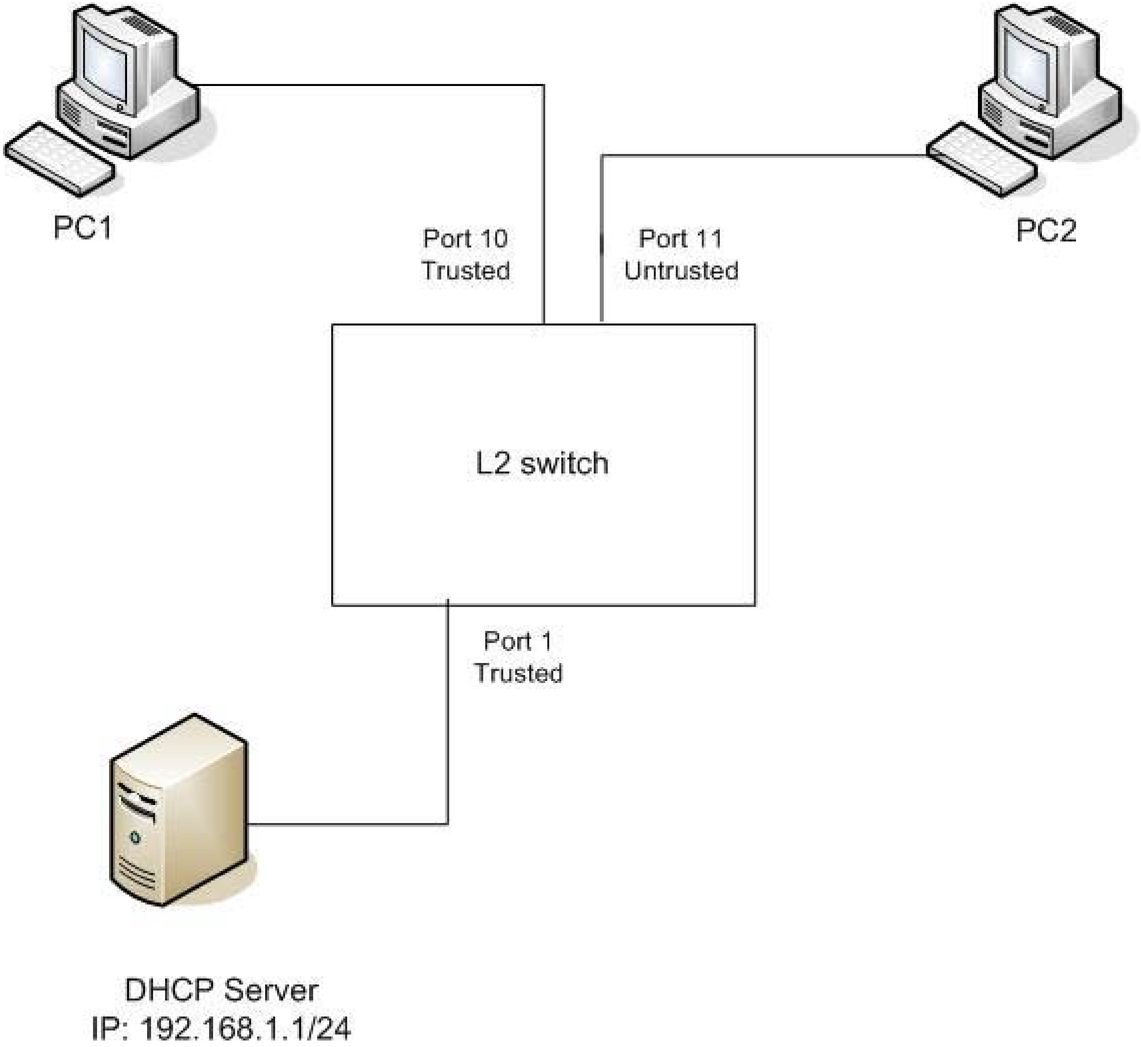
```
show ip dhcp-snooping binding
```

The output reports the total number of entries and lists current DHCP lease information for clients on untrusted ports: source MAC address, IP address, lease duration in seconds, VLAN ID, and port.

DHCP Snooping layer 2 configuration example

"Layer 2 configuration example" (page 118)depicts the network setup for this example. PC1 and PC2 act as DHCP clients. The device under test (DUT) is in layer 2 mode and must be configured with DHCP Snooping to increase network security. The DHCP server and clients must belong to the same L2 VLAN (VLAN #1 by default). You can configure the DHCP client lease time on the DHCP server.

Layer 2 configuration example



The DHCP server port must always be Trusted, because Untrusted DHCP ports drop DHCP replies coming from the DHCP server. All ports are DHCP Untrusted by default. You should connect DHCP clients to Untrusted DHCP ports, however, PC1 is connected to a Trusted port for this configuration example case.

This configuration example illustrates a security hole that permits PC1 to install a fake DHCP Server. Port10 (DHCP Trusted) allows DHCP replies to be forwarded to PC2 in this case.

DHCP Snooping configuration commands

The following section describes the detailed CLI commands required to configure DHCP Snooping for this example.

```
>en
#configure terminal
(config)#ip dhcp-snooping
(config)#ip dhcp-snooping vlan 1
(config)# interface fastEthernet 1,10
(config-if)#ip dhcp-snooping trusted
(config-if)#exit
```

Verifying the DHCP Snooping settings

This section describes the commands used to verify the settings and the expected response to each command.

```
(config)#show ip dhcp-snooping
```

```
Global DHCP snooping state: Enabled
DHCP
VLAN Snooping
---- --------
1    Enabled
```

```
(config)#show ip dhcp-snooping  interface 1,10,11
```

```
DHCP
 Port Snooping
---- --------
1    Trusted
10   Trusted
11   Untrusted
```

```
(config)#show ip dhcp-snooping binding
```

```
MAC                IP                Lease (sec)  VID   Port
---------------------------------------------------------------
Total Entries: 0
```

```
(config)#show running-config
```

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.159 enable configure terminal
!
! *** CORE ***
! autosave enable mac-address-table
aging-time 300
autotopology
no radius-server
radius-server host 0.0.0.0
radius-server secondary-host 0.0.0.0
radius-server port 1812
! radius-server key ********
radius-server timeout 2
tacacs server host  0.0.0.0
tacacs server secondary-host  0.0.0.0
tacacs server port 49
tacacs authorization disable
tacacs authorization level NONE
tacacs accounting disable
telnet-access login-timeout 1
telnet-access retry 3
telnet-access inactive-timeout 15
telnet-access logging all
cli password switch serial none
cli password switch telnet none
! cli password switch read-only "********"
! cli password switch read-write "********"
configure network load-on-boot disable
tftp-server 0.0.0.0
! ...
!
! *** DHCP SNOOPING *** Note information in this section.
!
ip dhcp-snooping
no ip dhcp-snooping vlan
ip dhcp-snooping vlan 1
interface FastEthernet ALL
default ip dhcp-snooping
ip dhcp-snooping port 1,10 trusted
exit
!
! *** ARP INPSECTION *** Note information in this section
!
no ip arp-inspection vlan
interface FastEthernet ALL
default ip arp-inspection
exit
! ...
```

Renew the IP addresses for PC1 and PC2. Both PCs obtain IP addresses from the DHCP server. A DHCP binding entry for PC2 appears in the DHCP binding table. No binding extry for PC1 exists because port10 is DHCP Trusted.

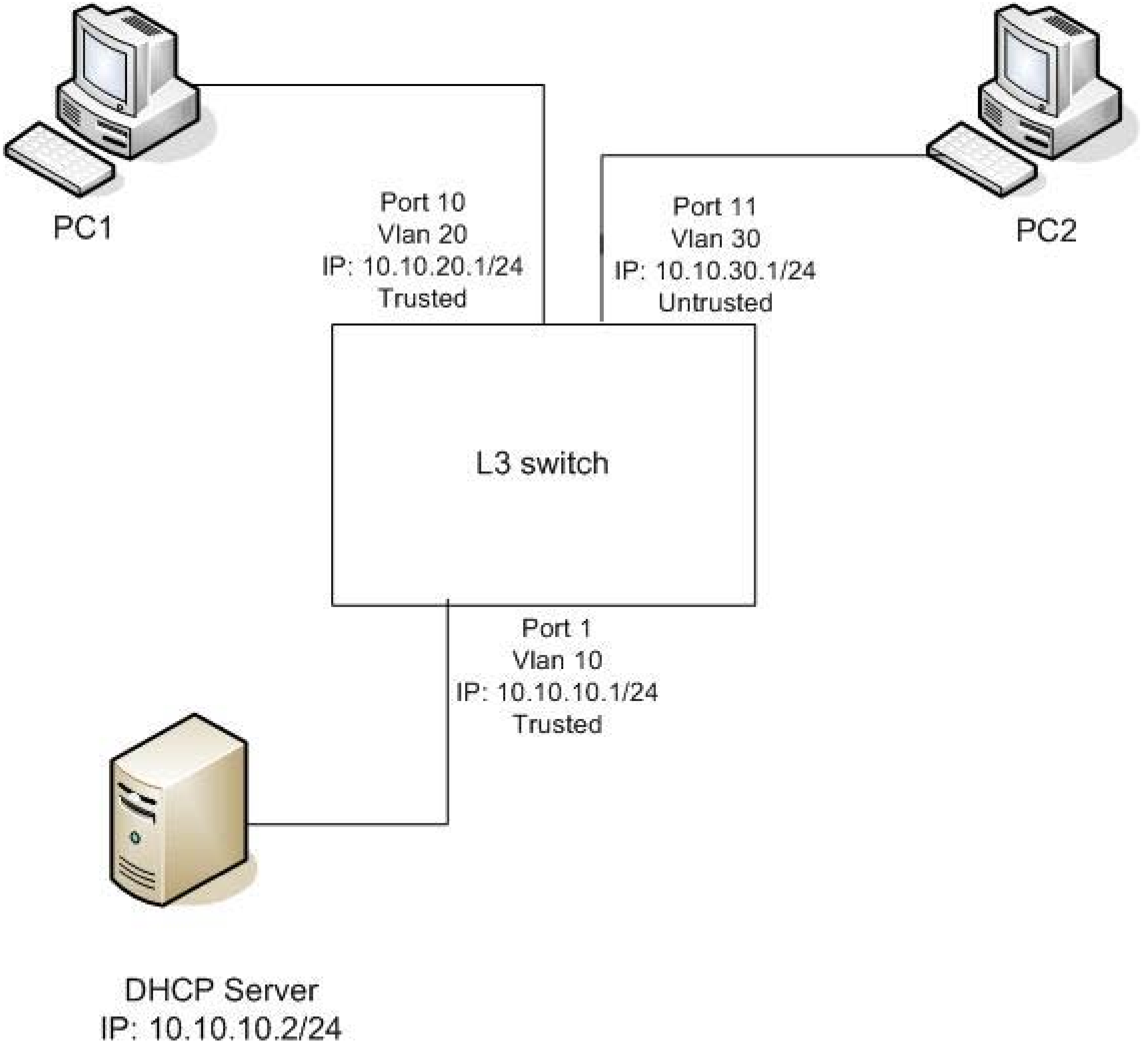
```
(config)#show ip dhcp-snooping binding
```

```
MAC               IP              Lease (sec)   VID   Port
---------------------------------------------------------------
00-02-44-ab-2d-f4 192.168.1.10      86460        1     11
Total Entries: 1
```

DHCP Snooping layer 3 configuration example

"Layer 3 configuration example" (page 121)depicts the network setup for this example. The device under test (DUT) runs in layer 3 mode. The DHCP clients and server are in different L3 VLANs.

Layer 3 configuration example



The DHCP server port must always be Trusted, because Untrusted DHCP ports drop DHCP replies coming from the DHCP server. All ports are DHCP Untrusted by default. You should connect DHCP clients to Untrusted DHCP ports, however, PC1 is connected to a Trusted port for this configuration example case.

DHCP Relay must be configured when the switch runs in Layer 3 mode. In L3 mode, switch-to-switch ports must be DHCP Trusted on both sides because DHCP replies must be forwarded, and because DHCP request packets are routed (or relayed).

This configuration example illustrates a security hole that permits PC1 to install a fake DHCP Server. Port10 (DHCP Trusted) allows DHCP replies to be forwarded to PC2 in this case.

To configure the preceding example , you must perform the following tasks:

Step	Action
1	Create the L3 VLANs.
2	Enable DHCP relay.
3	Enable DHCP snooping.

—End—

DHCP Snooping configuration commands

The following section describes the detailed CLI commands required to configure DHCP Snooping for this example.

Level 3 VLANs

```
>en
#configure terminal
(config)#vlan configcontrol automatic
(config)#vlan create 10 type port
(config)# vlan create 20 type port
(config)# vlan create 30 type port
(config)#vlan members 10 1
(config)#vlan members 20 10
(config)#vlan members 30 11
(config)#interface vlan 10
(config-if)#ip address 10.10.10.1 255.255.255.0
(config-if)#interface vlan 20
(config-if)#ip address 10.10.20.1 255.255.255.0
(config-if)#interface vlan 30
(config-if)#ip address 10.10.30.1 255.255.255.0
(config-if)#exit (config)#ip routing
```

DHCP relay

```
(config)#ip dhcp-relay fwd-path 10.10.20.1 10.10.10.2
(config)#ip dhcp-relay fwd-path 10.10.30.1 10.10.10.2
```

DHCP Snooping

```
(config)#ip dhcp-snooping
(config)#ip dhcp-snooping vlan 10
(config)#ip dhcp-snooping vlan 20
(config)#ip dhcp-snooping vlan 30
(config)# interface fastEthernet 1,10
(config-if)#ip dhcp-snooping trusted
(config-if)#exit
```

Verifying the DHCP Snooping settings

This section describes the commands used to verify the settings and the expected response to each command.

```
(config)#show ip dhcp-snooping
```

```
Global DHCP snooping state: Enabled
DHCP
VLAN Snooping
---- --------
10    Enabled
20    Enabled
30    Enabled
```

```
(config)#show ip dhcp-snooping  interface 1,10,11
```

```
 DHCP
Port Snooping
---- --------
1    Trusted
10   Trusted
11   Untrusted
```

```
(config)#show running-config
```

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.159
enable
configure terminal
!
! *** CORE ***
!
autosave enable
mac-address-table aging-time 300
autotopology
no radius-server
radius-server host 0.0.0.0
radius-server secondary-host 0.0.0.0
radius-server port 1812
! radius-server key ********
radius-server timeout 2
tacacs server host  0.0.0.0
tacacs server secondary-host  0.0.0.0
tacacs server port 49
tacacs authorization disable
tacacs authorization level NONE
tacacs accounting disable
telnet-access login-timeout 1
telnet-access retry 3
telnet-access inactive-timeout 15
telnet-access logging all
```

```
cli password switch serial none
cli password switch telnet none
! cli password switch read-only "********"
! cli password switch read-write "********"
configure network load-on-boot disable
tftp-server 0.0.0.0
! ...
!
! *** DHCP SNOOPING *** Note information in this section.
!
ip dhcp-snooping
no ip dhcp-snooping vlan
ip dhcp-snooping vlan 1
interface FastEthernet ALL
default ip dhcp-snooping
ip dhcp-snooping port 1,10 trusted
exit
!
! *** ARP INPSECTION *** Note information in this section
!
no ip arp-inspection
vlan interface FastEthernet ALL
default ip arp-inspection
exit
! ...
```

Renew the IP addresses for PC1 and PC2. Both PCs obtains IP addresses from the DHCP server. A DHCP binding entry for PC2 appears in the DHCP binding table. No binding extry for PC1 exists because port10 is DHCP Trusted.

```
(config)#show ip dhcp-snooping binding

MAC                IP              Lease (sec)   VID   Port
---------------------------------------------------------------
00-02-44-ab-2d-f4 192.168.1.10      86460         1     11
Total Entries: 1
```

Configuring dynamic ARP inspection

For information about the function and operation of dynamic Address Resolution Protocol (ARP) inspection in a Nortel Ethernet Routing Switch 5500 Series network, see "Dynamic ARP inspection" (page 57).

To configure dynamic ARP inspection, do the following:

1. Enable dynamic ARP inspection on the VLANs (see "Enabling dynamic ARP inspection on the VLANs" (page 125)).
2. Identify the ports as trusted (ARP traffic is not subjected to dynamic ARP inspection) or untrusted (ARP traffic is filtered through dynamic ARP inspection) (see "Configuring trusted and untrusted ports" (page 125)).

Note: For dynamic ARP inspection to function, DHCP snooping must be globally enabled. For information about configuring DHCP snooping, see "Configuring DHCP snooping" (page 115).

Enabling dynamic ARP inspection on the VLANs

You must enable dynamic ARP inspection separately for each VLAN.

To enable dynamic ARP inspection on a VLAN, use the following command in Global configuration mode:

```
ip arp-inspection vlan <vlanID>
```

where

`<vlanID>` is an integer in the range 1–4094 that specifies the preconfigured VLAN on which you want to enable dynamic ARP inspection.

The default is disabled.

To disable dynamic ARP inspection on a VLAN, use the following command in Global configuration mode:

```
no ip arp-inspection vlan <vlanID>
```

where

`<vlanID>` is an integer in the range 1–4094 that specifies the preconfigured VLAN on which you want to disable dynamic ARP inspection.

Configuring trusted and untrusted ports

To specify whether a particular port or range of ports is trusted (ARP traffic is not subject to dynamic ARP inspection) or untrusted (ARP traffic is subject to dynamic ARP inspection), use the following command in Interface configuration mode:

```
ip arp-inspection [port <portlist>] <trusted|untrusted>
```

where

`<portlist>` is the physical port number of the port you want to configure. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port number, the command applies to the ports specified upon entering the Interface configuration mode.

The default is untrusted.

To return a port or range of ports to default values, use the following command in Interface configuration mode:

```
default ip arp-inspection port <portlist>
```

where

<portlist> is the physical port number of the port you want to configure. You can enter a single port, a range of ports, several ranges, or all. You must specify a port.

To return all ports in the interface to default values, use the following command in Interface configuration mode:

```
default ip arp-inspection port ALL
```

Viewing dynamic ARP inspection settings

To view the VLANs on which dynamic ARP inspection has been enabled, use the following command in Global or Interface configuration mode:

```
show ip arp-inspection vlan
```

The output lists only the VLANs enabled for dynamic ARP inspection.

To view port settings, use the following command in Global or Interface configuration mode:

```
show ip arp-inspection interface [<interface type>] [<port>]
```

The output lists the ports and their associated dynamic ARP inspection status (trusted or untrusted). If you specify the interface type or port as part of the command, the output includes only the ports specified. If you do not specify the interface type or port as part of the command, the output displays all ports.

Dynamic ARP inspection layer 2 configuration example

This configuration example uses the same network setup and configuration created in the "Configuring DHCP snooping" (page 115)section and illustrated by the"Layer 2 configuration example" (page 118). To increase security in this network, you must enable Dynamic ARP inspection. If the device under test (DUT) has no IP address assigned, BOOTP must be DISABLED in order for ARP Inspection to work. The DHCP Server port must be ARP Trusted also.

> ***Note:*** When enabling ARP Inspection, issue the ’clear arp-cache’ command to clear the system ARP cache table. Nortel recommends prudent use of this command because it is system intensive.

Dynamic ARP inspection configuration commands

The following section details the commands required to configure Dynamic ARP Inspection for this example. The following commands are in addition to those specified in the "Configuring DHCP snooping" (page 115)section.

```
>en
```

```
#configure terminal
(config)#ip bootp server disable
(config)#ip arp-inspection vlan 1
(config)#interface fastEthernet 1,10
(config-if)#ip arp-inspection trusted
(config-if)#exit
```

Verifying Dynamic ARP Inspection settings

This section describes the commands used to verify the settings and the expected response to each command.

```
(config)#show ip arp-inspection
```

```
 ARP
VLAN Inspection
---- ----------
1    Enabled
```

```
(config)#show ip arp-inspection  interface 1,10,11
```

```
ARP
Port Inspection
---- ----------
1    Trusted
10   Trusted
11   Untrusted
```

```
(config)#show running-config
```

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.159 enable configure terminal
!
! *** CORE ***
!
autosave enable
mac-address-table aging-time 300
autotopology
no radius-server
radius-server host 0.0.0.0
radius-server secondary-host 0.0.0.0
radius-server port 1812
! radius-server key ********
radius-server timeout 2
tacacs server host  0.0.0.0
tacacs server secondary-host  0.0.0.0
tacacs server port 49
tacacs authorization disable
tacacs authorization level NONE
tacacs accounting disable
telnet-access login-timeout 1
telnet-access retry 3
```

```
telnet-access inactive-timeout 15
telnet-access logging all
cli password switch serial none
cli password switch telnet none
! cli password switch read-only "********"
! cli password switch read-write "********"
configure network load-on-boot disable
tftp-server 0.0.0.0
! ...
!
! *** IP *** Note information in this section.
!
ip bootp server disable
ip default-gateway 0.0.0.0
ip address netmask 0.0.0.0
ip address stack 0.0.0.0
ip address switch 0.0.0.0
! ...
!
!
! *** DHCP SNOOPING *** Note information in this section.
!
ip dhcp-snooping
no ip dhcp-snooping vlan
ip dhcp-snooping vlan 1
interface FastEthernet ALL
default ip dhcp-snooping
ip dhcp-snooping port 1,10 trusted
exit
!
! *** ARP INPSECTION *** Note information in this section.
!
no ip arp-inspection vlan
ip arp-inspection vlan 1
interface FastEthernet ALL
default ip arp-inspection
ip arp-inspection port 1,10 trusted
exit
! ...
```

Renew the IP addresses for PC1 and PC2. Both PCs will obtain IP addresses from the DHCP server. A DHCP binding entry for PC2 appears in the DHCP binding table although it is ARP Untrusted. No binding extry for PC1 exists because port10 is DHCP Trusted even though it is ARP Trusted.

Now clear the ARP cache on both PCs.

```
>arp –a
>arp -d <IP-address>
```

Attempt to start communication (use ping) between PCs or between the PCs and the DHCP server. You can establish communication in any direction because ARPs are allowed on port10 (PC1) (that port is ARP Trusted) and on port11 (PC2) because ARP packets coming from PC2 have an entry for ARP Untrusted port11 that matches the IP-MAC from the DHCP binding table.

Next make a link-down/link-up for port11(PC2) or change PC's2 IP address to a static one and set port10(PC1) as ARP Untrusted. Clear the ARP cache on both PCs and the DHCP server. Attempt to start communication (use ping) between PCs or between the PCs and the DHCP server. The PCs and DHCP server are unable to communicate with one another.

Dynamic ARP inspection layer 3 configuration example

This configuration example uses the same network setup and configuration created in the "Configuring DHCP snooping" (page 115)section and illustrated by the "Layer 3 configuration example" (page 121). To increase security in this network, you must enable Dynamic ARP inspection. If the device under test (DUT) has no IP address assigned, BOOTP must be disabled in order for ARP Inspection to work. The DHCP Server port must be ARP Trusted. In L3 mode, switch-to-switch ports must be ARP Trusted ports in order for static/non-local/RIP/OSPF routes to work

In L3 mode, DUT keeps an ARP table which learns IP-MAC for PC1, PC2 and DHCP server. ARP Inspection behavior is the same as in Layer 2 mode, except that ARP entries must sometimes be cleared from the ARP table on the L3 DUT for fast update of communication based on new ARP Inspection settings.

Dynamic ARP inspection configuration commands

The following section details the commands required to configure Dynamic ARP Inspection for this example. The following commands are in addition to those specified in the "Configuring DHCP snooping" (page 115)section.

```
>en
#configure terminal
(config)#ip bootp server disable
(config)#ip arp-inspection vlan 10
(config)#ip arp-inspection vlan 20
(config)#ip arp-inspection vlan 30
(config)#interface fastEthernet 1,10
(config-if)#ip arp-inspection trusted
(config-if)#exit
```

Verifying Dynamic ARP Inspection settings

This section describes the commands used to verify the settings and the expected response to each command.

```
(config)#show running-config
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.159
enable
configure terminal
!
! *** CORE ***
!
autosave enable
mac-address-table aging-time 300
autotopology
no radius-server
radius-server host 0.0.0.0
radius-server secondary-host 0.0.0.0
radius-server port 1812
! radius-server key ********
radius-server timeout 2
tacacs server host  0.0.0.0
tacacs server secondary-host  0.0.0.0
tacacs server port 49
tacacs authorization disable
tacacs authorization level NONE
tacacs accounting disable
telnet-access login-timeout 1
telnet-access retry 3
telnet-access inactive-timeout 15
telnet-access logging all
cli password switch serial none
cli password switch telnet none
! cli password switch read-only "********"
! cli password switch read-write "********"
configure network load-on-boot disable
tftp-server 0.0.0.0
! ...
!
! *** IP *** Note information in this section.
!
ip bootp server disable
ip default-gateway 0.0.0.0
ip address netmask 0.0.0.0
ip address stack 0.0.0.0
ip address switch 0.0.0.0
! ...
!
! *** VLAN *** Note information in this section.
!
vlan configcontrol automatic
auto-pvid
vlan name 1 "VLAN #1"
vlan create 10 name "VLAN #10" type port
vlan create 20 name "VLAN #20" type port
vlan create 30 name "VLAN #30" type port
vlan ports 1-24 tagging unTagAll  filter-untagged-frame
disable filter-unregist ered-frames enable priority 0
vlan members 1 2-9,12-24
vlan members 10 1
vlan members 20 10
vlan members 30 11
vlan ports 1 pvid 10
vlan ports 2-9 pvid 1
vlan ports 10 pvid 20
vlan ports 11 pvid 30
vlan ports 12-24 pvid 1
vlan igmp unknown-mcast-no-flood disable
vlan igmp 1 snooping disable
vlan igmp 1 proxy disable robust-value 2 query-interval 125
vlan igmp 10 snooping disable vlan igmp 10 proxy disable
robust-value 2 query-interval 125
vlan igmp 20 snooping disable
vlan igmp 20 proxy disable robust-value 2 query-interval 125
vlan igmp 30 snooping disable vlan igmp 30 proxy disable
robust-value 2 query-interval 125
vlan mgmt 1
! ...
!
! *** L3 *** Note information in this section.
!
no ip directed-broadcast enable
ip routing
interface vlan 10
ip address 10.10.10.1 255.255.255.0 2 ip dhcp-relay
min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 20 ip address 10.10.20.1 255.255.255.0 3
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
interface vlan 30 ip address 10.10.30.1 255.255.255.0 4
ip dhcp-relay min-sec 0 mode bootp_dhcp
no ip dhcp-relay broadcast
ip dhcp-relay
exit
ip arp timeout 360
ip dhcp-relay
ip dhcp-relay fwd-path 10.10.20.1 10.10.10.2 enable
ip dhcp-relay fwd-path 10.10.20.1 10.10.10.2 mode bootp-dhcp
ip dhcp-relay fwd-path 10.10.30.1 10.10.10.2 enable
ip dhcp-relay fwd-path 10.10.30.1 10.10.10.2 mode bootp-dhcp
ip blocking-mode none
! ...
!
! *** DHCP SNOOPING *** Note information in this section.
!
ip dhcp-snooping
no ip dhcp-snooping vlan
ip dhcp-snooping vlan 10
ip dhcp-snooping vlan 20
ip dhcp-snooping vlan 30
interface FastEthernet ALL
default ip dhcp-snooping
ip dhcp-snooping port 1,10 trusted
exit
!
! *** ARP INPSECTION *** Note information in this section.
!
no ip arp-inspection vlan
ip arp-inspection vlan 10
ip arp-inspection vlan 20
ip arp-inspection vlan 30
interface FastEthernet ALL
default ip arp-inspection
ip arp-inspection port 1,10 trusted
exit
! ...
```

IP Source Guard Configuration

IP Source Guard can be configured through the Nortel Networks Command Line Interface (NNCLI), Simple Network Management Protocol (SNMP), and JDM (Java Device Manager).

Perform the tasks in this section to configure IP Source Guard through the NNCLI, on the Nortel Stackable Ethernet Routing Switches 55xx (ERS 55xx). To configure IP Source Guard through the JDM, see"Configuring IP Source Guard using the Java Device Manager" (page 184)

For information on how IP Source Guard works, see "IP Source Guard" (page 53)

Prerequisites to IP Source Guard configuration

- Ensure that dynamic Host Control Protocol (DHCP) snooping is globally enabled. (See "Enabling DHCP snooping globally" (page 115)).
- Ensure that the port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- Ensure that the port is an untrusted DHCP snooping and dynamic ARP Inspection port.
- Ensure that a minimum of 10 rules are available on the port.
- Ensure that the following MIB object exists: bsSourceGuardConfigMode

  Note: This object is used to control the IP Source Guard mode on an interface.

- Ensure that the following applications are not enabled:
  - — IP Fix
  - — Baysecure
  - — Extensible Authentication Protocol over LAN (EAPoL)

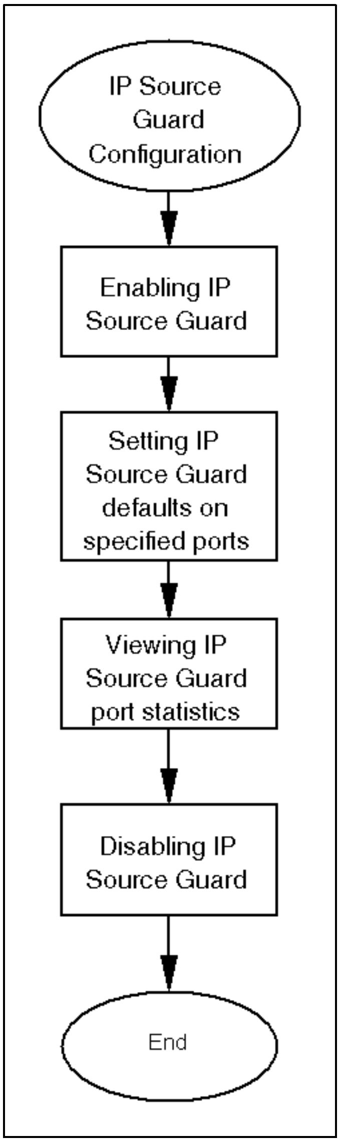
ATTENTION

Hardware resource might run out if IP Source Guard is enabled on trunk ports with a large number of VLANs that have DHCP snooping enabled. If this happens, some clients might not be able to send traffic. Hence, Nortel recommends that IP Source Guard not be enabled on trunk ports.

IP Source Guard configuration procedures

This task flow shows you the sequence of procedures you perform to configure IP Source Guard on the Nortel ERS 55xx. To link to any procedure, go to "IP Source Guard configuration procedure navigation" (page 135).

IP Source Guard configuration procedures


IP Source Guard Configuration
Enabling IP Source Guard
Setting IP Source Guard defaults on specified ports
Viewing IP Source Guard port statistics
Disabling IP Source Guard
End

IP Source Guard configuration procedure navigation

- "Enabling IP Source Guard" (page 135)
- "Viewing IP Source Guard port statistics" (page 135)
- "Disabling IP Source Guard" (page 136)

Enabling IP Source Guard

Enable IP Source Guard to add a higher level of security to the desired port by preventing IP spoofing.

Execute this command in the Ethernet, FastEthernet, or GigabitEthernet interface configuration mode.

> **ATTENTION**
> The IP addresses are obtained from DHCP snooping Binding Table entries defined automatically in the port. A maximum of 10 IP addresses from the Binding Table are allowed, and the rest are dropped.

Procedure steps

Step Action

1 Enter this command:

```
ip verify source [interface {[<interface type>]
[<interface id>]}
```

—End—

Variable definitions

Variable	Value
<interface id>	is the ID of the interface on which you want IP Source Guard enabled.
<interface type>	is the interface on which you want IP Source Guard enabled.

Viewing IP Source Guard port statistics

View IP Source Guard port statistics to see IP Source Guard configuration settings for interfaces. Execute this command in the Privileged Exec mode.

Procedure steps

Step Action

1 Enter this command:

```
show ip verify source [interface {[ <interface type>]
[<interface id>]}
```

—End—

Variable definitions

Variable	Value
<interface id>	is the ID of the interface for which you want IP Source Guard statistics displayed.
<interface type>	is the type of interface for which you want IP Source Guard statistics displayed.

View IP Source Guard port statistics to also see IP Source Guard-allowed addresses. Execute this command in the Privileged Exec mode.

Procedure steps

Step Action

1 Enter this command:

```
show ip source binding [<A.B.C.D.>][interface
{[<interface type>] [<interface id>]}]
```

—End—

Variable definitions

Variable	Value
<A.B.C.D>	is the IP address or group of addresses that IP Source Guard has allowed.
<interface id>	is the ID of the interface for which you want IP Source Guard-allowed addresses displayed.
<interface type>	is the type of interface for which you want IP Source Guard-allowed addresses displayed.

Disabling IP Source Guard

Disable IP Source Guard to allow all IP traffic to go through without being filtered.

Execute this command in the Ethernet, FastEthernet, or GigabitEthernet interface configuration mode.

Procedure steps

Step	Action
1	Enter this command:

```
no ip verify source interface {[<interface type>]
[<interface id>]}
```

—End—

Variable definitions

Variable	Value
<interface id>	is the ID of the interface on which you want IP Source Guard disabled.
<interface type>	is the interface on which you want IP Source Guard disabled.

Configuring and managing security using the Web-based management interface

This chapter describes the methods and procedures necessary to configure security on the Nortel Ethernet Routing Switch 5500 Series using the Web-based management interface.

Setting user access limitations

For a complete explanation of the configuration and management of user access limitations using the Web-based Management interface, refer to the *Nortel Ethernet Routing Switch 5500 Series Overview – System Configuration* (NN47200-500).

Configuring EAPOL-based security

Use the following procedure to configure and manage the Extensible Authentication Protocol over LAN (EAPOL) security with the Web-based Management interface.

Prerequisite: Ensure that IP Source Guard is not enabled. (IP Source Guard and EAPOL are mutually exclusive).

To configure EAPOL-based security, perform these tasks:

Step	Action
1	Open the **EAPOL Security Configuration** screen by selecting **Applications > EAPOL Security** from the menu. An example of this screen is illustrated in "EAPOL Security Configuration screen" (page 139). **EAPOL Security Configuration screen**
2	In the **EAPOL Administrative State Setting** section, select either **Enabled** or **Disabled** from the **EAPOL Administrative State** list. This enables or disables EAPOL security configuration.

3 Click the **Submit** button immediately under the **EAPOL Administrative State Setting** section.

4 In the **EAPOL Security Setting** section, use the fields provided to configure the EAPOL security for the desired ports. Not all ports are displayed in the **EAPOL Security Setting** section. Links to those ports not listed are provided at the bottom of the screen. "EAPOL Security Setting fields" (page 140)outlines the fields on this screen.

EAPOL Security Setting fields

Field	Description
Unit	Displays the unit being viewed. This field is only visible in stack configurations.
Port	Displays the port number.
Initialize	Setting this attribute to Yes causes this port's EAPOL state to be initialized.
Administrative Status	Allows you to set the EAPOL authorization status: • Force Unauthorized - Always unauthorized • Auto - Status depends on EAP authentication results • Force Authorized - Always authorized
Operational Status	Displays the current authorization status.
Administrative Traffic Control	Allows EAPOL authentication to be set for either incoming and outgoing traffic or for incoming traffic only.
Operational Traffic Control	Displays the current administrative traffic control setting.
Re-authenticate Now	Allows EAPOL authentication to be activated immediately without waiting for the re-authentication period to expire.
Re-authentication	Allows EAPOL authentication to be repeated according to the time value specified in Re-authentication Period field.
Re-authentication Period	With Re-authentication enabled, allows the time period to be specified between successive EAPOL authentications. The value can range from 1 to 604800.

Field	Description
Quiet Period	Allows the time interval to be specified between an authentication failure and the start of a new authentication attempt. The value can range from 0 to 65535.
Transmit Period	Specifies how long the switch waits for the supplicant to respond to EAP Request/Identity packets. The value can range from 1 to 65535.
Supplicant Timeout	Specifies how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets. The value can range from 1 to 65535.
Server Timeout	Specifies how long the switch waits for the RADIUS server to respond to all EAP packets. The value can range from 1 to 65535.
Maximum Requests	Specifies the number of times the switch attempts to resend EAP packets to a supplicant. The value can range from 1 to 10.

5 Click the **Submit** button immediately under the **EAPOL Security Setting** section.

—End—

Configuring MAC address-based security

The following sections outline how to configure and manage MAC Address-based security in the Web-based Management interface.

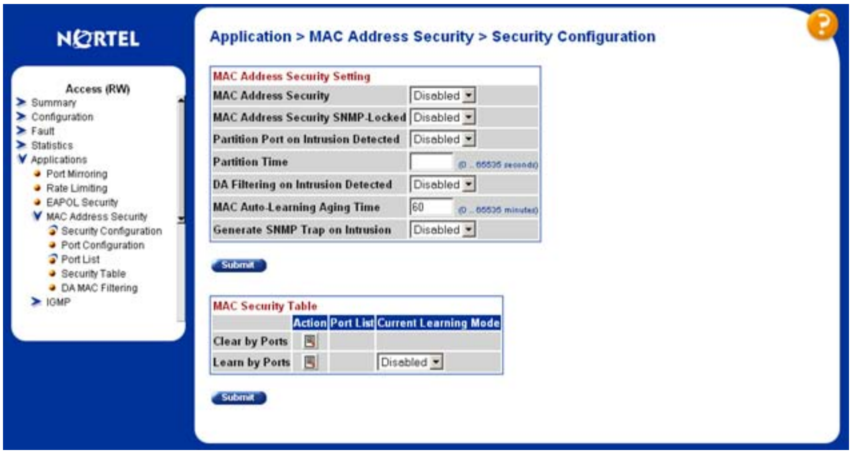
Security Configuration

To configure the MAC Address-based security, perform the following procedure:

Step Action

1 Open the **Security Configuration** screen by selecting **Applications > MAC Address Security > Security Configuration** from the menu. This screen is illustrated in "Security Configuration screen" (page 142).

Security Configuration screen



Application > MAC Address Security > Security Configuration

MAC Address Security Setting

MAC Address Security	Disabled
MAC Address Security SNMP-Locked	Disabled
Partition Port on Intrusion Detected	Disabled
Partition Time	(0 .. 65535 seconds)
DA Filtering on Intrusion Detected	Disabled
MAC Auto-Learning Aging Time	60 (0 .. 65535 minutes)
Generate SNMP Trap on Intrusion	Disabled

MAC Security Table

	Action	Port List	Current Learning Mode
Clear by Ports			
Learn by Ports			Disabled

2 The **MAC Address Security Setting** section is used to configure the security settings. Use the fields in this section to perform initial configuration. The fields in this section are outlined in "MAC Address Security Setting fields" (page 142).

MAC Address Security Setting fields

Field	Description
MAC Address Security	Enables the MAC address security features. The default value is Disabled.
MAC Address Security SNMP-Locked	Enables locking SNMP, so that you cannot use SNMP to modify the MAC address security features. The default value is Disabled.
Partition Port on Intrusion Detected	Configures how the switch reacts to an intrusion event: • Forever - The port is disabled and remains disabled (partitioned) until reset. The port does not reset after the Partition Time elapses. • Enabled - The port is disabled, and then automatically reset to enabled after the time specified in the Partition Time field elapses. • Disabled - The port remains enabled, even if an intrusion event is detected.

Field	Description
	The default value is Disabled.
Partition Time	Sets the time to partition a port on intrusion. ***Note:*** Use this field only if the Partition Port on Intrusion Detected field is set to Enabled. There is no default for this field.
DA Filtering on Intrusion Detected	Enables isolation of the intruding node. The default value is Disabled.
MAC Auto-Learning Aging Time	Specify the MAC address age-out time, in seconds, for the auto-learned MAC addresses. The default value is 0 (entry never ages out).
Generate SNMP Trap on Intrusion	Enables generation of an SNMP trap when an intrusion is detected. The default value is Disabled.

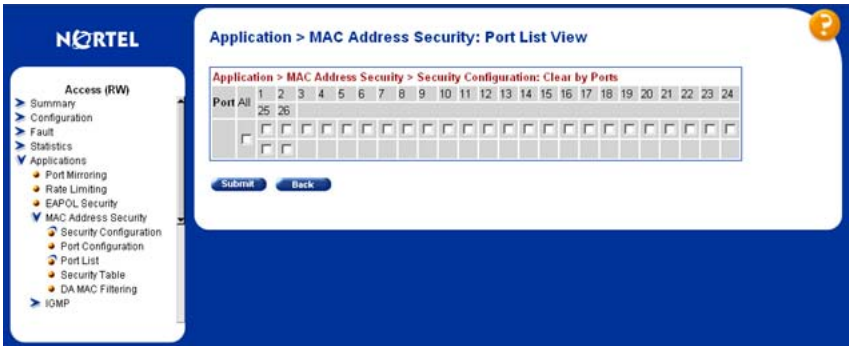
3 Click the **Submit** button immediately under the **MAC Address Security Setting** section.

4 The **MAC Security Table** section is used to clear ports from participation or allow ports to learn MAC Addresses.

a. To clear ports from MAC Address security participation, follow this procedure:

- In the **Clear by Ports** row, click the icon in the **Action** column. This opens the **Ports List View** screen ("Port List View screen" (page 144)). Uncheck the ports to be cleared from participation.
- Click **Submit**.

Port List View screen



Application > MAC Address Security: Port List View

Application > MAC Address Security > Security Configuration: Clear by Ports

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		25	26																						
	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
		□	□																						

b. To allow ports to learn MAC Addresses, follow this procedure:

- In the **Learn by Ports** row, click the icon in the Action column. This opens the **Ports List View** screen ("Port List View screen" (page 144)). Select the ports that will participate in MAC Address learning.
- Click **Submit**.

5 Set the state of port learning by selecting a value from the **Current Learning Mode** list.

6 Click the **Submit** under the **MAC Security Table** section.

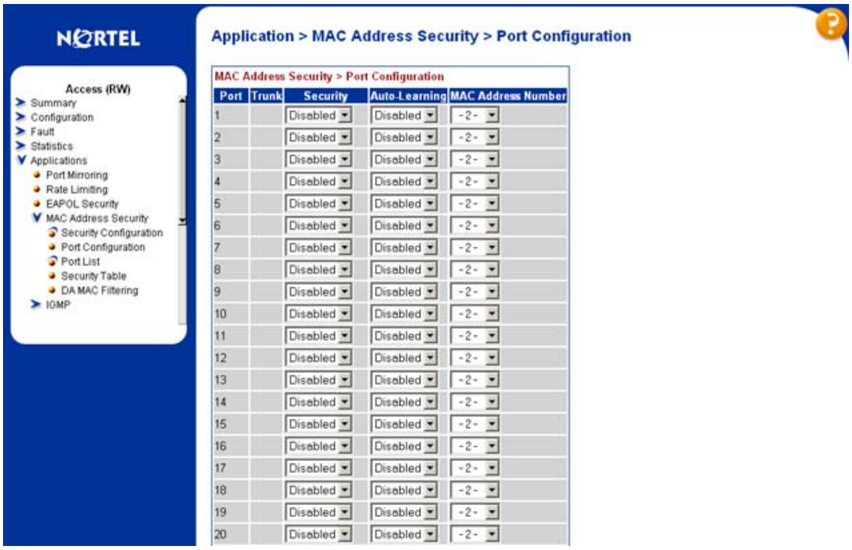
—End—

Enabling Port Security

To enable MAC security on a port, follow this procedure:

Step	Action
1	Open the **Port Configuration** screen by selecting **Applications > MAC Address Security > Port Configuration** from the menu. This window is illustrated in "Port Configuration screen" (page 145).

Port Configuration screen



Application > MAC Address Security > Port Configuration

MAC Address Security > Port Configuration

Port	Trunk	Security	Auto-Learning	MAC Address Number
1		Disabled	Disabled	-2-
2		Disabled	Disabled	-2-
3		Disabled	Disabled	-2-
4		Disabled	Disabled	-2-
5		Disabled	Disabled	-2-
6		Disabled	Disabled	-2-
7		Disabled	Disabled	-2-
8		Disabled	Disabled	-2-
9		Disabled	Disabled	-2-
10		Disabled	Disabled	-2-
11		Disabled	Disabled	-2-
12		Disabled	Disabled	-2-
13		Disabled	Disabled	-2-
14		Disabled	Disabled	-2-
15		Disabled	Disabled	-2-
16		Disabled	Disabled	-2-
17		Disabled	Disabled	-2-
18		Disabled	Disabled	-2-
19		Disabled	Disabled	-2-
20		Disabled	Disabled	-2-

2 Select the options from the lists that enable the MAC security to be set for that port. "Port Configuration fields" (page 145) outlines the fields on this screen.

Port Configuration fields

Field	Description
Security	Enables or disables MAC security on this port. The default value is Disabled.
Auto-Learning	Enables or disables auto-learning of MAC addresses on this port. The default value is Disabled.
MAC Address Number	Sets the maximum number of MAC addresses this port can learn. The default value is 2.

3 Click **Submit**.

—End—

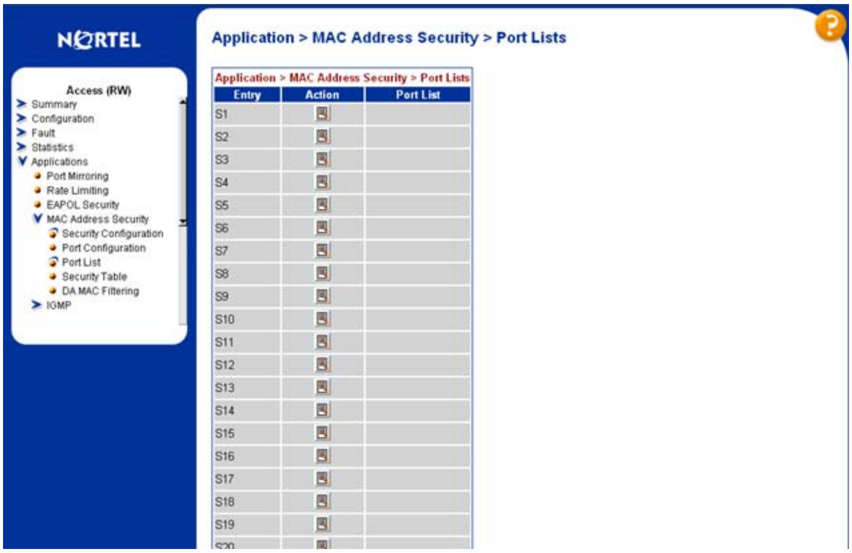
Port Lists

To add or delete ports in a list, follow this procedure:

Step	Action

1 Open the **Port Lists** screen by selecting **Applications > MAC Address Security > Port Lists** in the menu. This screen is illustrated in "Port Lists screen" (page 146).

Port Lists screen



Application > MAC Address Security > Port Lists

Entry	Action	Port List
S1	✎	
S2	✎	
S3	✎	
S4	✎	
S5	✎	
S6	✎	
S7	✎	
S8	✎	
S9	✎	
S10	✎	
S11	✎	
S12	✎	
S13	✎	
S14	✎	
S15	✎	
S16	✎	
S17	✎	
S18	✎	
S19	✎	

2 Click the icon in the **Action** column of the row containing the list to be edited.

3 A **Port Lists** screen similar to the one illustrated in "Port List View screen" (page 144) appears. Select the ports to add to the list or uncheck those ports that are to be removed from the list.

4 Click **Submit**.

—End—

The **Port Lists** screen re-appears with the new port list displayed.

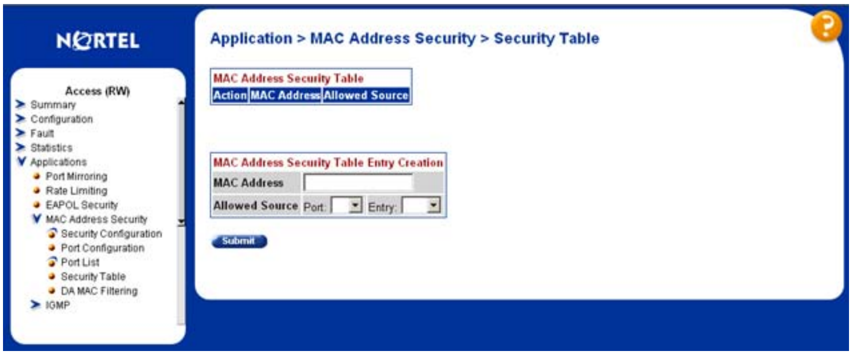
Adding MAC Addresses

To add a MAC Address to the MAC Address-based security, follow this procedure:

Step	Action

1 Open the **Security Table** screen by selecting **Applications > MAC Address Security > Security Table** from the menu. This screen is illustrated in "Security Table screen" (page 147).

Security Table screen



2 In the **MAC Address Security Table Entry Creation** section, enter the MAC address information to enter in the table. "MAC Address Security Table Entry Creation fields" (page 147) outlines the fields in this section.

MAC Address Security Table Entry Creation fields

Field	Description
MAC Address	Enter the MAC address that is allowed access to the switch.
Allowed Source - Port	Select the port through which the MAC address is allowed.
Allowed Source - Entry	Select the port list through which the MAC address is allowed.

3 Click **Submit**.

—End—

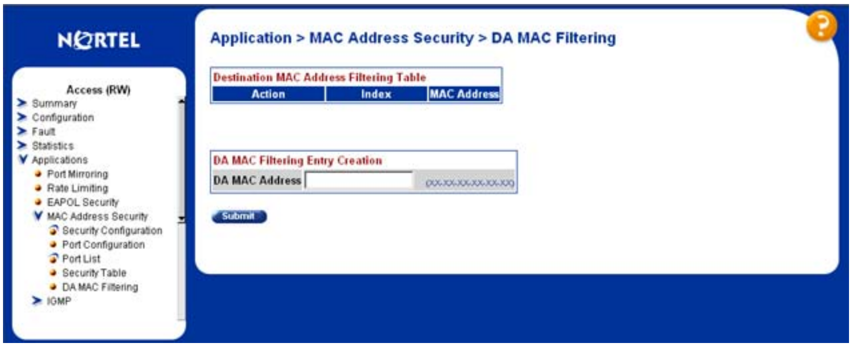
DA MAC Filtering

To drop all packets from a specified MAC destination address (DA), perform these tasks:

Step Action

1 Open the **DA MAC Filtering** screen by **selecting Applications > MAC Address Security > DA MAC Filtering**. This screen is illustrated in "DA MAC Filtering screen" (page 148).

DA MAC Filtering screen



Application > MAC Address Security > DA MAC Filtering

Destination MAC Address Filtering Table

Action	Index	MAC Address

DA MAC Filtering Entry Creation

DA MAC Address (XX:XX:XX:XX:XX:XX)

2 Enter the MAC Address in the **DA MAC Address** field.

3 Click **Submit**.

—End—

Deleting MAC DAs

To delete a MAC DA:

Step Action

1 Open the **DA MAC Filtering** screen by selecting **Applications > MAC Address Security > DA MAC Filtering**.

2 In the **Destination MAC Address Filtering Table**, click the **Delete** icon for the entry to be deleted.

A message is displayed prompting for confirmation of the request.

3 Click **Yes** to delete the MAC DA.

—End—

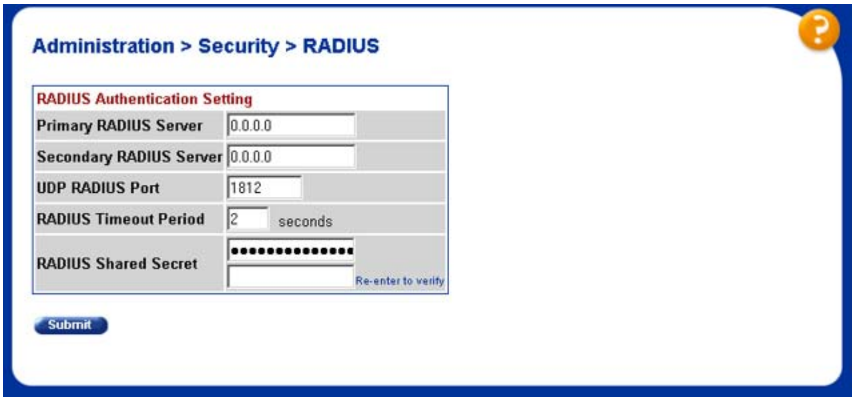
Configuring RADIUS security

Use the following procedure to configure and manage RADIUS-based security with the Web-based Management interface.

Step Action

1 Open the **RADIUS** screen by selecting **Administration > Security > RADIUS** from the menu. The following figure illustrates the RADIUS screen.

RADIUS screen



RADIUS Authentication Setting

Primary RADIUS Server	0.0.0.0
Secondary RADIUS Server	0.0.0.0
UDP RADIUS Port	1812
RADIUS Timeout Period	2 seconds
RADIUS Shared Secret	•••••••••••••• Re-enter to verify

2 In the **RADIUS Authentication Setting** section, use the fields provided to configure settings for the RADIUS server and RADIUS authentication.

The following table describes the fields on this screen.

RADIUS Authentication Setting fields

Field	Description
Primary RADIUS server	Specifies the IP address of the primary RADIUS server.
Secondary RADIUS server	Specifies the IP address of the secondary RADIUS server. The secondary server is used only if the primary server does not respond.
UDP RADIUS port	Specifies the UDP port for RADIUS. The range is 0-65535. The default is 1812.
RADIUS Timeout Period	Specifies the number of seconds before the service request times out. RADIUS allows three retries for each server (primary and secondary). The range of the timeout interval is 1-60. The default is 2.
RADIUS Shared Secret	Specifies the secret authentication and encryption key used for all communications between the NAS and the RADIUS server. The shared secret must be the same as the one defined on the server.

3 Click the **Submit** button immediately under the **RADIUS Authentication Setting** section.

—End—

Configuring and managing security using the Java Device Manager

This chapter describes the methods and procedures necessary to configure security on the Nortel Ethernet Routing Switch 5500 Series using the Java Device Manager (Device Manager).

Configuring security

All global security configuration procedures in the Device Manager are performed on the **Security** screen. Open the **Security** screen by selecting **Edit > Security > Security** from the menu. "EAPOL tab" (page 152)shows an example of this screen.

The following sections outline the security configuration tasks that can be performed on the tabs of this screen, and related topics:

- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "SecurityList tab" (page 166)
- "AuthConfig tab" (page 168)
- "AutoLearn tab" (page 170)
- "AuthStatus tab" (page 171)
- "AuthViolation tab" (page 174)
- "MacViolation tab" (page 176)
- "SSH tab" (page 177)
- "SSH Sessions tab" (page 179)
- "SSL tab" (page 180)
- "Radius Server tab" (page 182)

EAPOL Configuration

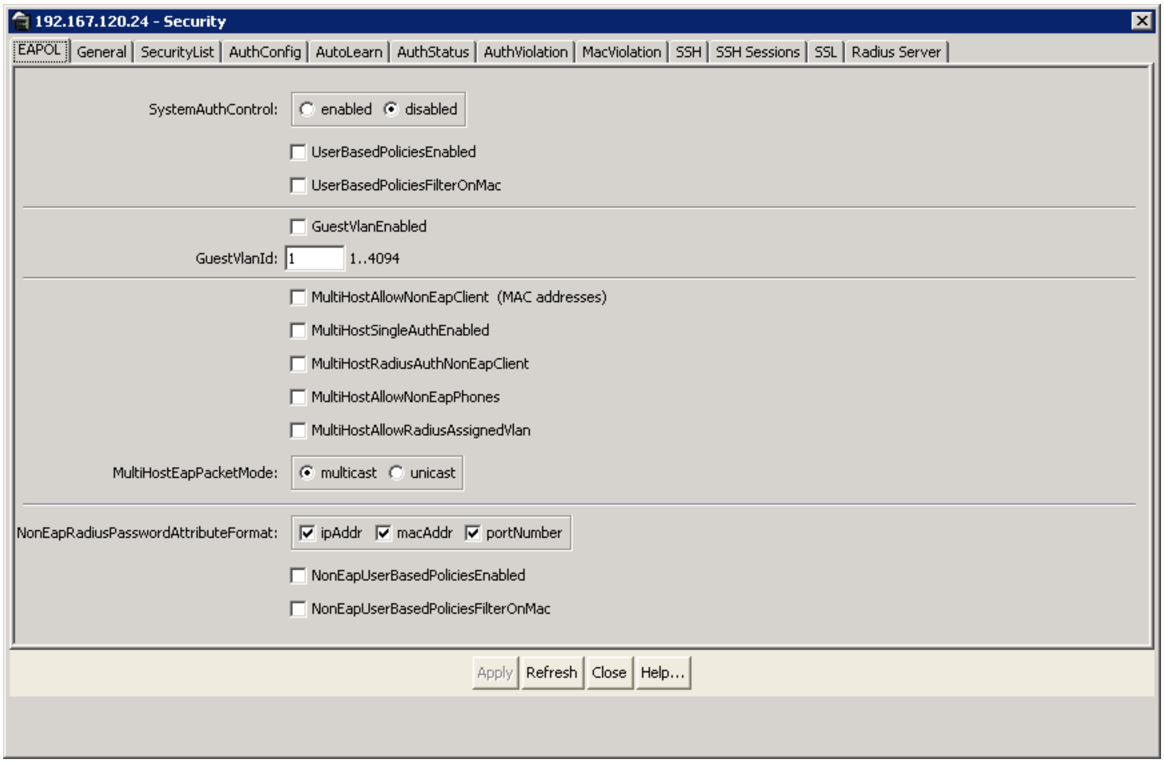
The following sections outline the configuration of EAPOL using Device Manager:

- "Global EAPOL configuration" (page 152)
- "Port-based EAPOL configuration" (page 154)
- "Non-EAPOL host support settings" (page 160)
- "Graphing EAPOL statistics" (page 163)

Global EAPOL configuration

Global EAPOL settings are configured on the **Security** screen on the EAPOL tab. "EAPOL tab" (page 152)illustrates the **EAPOL** tab.

EAPOL tab



SystemAuthControl: ○ enabled ● disabled

□ UserBasedPoliciesEnabled

□ UserBasedPoliciesFilterOnMac

□ GuestVlanEnabled

GuestVlanId: 1 1..4094

□ MultiHostAllowNonEapClient (MAC addresses)

□ MultiHostSingleAuthEnabled

□ MultiHostRadiusAuthNonEapClient

□ MultiHostAllowNonEapPhones

□ MultiHostAllowRadiusAssignedVlan

MultiHostEapPacketMode: ● multicast ○ unicast

NonEapRadiusPasswordAttributeFormat: ☑ ipAddr ☑ macAddr ☑ portNumber

□ NonEapUserBasedPoliciesEnabled

□ NonEapUserBasedPoliciesFilterOnMac

To edit the EAPOL settings, follow this procedure:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **EAPOL** tab.
2	In the fields provided, edit the EAPOL information. The following table outlines the fields on this tab.

EAPOL tab fields

Field	Description
SystemAuthControl	Enables or disables port access control on the switch.
UserBasedPolicies Enabled	Enables or disables EAPOL user-based policies. For more information about user-based policies, see *Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service* (NN47200-504).
GuestVlanEnabled	Enables or disables the Guest VLAN.
GuestVlanId	Sets the VLAN ID of the Guest VLAN.
MultiHostAllow NonEapClient	Enables or disables support for non-EAPOL hosts on EAPOL-enabled ports.
MultiHostSingle AuthEnabled	Enables or disables Multiple Host Single Authentication (MHSA). When selected, non-EAPOL hosts are allowed on a port if there is one authenticated EAPOL client on the port.
MultiHostRadiusAuth NonEapClient	Enables or disables RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports.
MultiHostAllowNonEapPhones	Enables or disables Nortel IP Phone clients as another non-EAP type.
MultiHostAllow RadiusAssignedVlan	Enables or disables the use of Radius-assigned VLAN values in the Multihost mode.
MultiHostEapPacketMode	Enables or disables the choice of packet mode (unicast or multicast) in the Multihost mode.
NonEapRadius PasswordAttributeFormat	Enables or disables setting the format of the Radius Server’s password attribute for non-EAP clients.
NonEapUserBased PoliciesEnabled	Enables or disables non-EAP user-based policies.
UserBasedPoliciesFilterOnMac	Enables or disables the filter on MAC addresses for user-based policies.
NonEapUserBased PoliciesFilterOnMac	Enables or disables the filter on MAC addresses for non-EAP user-based policies.

3 Click **Apply**.

—End—

Port-based EAPOL configuration

Port-specific EAPOL configuration is performed on the **EAPOL** and **EAPOL Advance** tabs of the **Port** screen.

For details, refer to the following:

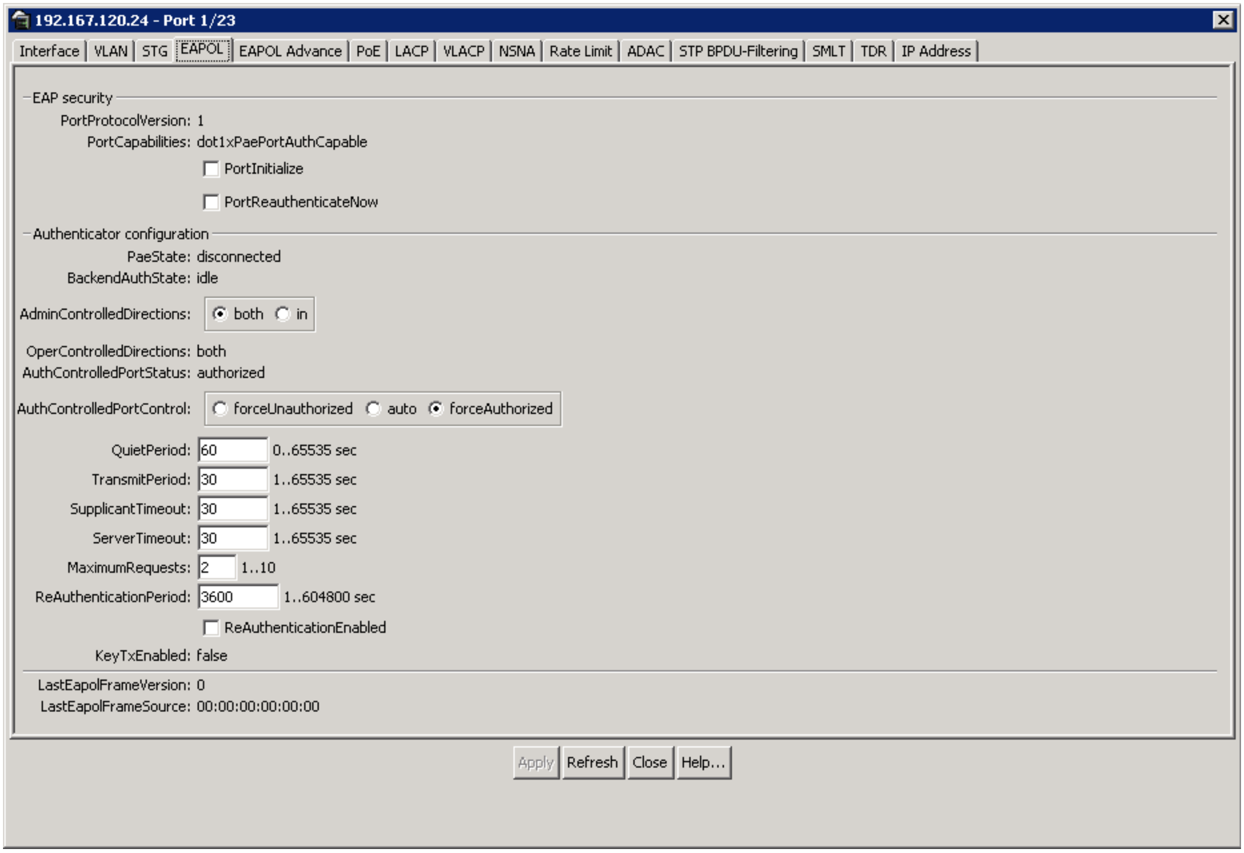
- "EAPOL tab for ports" (page 154)
- "EAPOL Advance tab for ports" (page 156)
- "Viewing Multihost information" (page 158)

EAPOL tab for ports Use the **EAPOL** tab to configure EAPOL-based security settings for a specific port.

To view the **EAPOL** tab, follow this procedure:

Step	Action
1	Select the port to edit from the **Device View**. Select **Edit > Port** from the menu. The **Port** screen appears. Select the **EAPOL** tab. " EAPOL-port tab" (page 154)illustrates the **EAPOL-port** tab.

EAPOL-port tab



EAP security

PortProtocolVersion: 1
PortCapabilities: dot1xPaePortAuthCapable
□ PortInitialize
□ PortReauthenticateNow

Authenticator configuration

PaeState: disconnected
BackendAuthState: idle
AdminControlledDirections: ● both ○ in
OperControlledDirections: both
AuthControlledPortStatus: authorized
AuthControlledPortControl: ○ forceUnauthorized ○ auto ● forceAuthorized
QuietPeriod: 60 0..65535 sec
TransmitPeriod: 30 1..65535 sec
SupplicantTimeout: 30 1..65535 sec
ServerTimeout: 30 1..65535 sec
MaximumRequests: 2 1..10
ReAuthenticationPeriod: 3600 1..604800 sec
□ ReAuthenticationEnabled
KeyTxEnabled: false

LastEapolFrameVersion: 0
LastEapolFrameSource: 00:00:00:00:00:00

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

EAPOL tab fields

Field	Description
PortProtocolVersion	Specifies the EAP Protocol version that is running on this port.
PortCapabilities	Specifies the PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Initializes the port’s EAPOL state. ***Note:*** Set this attribute to True to initialize the port’s EAPOL state.
PortReauthenticateNow	Reauthenticates the client. ***Note:*** Set this attribute to True to reauthenticate the client.
PaeState	Specifies the current authenticator PAE state machine state value.
BackendAuthState	Specifies the current state of the Backend Authentication state machine.
AdminControlledDirections	Specifies the current value of the administrative controlled directions parameter for the port.
OperControlledDirections	Specifies the current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	Specifies the current value of the controlled port status parameter for the port.
AuthControlledPortControl	Specifies the current value of the controlled port control parameter for the port.
QuietPeriod	Specifies the current value of the time interval between authentication failure and new authentication start.
TransmitPeriod	Specifies the time period to wait for a response from the supplicant for EAP requests/Identity packets.
Supplicant Timeout	Specifies the time period to wait for a response from the supplicant for all EAP packets except EAP Request/Identity. The default is 30 seconds. The time interval can be between 1 and 65535 seconds.
ServerTimeout	Specifies the time period to wait for a response from the RADIUS server. The default is 30 seconds. The time interval can be between 1 and 65535 seconds.
MaximumRequests	Specifies the number of allowed retries while sending packets to the supplicant. The default is 2 seconds. The number of retries can be between 1 and 10.
ReAuthenticationPeriod	Specifies the time interval between successive re-authentications. The default is 3600 seconds. The time interval can be between 1 and 604800 seconds.

Field	Description
ReAuthenticationEnabled	Specifies if reauthentication is required. ***Note:*** Set this attribute to True to reauthenticate an existing supplicant at the time interval specified in the ReauthenticationPeriod field.
KeyTxEnabled	Specifies the value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns a value of False because key transmission is irrelevant.
LastEapolFrameVersion	Specifies the protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	Specifies the source MAC address carried in the most recently received EAPOL frame.

2 Click **Apply** after making any changes.

—End—

See also:

- "EAPOL Advance tab for ports" (page 156)
- "Viewing Multihost information" (page 158)

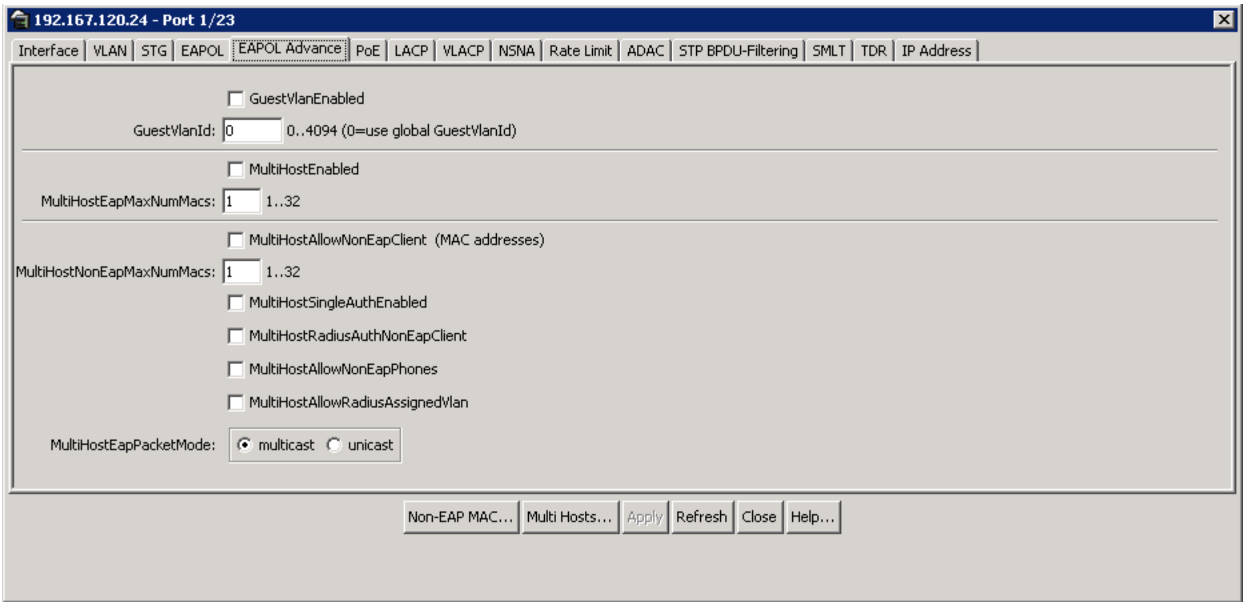
EAPOL Advance tab for ports Use the **EAPOL Advance** tab to configure advanced EAPOL options for a specific port.

> ***Note:*** The Multi Hosts and Non-EAP MAC buttons are not available when configuring multiple ports on the EAPOL Advance tab. To make use of these two options, only one port can be selected.

To view the **EAPOL Advance** tab, follow this procedure:

Step	Action
1	Select the port to edit from the **Device View**. Select **Edit > Port** from the menu. The **Port** screen appears. Select the **EAPOL Advance** tab. "Port Screen-EAPOL Advance tab" (page 157)illustrates the **EAPOL Advance** tab.

Port Screen-EAPOL Advance tab



☐ GuestVlanEnabled

GuestVlanId: 0 0..4094 (0=use global GuestVlanId)

☐ MultiHostEnabled

MultiHostEapMaxNumMacs: 1 1..32

☐ MultiHostAllowNonEapClient (MAC addresses)

MultiHostNonEapMaxNumMacs: 1 1..32

☐ MultiHostSingleAuthEnabled

☐ MultiHostRadiusAuthNonEapClient

☐ MultiHostAllowNonEapPhones

☐ MultiHostAllowRadiusAssignedVlan

MultiHostEapPacketMode: ● multicast ○ unicast

The following table describes the **EAPOL Advance** tab fields.

EAPOL Advance tab fields

Field	Description
GuestVlanEnabled	Enables or disables Guest VLAN functionality.
GuestVlanId	Specifies the VLAN ID of the VLAN that acts as the Guest VLAN. The default is 0. The Guest VLAN ID can be between 0 and 4094. ***Note:*** Use 0 to indicate a global Guest VLAN ID.
MultiHostEnabled	Enables or disables Multiple Host/MAC support with Multiple Authentication (MHMA).
MultiHostEapMaxNumMacs	Specifies the maximum number of EAPOL- authenticated clients allowed on this port. The default is 1. The maximum number can be between 1 and 32.
MultiHostAllowNonEapClient	Enables or disables support for non-EAPOL clients using local authentication.

Field	Description
MultiHostNonEapMaxNumMacs	Specifies the maximum number of non-EAPOL clients allowed on this port. The default is 1. The maximum number can be between 1 and 32.
MultiHostSingleAuthEnabled	Enables or disables Multiple Host with Single Authentication (MHSA) support for non-EAPOL clients.
MultiHostRadiusAuthNonEapClient	Enables or disables support for non-EAPOL clients using RADIUS authentication.
MultiHostAllowNonEapPhones	Enables or disables support for Nortel IP Phone clients as another non-EAP type.
MultiHostAllowRadiusAssignedVlan	Enables or disables support for VLAN values assigned by the Radius server.
MultiHostEapPacketMode	Specifies the mode of EAPOL packet transmission (multicast or unicast).

2 Click **Apply** after making any changes.

—End—

See also:

- "EAPOL tab for ports" (page 154)
- "Viewing Multihost information" (page 158)

Viewing Multihost information From the **EAPOL Advance** tab on the **Port** screen, it is possible to view Multihost information by clicking the **Multi Hosts** button on this tab.

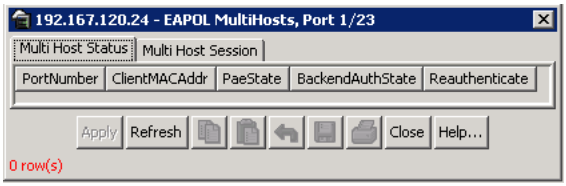
For details, refer to:

- "Multihost Status" (page 158)
- "Multihost sessions" (page 159)

Multihost Status To view multihost status information, do the following:

Step	Action
1	From the **EAPOL Advance** tab of the **Port** screen, click the **Multi Hosts** button. The **EAPOL MultiHosts** screen appears with the **Multi Host Status** tab selected. "EAPOL MultiHosts screen -- Multi Host Status tab" (page 159)illustrates this tab.

EAPOL MultiHosts screen -- Multi Host Status tab



The following table describes the fields on this screen.

EAPOL MultiHosts screen -- Multi Host Status tab

Field	Description
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.
PaeState	The current state of the authenticator PAE state machine.
BackendAuthState	The current state of the backend authentication state machine.
Reauthenticate	The value used to reauthenticate the EAPOL client.

—End—

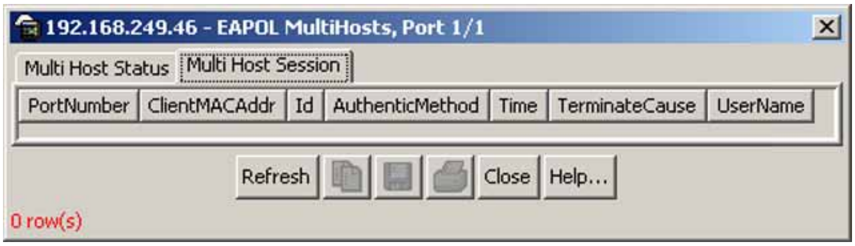
See also:

- "Multihost sessions" (page 159)

Multihost sessions To view multihost session information, do the following:

Step	Action
1	From the **EAPOL Advance** tab of the **Port** screen, click the **Multi Hosts** button. The **EAPOL MultiHosts** screen appears. Select the **Multi Host Session** tab. "EAPOL MultiHosts screen -- Multi Host Session tab" (page 159)illustrates this tab.

EAPOL MultiHosts screen -- Multi Host Session tab



The following table describes the fields on this tab.

EAPOL MultiHosts screen -- Multi Host Session tab

Field	Description
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.
Id	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.
AuthenticMethod	The authentication method used to establish the session.
Time	The elapsed time of the session.
TerminateCause	The cause of the session termination.
UserName	The username representing the identity of the supplicant PAE machine.

—End—

See also:

- "Multihost Status" (page 158)

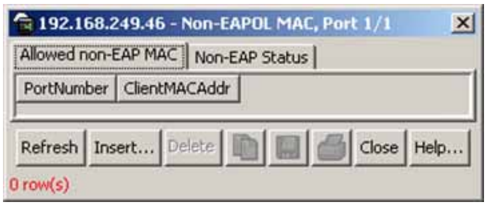
Non-EAPOL host support settings

From the **EAPOL Advance** tab on the **Port** screen, it is possible to view non-EAP host information and to configure the allowed non-EAP MAC address list by clicking the **Non-EAP MAC** button on this tab.

Managing the allowed non-EAP MAC address list To view and configure the list of MAC addresses for non-EAPOL clients that are authorized to access the port, do the following:

Step	Action
1	From the **EAPOL Advance** tab of the **Port** screen, click the **Non-EAP MAC** button. The **Non-EAPOL MAC** screen appears with the **Allowed non-EAP MAC** tab selected. "Non-EAPOL MAC screen -- Allowed non-EAP MAC tab" (page 161)illustrates this tab.

Non-EAPOL MAC screen -- Allowed non-EAP MAC tab



The following table describes the fields on this screen.

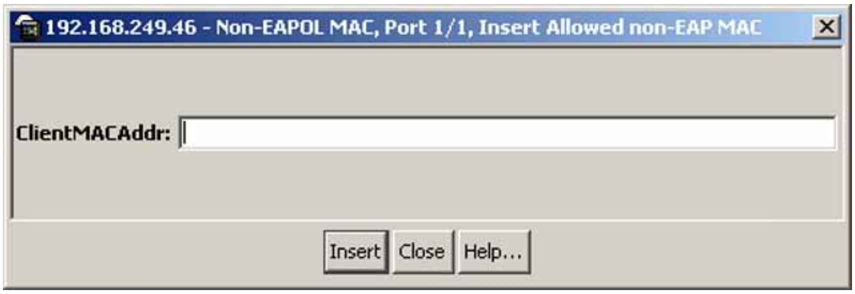
Non-EAPOL MAC screen -- Allowed non-EAP MAC tab

Field	Description
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.

2 To add a MAC address to the list of allowed non-EAPOL clients:

a. Click the **Insert** button. The **Insert Allowed non-EAP MAC** screen appears. "Insert Allowed non-EAP MAC screen" (page 161)illustrates this screen.

Insert Allowed non-EAP MAC screen


192.168.249.46 - Non-EAPOL MAC, Port 1/1, Insert Allowed non-EAP MAC
ClientMACAddr:
Insert
Close
Help...

b. Enter the MAC address of the non-EAPOL client you want to add to the list.

c. Click **Insert**.

3 To remove a MAC address from the list of allowed non-EAPOL clients:

a. Select the MAC address in the ClientMACAddr column on the **Allowed non-EAP MAC** tab.

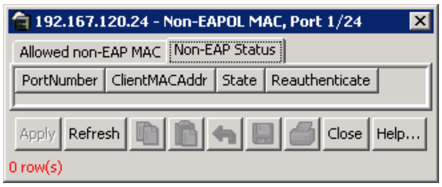
b. Click **Delete**.

—End—

Viewing non-EAPOL host support status To view the status of non-EAPOL host support on the port, do the following:

Step	Action
1	From the **EAPOL Advance** tab of the **Port** screen, click the **Non-EAP MAC** button. The **Non-EAPOL MAC** screen appears with the **Allowed non-EAP MAC** tab selected. Select the **Non-EAP Status** tab. "Non-EAPOL MAC screen -- Non-EAP Status tab" (page 162)illustrates this tab.

Non-EAPOL MAC screen -- Non-EAP Status tab



The following table describes the fields on this screen.

Non-EAPOL MAC screen -- Non-EAP Status tab

Field	Description
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.
State	The authentication status. Possible values are: • rejected: the MAC address cannot be authenticated on this port. • locallyAuthenticated: the MAC address was authenticated using the local table of allowed clients. • radiusPending: the MAC address is awaiting authentication by a RADIUS server. • radiusAuthenticated: the MAC address was authenticated by a RADIUS server. • adacAuthenticated: the MAC address was authenticated using ADAC configuration tables. • mhsaAuthenticated: the MAC address was auto-authenticated on a port following successful. authentication of an EAP client.

Field	Description
Reauthenticate	The value used to reauthenticate the MAC address of the client on the port.

—End—

Graphing EAPOL statistics

EAPOL port-based statistics can be graphed and analyzed on the **Graph Port** screen. Refer to the *Nortel Ethernet Routing Switch 5500 Series Configuration — System Monitoring* (NN47200-505) for specific instructions.

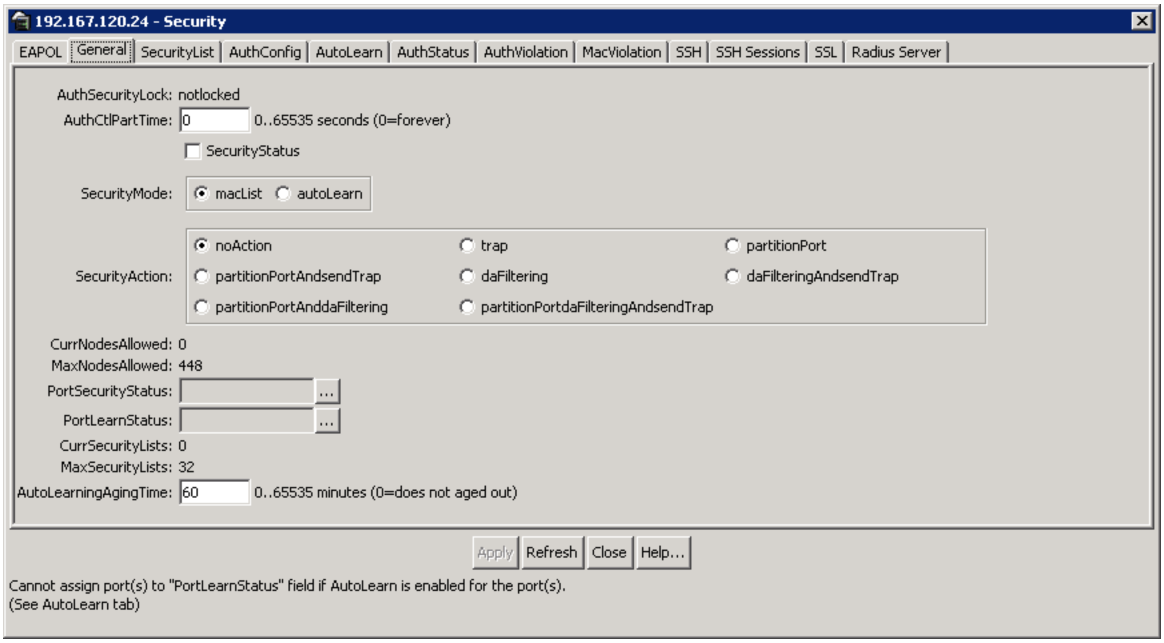
See also:

- "Global EAPOL configuration" (page 152)
- "Port-based EAPOL configuration" (page 154)
- "Non-EAPOL host support settings" (page 160)

General tab

The **General** tab is used to configure and manage general switch security settings. This tab is illustrated in "General Tab" (page 163).

General Tab



AuthSecurityLock: notlocked
AuthCtlPartTime: 0 0..65535 seconds (0=forever)
□ SecurityStatus
SecurityMode: ● macList ○ autoLearn
SecurityAction: ● noAction ○ trap ○ partitionPort ○ partitionPortAndsendTrap ○ daFiltering ○ daFilteringAndsendTrap ○ partitionPortAnddaFiltering ○ partitionPortdaFilteringAndsendTrap
CurrNodesAllowed: 0
MaxNodesAllowed: 448
PortSecurityStatus: ...
PortLearnStatus: ...
CurrSecurityLists: 0
MaxSecurityLists: 32
AutoLearningAgingTime: 60 0..65535 minutes (0=does not aged out)

Cannot assign port(s) to "PortLearnStatus" field if AutoLearn is enabled for the port(s).
(See AutoLearn tab)

To configure the items on this tab, follow this procedure:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **General** tab.
2	Using the fields provided, configure general switch security settings. "General tab fields" (page 164) outlines the fields on this tab.

General tab fields

Field	Description
AuthSecurityLock	If this parameter is listed as "locked," the agent refuses all requests to modify the security configuration. Entries also include: • other • notlocked
AuthCtlPartTime	This value indicates the duration of time for port partitioning in seconds. Default: 0 (zero). When the value is zero, port remains partitioned until it is manually re-enabled.
SecurityStatus	Indicates whether or not the switch security feature is enabled.
SecurityMode	Mode of switch security. Entries include: • macList - Indicates that the switch is in the MAC-list mode. It is possible to configure more than one MAC address per-port. • autoLearn - Indicates that the switch learns the MAC addresses on each port as allowed addresses of that port.

Field	Description
SecurityAction	Actions performed by the software when a violation occurs (when SecurityStatus is enabled). The security action specified here applies to all ports of the switch. A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include: • noAction - Port does not have any security assigned to it, or the security feature is turned off. • trap - Listed trap. • partitionPort - Port is partitioned. • partitionPortAndsendTrap - Port is partitioned and traps are sent to the trap receive station. • daFiltering - Port filters out the frames where the destination address field is the MAC address of unauthorized Station. • daFilteringAndsendTrap - Port filters out the frames where the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive stations. • partitionPortAnddaFiltering - Port is partitioned and filters out the frames with the destination address field is the MAC address of unauthorized station. • partitionPortdaFilteringAndsendTrap - Port is partitioned and filters out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive stations. ***Note:*** "da" means destination addresses.
CurrNodesAllowed	Current number of entries of the nodes allowed in the AuthConfig tab.

Field	Description
MaxNodesAllowed	Maximum number of entries of the nodes allowed in the AuthConfig tab.
PortSecurityStatus	Set of ports for which security is enabled.
PortLearnStatus	Set of ports where auto-learning is enabled.
CurrSecurityLists	Current number of entries of the Security listed in the SecurityList tab
MaxSecurityLists	Maximum entries of the Security listed in the SecurityList tab.
AutoLearningAgingTime	Specify the MAC address age-out time, in minutes, for the auto-learned MAC addresses. A value of zero (0) indicates that the address never ages out.

3 Click **Apply**.

—End—

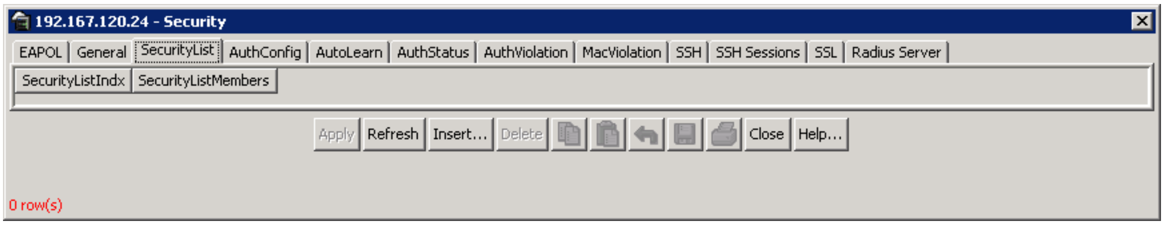
See also:

- " EAPOL Configuration" (page 152)
- "SecurityList tab" (page 166)
- "AuthConfig tab" (page 168)
- "AutoLearn tab" (page 170)
- "AuthStatus tab" (page 171)
- "AuthViolation tab" (page 174)
- "MacViolation tab" (page 176)
- "SSH tab" (page 177)
- "SSH Sessions tab" (page 179)
- "SSL tab" (page 180)
- "Radius Server tab" (page 182)

SecurityList tab

The **SecurityList** tab is used to add ports to a security list. This tab is illustrated in "SecurityList tab" (page 167).

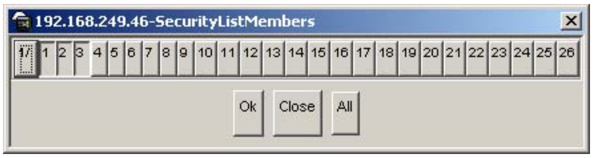
SecurityList tab



To configure ports for a security list, follow this procedure:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **SecurityList** tab.
2	To add ports to a security list, click **Insert**. To edit the port list for an existing security list, double-click in the **SecurityListMembers** field. In both cases, the **SecurityListMembers** screen appears. This screen is illustrated in " SecurityListMembers screen" (page 167).

SecurityListMembers screen



Step	Action
3	On the **SecurityListMembers** screen, select and uncheck the ports to be part of the security list by clicking the representative buttons. Click **All** to select all ports.
4	Click **Ok** on the **SecurityListMembers** screen.
5	Click **Insert**.

—End—

The **SecurityList** tab is now displayed with the modified port settings.

See also:

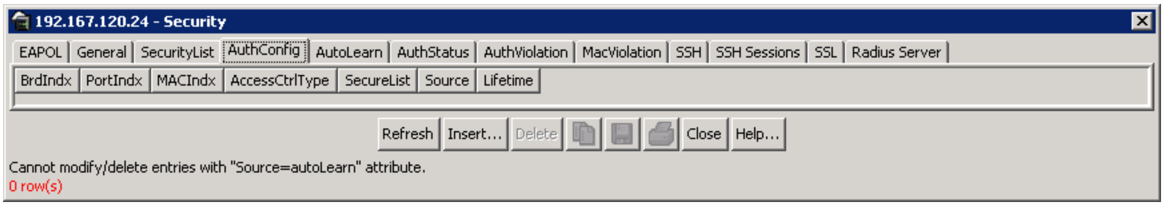
- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "AuthConfig tab" (page 168)
- "AutoLearn tab" (page 170)

- "AuthStatus tab" (page 171)
- "AuthViolation tab" (page 174)
- "MacViolation tab" (page 176)
- "SSH tab" (page 177)
- "SSH Sessions tab" (page 179)
- "SSL tab" (page 180)
- "Radius Server tab" (page 182)

AuthConfig tab

The **AuthConfig** tab contains a list of boards, ports and MAC addresses that have the security configuration. An SNMP SET PDU for a row in the tab requires the entire sequence of the MIB objects in each entry to be stored in one PDU. Otherwise, a GENERR return-value is returned. This tab is illustrated in "AuthConfig tab" (page 168).

AuthConfig tab

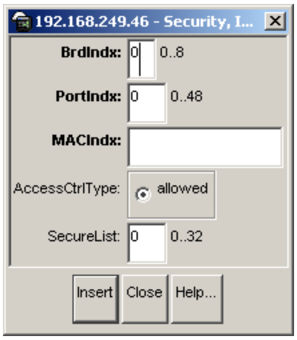


Cannot modify/delete entries with "Source=autoLearn" attribute.
0 row(s)

To add a new entry to the **AuthConfig** tab, follow this procedure:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **AuthConfig** tab.
2	Click **Insert**. The **Insert AuthConfig** screen appears. This screen is illustrated in " Insert AuthConfig screen" (page 168).

Insert AuthConfig screen



BrdIndx: 0 0..8
PortIndx: 0 0..48
MACIndx:
AccessCtrlType: ● allowed
SecureList: 0 0..32

3 In the fields provided, create the new entry for the **AuthConfig** tab. "Insert AuthConfig fields" (page 169) outlines the fields for this screen.

Insert AuthConfig fields

Field	Description
BrdIndx	Index of the board. This corresponds to the unit. ***Note:*** If this field is specified, the SecureList field is 0.
PortIndx	Index of the port. ***Note:*** If this field is specified, the SecureList field is 0.
MACIndx	An index of MAC addresses that are either designated as `allowed` (station) or `not-allowed` (station).
AccessCtrlType	Displays the node entry is `node allowed`. A MAC address can be allowed on multiple ports.
SecureList	The index of the security list. This value is meaningful only if BrdIndx and PortIndx values are set to zero. For other board and port index values, this field should also have the value of zero. The corresponding MAC Address of this entry is allowed or blocked on all ports of this port list.

4 Click **Insert**.

The new entry is now displayed in the **AuthConfig** tab.

—End—

See also:

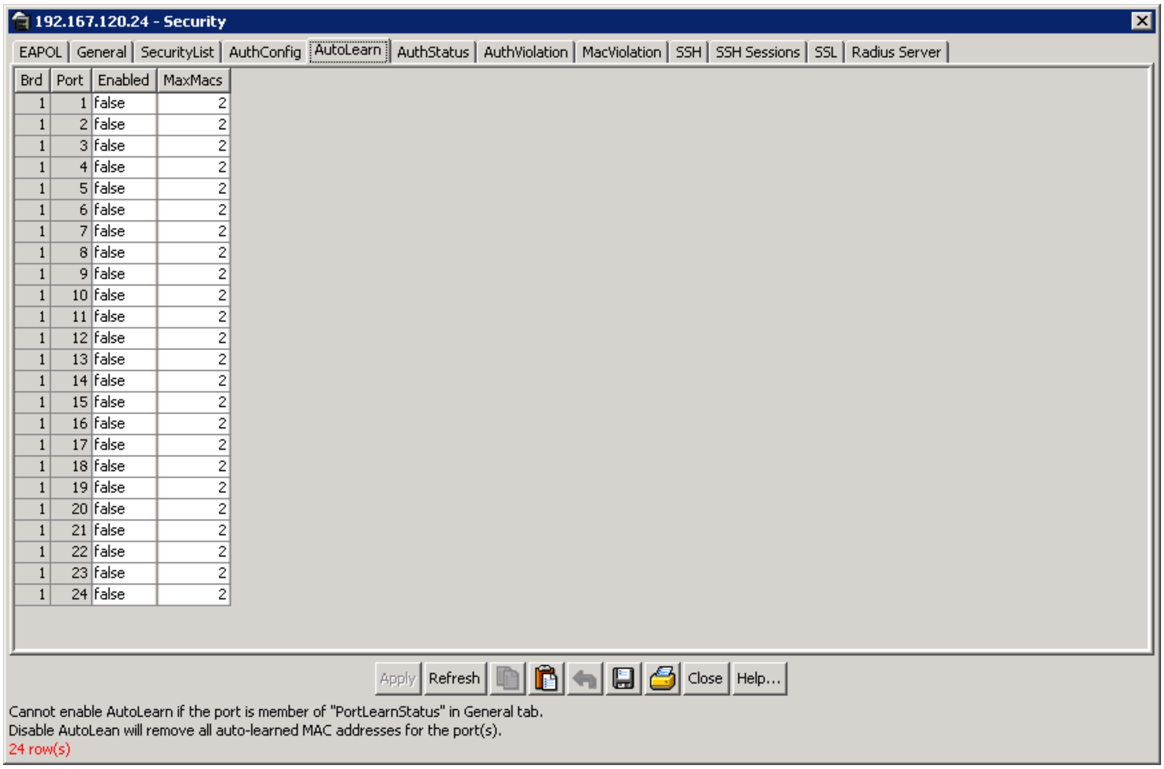
- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "SecurityList tab" (page 166)
- "AutoLearn tab" (page 170)

- "AuthStatus tab" (page 171)
- "AuthViolation tab" (page 174)
- "MacViolation tab" (page 176)
- "SSH tab" (page 177)
- "SSH Sessions tab" (page 179)
- "SSL tab" (page 180)
- "Radius Server tab" (page 182)

AutoLearn tab

The **AutoLearn** tab is used to configure the MAC Address auto-learning properties of the switch ports. The **AutoLearn** tab is illustrated in "AutoLearn Tab" (page 170).

AutoLearn Tab



Brd	Port	Enabled	MaxMacs
1	1	false	2
1	2	false	2
1	3	false	2
1	4	false	2
1	5	false	2
1	6	false	2
1	7	false	2
1	8	false	2
1	9	false	2
1	10	false	2
1	11	false	2
1	12	false	2
1	13	false	2
1	14	false	2
1	15	false	2
1	16	false	2
1	17	false	2
1	18	false	2
1	19	false	2
1	20	false	2
1	21	false	2
1	22	false	2
1	23	false	2
1	24	false	2

Cannot enable AutoLearn if the port is member of "PortLearnStatus" in General tab.
Disable AutoLean will remove all auto-learned MAC addresses for the port(s).
24 row(s)

To configure the auto-learning features, follow this procedure:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **AutoLearn** tab.

2 Select the port to be configured and change the desired settings. On this screen the following fields can be changed:

a. **Enabled** --This drop-down list enables or disables auto learning on the port.

b. **MaxMacs** -- The maximum number of MAC addresses the port will learn. This field can be a value between 1 and 25.

3 Click **Apply**.

—End—

See also:

- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "SecurityList tab" (page 166)
- "AuthConfig tab" (page 168)
- "AuthStatus tab" (page 171)
- "AuthViolation tab" (page 174)
- "MacViolation tab" (page 176)
- "SSH tab" (page 177)
- "SSH Sessions tab" (page 179)
- "SSL tab" (page 180)
- "Radius Server tab" (page 182)

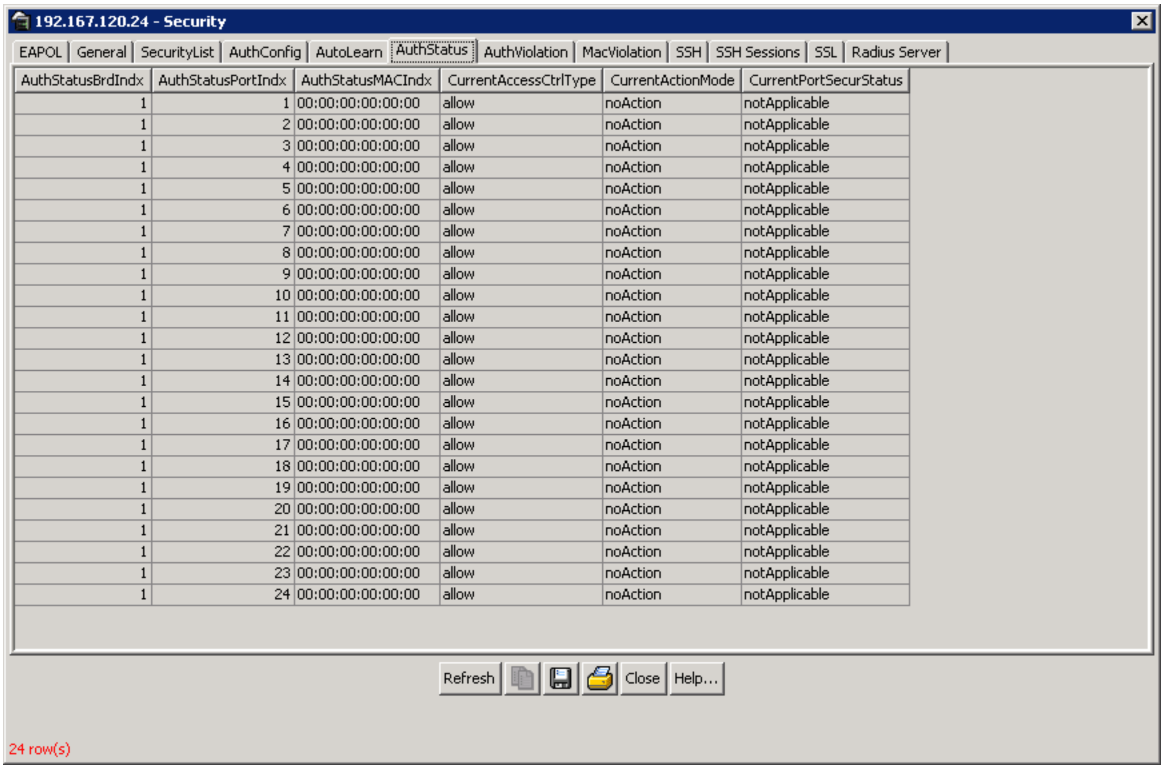
AuthStatus tab

The **AuthStatus** tab displays information of the authorized boards and port status data collection. Information includes actions to be performed when an unauthorized station is detected and the current security status of a port. Entries in this tab can include:

- A single MAC address
- All MAC addresses on a single port
- A single port
- All the ports on a single board
- A particular port on all the boards
- All the ports on all the boards

"AuthStatus Tab" (page 172)illustrates the **AuthStatus** tab.

AuthStatus Tab



AuthStatusBrdIndx	AuthStatusPortIndx	AuthStatusMACIndx	CurrentAccessCtrlType	CurrentActionMode	CurrentPortSecurStatus
1	1	00:00:00:00:00:00	allow	noAction	notApplicable
1	2	00:00:00:00:00:00	allow	noAction	notApplicable
1	3	00:00:00:00:00:00	allow	noAction	notApplicable
1	4	00:00:00:00:00:00	allow	noAction	notApplicable
1	5	00:00:00:00:00:00	allow	noAction	notApplicable
1	6	00:00:00:00:00:00	allow	noAction	notApplicable
1	7	00:00:00:00:00:00	allow	noAction	notApplicable
1	8	00:00:00:00:00:00	allow	noAction	notApplicable
1	9	00:00:00:00:00:00	allow	noAction	notApplicable
1	10	00:00:00:00:00:00	allow	noAction	notApplicable
1	11	00:00:00:00:00:00	allow	noAction	notApplicable
1	12	00:00:00:00:00:00	allow	noAction	notApplicable
1	13	00:00:00:00:00:00	allow	noAction	notApplicable
1	14	00:00:00:00:00:00	allow	noAction	notApplicable
1	15	00:00:00:00:00:00	allow	noAction	notApplicable
1	16	00:00:00:00:00:00	allow	noAction	notApplicable
1	17	00:00:00:00:00:00	allow	noAction	notApplicable
1	18	00:00:00:00:00:00	allow	noAction	notApplicable
1	19	00:00:00:00:00:00	allow	noAction	notApplicable
1	20	00:00:00:00:00:00	allow	noAction	notApplicable
1	21	00:00:00:00:00:00	allow	noAction	notApplicable
1	22	00:00:00:00:00:00	allow	noAction	notApplicable
1	23	00:00:00:00:00:00	allow	noAction	notApplicable
1	24	00:00:00:00:00:00	allow	noAction	notApplicable

24 row(s)

To view the **AuthStatus** tab:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **AuthStatus** tab. "AuthStatus tab fields" (page 172) describes the fields displayed on the AuthStatus tab.

AuthStatus tab fields

Field	Description
AuthStatusBrdIndx	The index of the board. This corresponds to the index of the slot containing the board if the index is greater than zero.
AuthStatusPortIndx	The index of the port on the board. This corresponds to the index of the last manageable port on the board if the index is greater than zero.

Field	Description
AuthStatusMACIndx	The index of MAC address on the port. This corresponds to the index of the MAC address on the port if the index is greater than zero.
CurrentAccessCtrlType	Displays whether the node entry is `node allowed` or `node blocked type`.
CurrentActionMode	A value representing the type of information contained, including: • noAction - Port does not have any security assigned to it, or the security feature is turned off. • partitionPort - Port is partitioned. • partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receive station. • Filtering - Port filters out the frames, where the destination address field is the MAC address of unauthorized station. • FilteringAndsendTrap - Port filters out the frames, where the destination address field is the MAC address of unauthorized station. Trap are sent to trap receive station. • sendTrap - A trap is sent to trap receive stations. • partitionPortAnddaFiltering - Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. • partitionPortdaFilteringAndsendTrap - Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive stations.
CurrentPortSecurStatus	Displays the security status of the current port, including: • If the port is disabled, notApplicable is returned. • If the port is in a normal state, portSecure is returned.

Field	Description
	• If the port is partitioned, portPartition is returned.

—End—

See also:

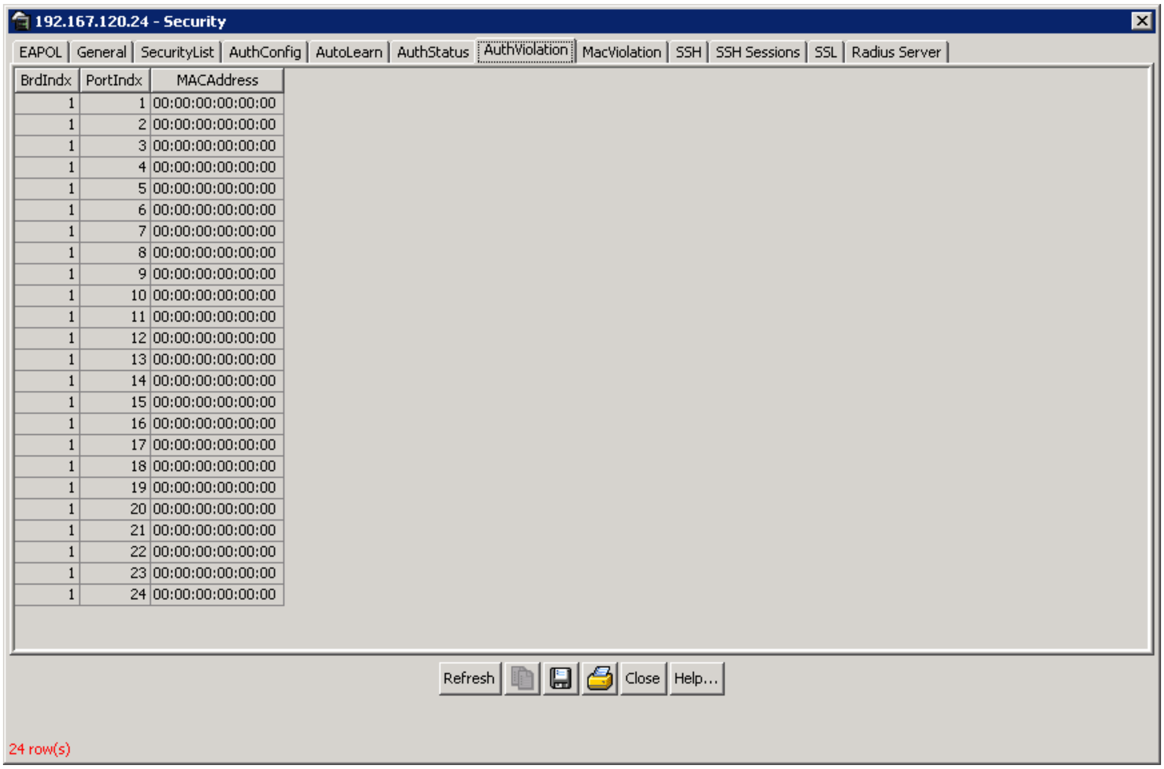
- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "SecurityList tab" (page 166)
- "AuthConfig tab" (page 168)
- "AutoLearn tab" (page 170)
- "AuthViolation tab" (page 174)
- "MacViolation tab" (page 176)
- "SSH tab" (page 177)
- "SSH Sessions tab" (page 179)
- "SSL tab" (page 180)
- "Radius Server tab" (page 182)

AuthViolation tab

The **AuthViolation** tab contains a list of boards and ports where network access violations have occurred, and also the identity of the offending MAC addresses.

"AuthViolation tab" (page 175) illustrates the **AuthViolation** tab.

AuthViolation tab



BrdIndx	PortIndx	MACAddress
1	1	00:00:00:00:00:00
1	2	00:00:00:00:00:00
1	3	00:00:00:00:00:00
1	4	00:00:00:00:00:00
1	5	00:00:00:00:00:00
1	6	00:00:00:00:00:00
1	7	00:00:00:00:00:00
1	8	00:00:00:00:00:00
1	9	00:00:00:00:00:00
1	10	00:00:00:00:00:00
1	11	00:00:00:00:00:00
1	12	00:00:00:00:00:00
1	13	00:00:00:00:00:00
1	14	00:00:00:00:00:00
1	15	00:00:00:00:00:00
1	16	00:00:00:00:00:00
1	17	00:00:00:00:00:00
1	18	00:00:00:00:00:00
1	19	00:00:00:00:00:00
1	20	00:00:00:00:00:00
1	21	00:00:00:00:00:00
1	22	00:00:00:00:00:00
1	23	00:00:00:00:00:00
1	24	00:00:00:00:00:00

24 row(s)

To view the **AuthViolation** tab:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **AuthViolation** tab. "AuthViolation tab fields" (page 175) outlines the fields on this tab.

AuthViolation tab fields

Field	Description
BrdIndx	The index of the board. This corresponds to the slot containing the board. The index is 1 where it is not applicable.
PortIndx	The index of the port on the board. This corresponds to the port on that a security violation was seen.
MACAddress	The MAC address of the device attempting unauthorized network access (MAC address-based security).

—End—

See also:

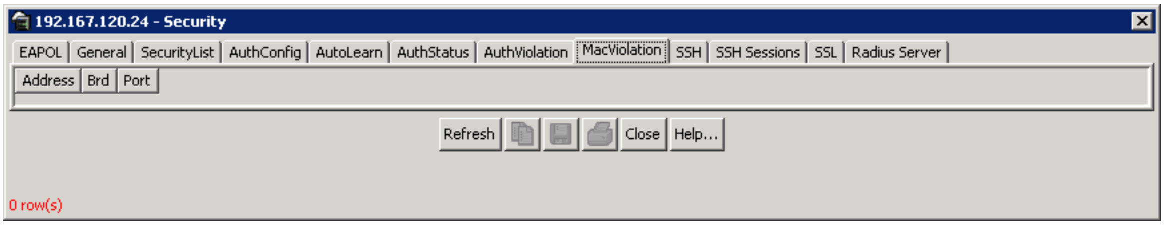
- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "SecurityList tab" (page 166)
- "AuthConfig tab" (page 168)
- "AutoLearn tab" (page 170)
- "AuthStatus tab" (page 171)
- "MacViolation tab" (page 176)
- "SSH tab" (page 177)
- "SSH Sessions tab" (page 179)
- "SSL tab" (page 180)
- "Radius Server tab" (page 182)

MacViolation tab

The **MacViolation** tab contains a list of boards and ports where network access violations have occurred, and also the identity of the offending MAC addresses.

"MacViolation tab" (page 176)illustrates this tab.

MacViolation tab



192.167.120.24 - Security

0 row(s)

To view the **MacViolation** tab:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **MacViolation** tab. "MacViolation tab fields" (page 177) outlines the fields on this tab.

MacViolation tab fields

Field	Description
Address	The MAC address of the device attempting unauthorized network access (MAC address-based security).
Brd	The index of the board. This corresponds to the slot containing the board. The index is 1 when it is not applicable.
Port	The index of the port on the board. This corresponds to the port on which a security violation was seen.

—End—

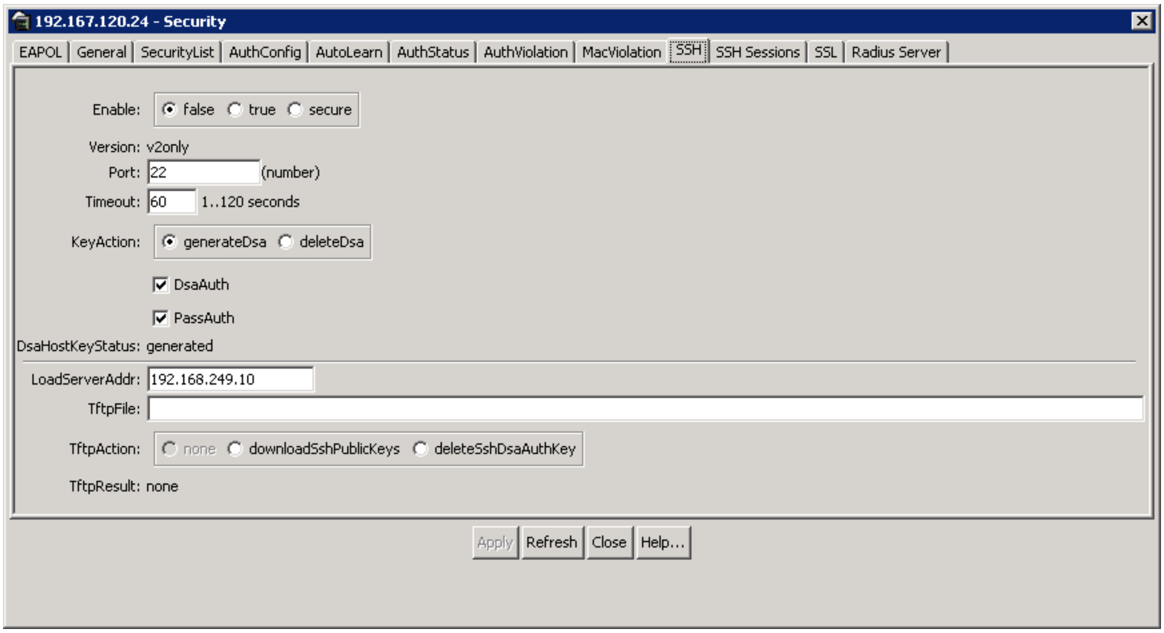
See also:

- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "SecurityList tab" (page 166)
- "AuthConfig tab" (page 168)
- "AutoLearn tab" (page 170)
- "AuthStatus tab" (page 171)
- "AuthViolation tab" (page 174)
- "SSH tab" (page 177)
- "SSH Sessions tab" (page 179)
- "SSL tab" (page 180)
- "Radius Server tab" (page 182)

SSH tab

The **SSH** tab provides parameters for configuring SSH. This tab is illustrated in "SSH tab" (page 178).

SSH tab


192.167.120.24 - Security
EAPOL | General | SecurityList | AuthConfig | AutoLearn | AuthStatus | AuthViolation | MacViolation | SSH | SSH Sessions | SSL | Radius Server
Apply | Refresh | Close | Help...

Enable: ● false ○ true ○ secure

Version: v2only

Port: 22 (number)

Timeout: 60 1..120 seconds

KeyAction: ● generateDsa ○ deleteDsa

☑ DsaAuth

☑ PassAuth

DsaHostKeyStatus: generated

LoadServerAddr: 192.168.249.10

TftpFile:

TftpAction: ○ none ○ downloadSshPublicKeys ○ deleteSshDsaAuthKey

TftpResult: none

To edit the SSH parameters on this tab, follow this procedure:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **SSH** tab.
2	In the fields provided, edit the SSH parameters. "SSH tab fields" (page 178) describes the fields on this tab.

SSH tab fields

Field	Description
Enable	Enables or disables SSH RSA authentication.
Version	Displays the SSH version.
Port	Displays the SSH connection port.
Timeout	Displays the SSH connection timeout in seconds.
KeyAction	Specifies the SSH key action.
DsaAuth	Enables or disables SSH DSA authentication.
PassAuth	Enables or disables SSH RSA authentication.

Field	Description
DsaHostKeyStatus	Indicates the current status of the SSH DSA host key. If the DSA host key has not yet been generated, the value is notGenerated(1). If it has already been generated, the value is generated(2). If it is currently being generated, the value is generating(3).
LoadServerAddr	Indicates the current server IP address.
TftpFile	Indicates the name of file for the TFTP transfer.
TftpAction	Specifies the action for the TFTP transfer.
TftpResult	Displays the result of the last TFTP action request.

3 Click **Apply**.

—End—

See also:

- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "SecurityList tab" (page 166)
- "AuthConfig tab" (page 168)
- "AutoLearn tab" (page 170)
- "AuthStatus tab" (page 171)
- "AuthViolation tab" (page 174)
- "MacViolation tab" (page 176)
- "SSH Sessions tab" (page 179)
- "SSL tab" (page 180)
- "Radius Server tab" (page 182)

SSH Sessions tab

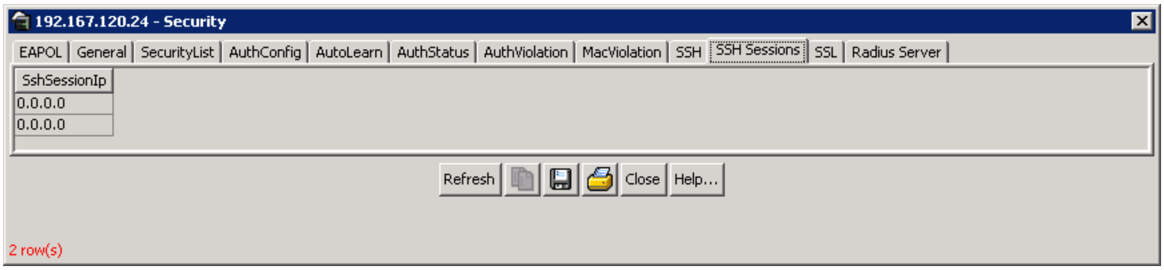
The **SSH Sessions** tab displays the currently active SSH sessions.

To view the **SSH Sessions** tab:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **SSH Sessions** tab.

"SSH Sessions tab" (page 180)illustrates the SSH Sessions tab.

SSH Sessions tab



SshSessionIp
0.0.0.0
0.0.0.0

2 row(s)

—End—

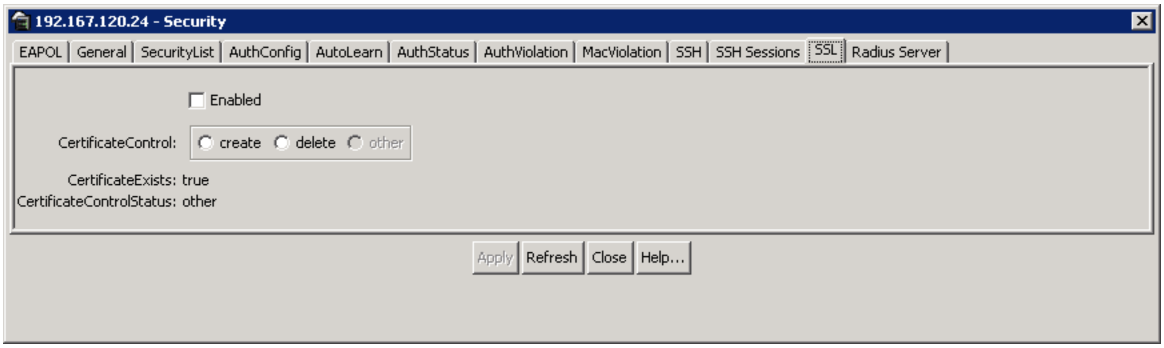
See also:

- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "SecurityList tab" (page 166)
- "AuthConfig tab" (page 168)
- "AutoLearn tab" (page 170)
- "AuthStatus tab" (page 171)
- "AuthViolation tab" (page 174)
- "MacViolation tab" (page 176)
- "SSH tab" (page 177)
- "SSL tab" (page 180)
- "Radius Server tab" (page 182)

SSL tab

The SSL tab is used to configure SSL operations on the switch. "SSL tab" (page 181)illustrates the SSL tab.

SSL tab



192.167.120.24 - Security

EAPOL | General | SecurityList | AuthConfig | AutoLearn | AuthStatus | AuthViolation | MacViolation | SSH | SSH Sessions | SSL | Radius Server

□ Enabled

CertificateControl: ○ create ○ delete ○ other

CertificateExists: true

CertificateControlStatus: other

To edit the SSL configuration from this tab, perform the following procedure:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **SSL** tab.
2	In the fields provided, edit the SSL configuration. "SSL tab fields" (page 181) outlines the fields on this tab.

SSL tab fields

Field	Description
Enabled	Indicates whether SSL is enabled or disabled
CertificateControl	Enables the creation and deletion of SSL certificates. Create allows you to create an SSL certificate, delete allows you to delete an SSL certificate. Setting the value to other (3) results in a wrongValue error. When retrieved, the object returns the value of the last value set, or other (3) if the object was never set.
CertificateExists	Indicates whether a valid SSL certificate has been created. A valid of true(1) indicates that a valid certificate has been created. A value of false(2) indicates that no valid certificate has been created, or that the certificate has been deleted.
CertificateControlStatus	Indicates the status of the most recent attempt to create or delete a certificate, The following status are displayed: • inProgress - the operation is not yet completed

Field	Description
	• success - the operation is complete • failure - the operation failed • other - the s5AgSslCertificateControl object was never set

—End—

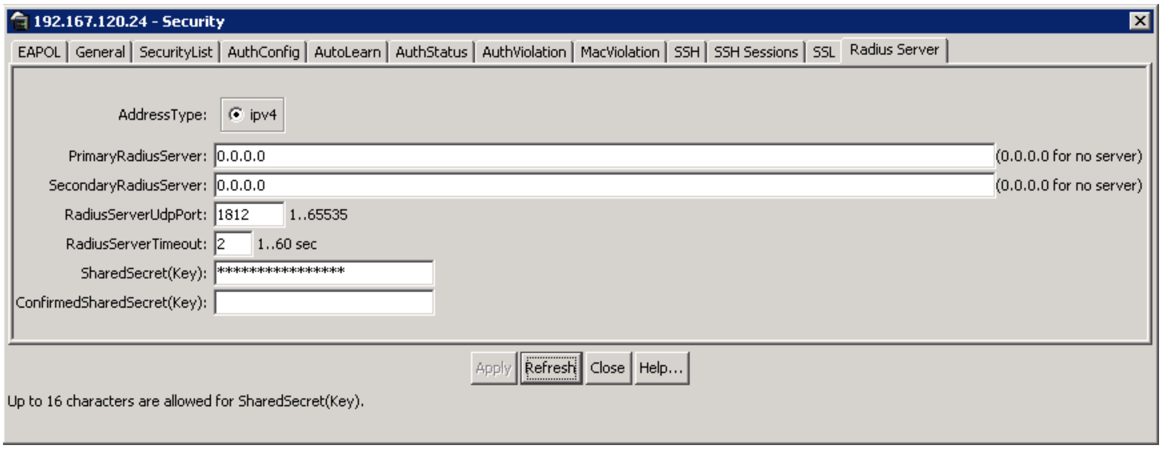
See also:

- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "SecurityList tab" (page 166)
- "AuthConfig tab" (page 168)
- "AutoLearn tab" (page 170)
- "AuthStatus tab" (page 171)
- "AuthViolation tab" (page 174)
- "MacViolation tab" (page 176)
- "SSH tab" (page 177)
- "SSH Sessions tab" (page 179)
- "Radius Server tab" (page 182)

Radius Server tab

The Radius Server tab is used to configure the primary and secondary RADIUS server settings. "Radius Server tab" (page 183) illustrates the Radius Server tab.

Radius Server tab


192.167.120.24 - Security
EAPOL | General | SecurityList | AuthConfig | AutoLearn | AuthStatus | AuthViolation | MacViolation | SSH | SSH Sessions | SSL | Radius Server
Apply | Refresh | Close | Help...

AddressType: ● ipv4

PrimaryRadiusServer: 0.0.0.0 (0.0.0.0 for no server)

SecondaryRadiusServer: 0.0.0.0 (0.0.0.0 for no server)

RadiusServerUdpPort: 1812 1..65535

RadiusServerTimeout: 2 1..60 sec

SharedSecret(Key): ****************

ConfirmedSharedSecret(Key):

Up to 16 characters are allowed for SharedSecret(Key).

To edit the Radius Server from this tab, perform the following procedure:

Step	Action
1	Open the **Security** screen by selecting **Edit > Security > Security** from the menu. Select the **Radius Server** tab.
2	In the fields provided, edit the Radius Server configuration. The following table outlines the fields on this tab.

Radius Server tab fields

Field	Description
Addresstype	Specifies the type of IP address used by the Radius server. IPv4 is currently the only available option.
PrimaryRadiusServer	Specifies the IP address of the primary server (default: 0.0.0.0). ***Note:*** If there is no primary Radius server, set the value of this field to 0.0.0.0 .
SecondaryRadiusServer	Specifies the IP address of the secondary Radius server (default: 0.0.0.0). The secondary Radius server is used only if the primary server is unavailable or unreachable.
RadiusServerUdpPort	Specifies the UDP port number (default: 1812). The port number can range between 1 and 65535.

Field	Description
RadiusServerTimeout	Specifies the timeout interval between each retry, for service requests to the Radius server. The default is 2 Seconds. The timeout period can range between 1 and 60 seconds.
SharedSecret(Key)	Specifies the value of the shared secret key. ***Note:*** The shared secret key has a maximum of 16 characters.
ConfirmedSharedSecret(Key)	Displays confirmation of the shared secret specified in the SharedSecret(Key) field.

3 Click **Apply**.

—End—

See also:

- " EAPOL Configuration" (page 152)
- "General tab" (page 163)
- "SecurityList tab" (page 166)
- "AuthConfig tab" (page 168)
- "AutoLearn tab" (page 170)
- "AuthStatus tab" (page 171)
- "AuthViolation tab" (page 174)
- "MacViolation tab" (page 176)
- "SSH tab" (page 177)
- "SSH Sessions tab" (page 179)

Configuring IP Source Guard using the Java Device Manager

IP Source Guard is a per-port security feature that works closely with values from the Dynamic Host Control Protocol (DHCP) snooping Binding Entry table. When IP Source Guard is enabled on an untrusted DHCP snooping port, an IP filter entry is created or deleted for that port automatically, based on IP information stored in the corresponding DHCP snooping Binding Table entry. IP Source Guard can be configured through the Nortel Networks Command Line Interface (NNCLI), the JDM and SNMP. To configure IP

Source Guard through the NNCLI, see "IP Source Guard Configuration" (page 133). For information about how IP Source Guard works, see "IP Source Guard" (page 53).

Prerequisites to IP Source Guard Configuration:

- Ensure that DHCP snooping is globally enabled. To configure DHCP snooping, see
  - — "Globally enabling DHCP snooping through the JDM" (page 185)
  - — "Enabling DHCP snooping globally" (page 115)
- Ensure that the port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- Ensure that the port is an untrusted DHCP Snooping and dynamic ARP Inspection port.
- Ensure that a minimum of 10 rules are available on the port.
- Ensure that the following MIB object exists:

  bsSourceGuardConfigMode

  Note: This object is used to control the IP Source Guard mode on an interface.
- Ensure that the following applications are not enabled:
  - — IP Fix
  - — Baysecure
  - — Extensible Authentication Protocol over LAN (EAPoL)

ATTENTION

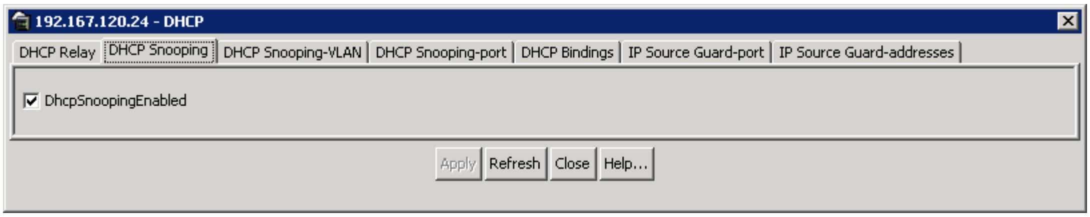
The IP addresses are obtained from DHCP snooping Binding Table entries defined automatically in the port. A maximum 10 IP addresses from the Binding Table are allowed and the rest are dropped.

Globally enabling DHCP snooping through the JDM

Globally enable DHCP snooping through the **DHCP snooping** tab of the **DHCP** screen. To enable DHCP snooping, follow this procedure:

Step	Action
1	Select the port to edit from the **Device View**. Select **IP Routing>DHCP** from the menu. The **DHCP** Screen appears. Select the **DHCP snooping** tab. "DHCP snooping tab" (page 186)illustrates the **DHCP snooping** tab.

DHCP snooping tab



☑ DhcpSnoopingEnabled

2 Enable the **DhcpSnoopingEnabled** field to enable DHCP snooping globally.

3 Click **Apply** after making any changes.

—End—

Enabling IP Source Guard

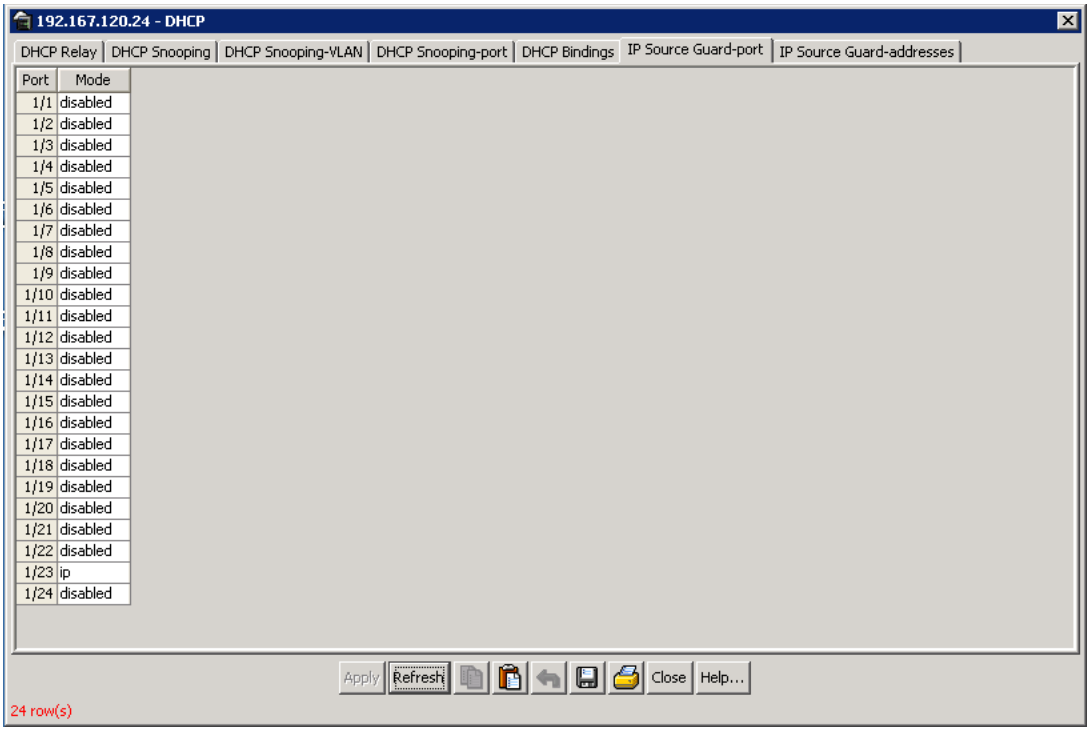
Enable IP Source Guard to add a higher level of security to the desired port by preventing IP spoofing. IP Source Guard can be enabled through the **IP Source Guard-port** tab of the **DHCP** screen.

To enable IP Source Guard for specific ports, follow this procedure:

Step Action

1 Select the port to edit from the **Device View.** Select **IP Routing> DHCP** from the menu. The **DHCP** Screen appears. Select the **IP Source Guard-port** tab. "IP Source Guard-port tab" (page 187)illustrates the **IP Source Guard-port** tab.

IP Source Guard-port tab



Port	Mode
1/1	disabled
1/2	disabled
1/3	disabled
1/4	disabled
1/5	disabled
1/6	disabled
1/7	disabled
1/8	disabled
1/9	disabled
1/10	disabled
1/11	disabled
1/12	disabled
1/13	disabled
1/14	disabled
1/15	disabled
1/16	disabled
1/17	disabled
1/18	disabled
1/19	disabled
1/20	disabled
1/21	disabled
1/22	disabled
1/23	ip
1/24	disabled

24 row(s)

The following table describes the fields on this screen:

IP Source Guard-port tab fields

Field	Description
Port	The port number.
Mode	The Source Guard mode of the port. The mode can be ’disabled’ or ’ip’.

2 Double-click on the mode next to the desired port and select **ip** from the drop-down list.

3 Click **Apply** after making any changes.

—End—

Setting IP Source Guard defaults on specified ports

Set IP Source Guard defaults on specified ports through the **IP Source Guard-port** tab of the **DHCP** screen.

To set the IP Source Guard defaults for specific ports, follow this procedure:

Step	Action
1	Select the port to edit from the **Device view**. Select **IP Routing> DHCP** from the menu. The **DHCP** Screen appears.
2	Select the **IP Source Guard-port** tab. "IP Source Guard-port tab" (page 187) illustrates the **IP Source Guard-port** tab. The following table describes the fields on this screen:

IP Source Guard-port tab fields

Field	Description
Port	The port number in the interface.
Mode	The Source Guard mode of the port. The mode can be 'disabled' or 'ip'.

3	Click **Refresh** to set the IP Source Guard defaults.

—End—

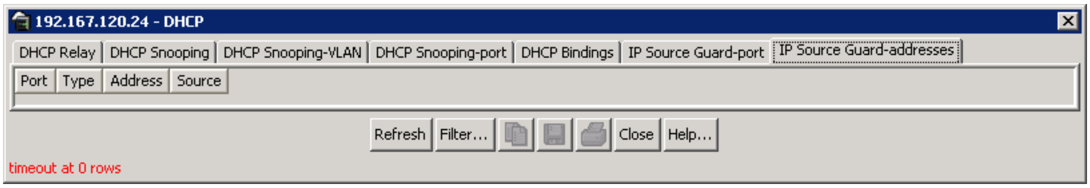
Viewing IP Source Guard port statistics

The **IP Source Guard-addresses** tab displays information about IP Source Guard.

To view the **IP Source Guard-addresses** tab, follow this procedure:

Step	Action
1	Select the port to edit from the **Device View**. Select **IP Routing> DHCP** from the menu. The **DHCP** Screen appears. Select the **IP Source Guard-addresses** tab. "IP Source Guard-addresses tab" (page 188)illustrates the **IP Source Guard-addresses** tab.

IP Source Guard-addresses tab



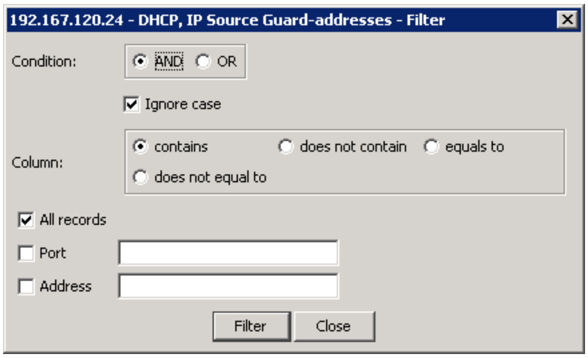
The following table describes the fields on this screen:

IP Source Guard-addresses tab fields

Field	Description
Port	The port number.
Type	The internet address type.
Address	The IP address allowed by IP Source Guard..
Source	The source of the address. ***Note:*** Currently, the only source is from DHCP snooping.

2 Click **Filter** to display selected IP addresses. The **IP Source Guard-addresses--Filter** screen appears. "IP Source Guard-addresses--Filter Screen" (page 189) illustrates the **IP Source Guard-addresses--Filter** screen.

IP Source Guard-addresses--Filter Screen



192.167.120.24 - DHCP, IP Source Guard-addresses - Filter

Condition: ● AND ○ OR

☑ Ignore case

Column: ● contains ○ does not contain ○ equals to ○ does not equal to

☑ All records

□ Port

□ Address

The following table describes the fields in this screen:

IP Source Guard-addresses Filter Screen tab fields

Field	Description
Condition	The type of search condition used. Possible values are: • AND: Includes keywords specified in both the Port and Address fields while filtering results. • OR: Includes either one of the keywords specified in the Port and Address fields while filtering results.
Ignore Case	Ignores the letter case while searching.

Column	Searches the columns based on the content of column search specified. Possible values are: • Contains • Does not contain • Equals to • Does not equal to
All records	Displays all entries in the table.
Port	Searches for the specified port.
Address	Searches for the specified IP address.

—End—

Disabling IP Source Guard

Disable IP Source Guard to allow all IP traffic to go through without being filtered. IP Source Guard can be disabled on the **IP Source Guard-port** tab of the **DHCP** screen.

To disable IP Source Guard for specific ports, follow this procedure:

Step Action

1 Select the port to edit from the **Device View**. Select **IP Routing> DHCP** from the menu. The **DHCP** Screen appears. Select the **IP Source Guard-port** tab. "IP Source Guard-port tab" (page 187) illustrates the **IP Source Guard-port** tab.

The following table describes the fields on this screen.

IP Source Guard-port tab fields

Field	Description
Port	The port number.
Mode	The mode of the port. The mode can be either ’disabled’ or ’ip’.

2 Double-click on the mode next to the desired port and select **Disabled** from the drop-down list.

3 Click **Apply** after making any changes.

—End—

Configuring DHCP snooping using the Java Device Manager

The following sections outline the configuration of DHCP snooping using the Java Device Manager:

- "Configuring DHCP snooping Globally" (page 191)
- "Configuring DHCP snooping on a VLAN" (page 193)
- "Configuring DHCP snooping on Ports" (page 195)

Configuring DHCP snooping Globally

The following sections outline the tasks that can be performed while configuring DHCP snooping globally:

- "Enabling DHCP snooping Globally" (page 191)
- "Disabling DHCP snooping Globally" (page 191)
- "Setting DHCP snooping to its default" (page 192)

Enabling DHCP snooping Globally

To enable DHCP snooping globally, see "Globally enabling DHCP snooping through the JDM" (page 185).

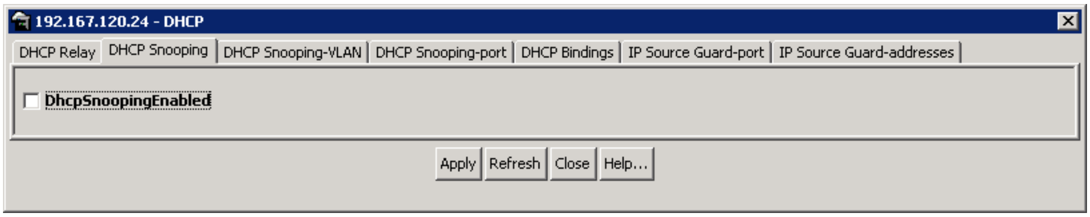
Disabling DHCP snooping Globally

Globally disable DHCP snooping through the **DHCP snooping** tab of the **DHCP** screen.

To disable DHCP snooping, follow this procedure:

Step	Action
1	Select the port to edit from the **Device View**.
2	Select **IP Routing > DHCP** from the menu. The **DHCP** screen appears.
3	Select the **DHCP snooping** tab. "DHCP snooping tab - Disable" (page 191) illustrates the DHCP snooping tab.

DHCP snooping tab - Disable



□ DhcpSnoopingEnabled

The following table outlines the fields on this tab.

DHCP snooping tab fields

Field	Description
DhcpSnoopingEnabled	Indicates whether DHCP snooping can be enabled or disabled.

4 Uncheck the **DhcpSnoopingEnabled** field to disable DHCP snooping globally.

5 Click **Apply** to make changes.

—End—

Setting DHCP snooping to its default

The changes made in the DHCP snooping tab of the DHCP screen can be restored to its default value. To set the default value, follow this procedure:

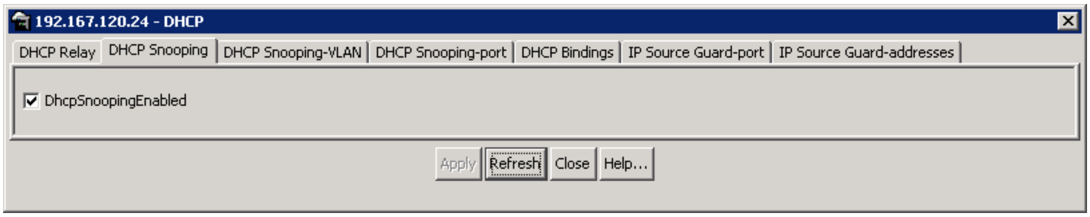
Step Action

1 Select the port to edit from the **Device View**.

2 Select **IP Routing > DHCP** from the menu. The **DHCP** screen appears.

3 Select the **DHCP snooping** tab. "DHCP snooping tab - Refresh" (page 192) illustrates the **DHCP snooping** tab.

DHCP snooping tab - Refresh



☑ DhcpSnoopingEnabled

The following table outlines the fields on this tab:

DHCP snooping tab fields

Field	Description
DhcpSnoopingEnabled	Indicates whether DHCP Snooping can be enabled or disabled.

4 Make changes to the fields in the DHCP snooping tab.

5 Click **Refresh** to restore the values in the tab to its default.

—End—

Configuring DHCP snooping on a VLAN

The following sections outline the tasks that can be performed while configuring DHCP snooping on a VLAN:

- "Enabling DHCP snooping on a VLAN" (page 193)
- "Disabling DHCP snooping on a VLAN" (page 194)

Enabling DHCP snooping on a VLAN

DHCP snooping can be enabled on a VLAN through the **DHCP snooping-VLAN** tab of the **DHCP** screen. You must enable DHCP snooping separately for each Vlan ID. if DHCP snooping is disabled on a VLAN, the switch forwards DHCP reply packets to all applicable ports, regardless of whether the port is trusted or untrusted.

To enable DHCP snooping on a VLAN, follow this procedure:

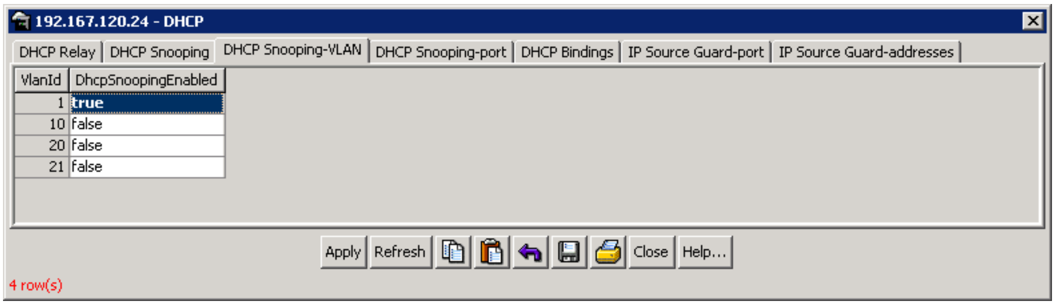
Step Action

1 Select the port to edit from the **Device view**.

2 Select **IP Routing > DHCP** from the menu. The **DHCP** screen appears.

3 Select the **DHCP snooping-VLAN** tab. "DHCP snooping-Vlan tab - Enable" (page 193) illustrates the **DHCP snooping-VLAN** tab.

DHCP snooping-Vlan tab - Enable



VlanId	DhcpSnoopingEnabled
1	true
10	false
20	false
21	false

4 row(s)

The following table outlines the fields on this tab:

DHCP snooping-VLAN tab fields

Field	Description
VlanId	Indicates the VlanId on the VLAN.
DhcpSnoopingEnabled	Indicates whether DHCP snooping can be enabled or disabled.

4 Double-click on the **DhcpSnoopingEnabled** field next to the appropriate VlanId.

The field changes to a drop-down list.

5 Select **true** from the drop-down list to enable DHCP snooping on the VLAN for the VlanId.

6 Click **Apply** to make the changes.

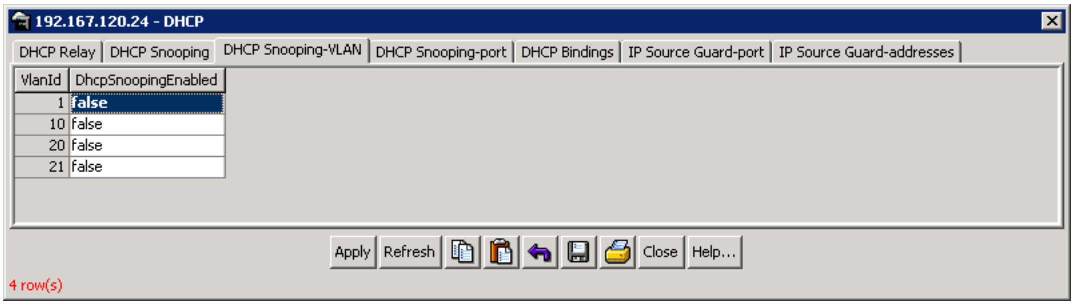
—End—

Disabling DHCP snooping on a VLAN

DHCP snooping can be disabled for a VLAN through the **DHCP Snooping-VLAN** tab of the **DHCP** screen.

Step	Action
1	Select the port to edit from the **Device view**.
2	Select **IP Routing > DHCP** from the menu. The **DHCP** screen appears.
3	Select the **DHCP snooping-VLAN** tab. "DHCP snooping-VLAN tab - Disable" (page 194) illustrates the **DHCP snooping-VLAN** tab.

DHCP snooping-VLAN tab - Disable



VlanId	DhcpSnoopingEnabled
1	false
10	false
20	false
21	false

4 row(s)

The following table outlines the fields on this tab:

DHCP snooping-VLAN tab fields

Field	Description
VlanId	Indicates the VlanId on the VLAN.
DhcpSnoopingEnabled	Indicates whether DHCP snooping can be enabled or disabled.

4 Double-click on the **DhcpSnoopingEnabled** field next to the appropriate VlanId.

The field changes to a drop-down list.

5 Select **false** from the drop-down list to disable DHCP snooping on the VLAN for the VlanId.

6 Click **Apply** to make the changes.

—End—

Configuring DHCP snooping on Ports

The following sections outline the tasks that can be performed while configuring DHCP snooping on ports:

- "Setting trusted ports for DHCP snooping" (page 195)
- "Setting untrusted ports for DHCP snooping" (page 196)

Setting trusted ports for DHCP snooping

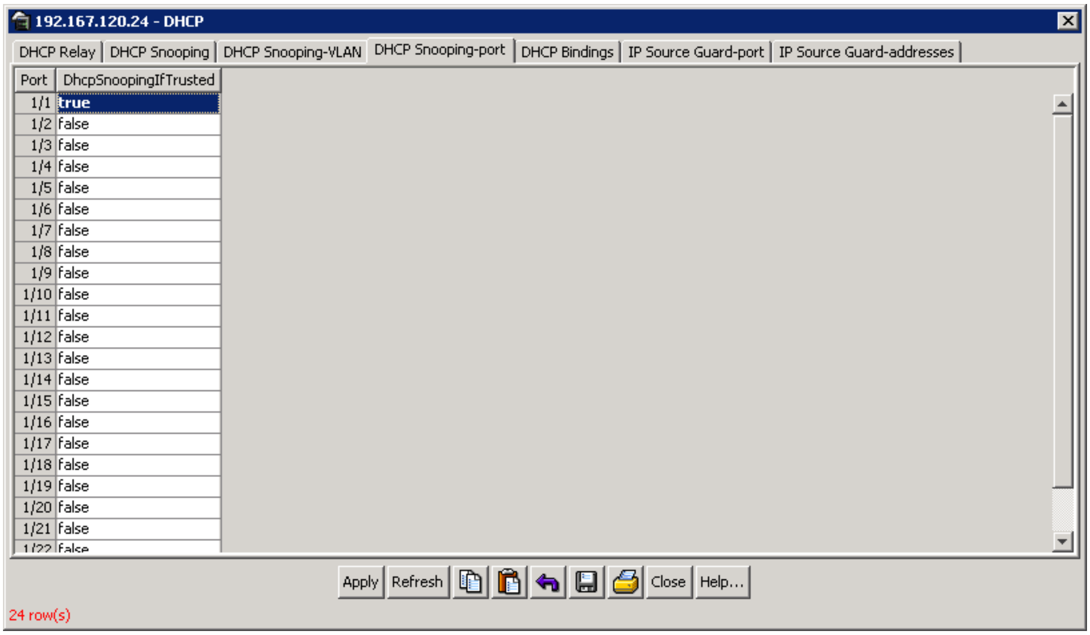
Ports can be set to be trusted or untrusted for DHCP snooping from the **DHCP Snooping-port** tab of the **DHCP** screen. To set a port to be trusted, follow this procedure:

Step Action

1 Select **IP Routing>DHCP** from the menu. The **DHCP** screen appears.

2 Select the **DHCP snooping-port** tab. "DHCP snooping-port tab - Trusted" (page 196) illustrates the **DHCP snooping-port** tab.

DHCP snooping-port tab - Trusted



Port	DhcpSnoopingIfTrusted
1/1	true
1/2	false
1/3	false
1/4	false
1/5	false
1/6	false
1/7	false
1/8	false
1/9	false
1/10	false
1/11	false
1/12	false
1/13	false
1/14	false
1/15	false
1/16	false
1/17	false
1/18	false
1/19	false
1/20	false
1/21	false
1/22	false

24 row(s)

The following table outlines the fields on this tab:

DHCP Snooping-port tab fields

Field	Description
Port	Indicates the port on the switch.
DhcpSnoopingIfTrusted	Indicates whether the port is trusted or untrusted. Default is false.

3 Double-click on the **DhcpSnoopingIfTrusted** field next to the appropriate port.

The field changes to a drop-down list.

4 Select **true** from the drop-down list to set the port to be trusted.

5 Click **Apply** to make the changes.

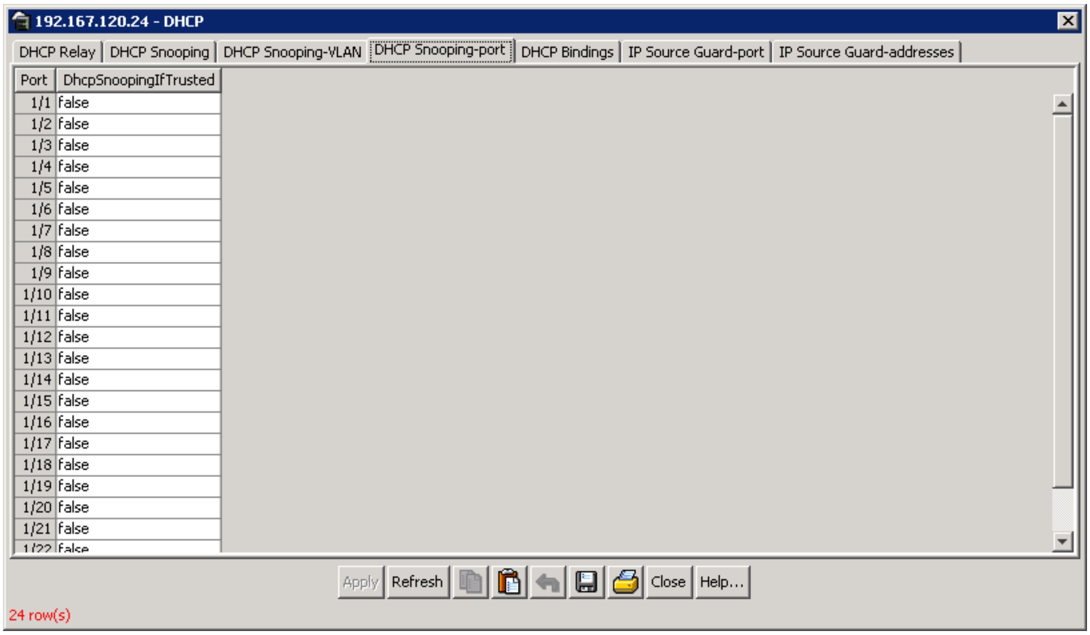
—End—

Setting untrusted ports for DHCP snooping

Ports can be set to be trusted or untrusted for DHCP snooping from the **DHCP Snooping-port** tab of the **DHCP** screen. To set a port to be untrusted, follow this procedure:

Step	Action
1	Select **IP Routing>DHCP** from the menu. The **DHCP** screen appears.
2	Select the **DHCP snooping-port** tab. "DHCP snooping-port tab - Untrusted" (page 197) illustrates the **DHCP snooping-port** tab.

DHCP snooping-port tab - Untrusted



Port	DhcpSnoopingIfTrusted
1/1	false
1/2	false
1/3	false
1/4	false
1/5	false
1/6	false
1/7	false
1/8	false
1/9	false
1/10	false
1/11	false
1/12	false
1/13	false
1/14	false
1/15	false
1/16	false
1/17	false
1/18	false
1/19	false
1/20	false
1/21	false
1/22	false

24 row(s)

The following table outlines the fields on this tab:

DHCP snooping-port tab fields

Field	Description
Port	Indicates the port on the switch.
DhcpSnoopingIfTrusted	Indicates whether the port is trusted or untrusted. Default is false.

3	Double-click on the **DhcpSnoopingIfTrusted** field next to the appropriate port. *The field changes to a drop-down list.*
4	Select **false** from the drop-down list to set the port to be trusted.
5	Click **Apply** to make the changes.

—End—

Configuring ARP Inspection using the Java Device Manager

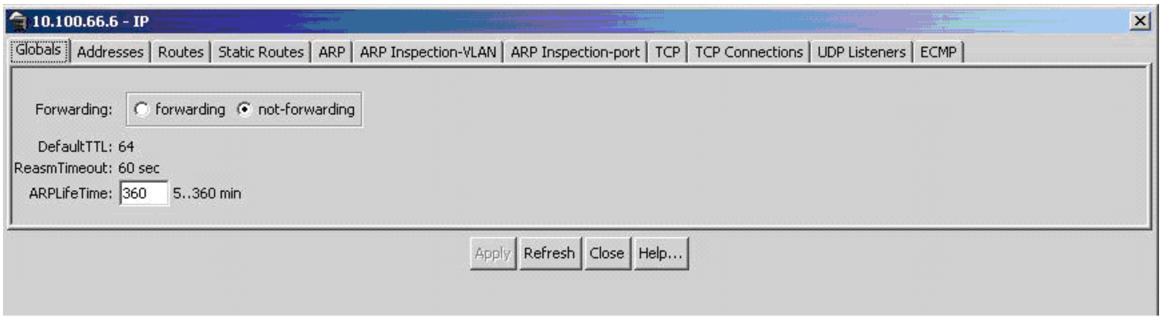
ARP Inspection can be configured using the JDM (Java Device Manager).

Use the following procedure to configure ARP Inspection through the JDM:

Step	Action

1 Select **IP Routing>IP** from the menu. The **IP** screen appears.

IP Routing - IP



Forwarding: ○ forwarding ● not-forwarding

DefaultTTL: 64

ReasmTimeout: 60 sec

ARPLifeTime: 360 5..360 min

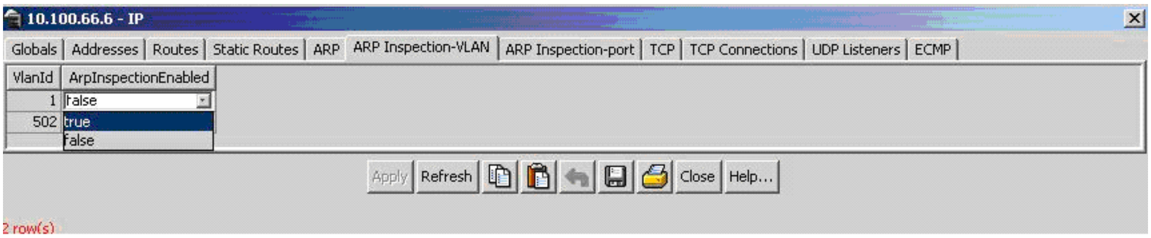
Note: The ARP Inspection has two tabs. They are

- ARP Inspection-VLAN
- ARP Inspection-port

2 Double-click on the **ARP Inspection-VLAN** field next to the ARP field.

The field changes to a drop-down list.

ARP Inspection-VLAN



VlanId	ArpInspectionEnabled
1	false
502	true false

2 row(s)

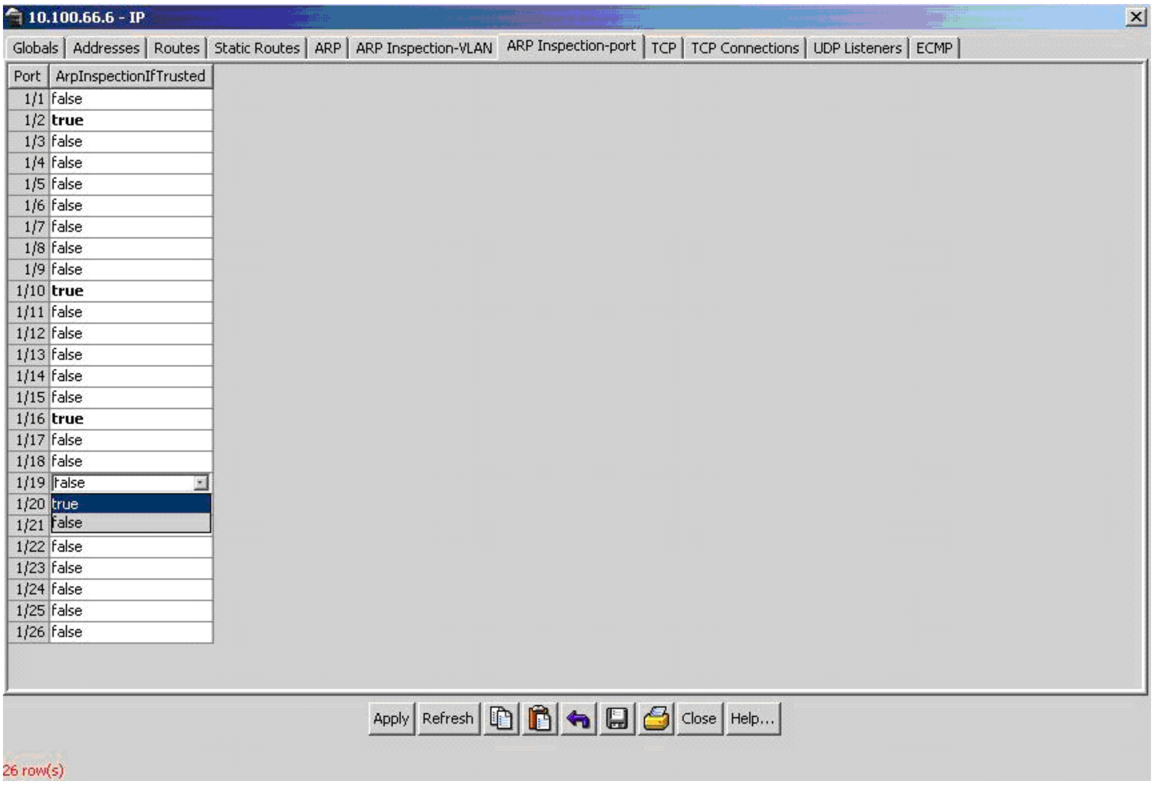
3 Select **true** from the drop-down list to enable the ARP Inspection per VLAN.

4 Click **Apply** to make the changes.

5 Double-click on the **ARP Inspection-port** field next to the ARP Inspection-VLAN field to configure the port as trusted or untrusted

The field changes to a drop-down list.

ARP Inspection-port



Port	ArpInspectionIfTrusted
1/1	false
1/2	**true**
1/3	false
1/4	false
1/5	false
1/6	false
1/7	false
1/8	false
1/9	false
1/10	**true**
1/11	false
1/12	false
1/13	false
1/14	false
1/15	false
1/16	**true**
1/17	false
1/18	false
1/19	false
1/20	true
1/21	false
1/22	false
1/23	false
1/24	false
1/25	false
1/26	false

6 Set the ARP Inspection Trusted field as **true** for trusted port and **false** for untrusted port.

7 Click **Apply** to make the changes.

—End—

Configuring the Simple Network Management Protocol

This chapter details the configuration and use of SNMP with the Nortel Ethernet Routing Switch.

Setting SNMP v1, v2c, v3 Parameters

Earlier releases of SNMP used a proprietary method for configuring SNMP communities and trap destinations for specifying SNMPv1 configuration that included:

- A single read-only community string that can only be configured using the console menus.
- A single read-write community string that can only be configured using the console menus.
- Up to four trap destinations and associated community strings that can be configured either in the console menus, or using SNMP Set requests on the s5AgTrpRcvrTable

With the Nortel Ethernet Routing Switch 5500 Series support for SNMPv3, you can configure SNMP using the new standards-based method of configuring SNMP communities, users, groups, views, and trap destinations.

The Nortel Ethernet Routing Switch 5500 Series also supports the previous proprietary SNMP configuration methods for backward compatibility.

All the configuration data configured in the proprietary method is mapped into the SNMPv3 tables as read-only table entries. In the new standards-based SNMPv3 method of configuring SNMP, all processes are configured and controlled through the SNMPv3 MIBs. The Command Line Interface commands change or display the single read-only community, read-write community, or four trap destinations of the proprietary method of configuring SNMP. Otherwise, the commands change or display SNMPv3 MIB data.

The Nortel Ethernet Routing Switch 5500 Series software supports MD5 and SHA authentication, as well as AES and DES encryption.

The SNMP agent supports exchanges using SNMPv1, SNMPv2c and SNMPv3. Support for SNMPv2c introduces a standards-based GetBulk retrieval capability using SNMPv1 communities. SNMPv3 support introduces industrial-grade user authentication and message security. This includes MD5 and SHA-based user authentication and message integrity verification, as well as AES- and DES-based privacy encryption. Export restrictions on SHA and DES necessitate support for domestic and non-domestic executable images or defaulting to no encryption for all customers.

The traps can be configured in SNMPv1, v2, or v3 format. If you do not identify the version (v1, v2, or v3), the system formats the traps in the v1 format. A community string can be entered if the system requires one.

SNMPv3 table entries stored in NVRAM

The number of non-volatile entries (entries stored in NVRAM) allowed in the SNMPv3 tables are shown in the following list. The system does not allow you to create more entries marked non-volatile when you reach these limits:

- snmpCommunityTable: 20
- vacmViewTreeFamilyTable: 60
- vacmSecurityToGroupTable: 40
- vacmAccessTable: 40
- usmUserTable: 20
- snmpNotifyTable: 20
- snmpTargetAddrTabel: 20
- snmpTargetParamsTable: 20

Configuring SNMP using the CLI

The commands detailed in this section are used for SNMP configuration and management.

show snmp-server command

The **show snmp-server** command displays SNMP configuration.

The syntax for the **show snmp-server** command is:

```
show snmp-server {host|user|view}
```

The **show snmp-server** command is executed in the Privileged EXEC command mode.

"show snmp-server command parameters and variables" (page 203) describes the parameters and variables for the **show snmp-server** command.

show snmp-server command parameters and variables

Parameters and variables	Description
host	Displays the trap receivers configured in the SNMPv3 MIBs.
user	Displays the SNMPv3 users, including views accessible to each user.
view	Displays SNMPv3 views.

snmp-server authentication-trap command

The **snmp-server authentication-trap** command enables or disables the generation of SNMP authentication failure traps.

The syntax for the **snmp-server authentication-trap** command is:

```
snmp-server authentication-trap {enable|disable}
```

The **snmp-server authentication-trap** command is executed in the Global Configuration command mode.

"snmp-server authentication-trap command parameters and variables" (page 203) describes the parameters and variables for the snmp-server authentication-trap command.

snmp-server authentication-trap command parameters and variables

Parameters and variables	Description
enable|disable	Enables or disables the generation of authentication failure traps.

no snmp-server authentication-trap command

The **no snmp-server authentication-trap** command disables generation of SNMP authentication failure traps.

The syntax for the no **snmp-server authentication-trap** command is:

```
no snmp-server authentication-trap
```

The **no snmp-server authentication-trap** command is executed in the Global Configuration command mode.

default snmp-server authentication-trap command

The **`default snmp-server authentication-trap`** command restores SNMP authentication trap configuration to the default settings.

The syntax for the **`default snmp-server authentication-trap`** command is:

```
default snmp-server authentication-trap
```

The **`default snmp-server authentication-trap command`** is executed in the Global Configuration command mode.

snmp-server community for read or write command

This command configures a single read-only or a single read-write community. A community configured using this command does not have access to any of the SNMPv3 MIBs. The community strings created by this command are controlled by the SNMP Configuration screen in the console interface. These community strings have a fixed MIB view.

The **`snmp-server community`** command for read/write modifies the community strings for SNMPv1 and SNMPv2c access.

The syntax for the **`snmp-server community`** for read/write command is:

```
snmp-server community [ro|rw]
```

The **`snmp-server community`** for read/write command is executed in the Global Configuration command mode.

"snmp-server community for read/write command" (page 204) describes the parameters and variables for the **`snmp-server community`** for read/write command.

snmp-server community for read/write command

Parameters and variables	Description
ro|rw (read-only I read-write)	Specifies read-only or read-write access. Stations with ro access can only retrieve MIB objects, and stations with rw access can retrieve and modify MIB objects. ***Note:*** If neither ro nor rw is specified, ro is assumed (default).

snmp-server community command

The **snmp-server community** command allows you to create community strings with varying levels of read, write, and notification access based on SNMPv3 views. These community strings are separate from those created using the **snmp-server community** for read/write command.

This command affects community strings stored in the SNMPv3 snmpCommunity Table, which allows several community strings to be created. These community strings can have any MIB view.

The syntax for the **snmp-server community** command is:

```
snmp-server community {read-view <view-name>|write-view
<view-name>|notify-view <view-name>}
```

The **snmp-server community** command is executed in the Global Configuration command mode.

"snmp-server community command parameters and variables" (page 205) describes the parameters and variables for the **snmp-server community** command.

snmp-server community command parameters and variables

Parameters and variables	Description
read-view <view-name>	Changes the read view used by the new community string for different types of SNMP operations. view-name--specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.
write-view <view-name>	Changes the write view used by the new community string for different types of SNMP operations. view-name--specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.
notify-view <view-name>	Changes the notify view settings used by the new community string for different types of SNMP operations. view-name--specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.

no snmp-server community command

The **no snmp-server community** command clears the snmp-server community configuration.

The syntax for the **no snmp-server community** command is:

```
no snmp-server community {ro|rw|<community-string>}
```

The **no snmp-server community** command is executed in the Global Configuration command mode.

If you do not specify a read-only or read-write community parameter, all community strings are removed, including all the communities controlled by the **snmp-server community** command and the **snmp-server community** for read-write command.

If you specify read-only or read-write, then just the read-only or read-write community is removed. If you specify the name of a community string, then the community string with that name is removed.

"no snmp-server community command parameters and variables" (page 206) describes the parameters and variables for the no **snmp-server community** command.

no snmp-server community command parameters and variables

Parameters and variables	Description
ro |rw|<community-string>	Changes the settings for SNMP: • ro|rw--sets the specified old-style community string value to NONE, thereby disabling it. • community-string--deletes the specified community string from the SNMPv3 MIBs (that is, from the new-style configuration).

default snmp-server community command

The **default snmp-server community** command restores the community string configuration to the default settings.

The syntax for the **default snmp-server community** command is:

```
default snmp-server community [ro|rw]
```

The **default snmp-server community** command is executed in the Global Configuration command mode.

If the read-only or read-write parameter is omitted from the command, then all communities are restored to their default settings. The read-only community is set to Public, the read-write community is set to Private, and all other communities are deleted.

Undefined Resource describes the parameters and variables for the `default snmp-server community` command.

default snmp-server community command parameters and variables

Parameters and variables	Description
ro|rw	Restores the read-only community to Public, or the read-write community to Private.

snmp-server contact command

The `snmp-server contact` command configures the SNMP sysContact value.

The syntax for the `snmp-server contact` command is:

```
snmp-server contact <text>
```

The `snmp-server contact` command is executed in the Global Configuration command mode.

"snmp-server contact command parameters and variables" (page 207) describes the parameters and variables for the `snmp-server contact` command.

snmp-server contact command parameters and variables

Parameters and variables	Description
text	Specifies the SNMP sysContact value.

no snmp-server contact command

The `no snmp-server contact` command clears the sysContact value.

The syntax for the no `snmp-server contact` command is:

```
no snmp-server contact
```

The `no snmp-server contact` command is executed in the Global Configuration command mode.

default snmp-server contact command

The **default snmp-server contact** command restores sysContact to the default value.

The syntax for the **default snmp-server contact** command is:

```
default snmp-server contact
```

The **default snmp-server contact** command is executed in the Global Configuration command mode.

snmp-server command

The **snmp-server** command enables or disables the SNMP server.

The syntax for the **snmp-server** command is:

```
snmp-server {enable|disable}
```

The **snmp-server** command is executed in the Global Configuration command mode.

"snmp-server command parameters and variables" (page 208) describes the parameters and variables for the **snmp-server** command.

snmp-server command parameters and variables

Parameters and variables	Description
enable|disable	Enables or disables the SNMP server.

no snmp-server command

The **no snmp-server** command disables SNMP access.

The syntax for the **no snmp-server** command is:

```
no snmp-server
```

The **no snmp-server** command is executed in the Global Configuration command mode.

The **no snmp-server** command has no parameters or variables.

> ***Note:*** If you disable SNMP access to the switch, you cannot use Device Manager for the switch.

snmp-server host command

The **snmp-server host** command adds a trap receiver to the trap-receiver table.

In the proprietary method, the table has a maximum of four entries, and these entries can generate only SNMPv1 traps. This command controls the contents of the s5AgTrpRcvrTable, which is the set of trap destinations controlled by the SNMP Configuration screen in the console interface.

The proprietary method syntax for the **`snmp-server host`** for command is:

```
snmp-server host <host-ip> <community-string>
```

Using the new standards-based SNMP method, you can create several entries in this table, and each can generate v1, v2c, or v3 traps.

> ***Note:*** Before using the desired community string or user in this command, ensure that it has been configured with a notify-view.

The new standards-based method syntax for the **`snmp-server host`** command is:

```
snmp-server host <host-ip> [port <trap-port>] {v1 <community-
string>|v2c <community-string>|v3 {auth|no-auth|auth-priv}
<username>}
```

The **`snmp-server host`** command is executed in the Global Configuration command mode.

"snmp-server host command parameters and variables" (page 209) describes the parameters and variables for the **`snmp-server host`** command.

snmp-server host command parameters and variables

Parameters and variables	Description
host-ip	Enter a dotted-decimal IP address of a host to be the trap destination.
community-string	If you are using the proprietary method for SNMP, enter a community string that works as a password and permits access to the SNMP protocol.
port <trap-port>	If you are using the new standards-based tables, enter a value from 1 to 65535 for the SNMP trap port.
v1 <community-string>	To configure the new standards-based tables, using v1 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels can be created.

Parameters and variables	Description
v2c <community-string>	To configure the new standards-based tables, using v2c creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels can be created.
v3 {auth|no-auth|auth-priv}	To configure the new standards-based tables, using v3 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels can be created. Enter the following variables: • auth--auth specifies SNMPv3 traps are sent using authentication and no privacy; • no-auth--no-auth specifies SNMPv3 traps are sent using with no authentication and no privacy. • auth-priv--specifies traps are sent using authentication and privacy; this parameter is available only if the image has full SHA/DES support.
username	To configure the new standards-based tables; specifies the SNMPv3 username for trap destination; enter an alphanumeric string.

no snmp-server host command

The **`no snmp-server host`** command deletes trap receivers from the table.

The proprietary method syntax for the **`no snmp-server host`** command is:

```
no snmp-server host [<host-ip> [<community-string>]]
```

Using the standards-based method of configuring SNMP, any trap receiver matching the IP address and SNMP version is deleted.

The standards-based method syntax for the **`no snmp-server host`** command is:

```
no snmp-server host <host-ip> [port <trap-port>]
{v1|v2c|v3|<community-string>}
```

The **`no snmp-server host`** command is executed in the Global Configuration command mode.

If you do not specify any parameters, this command deletes all trap destinations from the s5AgTrpRcvrTable and from SNMPv3 tables.

"no snmp-server host command parameters and variables" (page 211) describes the parameters and variables for the **`no snmp-server host`** command.

no snmp-server host command parameters and variables

Parameters and variables	Description
<host-ip> [<community-string>]	In the proprietary method, enter the following variables: • host-ip--the IP address of a trap destination host. • community-string--the community string that works as a password and permits access to the SNMP protocol. If both parameters are omitted, nothing is cleared. If a host IP is included, the community-string is required or an error is reported.
<host-ip>	Using the standards-based method, enter the IP address of a trap destination host.
port <trap-port>	Using the standards-based method, enter the SNMP trap port.
v1|v2c|v3|<community-string>	Using the standards-based method, specifies trap receivers in the SNMPv3 MIBs. <community-string>--the community string that works as a password and permits access to the SNMP protocol.

default snmp-server host command

The **`default snmp-server host`** command restores the-old style SNMP server and the standards based tables are reset (cleared).

The syntax for the **`default snmp-server host`** command is:

```
default snmp-server host
```

The **`default snmp-server host`** command is executed in the Global Configuration command mode.

The **`default snmp-server host`** command has no parameters or variables.

snmp-server location command

The **`snmp-server location`** command configures the SNMP sysLocation value.

The syntax for the **`snmp-server location`** command is:

```
snmp-server location <text>
```

The **`snmp-server location`** command is executed in the Global Configuration command mode.

"snmp-server location command parameters and variables" (page 212) describes the parameters and variables for the **`snmp-server location`** command.

snmp-server location command parameters and variables

Parameters	Description
text	Specify the SNMP sysLocation value; enter an alphanumeric string of up to 255 characters.

no snmp-server location command

The **`no snmp-server location`** command clears the SNMP sysLocation value.

The syntax for the **`no snmp-server location`** command is:

```
no snmp-server location
```

The **`no snmp-server location`** command is executed in the Global Configuration command mode.

default snmp-server location command

The **`default snmp-server location`** command restores sysLocation to the default value.

The syntax for the **`default snmp-server location`** command is:

```
default snmp-server location
```

The **`default snmp-server location`** command is executed in the Global Configuration command mode.

snmp-server name command

The **`snmp-server name`** command configures the SNMP sysName value.

The syntax for the **`snmp-server name`** command is:

```
snmp-server name <text>
```

The **snmp-server name** command is executed in the Global Configuration command mode.

"snmp-server name command parameters and variables" (page 213) describes the parameters and variables for the **snmp-server name** command.

snmp-server name command parameters and variables

Parameters and variables	Description
text	Specify the SNMP sysName value; enter an alphanumeric string of up to 255 characters.

no snmp-server name command

The **no snmp-server name** command clears the SNMP sysName value.

The syntax for the **no snmp-server name** command is:

```
no snmp-server name
```

The **no snmp-server name** command is executed in the Global Configuration command mode.

default snmp-server name command

The **default snmp-server name** command restores sysName to the default value.

The syntax for the **default snmp-server name** command is:

```
default snmp-server name
```

The **default snmp-server name** command is executed in the Global Configuration command mode.

snmp-server user command

The **snmp-server user** command creates an SNMPv3 user.

For each user, you can create three sets of read/write/notify views:

- for unauthenticated access
- for authenticated access
- for authenticated and encrypted access

The syntax for the **snmp-server user** command for unauthenticated access is:

```
snmp-server user <username> [read-view <view-name>]
[write-view <view-name>] [notify-view <view-name>]
```

The syntax for the **snmp-server user** command for authenticated access is:

```
snmp-server user <username> [[read-view <view-name>]
[write-view <view-name>] [notify-view <view-name>]] md5|sha
<password> [read-view <view-name>] [write-view <view-name>]
[notify-view <view-name>]
```

The syntax for the **snmp-server user** command for authenticated and encrypted access is:

```
snmp-server user <username>[[read-view <view-name>]
[write-view <view-name>] [notify-view <view-name>]] md5|sha
<password> [[read-view <view-name>] [write-view <view-name>]
[notify-view <view-name>]] {3des|aes|des} <password>
[read-view <view-name>] [write-view <view-name>] [notify-view
<view-name>]
```

The **snmp-server user** command is executed in the Global Configuration command mode.

The sha and 3des/aes/des parameters are only available if the switch/stack image has SSH support.

For authenticated access, you must specify the md5 or sha parameter. For authenticated and encrypted access, you must also specify the 3des, aes, or des parameter.

For each level of access, you can specify read, write, and notify views. If you do not specify view parameters for authenticated access, the user will have access to the views specified for unauthenticated access. If you do not specify view parameters for encrypted access, the user will have access to the views specified for authenticated access or, if no authenticated views were specified, the user will have access to the views specified for unauthenticated access.

"snmp-server user parameters" (page 214) describes the parameters and variables for the **snmp-server user** command.

snmp-server user parameters

Parameters	Description
username	Specifies the user name. Enter an alphanumeric string of up to 255 characters.

Parameters	Description
md5 <password>	Specifies the use of an md5 password. <password> specifies the new user md5 password; enter an alphanumeric string. If this parameter is omitted, the user is created with only unauthenticated access rights.
read-view <view-name>	Specifies the read view to which the new user has access: • view-name--specifies the viewname; enter an alphanumeric string of up to 255 characters.
write-view <view-name>	Specifies the write view to which the new user has access: • view-name--specifies the viewname; enter an alphanumeric string that can contain at least some of the non-alphanumeric characters.
notify-view <view-name>	Specifies the notify view to which the new user has access: • view-name--specifies the viewname; enter an alphanumeric string that can contain at least some of the non-alphanumeric characters.
SHA	Specifies SHA authentication.
3DES	Specifies 3DES privacy encryption.
AES	Specifies AES privacy encryption.
DES	Specifies DES privacy encryption.
engine-id	Specifies the new remote user to receive notifications. • notify-view—specifies the viewname to notify.

Note: If a view parameter is omitted from the command, that view type cannot be accessed.

no snmp-server user command

The **`no snmp-server user`** command deletes the specified user.

The syntax for the **`no snmp-server user`** command is:

```
no snmp-server user [engine-id <engine ID>] <username>
```

The **no snmp-server user** command is executed in the Global Configuration command mode.

"no snmp-server user command parameters and variables" (page 216) describes the parameters and variables for the **no snmp-server user** command.

no snmp-server user command parameters and variables

Parameters and variables	Description
[engine-id <engine ID>]	Specifies the SNMP engine ID of the remote SNMP entity.
username	Specifies the user to be removed.

snmp-server view command

The **snmp-server view** command creates an SNMPv3 view. The view is a set of MIB object instances which can be accessed.

The syntax for the **snmp-server view** command is:

```
snmp-server view <view-name> <OID> [<OID> [<OID> [<OID>
[<OID> [<OID> [<OID> [<OID> [<OID> [<OID>]]]]]]]]]
```

The **snmp-server view** command is executed in the Global Configuration command mode.

"snmp-server view command parameters and variables" (page 216) describes the parameters and variables for the **snmp-server view** command.

snmp-server view command parameters and variables

Parameters and variables	Description
viewname	Specifies the name of the new view; enter an alphanumeric string.
OID	Specifies Object identifier. OID can be entered as a dotted form OID. Each OID must be preceded by a + or - sign (if this is omitted, a + sign is implied). The + is not optional. For the dotted form, a sub-identifier can be an asterisk, indicating a wildcard. Here are some examples of valid OID parameters: • sysName

Parameters and variables	Description
	• +sysName • -sysName • +sysName.0 • +ifIndex.1 • -ifEntry.*.1 (this matches all objects in the ifTable with an instance of 1; that is, the entry for interface #1) • 1.3.6.1.2.1.1.1.0 (the dotted form of sysDescr) The + or - indicates whether the specified OID is included in or excluded from, respectively, the set of MIB objects that are accessible using this view. For example, if you create a view like this: • snmp-server view myview +system -sysDescr And you use that view for the read-view of a user, then the user can read only the system group except for sysDescr. ***Note:*** there are 10 possible OID values.

no snmp-server view command

The **`no snmp-server view`** command deletes the specified view.

The syntax for the **`no snmp-server view`** is:

```
no snmp-server view <viewname>
```

The **`no snmp-server view`** is executed in the Global Configuration command mode.

"no snmp-server view command parameters and variables" (page 218) describes the parameters and variables for the **`no snmp-server view`** command.

no snmp-server view command parameters and variables

Parameters and variables	Description
viewname	Specifies the name of the view to be removed. If no view is specified, all views are removed.

snmp-server bootstrap command

The **`snmp-server bootstrap`** command allows you to specify how you wish to secure SNMP communications, as described in the SNMPv3 standards. It creates an initial set of configuration data for SNMPv3. This configuration data follows the conventions described in the SNMPv3 standard (in RFC 3414 and 3415). This commands creates a set of initial users, groups and views.

> ***Note:*** This Command deletes *all* existing SNMP configurations, hence must be used with care.

The syntax for the **`snmp-server bootstrap`** command is:

```
snmp-server bootstrap <minimum-secure>|<semi-secure>
|<very-secure>
```

The **`snmp-server bootstrap`** command is executed in the Global Configuration command mode.

"snmp-server bootstrap command parameters and variables" (page 218) describes the parameters and variables for the **`snmp-server bootstrap`** command.

snmp-server bootstrap command parameters and variables

Parameters and variables	Description
<minimum-secure>	Specifies a minimum security configuration that allows read access and notify access to all processes (view restricted) with noAuth-noPriv and read, write, and notify access to all processes (internet view) using Auth-noPriv and Auth-Priv. ***Note:*** In this configuration, view restricted matches view internet.

Parameters and variables	Description
<semi-secure>	Specifies a minimum security configuration that allows read access and notify access to all processes (view restricted) with noAuth-noPriv and read, write, and notify access to all processes (internet view) using Auth-noPriv and Auth-Priv. ***Note:*** In this configuration, restricted contains a smaller subset of views than internet view. The subsets are defined according to RFC 3414.
<very-secure>	Specifies a maximum security configuration that allows no access to the users.

Configuring SNMP using the Web-based management interface

This section describes the SNMP configuration procedures available in the Web-based management interface.

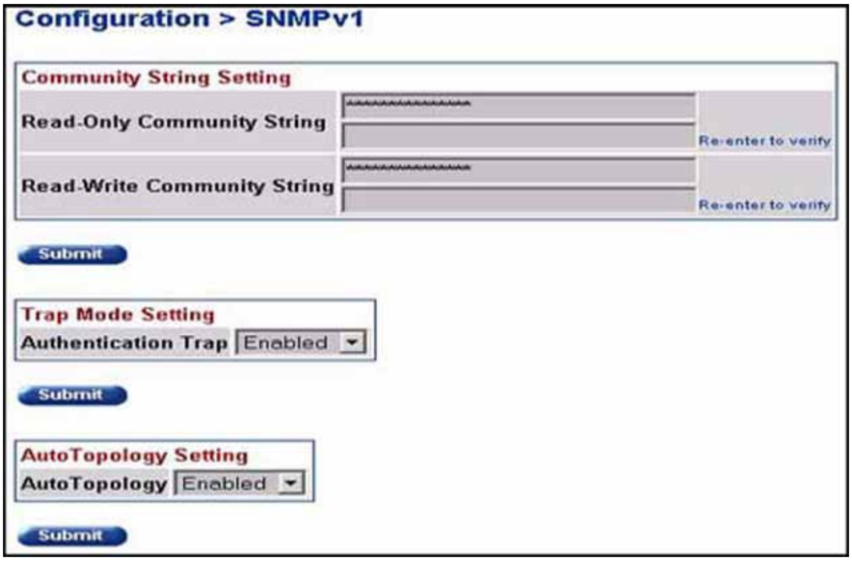
Configuring SNMPv1

SNMPv1 read-write and read-only community strings can be configured, enable or disable trap mode settings, and/or enable or disable the Autotopology feature. The Autotopology feature, when enabled, performs a process that recognizes any device on the managed network and defines and maps its relation to other network devices in real time.

To configure the community string, trap mode, and Autotopology settings and features:

Step	Action
1	Open the **SNMPv1** screen by selecting **Configuration > SNMPv1** from the menu. This screen is illustrated in "SNMPv1 page" (page 220).

SNMPv1 page



Configuration > SNMPv1

Community String Setting

Read-Only Community String ****************

Re-enter to verify

Read-Write Community String ****************

Re-enter to verify

Trap Mode Setting

Authentication Trap Enabled

AutoTopology Setting

AutoTopology Enabled

The following table "SNMPv1 screen items" (page 220) describes the items on the SNMPv1 screen.

SNMPv1 screen items

Section	Item	Range	Description
Community String Setting	Read-Only Community String	1-32	Type a character string to identify the community string for the SNMPv1 read-only community, for example, public or private. The default value is public.
	Read-Write Community String	1-32	Type a character string to identify the community string for the SNMPv1 read-write community, for example, public or private. The default value is private.
Trap Mode Setting	Authentication Trap	(1) Enabled (2) Disabled	Choose to enable or disable the authentication trap.
AutoTopology Setting	AutoTopology	(1) Enabled (2) Disabled	Choose to enable or disable the Autotopology feature.

2 Type information in the text boxes, or select from a list.

3 Click **Submit** in any section to save the changes.

—End—

Configuring SNMPv3

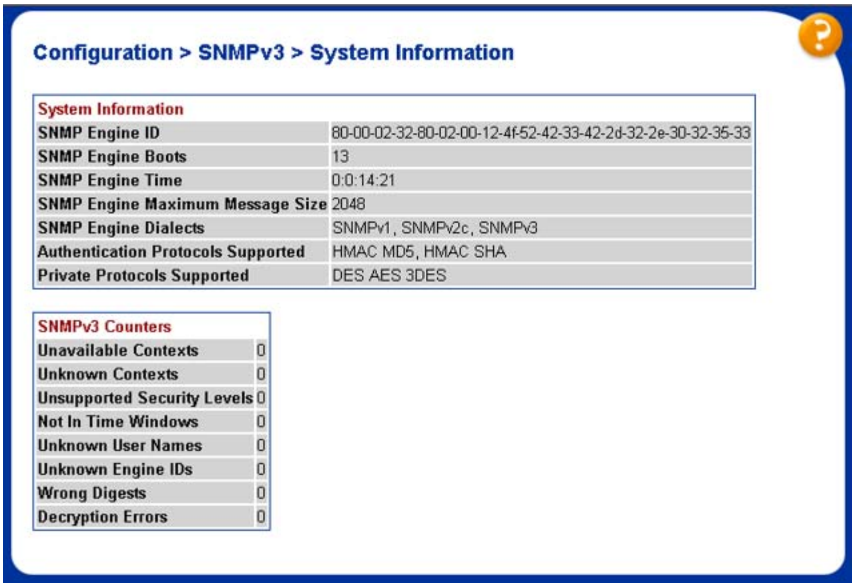
This section describes the steps to build and manage SNMPv3 in the Web-based management user interface.

Viewing SNMPv3 system information Information can be viewed about the SNMPv3 engine that exists and the private protocols that are supported in the network configuration. Information can also be viewed about packets received by the system having particular errors, such as unavailable contexts, unknown contexts, decrypting errors, or unknown usernames.

To view SNMPv3 system information:

Step	Action
1	Open the **System Information** screen by selecting **Configuration > SNMPv3 > System Information** from the menu. This screen is illustrated in "System Information screen" (page 221).

System Information screen



Configuration > SNMPv3 > System Information

System Information	
SNMP Engine ID	80-00-02-32-80-02-00-12-4f-52-42-33-42-2d-32-2e-30-32-35-33
SNMP Engine Boots	13
SNMP Engine Time	0:0:14:21
SNMP Engine Maximum Message Size	2048
SNMP Engine Dialects	SNMPv1, SNMPv2c, SNMPv3
Authentication Protocols Supported	HMAC MD5, HMAC SHA
Private Protocols Supported	DES AES 3DES

SNMPv3 Counters	
Unavailable Contexts	0
Unknown Contexts	0
Unsupported Security Levels	0
Not In Time Windows	0
Unknown User Names	0
Unknown Engine IDs	0
Wrong Digests	0
Decryption Errors	0

—End—

The following table "System Information section fields" (page 222) describes the fields on the System Information section of the SNMPv3 System Information screen.

System Information section fields

Item	Description
SNMP Engine ID	The SNMP engine identification number.
SNMP Engine Boots	The number of times that the SNMP engine has re-initialized itself since its initial configuration.
SNMP Engine Time	The number of seconds since the SNMP engine last incremented the snmpEngineBoots object.
SNMP Engine Maximum Message Size	The maximum length, in octets, of an SNMP message which this SNMP engine can send or receive and process determined as the minimum of the maximum message size values supported among all transports available to and supported by the engine.
SNMP Engine Dialects	The SNMP dialect the engine recognizes. The dialects are: SNMPv1, SNMPv2C, and SNMPv3.
Authentication Protocols Supported	The registration point for standards-track authentication protocols used in SNMP Management Frameworks. The registration points are: None, HMAC MD5, HMAC SHA.
Private Protocols Supported	The registration point for standards-track privacy protocols used in SNMP Management Frameworks. The registration points are: DES, AES, 3DES, or None.

The following table "SNMPv3 Counters section fields" (page 222) describes the fields on the SNMPv3 Counters section of the SNMPv3 System Information screen

SNMPv3 Counters section fields

Item	Description
Unavailable Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unavailable.
Unknown Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unknown.
Unsupported Security Levels	The total number of packets dropped by the SNMP engine because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
Not in Time Windows	The total number of packets dropped by the SNMP engine because they appeared outside of the authoritative SNMP engine's window.
Unknown User Names	The total number of packets dropped by the SNMP engine because they referenced an unknown user.
Unknown Engine IDs	The total number of packets dropped by the SNMP engine because they referenced an snmpEngineID that was not known to the SNMP engine.

Item	Description
Wrong Digests	The total number of packets dropped by the SNMP engine because they did not contain the expected digest value.
Decryption Errors	The total number of packets dropped by the SNMP engine because they cannot be decrypted.

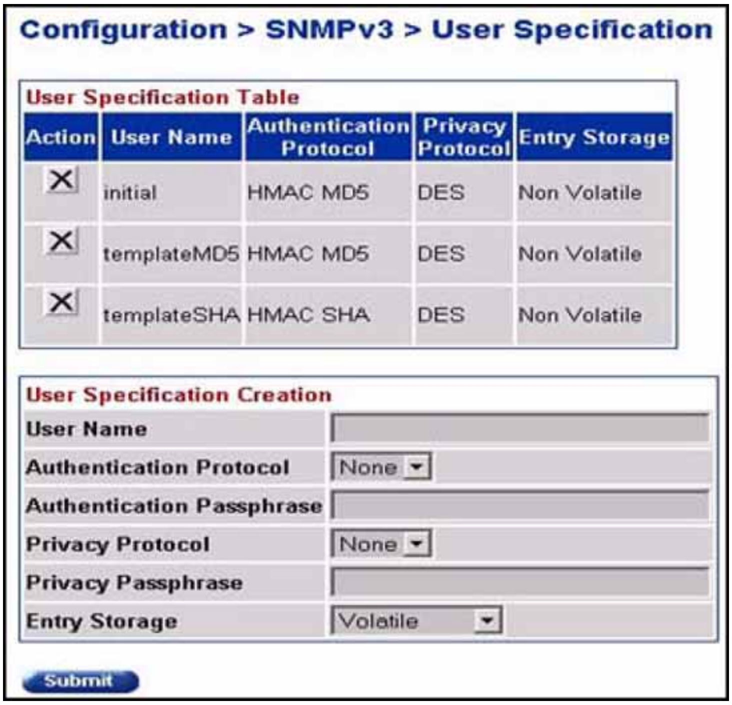
Configuring user access to SNMPv3 Information can be viewed about all current SNMPv3 user security parameters such as authentication/privacy protocols in use or create and delete SNMPv3 system user configurations.

Creating an SNMPv3 system user configuration To create an SNMPv3 system user configuration:

Step	Action

1 Open the **User Specification** screen by selecting **Configuration > SNMPv3 > User Specification** from the menu. This screen is illustrated in "User Specification screen" (page 223).

User Specification screen



Configuration > SNMPv3 > User Specification

User Specification Table

Action	User Name	Authentication Protocol	Privacy Protocol	Entry Storage
☒	initial	HMAC MD5	DES	Non Volatile
☒	templateMD5	HMAC MD5	DES	Non Volatile
☒	templateSHA	HMAC SHA	DES	Non Volatile

User Specification Creation

User Name	
Authentication Protocol	None
Authentication Passphrase	
Privacy Protocol	None
Privacy Passphrase	
Entry Storage	Volatile

The following table "User Specification Table section items" (page 224) describes the items on the User Specification Table section of the User Specification screen.

User Specification Table section items

Item and MIB association	Description
☒	Deletes the row.
User Name (usmUserSecurityName)	The name of an existing SNMPv3 user.
Authentication Protocol (usmUserAuthProtocol)	Indicates whether the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated by the MD5 and SHA authentication protocols.
Private Protocol (usmUserPrivProtocol)	Displays whether or not messages sent on behalf of this user to or from the SNMP engine identified by usmUserEngineID can be protected from disclosure, and if so, the type of privacy protocol that is used.
Entry Storage	The current storage type for this row. If Volatile is displayed, information is dropped (lost) when you turn the power off. If Non-Volatile is displayed, information is saved in NVRAM when you turn the power off

The following table "User Specification Creation section items" (page 224) describes the items on the User Specification Creation section of the User Specification screen.

User Specification Creation section items

Item and MIB association	Range	Description
User Name	1..32	Type a string of characters to create an identity for the user.
Authentication Protocol (usmUserAuthProtocol)	None MD5 SHA	Choose whether or not the message sent on behalf of this user to or from the SNMP engine identified UserEngineID can be authenticated with the MD5 protocol.
Authentication Passphrase (usmUserAuthPassword)	1..32	Type a string of character to create a password to use in conjunction with the authorization protocol.

Item and MIB association	Range	Description
Privacy Protocol	(1) None (2) 3DES (3) AES (4) DES	Choose the privacy protocol you want to use.
Privacy Passphrase	Must be at least 8 characters long	Enter a string of at least 8 characters to create the passphrase. This passphrase is used to generate an encryption key for the user.
Entry Storage (usmUserStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the **User Specification Creation Table** section, **Action** column, type information in the text boxes, or select from a list.

3 Click **Submit**.

The new configuration is displayed in the **User Specification Table**.

—End—

Deleting an SNMPv3 system user configuration To delete an existing SNMPv3 user configuration:

Step Action

1 Open the **User Specification** screen by selecting **Configuration > SNMPv3 > User Specification** from the menu. This screen is illustrated in "User Specification screen" (page 223).

2	In **the User Specification Table**, click the **Delete** icon for the entry to delete.
3	A message prompts for confirmation of the request. Click **OK**.

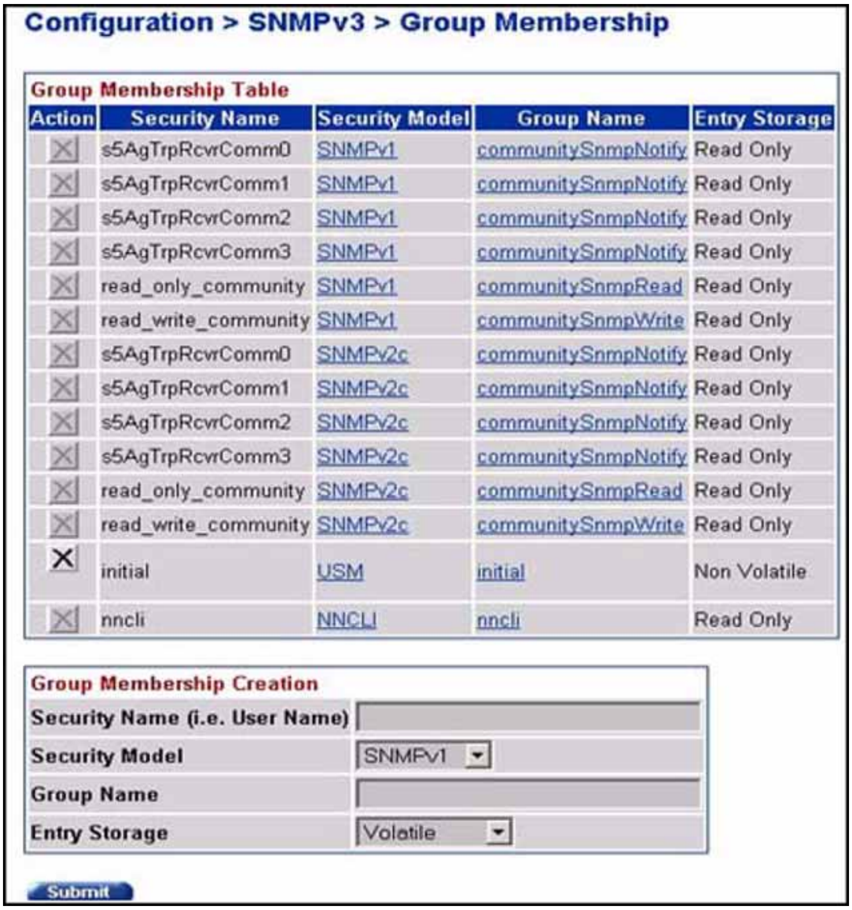
—End—

Configuring an SNMPv3 system user group membership Information can be viewed about existing SNMPv3 group membership configurations as well as mapping or deleting an SNMPv3 user to group configuration.

Mapping an SNMPv3 system user to a group To map an SNMPv3 system user to a group:

Step	Action
1	Open the **Group Membership** screen by selecting **Configuration > SNMPv3 > Group Membership** from the menu. This screen is illustrated in "Group Membership screen" (page 227)

Group Membership screen



Configuration > SNMPv3 > Group Membership

Group Membership Table

Action	Security Name	Security Model	Group Name	Entry Storage
☒	s5AgTrpRcvrComm0	SNMPv1	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm1	SNMPv1	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm2	SNMPv1	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm3	SNMPv1	communitySnmpNotify	Read Only
☒	read_only_community	SNMPv1	communitySnmpRead	Read Only
☒	read_write_community	SNMPv1	communitySnmpWrite	Read Only
☒	s5AgTrpRcvrComm0	SNMPv2c	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm1	SNMPv2c	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm2	SNMPv2c	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm3	SNMPv2c	communitySnmpNotify	Read Only
☒	read_only_community	SNMPv2c	communitySnmpRead	Read Only
☒	read_write_community	SNMPv2c	communitySnmpWrite	Read Only
☒	initial	USM	initial	Non Volatile
☒	nncli	NNCLI	nncli	Read Only

Group Membership Creation

Security Name (i.e. User Name)	
Security Model	SNMPv1 ▾
Group Name	
Entry Storage	Volatile ▾

The following table "Group Membership screen items" (page 227) describes the items on the Group Membership screen.

Group Membership screen items

Item and MIB association	Range	Description
☒		Deletes the row.
Security Name (vacmSecurityToGroupStatus)	1..32	Type a string of character to create a security name for the principal that is mapped by this entry to a group name.
Security Model (vacmSecurityToGroupStatus)	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model within which the security- name-to-group-name mapping is valid.

Item and MIB association	Range	Description
Group Name (vacmGroupName)	1 -- 32	Type a string of character to specify the group name.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the **Group Membership Creation** section, type information in the text boxes, or select from a list.

3 Click **Submit**.

The new entry appears in the **Group Membership Table**.

—End—

Deleting an SNMPv3 group membership configuration To delete an SNMPv3 group membership configuration:

Step Action

1 Open the **Group Membership** screen by selecting **Configuration > SNMPv3 > Group Membership** from the menu. This screen is illustrated in "Group Membership screen" (page 227)

2 In the **Group Membership Table**, click the **Delete** icon for the entry to delete.

3 A message prompts for confirmation of the request. Click **OK**.

Note: This Group Membership Table section of the Group Membership page contains hyperlinks to the SNMPv3 User Specification and Group Access Rights screens.

—End—

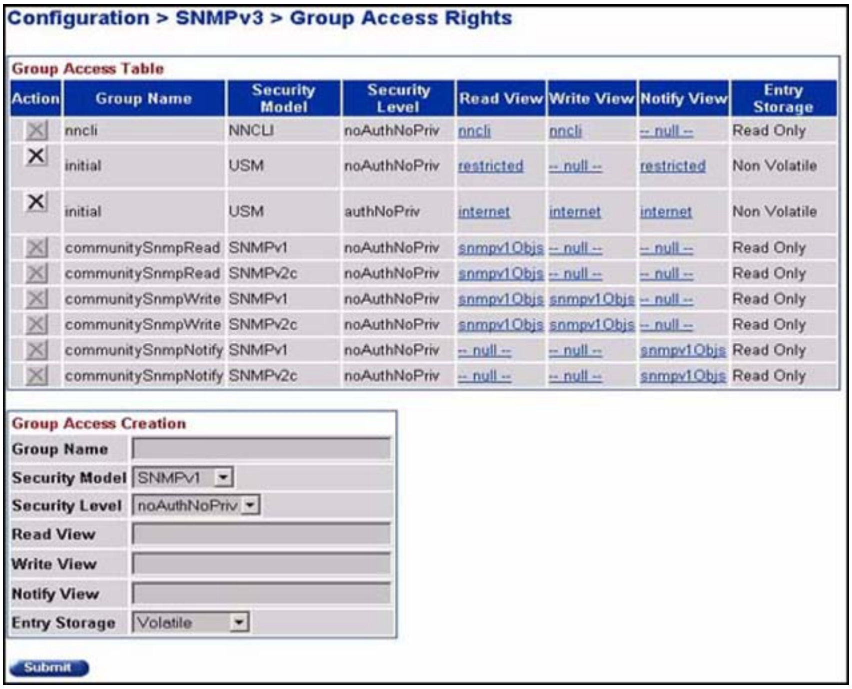
Configuring SNMPv3 group access rights

SNMPv3 group access right configurations can be viewed, created, or deleted using the Web-based Management interface.

Creating an SNMPv3 group access rights configuration To create a group's SNMPv3 system-level access right configuration:

Step	Action
1	Open the **Group Access Rights** screen by selecting **Configuration > SNMPv3 > Group Access Rights** from the menu. This screen is illustrated in "Group Access Rights page" (page 229).

Group Access Rights page



Configuration > SNMPv3 > Group Access Rights

Group Access Table

Action	Group Name	Security Model	Security Level	Read View	Write View	Notify View	Entry Storage
☒	nncli	NNCLI	noAuthNoPriv	nncli	nncli	-- null --	Read Only
☒	initial	USM	noAuthNoPriv	restricted	-- null --	restricted	Non Volatile
☒	initial	USM	authNoPriv	internet	internet	internet	Non Volatile
☒	communitySnmpRead	SNMPv1	noAuthNoPriv	snmpv1Objs	-- null --	-- null --	Read Only
☒	communitySnmpRead	SNMPv2c	noAuthNoPriv	snmpv1Objs	-- null --	-- null --	Read Only
☒	communitySnmpWrite	SNMPv1	noAuthNoPriv	snmpv1Objs	snmpv1Objs	-- null --	Read Only
☒	communitySnmpWrite	SNMPv2c	noAuthNoPriv	snmpv1Objs	snmpv1Objs	-- null --	Read Only
☒	communitySnmpNotify	SNMPv1	noAuthNoPriv	-- null --	-- null --	snmpv1Objs	Read Only
☒	communitySnmpNotify	SNMPv2c	noAuthNoPriv	-- null --	-- null --	snmpv1Objs	Read Only

Group Access Creation

Group Name	
Security Model	SNMPv1
Security Level	noAuthNoPriv
Read View	
Write View	
Notify View	
Entry Storage	Volatile

The following table "Group Access Rights screen items" (page 229) describes the items on the Group Access Rights screen.

Group Access Rights screen items

Item and MIB association	Range	Description
☒		Deletes the row.
Group Name (vacmAccessToGroupStatus)	1 -- 32	Type a character string to specify the group name to which access is granted.
Security Model (vacmAccessSecurityModel)l	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model to which access is granted.
Security Level (vacmAccessSecurityLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the minimum level of security required to gain the access rights allowed to the group.

Item and MIB association	Range	Description
Read View (vacmAccessReadViewName)	1 -- 32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes read access.
Write View (vacmAccessWriteViewName)	1 -- 32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes write access.
Notify View (vacmAccessNotifyViewName)	1 -- 32	Type a character string to identify the MIB view to which this entry authorizes access to notifications.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the **Group Access Creation** section, type information in the text boxes, or select from a list.

3 Click **Submit**.

The new entry appears in the **Group Access Table**.

—End—

Deleting an SNMPv3 group access rights configuration To delete an SNMPv3 group access configuration:

Step Action

1 Open the **Group Access Rights** screen by selecting **Configuration > SNMPv3 > Group Access Rights** from the menu.

2 In the **Group Access Table**, click the **Delete** icon for the entry to delete.

3 A message prompts for confirmation of the request. Click **OK**.

Note: This Group Access Table section of the Group Access Rights screen contains hyperlinks to the Management Information View screen.

—End—

Configuring an SNMPv3 management information view A table of existing SNMPv3 management information view configurations can be viewed, and SNMPv3 management information view configurations can be created or deleted.

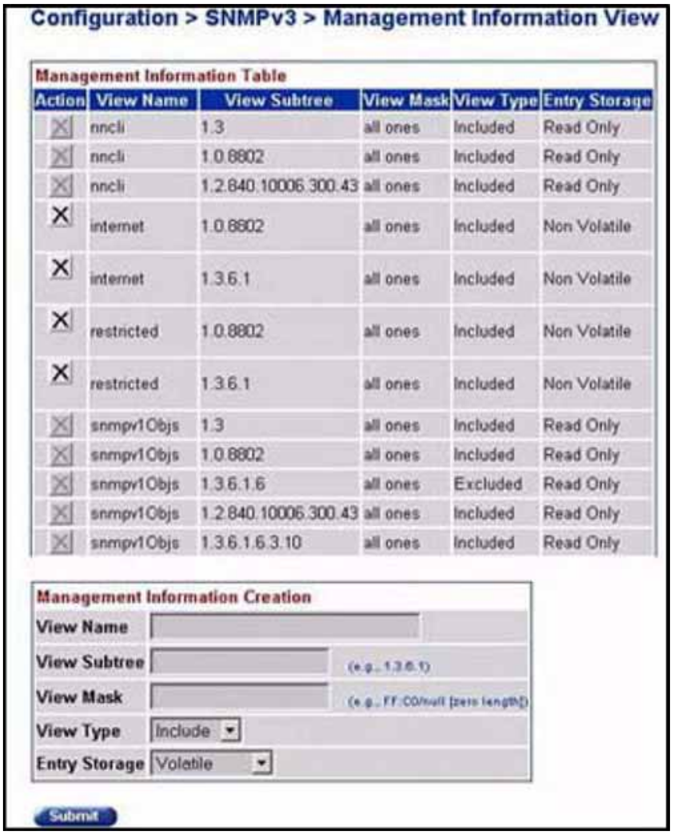
> ***Note:*** A view can consist of multiple entries in the table, each with the same view name, but a different view subtree.

Creating an SNMPv3 management information view configuration To create an SNMPv3 management information view configuration:

Step	Action

1 Open the **Management Info View** screen by selecting **Configuration > SNMPv3 > Management Info View** from the menu. This screen is illustrated in "Management Information View screen" (page 231).

Management Information View screen



Configuration > SNMPv3 > Management Information View

Management Information Table

Action	View Name	View Subtree	View Mask	View Type	Entry Storage
☒	nncli	1.3	all ones	Included	Read Only
☒	nncli	1.0.8802	all ones	Included	Read Only
☒	nncli	1.2.840.10006.300.43	all ones	Included	Read Only
☒	internet	1.0.8802	all ones	Included	Non Volatile
☒	internet	1.3.6.1	all ones	Included	Non Volatile
☒	restricted	1.0.8802	all ones	Included	Non Volatile
☒	restricted	1.3.6.1	all ones	Included	Non Volatile
☒	snmpv1Objs	1.3	all ones	Included	Read Only
☒	snmpv1Objs	1.0.8802	all ones	Included	Read Only
☒	snmpv1Objs	1.3.6.1.6	all ones	Excluded	Read Only
☒	snmpv1Objs	1.2.840.10006.300.43	all ones	Included	Read Only
☒	snmpv1Objs	1.3.6.1.6.3.10	all ones	Included	Read Only

Management Information Creation

View Name		
View Subtree		(e.g., 1.3.6.1)
View Mask		(e.g., FF:C0/null [zero length])
View Type	Include ▾	
Entry Storage	Volatile ▾	

The following table "Management Information View screen items" (page 232) describes the items on the Management Information View screen.

Management Information View screen items

Item and MIB association	Range	Description
☒		Deletes the row.
View Name(vacmViewTreeFamilyViewName)	1 -- 32	Type a character string to create a name for a family of view subtrees.
View Subtree(vacmViewTreeFamilySubtree)	X.X.X.X.X...	Type an object identifier (OID) to specify the MIB subtree that, when combined with the corresponding instance of vacmViewTreeFamilyMask, defines a family of view subtrees. ***Note:*** If no OID is entered and the field is blank, a default mask value consisting of 1s is recognized.
View Mask(vacmViewTreeFamilyMask)	Octet String (0 -- 16)	Type the bit mask which, in combination with the corresponding instance of vacmViewFamilySubtree, defines a family of view subtrees.
View Type(vacmViewTreeFamilyType)	(1) Include (2) Exclude	Choose to include or exclude a family of view subtrees.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the **Management Information Creation** section, type information in the text boxes, or select from a list.

3 Click **Submit**.

The new entry appears in the **Management Information Table**.

—End—

Deleting an SNMPv3 management information view configuration To delete an existing SNMPv3 management information view configuration:

Step	Action
1	Open the **Management Info View** screen by selecting **Configuration > SNMPv3 > Management Info View** from the menu. This screen is illustrated in "Management Information View screen" (page 231).
2	In the **Management Information Table**, click the **Delete** icon for the entry to delete.
3	A message prompts for confirmation of the request. Click **OK**.

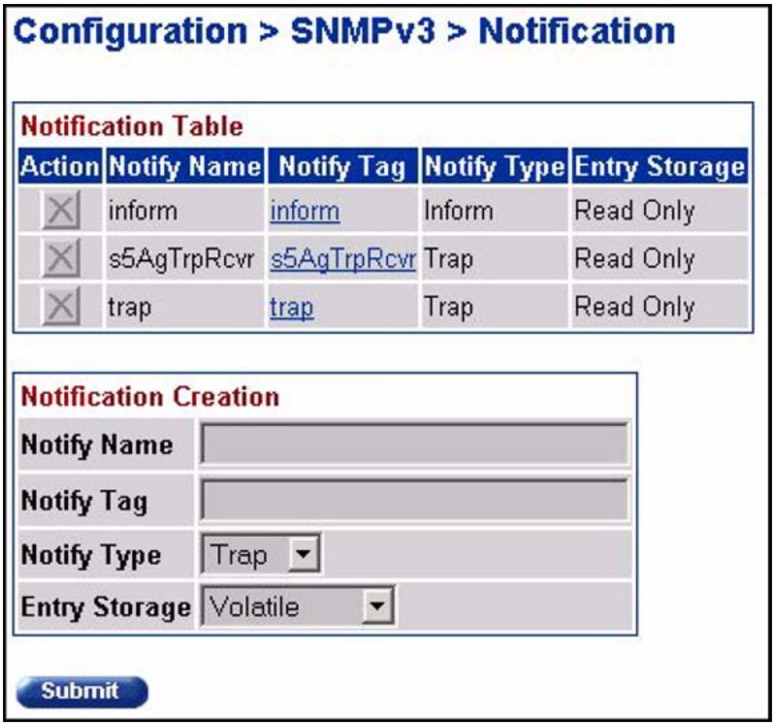
—End—

Configuring an SNMPv3 system notification entry SNMPv3 system notification configurations and system notification types can be viewed, configured, and deleted.

Creating an SNMPv3 system notification configuration To create an SNMPv3 system notification configuration:

Step	Action
1	Open the **Notification** screen by selecting **Configuration > SNMPv3 > Notification** from the menu. This screen is illustrated in "Notification screen" (page 234).

Notification screen



Configuration > SNMPv3 > Notification

Notification Table

Action	Notify Name	Notify Tag	Notify Type	Entry Storage
☒	inform	inform	Inform	Read Only
☒	s5AgTrpRcvr	s5AgTrpRcvr	Trap	Read Only
☒	trap	trap	Trap	Read Only

Notification Creation

Notify Name	
Notify Tag	
Notify Type	Trap
Entry Storage	Volatile

The following table "Notification page items" (page 234) describes the items on the Notification screen.

Notification page items

Item and MIB association	Range	Description
☒		Deletes the row.
Notify Name(snmpNotifyRowStatus)	1 -- 32	Type a character string to identify the entry.
Notify Tag(snmpNotifyTag)	1 -- 32	Type a value which to use to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object carries a zero length, no entries are selected

Item and MIB association	Range	Description
Notify Type(snmpNotifyType)	(1) Trap (2) Inform	Choose the type of notification to generate.
Entry Storage (snmpNotifyStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the **Notification Creation** section, type information in the text boxes, or select from a list.

3 Click **Submit**.

The new entry appears in the **Notification Table** section.

—End—

Note: This **Notification Table** section of the **Notification** screen contains hyperlinks to the **Target Parameter** screen.

Deleting an SNMPv3 system notification configuration To delete an SNMPv3 notification configuration:

Step Action

1 Open the **Notification** screen by selecting **Configuration > SNMPv3 > Notification** from the menu. This screen is illustrated in "Notification screen" (page 234).

2 In the **Notification Table**, click the **Delete** icon for the entry to delete.

3 A message prompts for confirmation of the request. Click **OK**.

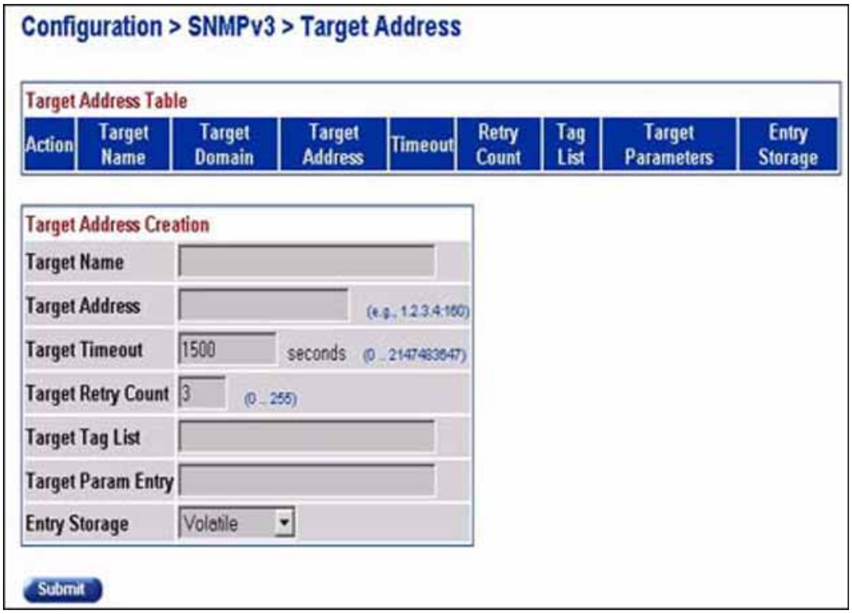
—End—

Configuring an SNMPv3 management target address SNMPv3 management target configurations and management target address configurations can be viewed, configured, and deleted.

Creating an SNMPv3 target address configuration To create an SNMPv3 target address configuration:

Step	Action
1	Open the **Target Address** screen by selecting **Configuration > SNMPv3 > Target Address** from the menu. This screen is illustrated in "Target Address screen" (page 236).

Target Address screen



Configuration > SNMPv3 > Target Address

Target Address Table

Action	Target Name	Target Domain	Target Address	Timeout	Retry Count	Tag List	Target Parameters	Entry Storage

Target Address Creation

Target Name		
Target Address		(e.g., 1.2.3.4:160)
Target Timeout	1500 seconds	(0 .. 2147483647)
Target Retry Count	3	(0 .. 255)
Target Tag List		
Target Param Entry		
Entry Storage	Volatile	

The following table "Target Address screen items" (page 236) describes the items on the Target Address screen.

Target Address screen items

Item and MIB association	Range	Description
☒		Deletes the row.
Target Name(snmpTargetAddrName)	1 -- 32	Type a character string to create a target name.
Target Domain (snmpTargetAddrTDomain)	1 -- 32	Transport type of the address contained in the snmpTargetAddrTAddress object.

Item and MIB association	Range	Description
Target Address (snmpTargetAddrTAddress)	XXX.XXX.XXX.XXX:XXX	Type a transport address in the format of an IP address, colon, and UDP port number. For example: 10.30.31.99:162 (see "Target Address screen" (page 236)).
Target Timeout (snmpTargetAddrTimeout)	Integer	Type the number, in seconds, to designate as the maximum time to wait for a response to an inform notification before resending the Inform notification.
Target Retry Count (snmpTargetAddrRetryCount)	0 -- 255	Type the default number of retires to be attempted when a response is not received for a generated message. An application can provide its own retry count, in which case the value of this object is ignored.
Target Tag List(snmpTargetAddrTagList)	1 -- 20	Type the space-separated list of tag values to be used to select target addresses for a particular operation.
Target Parameter Entry (snmpTargetAddr)	1 -- 32	Type a numeric string to identify an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generated messages are to be sent to this transport address.
Entry Storage	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the **Target Address Creation** section, type information in the text boxes, or select from a list.

3 Click **Submit**.

The new entry appears in the **Target Address Table**.

—End—

> ***Note:*** This Target Address Table section of the Target Address screen contains hyperlinks to the Target Parameter screen.

Deleting an SNMPv3 target address configuration To delete an SNMPv3 target address configuration:

Step	Action
1	Open the **Target Address** screen by selecting **Configuration > SNMPv3 > Target Address** from the menu. This screen is illustrated in "Target Address screen" (page 236).
2	In the **Target Address Table**, click the **Delete** icon for the entry you to delete.
3	A message prompts for confirmation of the request. Click **OK**.

—End—

Configuring an SNMPv3 management target parameter

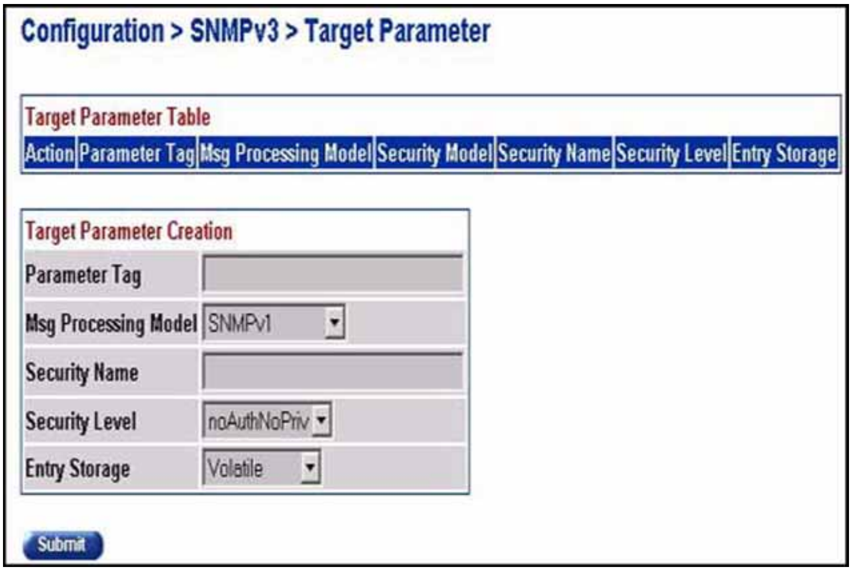
SNMPv3 management target parameters are used during notification generation to specify the communication parameters used for exchanges with notification recipients.

A table of existing SNMPv3 target parameter configurations can be viewed, SNMPv3 target parameters that associate notifications with particular recipients created, and existing SNMPv3 target parameter configurations deleted.

Creating an SNMPv3 target parameter configuration To create an SNMPv3 target parameter configuration:

Step	Action
1	Open the **Target Parameter** screen by selecting **Configuration > SNMPv3 > Target Parameter** from the menu. This screen is illustrated in "Target Parameter screen" (page 239).

Target Parameter screen



Configuration > SNMPv3 > Target Parameter

Target Parameter Table

Action	Parameter Tag	Msg Processing Model	Security Model	Security Name	Security Level	Entry Storage

Target Parameter Creation	
Parameter Tag	
Msg Processing Model	SNMPv1
Security Name	
Security Level	noAuthNoPriv
Entry Storage	Volatile

The following table "Target Parameter screen items" (page 239) describes the items on the Target Parameter screen.

Target Parameter screen items

Item	Range	Description
☒		Deletes the row.
Parameter Tag (snmpTargetParamsRowStatus)	1 -- 32	Type a unique character string to identify the parameter tag.
Msg Processing Model (snmpTargetParamsMPModel)	SNMPv1 SNMPv2c SNMPv3 /USM	Choose the message processing model to be used when generating SNMP messages using this entry.
Security Name (snmpTargetParamsSecuirtyName)	1 -- 32	Type the principal on whose behalf SNMP messages are generated using this entry
Security Level (snmpTargetParamsSecuirtyLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the level of security to be used when generating SNMP messages using this entry.
Entry Storage (snmpTargetParamsStorageType)	(1) Volatile (2) Non-Volatile	Choose the storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the **Target Parameter Creation** section, type information in the text boxes, or select from a list.

3 Click **Submit**.

The new entry appears in the **Target Parameter Table**.

—End—

Deleting an SNMPv3 target parameter configuration To delete an SNMPv3 target parameter configuration:

Step	Action
1	Open the **Target Parameter** screen by selecting **Configuration > SNMPv3 > Target Parameter** from the menu. This screen is illustrated in "Target Parameter screen" (page 239).
2	In the **Target Parameter Table**, click the **Delete** icon for the entry to delete.
3	A message prompts for confirmation of the request. Click **OK**.

—End—

Configuring SNMP traps

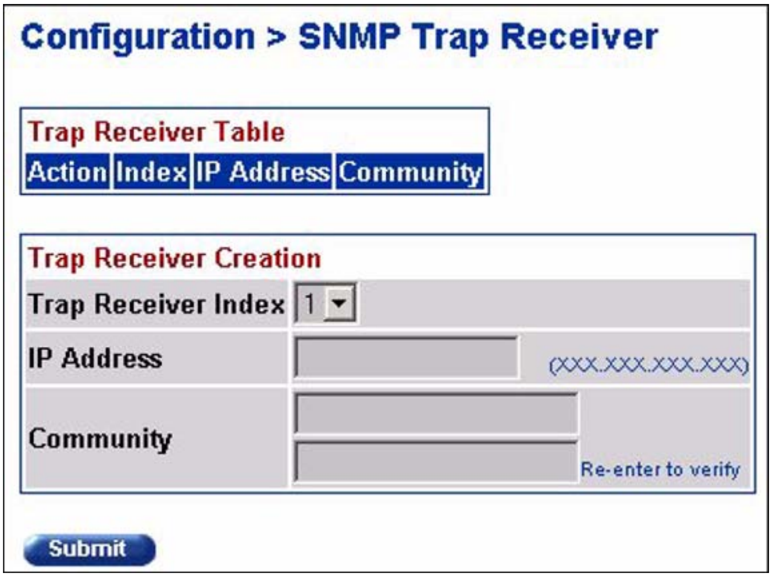
SNMP trap receivers can be viewed, configured, or deleted in the Web-based Management interface.

> ***Note:*** The SNMP Trap Receiver Table is an alternative to using the SNMPv3 Target Table and SNMPv3 Parameter Table. However, only SNMPv1 traps are configurable using this table.

Creating an SNMP trap receiver configuration To create an SNMP trap receiver configuration:

Step	Action
1	Open **the SNMP Trap Receiver** screen by selecting **Configuration > SNMP Trap**. This screen is illustrated in "SNMP Trap Receiver screen" (page 241).

SNMP Trap Receiver screen



Configuration > SNMP Trap Receiver

Trap Receiver Table

Action	Index	IP Address	Community

Trap Receiver Creation

Trap Receiver Index	1	
IP Address		(XXX.XXX.XXX.XXX)
Community	 	Re-enter to verify

Submit

The following table "SNMP Trap Receiver screen items" (page 241) describes the items on the Trap Receiver Table and Trap Receiver Creation sections of the SNMP Trap Receiver screen.

SNMP Trap Receiver screen items

Items	Range	Description
☒		Deletes the row.
Trap Receiver Index	1 -- 4	Choose the number of the trap receiver to create or modify.
IP Address	XXX.XXX.XXX.XXX	Type the network address for the SNMP manager that is to receive the specified trap.
Community	0 -- 32	Type the community string for the specified trap receiver.

2 In the **Trap Receiver Creation** section, type information in the text boxes, or select from a list.

3 Click **Submit**.

The new entry appears in the **Trap Receiver Table**.

—End—

Deleting an SNMP trap receiver configuration To delete SNMP trap receiver configurations:

Step	Action
1	Open the **SNMP Trap Receiver** screen by selecting **Configuration > SNMP Trap**. This screen is illustrated in "SNMP Trap Receiver screen" (page 241).
2	In the **Trap Receiver Table**, click the **Delete** icon for the entry to delete.
3	A message prompts for confirmation of the request. Click **OK**.

—End—

Configuring SNMP using the Java Device Manager

This section details the configuration options available in the JDM for SNMP. It contains information on the following topics:

- "Using SNMPv3 in Device Manager" (page 242)
- "Configuring the switch to use SNMP" (page 261)

Using SNMPv3 in Device Manager

The Nortel Ethernet Routing Switch 5500 Series allows for configuration of SNMPv3 using the Device Manager, Web-based management, or CLI.

The SNMP agent supports exchanges using SNMPv1, SNMPv2c and SNMPv3.

Support for SNMPv2c introduces a standards-based GetBulk retrieval capability using SNMPv1 communities.

SNMPv3 support introduces industrial-grade user authentication and message security. This includes MD5 and SHA-based user authentication and message integrity verification, as well as AES- and DES-based privacy encryption.

> ***Note:*** You must configure views and users in the CLI before SNMPv3 can be used. For information about creating SNMPv3 views and users, see "Configuring SNMP using the CLI" (page 202).

For instructions on configuring SNMPv3 using Device Manager, refer to the following:

- "Viewing the details of an SNMPv3 user" (page 243)
- "Viewing group membership" (page 245)
- "Viewing group access rights" (page 248)

- "Viewing MIBs assigned to an object" (page 252)
- "Creating a community" (page 254)
- "Creating a Target Table" (page 256)
- "Creating Target parameters" (page 258)
- "Creating a Notify Table" (page 259)

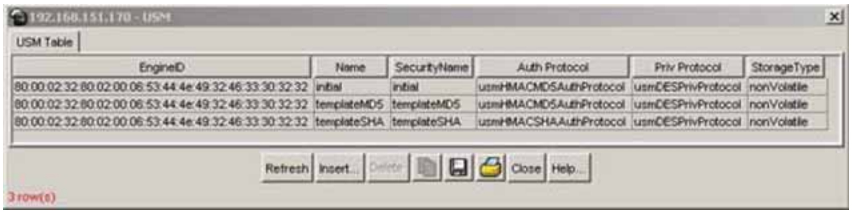
Viewing the details of an SNMPv3 user

To view the details of an SNMPv3 user, complete this task:

Step Action

1 Open the **USM Table** screen by selecting **Edit > SnmpV3 > USM Table** from the menu. This screen is illustrated in "USM Table screen" (page 243).

USM Table screen



EngineID	Name	SecurityName	Auth Protocol	Priv Protocol	StorageType
80:00:02:32:80:02:00:06:53:44:4e:49:32:46:33:30:32:32	initial	initial	usmHMACMD5AuthProtocol	usmDESPrivProtocol	nonVolatile
80:00:02:32:80:02:00:06:53:44:4e:49:32:46:33:30:32:32	templateMD5	templateMD5	usmHMACMD5AuthProtocol	usmDESPrivProtocol	nonVolatile
80:00:02:32:80:02:00:06:53:44:4e:49:32:46:33:30:32:32	templateSHA	templateSHA	usmHMACSHAAuthProtocol	usmDESPrivProtocol	nonVolatile

The following table "USM Table screen items" (page 243) describes the USM Table screen items.

USM Table screen items

Field	Description
EngineID	Indicates the SNMP engine’s unique Identifier.
Name	Indicates the name of the user in usmUser.
SecurityName	Creates the name used as an index to the table. The range is 1 to 32 characters.
AuthProtocol	Identifies the Authentication protocol used.
PrivProtocol	Identifies the privacy protocol used.
StorageType	Identifies the storage type used.

—End—

See also:

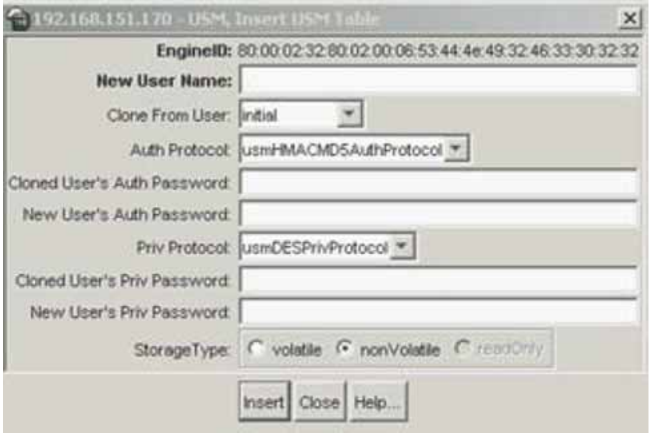
- "Creating an SNMPv3 user" (page 244)

Creating an SNMPv3 user To create an SNMPv3 user, you must clone and then modify the properties of an existing SNMPv3 user.

To create an SNMPv3 user, follow this procedure:

Step	Action
1	Open the **USM Table** screen by selecting **Edit > SnmpV3 > USM Table** from the menu. This screen is illustrated in "USM Table screen" (page 243).
2	Click **Insert**. The **Insert USM Table** screen appears. This screen is illustrated in "USM, Insert USM Table screen" (page 244).

USM, Insert USM Table screen



192.168.151.170 - USM, Insert USM Table

EngineID: 80:00:02:32:80:02:00:06:53:44:4e:49:32:46:33:30:32:32

New User Name:

Clone From User: initial

Auth Protocol: usmHMACMD5AuthProtocol

Cloned User's Auth Password:

New User's Auth Password:

Priv Protocol: usmDESPrivProtocol

Cloned User's Priv Password:

New User's Priv Password:

StorageType: ○ volatile ● nonVolatile ○ readOnly

The following table "Insert USM Table screen fields" (page 244) describes the Insert USM Table screen fields.

Insert USM Table screen fields

Field	Description
New User Name	Creates the new entry with this user name. The name is used as an index to the table. The range is 1 to 32 characters.
Clone From User	Specifies the user name from which the new entry must copy privacy and authentication parameters. The range is 1 to 32 characters.
Auth Protocol (Optional)	Assigns an authentication protocol (or no authentication) from a pull-down menu. If this field is selected, an old AuthPass and a new AuthPass must be entered.
Cloned User’s Auth Password	Specifies the cloned from the user’s authentication password.

Field	Description
New User’s Auth Password	Specifies the new user’s authentication password.
Priv Protocol (Optional)	Assigns a privacy protocol (or no privacy) from a pull-down menu. If this is selected, an old PrivPass and a new PrivPass must be entered.
Cloned User’s Priv Password	Specifies the cloned from user’s privacy password.
New User’s Priv Password	Specifies the name of the new privacy password.
StorageType	Specifies the type of storage: • volatile • nonVolatile • readOnly (not available)

3 Type and select the required information in the **Insert USM Table** screen.

4 Click **Insert**.

—End—

See also:

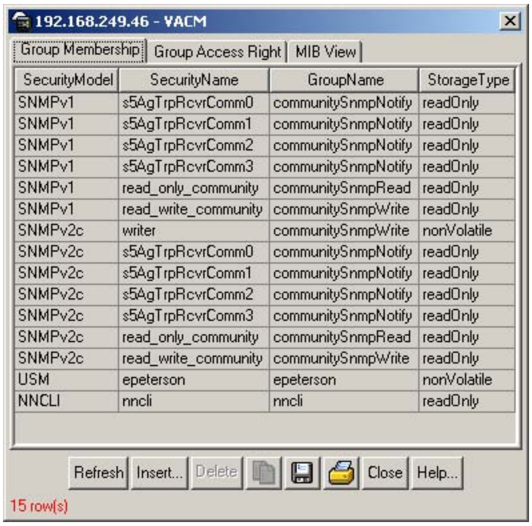
- "Viewing the details of an SNMPv3 user" (page 243)
- "Viewing group membership" (page 245)
- "Viewing group access rights" (page 248)
- "Viewing MIBs assigned to an object" (page 252)
- "Creating a community" (page 254)
- "Creating a Target Table" (page 256)
- "Creating Target parameters" (page 258)
- "Creating a Notify Table" (page 259)

Viewing group membership

To view group membership details in the view-based access control model (VACM):

Step	Action
1	Open the **VACM** screen by selecting **Edit > SnmpV3 > VACM Table...** from the menu. This screen is illustrated in "VACM screen" (page 246).

VACM screen



SecurityModel	SecurityName	GroupName	StorageType
SNMPv1	s5AgTrpRcvrComm0	communitySnmpNotify	readOnly
SNMPv1	s5AgTrpRcvrComm1	communitySnmpNotify	readOnly
SNMPv1	s5AgTrpRcvrComm2	communitySnmpNotify	readOnly
SNMPv1	s5AgTrpRcvrComm3	communitySnmpNotify	readOnly
SNMPv1	read_only_community	communitySnmpRead	readOnly
SNMPv1	read_write_community	communitySnmpWrite	readOnly
SNMPv2c	writer	communitySnmpWrite	nonVolatile
SNMPv2c	s5AgTrpRcvrComm0	communitySnmpNotify	readOnly
SNMPv2c	s5AgTrpRcvrComm1	communitySnmpNotify	readOnly
SNMPv2c	s5AgTrpRcvrComm2	communitySnmpNotify	readOnly
SNMPv2c	s5AgTrpRcvrComm3	communitySnmpNotify	readOnly
SNMPv2c	read_only_community	communitySnmpRead	readOnly
SNMPv2c	read_write_community	communitySnmpWrite	readOnly
USM	epeterson	epeterson	nonVolatile
NNCLI	nncli	nncli	readOnly

15 row(s)

The following table "VACM screen, Group Membership tab fields" (page 246) describes the VACM screen, Group Membership fields.

VACM screen, Group Membership tab fields

Field	Description
SecurityModel	The security model currently in use.
SecurityName	The name representing the user in usm user. The range is 1 to 32 characters.
GroupName	The name of the group to which this entry (combination of securityModel and securityName) belongs.
StorageType	The security type of the group to which this entry belongs.

—End—

See also:

- "Creating membership for a group" (page 247)

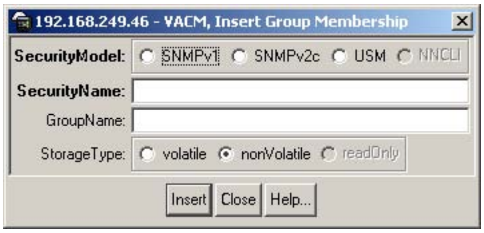
Creating membership for a group

Step	Action

1 Open the **VACM** screen by selecting **Edit > SnmpV3 > VACM Table...** from the menu. This screen is illustrated in "VACM screen" (page 246).

2 Click **Insert**. The **Insert Group Membership** screen appears. This screen is illustrated in "VACM, Insert Group Membership dialog box" (page 247).

VACM, Insert Group Membership dialog box



192.168.249.46 - VACM, Insert Group Membership

SecurityModel: ○ SNMPv1 ○ SNMPv2c ○ USM ○ NNCLI

SecurityName:

GroupName:

StorageType: ○ volatile ● nonVolatile ○ readOnly

The following table "VACM, Insert Group Membership tab fields" (page 247) describes the Insert Group Membership tab fields.

VACM, Insert Group Membership tab fields

Field	Description
SecurityModel	The authentication checking to communicate to the switch.
SecurityName	The security name assigned to this entry in the VACM table. The range is 1 to 32 characters.
GroupName	The name assigned to this group in the VACM table. The range is 1 to 32 characters.
StorageType	Choose the type of storage: • volatile • nonVolatile • readOnly (not available)

3 Select and type the required information.

4 Click **Insert**.

—End—

See also:

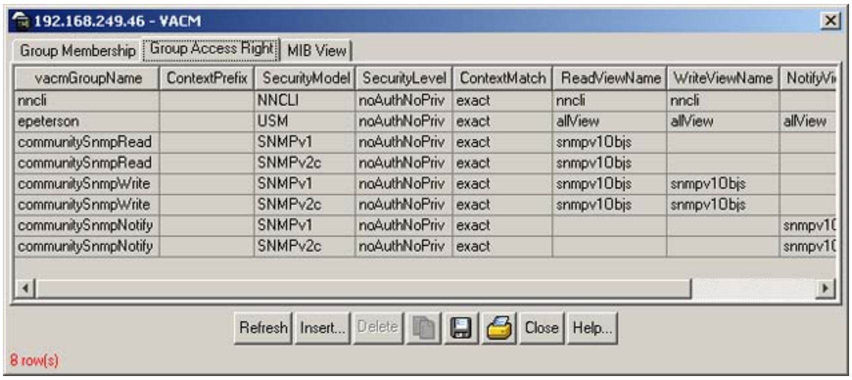
- "Viewing group membership" (page 245)
- "Viewing the details of an SNMPv3 user" (page 243)
- "Viewing group access rights" (page 248)
- "Viewing MIBs assigned to an object" (page 252)
- "Creating a community" (page 254)
- "Creating a Target Table" (page 256)
- "Creating Target parameters" (page 258)
- "Creating a Notify Table" (page 259)

Viewing group access rights

To view access rights for a group:

Step	Action
1	Open the **VACM** screen by selecting **Edit > SnmpV3 > VACM Table...** from the menu. This screen is illustrated in "VACM screen" (page 246).
2	Select the **Group Access Right** tab. This tab is illustrated in "VACM screen, Group Access tab" (page 248).

VACM screen, Group Access tab



vacmGroupName	ContextPrefix	SecurityModel	SecurityLevel	ContextMatch	ReadViewName	WriteViewName	NotifyVi
nncli		NNCLI	noAuthNoPriv	exact	nncli	nncli	
epeterson		USM	noAuthNoPriv	exact	allView	allView	allView
communitySnmpRead		SNMPv1	noAuthNoPriv	exact	snmpv1Objs		
communitySnmpRead		SNMPv2c	noAuthNoPriv	exact	snmpv1Objs		
communitySnmpWrite		SNMPv1	noAuthNoPriv	exact	snmpv1Objs	snmpv1Objs	
communitySnmpWrite		SNMPv2c	noAuthNoPriv	exact	snmpv1Objs	snmpv1Objs	
communitySnmpNotify		SNMPv1	noAuthNoPriv	exact			snmpv1(
communitySnmpNotify		SNMPv2c	noAuthNoPriv	exact			snmpv1(

8 row(s)

The following table "VACM screen, Group Access Right tab fields" (page 249) describes the VACM screen, Group Access Right tab fields.

VACM screen, Group Access Right tab fields

Field	Description
vacmGroupName	The name of the new group name in the VACM table. The name is a numeral. The range is 1 to 32 characters.
ContextPrefix	The contextName of an incoming SNMP packet must match exactly or partially the value of the instance of this object. The range is an SnmpAdminString, 0 to 32 characters.
SecurityModel	The security model of the entry, either SNMPv1, SNMPv2, or SNMPv3.
SecurityLevel	The minimum level of security required to gain access rights. The security levels are: • noAuthNoPriv • authNoPriv • authPriv
ContextMatch (Optional)	Specifies the exact or prefix-only match to the contextName for an incoming SNMP packet
ReadViewName	Specifies the MIB view to which read access is authorized.
WriteViewName	Specifies the MIB view to which write access is authorized.
NotifyViewName	Specifies the MIB view to which notify access is authorized.
StorageType	Specifies the storage type.

—End—

See also:

- "Creating access for a group" (page 249)

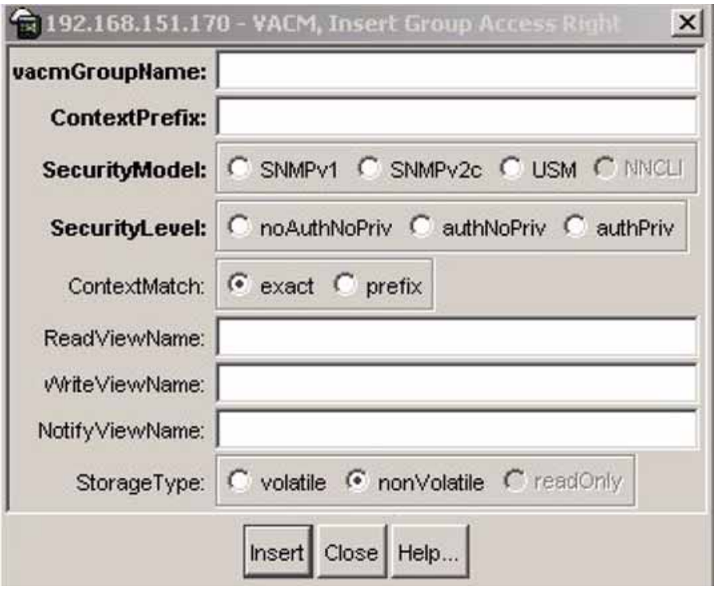
Creating access for a group To create new access for a group:

Step	Action
1	Open the **VACM** screen by selecting **Edit > SnmpV3 > VACM Table...** from the menu. This screen is illustrated in "VACM screen" (page 246).

2 Select the **Group Access Right** tab. This tab is illustrated in "VACM screen, Group Access tab" (page 248).

3 Click **Insert**. The **Insert Group Access Right** screen appears. This screen is illustrated in "VACM, Insert Group Access Right screen" (page 250).

VACM, Insert Group Access Right screen



vacmGroupName:

ContextPrefix:

SecurityModel: ○ SNMPv1 ○ SNMPv2c ○ USM ○ NNCLI

SecurityLevel: ○ noAuthNoPriv ○ authNoPriv ○ authPriv

ContextMatch: ● exact ○ prefix

ReadViewName:

WriteViewName:

NotifyViewName:

StorageType: ○ volatile ● nonVolatile ○ readOnly

The following table "Insert Group Access Right screen fields" (page 250) describes the Insert Group Access Right screen fields

Insert Group Access Right screen fields

Field	Description
vacmGroupName	The name of the new group name in the VACM table. The name is a numeral. The range is 1 to 32 characters.
ContextPrefix	The contextName of an incoming SNMP packet must match exactly or partially the value of the instance of this object. The range is an SnmpAdminString, 0 to 32 characters. For the 5500 Series switches, the ContextPrefix value should be an empty string.
SecurityModel	The security model of the entry, either SNMPv1, SNMPv2, or SNMPv3.

Field	Description
SecurityLevel	The minimum level of security required to gain access rights. The security levels are: • noAuthNoPriv • authNoPriv • AuthPriv
ContextMatch (Optional)	Specifies the exact or prefix-only match to the contextName for an incoming SNMP packet. For Nortel Ethernet Routing Switch products, the ContextMatch value should be exact, because these products support only a single context.
ReadViewName	Specifies the MIB view to which read access is authorized.
WriteViewName	Specifies the MIB view to which write access is authorized.
NotifyViewName	Specifies the MIB view to which notify access is authorized.
StorageType	Specifies the storage type.

4 Type and select the required information.

5 Click **Insert**.

—End—

See also:

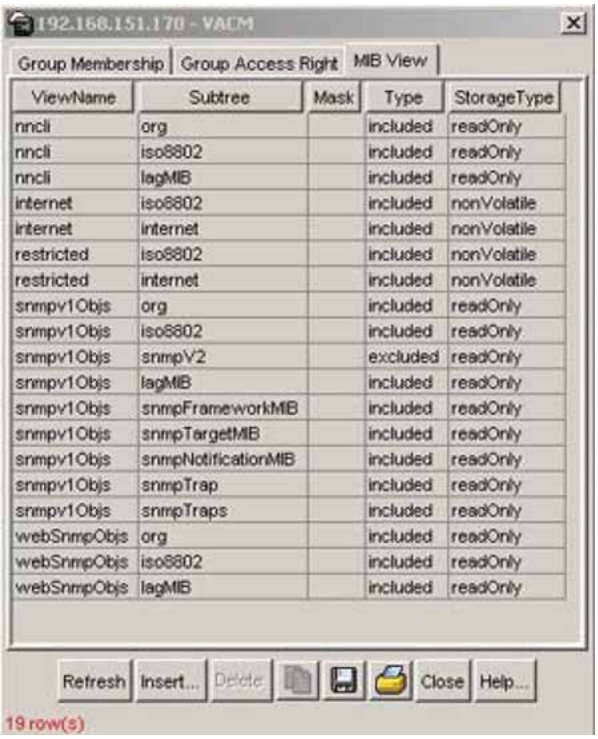
- "Viewing group access rights" (page 248)
- "Viewing the details of an SNMPv3 user" (page 243)
- "Viewing group membership" (page 245)
- "Viewing MIBs assigned to an object" (page 252)
- "Creating a community" (page 254)
- "Creating a Target Table" (page 256)
- "Creating Target parameters" (page 258)
- "Creating a Notify Table" (page 259)

Viewing MIBs assigned to an object

To view MIBs assigned to an object:

Step	Action
1	Open the **VACM** screen by selecting **Edit > SnmpV3 > VACM Table...** from the menu. This screen is illustrated in "VACM screen" (page 246).
2	Select the **MIB View** tab. This tab is illustrated in "VACM screen, MIB View tab" (page 252).

VACM screen, MIB View tab



ViewName	Subtree	Mask	Type	StorageType
nncli	org		included	readOnly
nncli	iso8802		included	readOnly
nncli	lagMIB		included	readOnly
internet	iso8802		included	nonVolatile
internet	internet		included	nonVolatile
restricted	iso8802		included	nonVolatile
restricted	internet		included	nonVolatile
snmpv1Objs	org		included	readOnly
snmpv1Objs	iso8802		included	readOnly
snmpv1Objs	snmpV2		excluded	readOnly
snmpv1Objs	lagMIB		included	readOnly
snmpv1Objs	snmpFrameworkMIB		included	readOnly
snmpv1Objs	snmpTargetMIB		included	readOnly
snmpv1Objs	snmpNotificationMIB		included	readOnly
snmpv1Objs	snmpTrap		included	readOnly
snmpv1Objs	snmpTraps		included	readOnly
webSnmpObjs	org		included	readOnly
webSnmpObjs	iso8802		included	readOnly
webSnmpObjs	lagMIB		included	readOnly

19 row(s)

The following table "VACM screen, MIB View tab fields" (page 252) describes the MIB View tab fields.

VACM screen, MIB View tab fields

Field	Description
ViewName	Creates a new entry with this group name. The range is 1 to 32 characters.
Subtree	Any valid object identifier that defines the set of MIB objects accessible by this SNMP entity; for example, 1.3.6.1.1.5

Field	Description
Mask (Optional)	Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.
Type	Determines whether access to a MIB object is granted (Included) or denied (Excluded). Included is the default.
StorageType	Displays the type of storage for this view.

—End—

See also:

- "Creating a new MIB view" (page 253)

Creating a new MIB view To create a new MIB view:

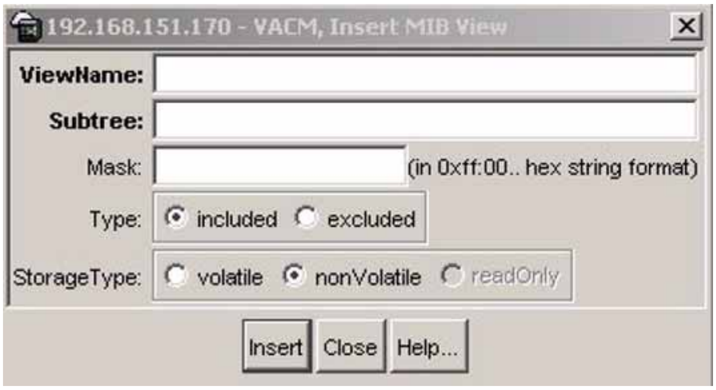
Step Action

1 Open the **VACM** screen by selecting **Edit > SnmpV3 > VACM Table...** from the menu. This screen is illustrated in "VACM screen" (page 246).

2 Select the **MIB View** tab. This tab is illustrated in "VACM screen, MIB View tab" (page 252).

3 Click **Insert**. The **Insert MIB View** screen appears. This screen is illustrated in "Insert MIB View screen" (page 253).

Insert MIB View screen



192.168.151.170 - VACM, Insert MIB View

ViewName:

Subtree:

Mask: (in 0xff:00.. hex string format)

Type: ● included ○ excluded

StorageType: ○ volatile ● nonVolatile ○ readOnly

The following table "Insert MIB View screen fields" (page 254) describes the Insert MIB View screen fields.

Insert MIB View screen fields

Field	Description
ViewName	Creates a new entry with this group name. The range is 1 to 32 characters.
Subtree	Any valid object identifier that defines the set of MIB objects accessible by this SNMP entity, for example, 1.3.6.1.1.5
Mask (Optional)	Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.
Type	Determines whether access to a mib object is granted (Included) or denied (Excluded). Included is the default.
StorageType	Displays the type of storage for this view.

4 Type and select the required information.

5 Click **Insert**.

—End—

See also:

- "Viewing MIBs assigned to an object" (page 252)
- "Viewing the details of an SNMPv3 user" (page 243)
- "Viewing group membership" (page 245)
- "Viewing group access rights" (page 248)
- "Creating a community" (page 254)
- "Creating a Target Table" (page 256)
- "Creating Target parameters" (page 258)
- "Creating a Notify Table" (page 259)

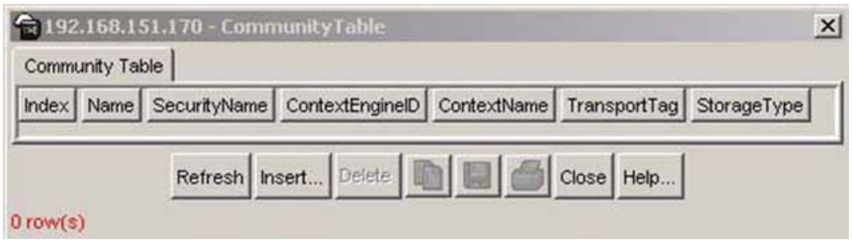
Creating a community

A community table contains objects for mapping between community strings and the security name created in VACM Group Member. To create a community:

Step	Action

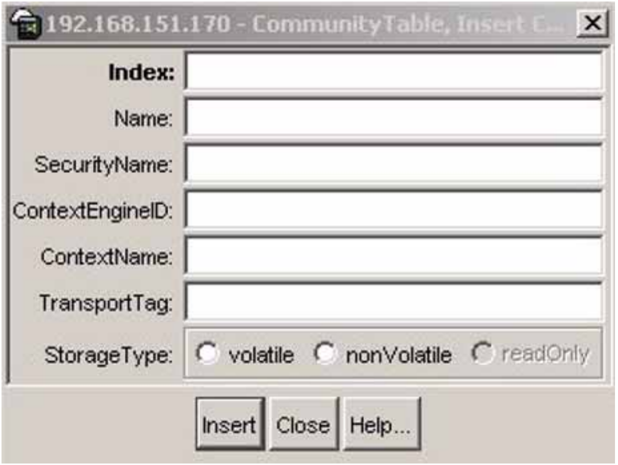
1 Open the **Community Table** screen by selecting **Edit > SnmpV3 > Community Table** from the menu. This screen is illustrated in "Community Table screen" (page 255).

Community Table screen



2 Click **Insert**. The **Insert Community Table** screen appears ("Insert Community Table screen" (page 255)).

Insert Community Table screen



The following table "Community Table screen fields" (page 255) describes the Community Table screen fields.

Community Table screen fields

Field	Description
Index	The unique index value of a row in this table. SnmpAdminString 1-32 characters.
Name	The community string for which a row in this table represents a configuration
SecurityName	The security name assigned to this entry in the Community table. The range is 1 to 32 characters.

Field	Description
ContextEngineID	The context engine ID.
ContextName	The context name.
TransportTag	The transport tag.
StorageType	The storage type.

3 Type and select the required information.

4 Click **Insert**.

—End—

See also:

- "Viewing the details of an SNMPv3 user" (page 243)
- "Viewing group membership" (page 245)
- "Viewing group access rights" (page 248)
- "Viewing MIBs assigned to an object" (page 252)
- "Creating a Target Table" (page 256)
- "Creating Target parameters" (page 258)
- "Creating a Notify Table" (page 259)

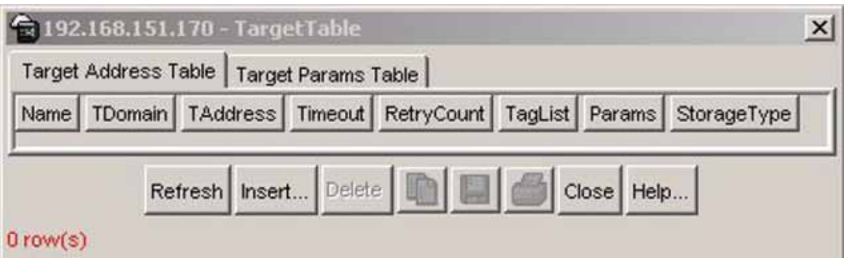
Creating a Target Table

To create a Target Address table:

Step Action

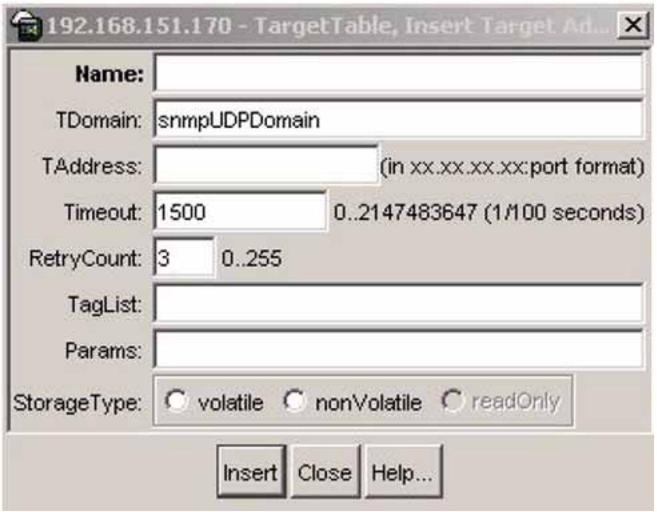
1 Open the **Target Table** screen by selecting **Edit > SnmpV3 > Target Table** from the menu. This screen is illustrated in "Target Table screen, Target Address Table tab" (page 256).

Target Table screen, Target Address Table tab



2 Click **Insert**. The **Insert Target Address** screen appears ("Insert Target Table screen" (page 257)).

Insert Target Table screen



192.168.151.170 - TargetTable, Insert Target Ad...

Name:

TDomain: snmpUDPDomain

TAddress: (in xx.xx.xx.xx:port format)

Timeout: 1500 0..2147483647 (1/100 seconds)

RetryCount: 3 0..255

TagList:

Params:

StorageType: ○ volatile ○ nonVolatile ○ readOnly

The following table "Target Address Table screen fields" (page 257) describes the Target Address Table screen.

Target Address Table screen fields

Field	Description
Name	Specifies the name of the target table.
TDomain	Specifies the TDomain for the target table.
TAddress	Specifies the TAddress for the target table.
Timeout	Specifies the length of the timeout.
RetryCount	Specifies the retrycount.
Taglist	Specifies the taglist.
Params	Specifies an entry in the Target Params Table.
StorageType	Specifies the storage type.

3 Type and select the required information.

4 Click **Insert**.

—End—

See also:

- "Viewing the details of an SNMPv3 user" (page 243)
- "Viewing group membership" (page 245)
- "Viewing group access rights" (page 248)

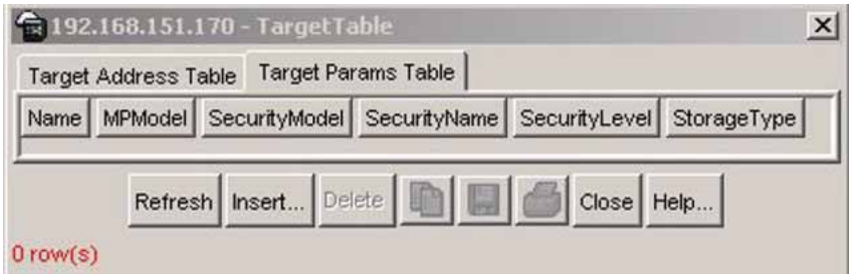
- "Viewing MIBs assigned to an object" (page 252)
- "Creating a community" (page 254)
- "Creating Target parameters" (page 258)
- "Creating a Notify Table" (page 259)

Creating Target parameters

To create a target parameter:

Step	Action
1	Open the **Target Table** screen by selecting **Edit > SnmpV3 > Target Table** from the menu. This screen is illustrated in "Target Table screen, Target Address Table tab" (page 256).
2	Select the **Target Params Table** tab. This tab is illustrated in "Target Table screen, Target Params Table tab" (page 258).

Target Table screen, Target Params Table tab

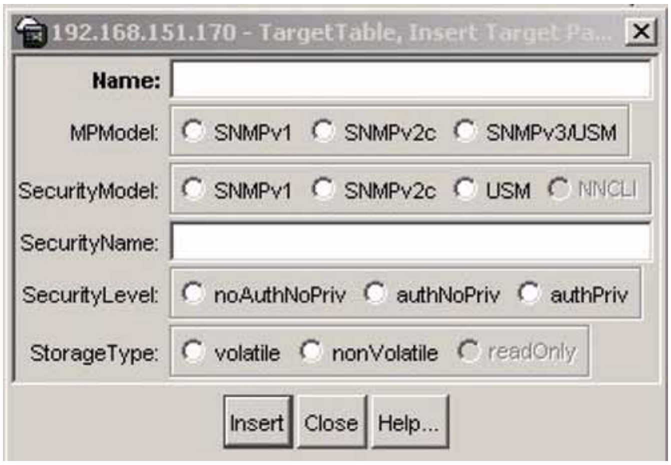


Name	MPModel	SecurityModel	SecurityName	SecurityLevel	StorageType

0 row(s)

3	Click **Insert**. The **Insert Target Params Table** screen appears ("Insert Target Params Table screen" (page 258)).

Insert Target Params Table screen


192.168.151.170 - TargetTable, Insert Target Pa...
Name:
MPModel: ○ SNMPv1 ○ SNMPv2c ○ SNMPv3/USM
SecurityModel: ○ SNMPv1 ○ SNMPv2c ○ USM ○ NNCLI
SecurityName:
SecurityLevel: ○ noAuthNoPriv ○ authNoPriv ○ authPriv
StorageType: ○ volatile ○ nonVolatile ○ readOnly
Insert
Close
Help...

The following table "Target Params Table screen fields" (page 259)describes the Target Params Table screen fields.

Target Params Table screen fields

Field	Description
Name	Specifies the name of the target parameters table.
MPModel	Specifies the Message Processing model, SNMPv1, SNMPv2c, or SNMPv3/USM.
SecurityModel	Specifies the security model, SNMPv1, SNMPv2c, or SNMPv3/USM.
SecurityName	Specifies the security name for generating SNMP messages.
SecurityLevel	Specifies the security level for SNMP messages: noAuthnoPriv, authnoPriv, or authPriv.
Storage Type	Specifies the storage type: volatile or non-volatile.

4 Type and select the required information.

5 Click **Insert**.

—End—

See also:

- "Viewing the details of an SNMPv3 user" (page 243)
- "Viewing group membership" (page 245)
- "Viewing group access rights" (page 248)
- "Viewing MIBs assigned to an object" (page 252)
- "Creating a community" (page 254)
- "Creating a Target Table" (page 256)
- "Creating a Notify Table" (page 259)

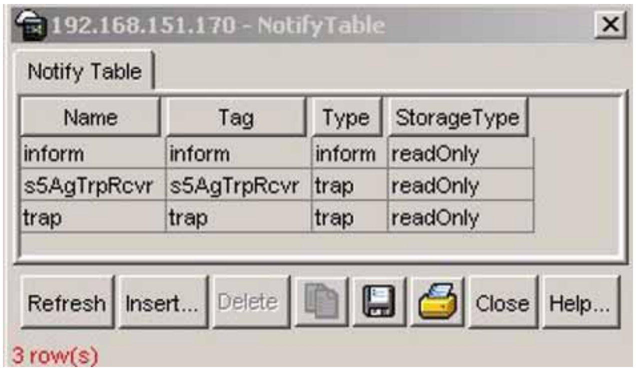
Creating a Notify Table

To create a Notify Table:

Step Action

1 Open the **Notify Table** screen by selecting **Edit > SnmpV3 > Notify Table** from the menu. This screen is illustrated in "Notify Table dialog box" (page 260).

Notify Table dialog box



192.168.151.170 - NotifyTable

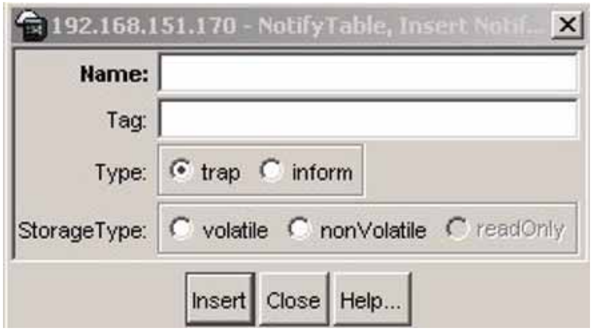
Notify Table

Name	Tag	Type	StorageType
inform	inform	inform	readOnly
s5AgTrpRcvr	s5AgTrpRcvr	trap	readOnly
trap	trap	trap	readOnly

3 row(s)

2 Click **Insert**. The **Insert Notify Table** screen appears ("Insert Notify Table screen" (page 260)).

Insert Notify Table screen



192.168.151.170 - NotifyTable, Insert Notif...

Name:

Tag:

Type: ● trap ○ inform

StorageType: ○ volatile ○ nonVolatile ○ readOnly

The following table "Notify Table screen fields" (page 260)describes the Notify Table screen fields.

Notify Table screen fields

Field	Description
Name	Specifies the unique identifier associated for the notify table.
Tag	A single tag value used to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object contains a value of zero length, no entries are selected.

Field	Description
Type	This object determines the type of notification generated for entries in the snmpTargetAddrTable selected by the corresponding instance of snmpNotifyTag. If the value of this object is trap, then any messages generated for selected rows contain SNMPv2-Trap PDUs. If the value of this object is inform, then any messages generated for selected rows contain Inform PDUs. ***Note:*** If an SNMP entity only supports generation of traps (and not informs), then this object can be read-only.
StorageType	Specifies the type of storage, volatile or non-volatile.

3 Type and select the required information.

4 Click **Insert**.

—End—

See also:

- "Viewing the details of an SNMPv3 user" (page 243)
- "Viewing group membership" (page 245)
- "Viewing group access rights" (page 248)
- "Viewing MIBs assigned to an object" (page 252)
- "Creating a community" (page 254)
- "Creating a Target Table" (page 256)
- "Creating Target parameters" (page 258)

Configuring the switch to use SNMP

For information on configuring SNMP on the switch, refer to the following:

- "SNMP tab" (page 262)
- "Trap Receivers tab" (page 263)

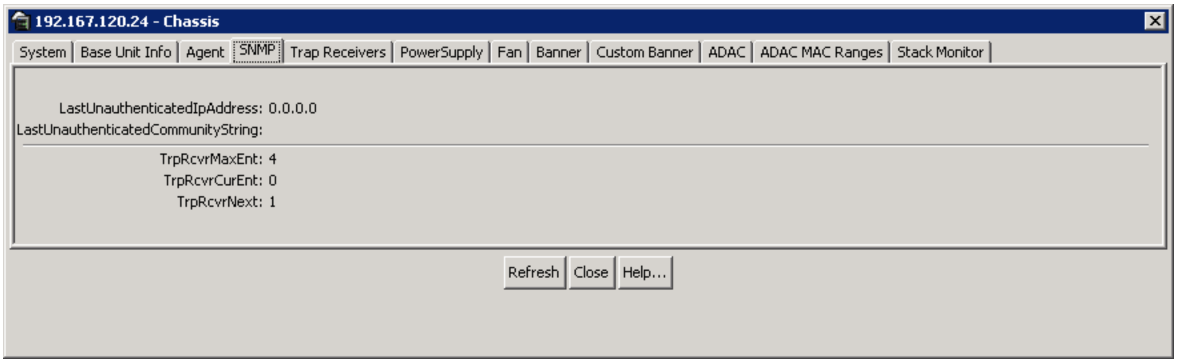
SNMP tab

The **SNMP** tab provides read-only information about the addresses that the agent software uses to identify the switch.

To open the **SNMP** tab:

Step	Action
1	Select the chassis in the Device View.
2	Open the **Edit Chassis** screen by selecting **Edit > Chassis** from the menu.
3	Select the **SNMP** tab. The following figure illustrates this tab.

Edit Chassis screen -- SNMP tab



LastUnauthenticatedIpAddress: 0.0.0.0
LastUnauthenticatedCommunityString:
TrpRcvrMaxEnt: 4
TrpRcvrCurEnt: 0
TrpRcvrNext: 1

The following table describes the SNMP tab fields.

SNMP tab fields

Field	Description
LastUnauthenticatedIpAddress	The last IP address that was not authenticated by the device.
LastUnauthenticatedCommunityString	The last community string that was not authenticated by the device.
TrpRcvrMaxEnt	The maximum number of trap receiver entries.
TrpRcvrCurEnt	The current number of trap receiver entries.
TrpRcvrNext	The next trap receiver entry to be created.

—End—

See also:

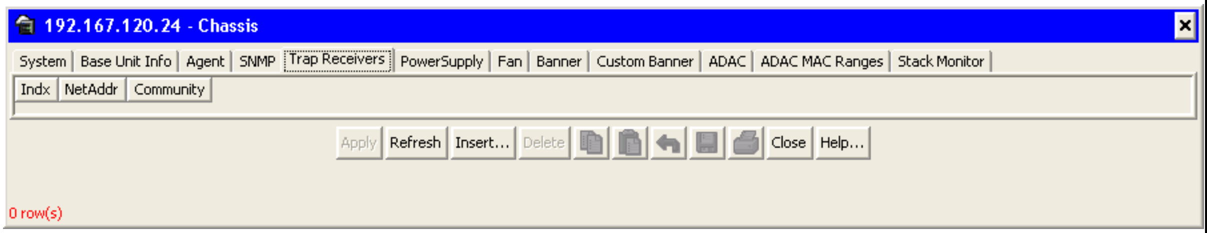
- "Trap Receivers tab" (page 263)

Trap Receivers tab

The Trap Receivers tab lists the devices that receive SNMP traps from the Nortel Ethernet Routing Switch 5500 Series.

To open the **Trap Receivers** tab:

Step	Action
1	Select the chassis in the Device View.
2	Open the **Edit Chassis** screen by selecting **Edit > Chassis** from the menu.
3	Select the **Trap Receivers** tab. The following figure illustrates this tab.



The following table describes the Trap Receivers tab fields.

Trap Receivers tab fields

Field	Description
Indx	The index of the entry in the table.
NetAddr	The IP address for the trap receiver.
Community	Community string used for trap messages to this trap receiver.

—End—

- "SNMP tab" (page 262)

- "Editing network traps" (page 264)

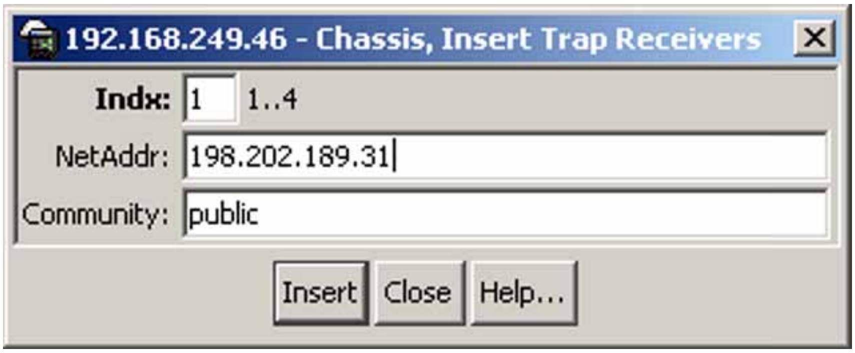
Editing network traps To edit the network traps table:

Step	Action

1 In the **Trap Receivers** tab, click **Insert**.

The **Insert Trap Receivers** screen appears (see the following figure).

Insert Trap Receivers screen



192.168.249.46 - Chassis, Insert Trap Receivers

Indx: 1 1..4

NetAddr: 198.202.189.31

Community: public

2 Type the **Index**, **NetAddr**, and **Community** information.

3 Click **Insert**.

—End—

Implementing the Nortel Secure Network Access solution

This chapter includes the following topics:

Overview

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

The 5500 Series Nortel Ethernet Routing Switch Series is referred to as an NSNA network access device in the context of the Nortel SNA solution. Host computers can connect using dynamic or static IP addressing. Windows, MacOSX, and Linux operating systems are supported. Access to the corporate network requires successful:

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

Access to the network proceeds as follows:

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

Red zone pending successful authentication. Either the MAC address of the host or a username/password of the end user can be used for authentication.

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

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

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

For information about configuring the Nortel Ethernet Routing Switch 5500 Series for the Nortel SNA solution using the CLI, see "Configuring Nortel Secure Network Access using the CLI" (page 283). For information about configuring the Nortel Ethernet Routing Switch 5500 Series for the Nortel SNA solution using Java Device Manager, see "Configuring Nortel Secure Network Access using Device Manager" (page 297).

NSNA configuration example for MAC authorization enhancement

This enhancement is to distinguish the trusted users from untrusted users and grant quick access.

The MAC addresses of devices are known prior and this knowledge can be used to authenticate such devices in a simple, centralized way.

MAC Authentication Support on NSNA Ports :

- Mac Authentication by the SNAS is automatically enabled on a NSNA Dynamic Port.
- Mac Authentication is used for PCs and Passive devices.

- Phones will still be authenticated by their DHCP signature. Provision to configure a list of signatures is provided.
- Initial State of an NSNA port will be in Red VLAN and Red Filter

New MAC Event at the Port:

- If the Mac comes in on a VoIP VLAN, treat as a phone and inform SNAS, else, the switch sends an Authenticate Request to the SNAS via SSCP
- If SNAS has the MAC in its Data Base (DB), it will send back an AuthenticateResponse=Success to the switch via SSCP.
- SSCP message changes are handled between the switch and SNAS internals.

MAC Age Event at the Port:

The MAC will remain in the list (as aged out) until replaced by another MAC.

Reset Event at the Port:

The port can be reset by physical link down/up or through an SSCP message from the SNAS. either case, all devices will be deleted and the port moved to red VLAN/filter.

VLAN-Filter Change at the port:

This can happen by a SSCP message from SNAS to the switch, typically for TG-users.

MAC Authentication Success:

The Success Response contains the following:

- Auth. Result = Success
- Device Type = PC or Passive
- Filter Id (as VID) to indicate Red, Yellow or Green filter
- Client IP Address if available or 0

Switch saves the device Information in its local list and move the port to the appropriate filter. If the device has a static IP, it will be populated in the SNAS and the switch will learn it in the Auth-Response. If the device does DHCP, the IP Address will be learned by DHCP filtering at the switch. Any time a Device-IP is learned, the SNAS will be informed via SSCP

MAC Authentication Failure:

No Response sent on Auth-Failure, but TG (tunnel-guard) Authentication can still happen.

Port modes

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

- Default mode

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

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

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

- Nortel SNA dynamic IP mode:

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

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

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

Filters in the Nortel SNA solution

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

For information about modifying the filter sets, see *Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service* (NN47200-504). For an example of the current default Nortel SNA filter set rules, see "Default Nortel SNA filters" (page 334).

> ***Note:*** When the Nortel SNA filters are applied to a port, any existing Quality of Service (QoS) filters on that port are disabled, and the Nortel SNA filters are applied (pre-existing policies are re-enabled when Nortel SNA is disabled). See "Rolling back Nortel SNA mode to default mode" (page 282) and "Deploying the Nortel SNA solution in an active network" (page 279) for more information.

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

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

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

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

Red, Yellow, and Green VLANs must be configured on the Nortel SNA uplink ports of the NSNA network access device when the NSNA filter sets for each enforcement zone are assigned to specific VLANs. When only the filter sets are used, a Red VLAN must be configured on the Nortel SNA uplink ports. To configure the uplink ports, use **`nsna port <portlist> uplink vlans <vidlist>`** (see "Enabling Nortel SNA on ports " (page 288)

Only Nortel SNA ports (uplink or dynamic) can be in the Red, Yellow, Green, and VoIP VLANs.

Nortel SNA ports become members of Nortel SNA VLANs when Nortel SNA is enabled. Manually attaching dynamic Nortel SNA ports to a non-Nortel SNA VLAN is not allowed.

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

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

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

The Red, Yellow, and Green VLANs can be Layer 2 or Layer 3 (see "Topologies" (page 274) for more information).

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

> ***Note:*** With Ethernet Routing Switch 5500 Series, Software Release 5.1, each switch can support five Yellow VLANs, five Green VLANs, and five VoIP VLANs.

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

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

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

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

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

Default Nortel SNA filter consumption

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

Filter parameters

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

The default Nortel SNA filters protect the workstations. For a detailed listing of the parameters in the default filter sets, see "Default Nortel SNA filters" (page 334).

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

Traffic allowed in the default Nortel SNA filter sets

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

Filter set	Traffic type								
	DNS	**HTTP**	**HTTPS**	**ARP**	**DHCP**	**UDP**	**ICMP**	**Yellow subnet**	**All**
VoIP				Yes	Yes	Yes	Yes		

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

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

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

Note that adding these two filters consumes another precedence level.

Refer to "Configuring filters for Novell Netware log on" (page 273) for information about configuring the filters for Novell Netware log on. If you use any other log on controller, you must modify the filter set to allow the log on to work

Note: In the Yellow VLAN, the default filters allow all IP traffic for the Yellow subnet. You specify the Yellow subnet in the command **`nsna vlan <vid> color yellow filter <filter name> yellow-subnet <ipaddr/mask>`** (see "Configuring Nortel SNA per VLAN " (page 285).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Topologies

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

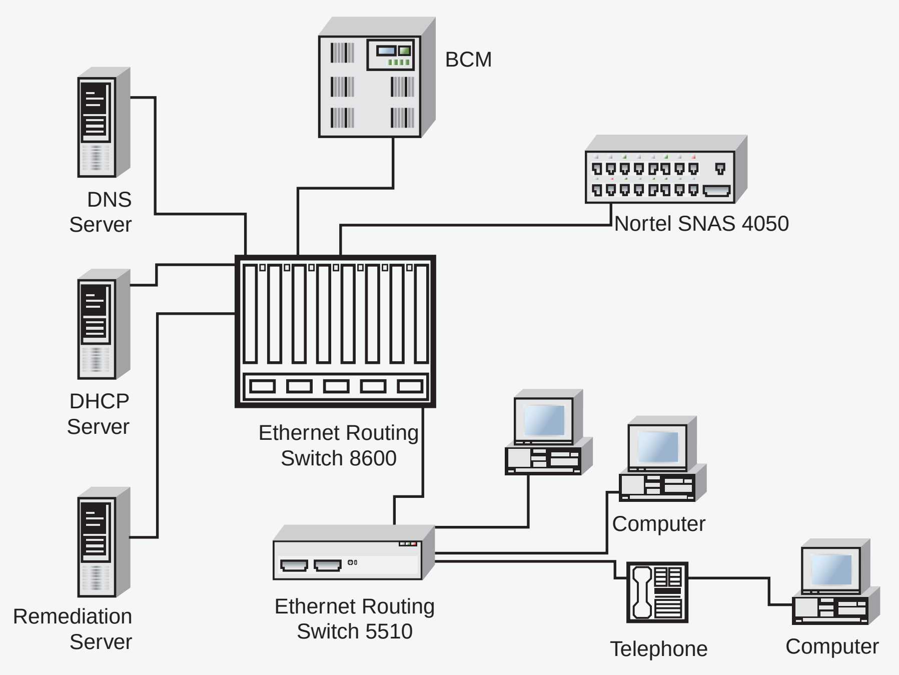
Layer 2

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

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

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

Network access device-Layer 2 mode



Layer 3

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

Basic switch configuration for Nortel SNA

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

Before you begin

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

- Generate the SSH keys on the Nortel SNAS 4050, and upload the public key to a TFTP server.
- Identify the Nortel SNAS 4050 portal Virtual IP address (pVIP) and mask.

- Identify VLAN IDs for Nortel SNA use (that is, for Red and VoIP VLANs; plus Yellow and Green when enforcement zones are configured with VLANs and filters).
- Identify ports to use for uplink ports (in Layer 2 mode only).
- Identify ports to use for Nortel SNA client ports.

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

Configuring the network access device

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

For information about the CLI commands to configure the Nortel SNA solution on the switch, see "Configuring Nortel Secure Network Access using the CLI" (page 283). For information about configuring the Nortel SNA solution using Device Manager, see "Configuring Nortel Secure Network Access using Device Manager" (page 297).

1. Configure static routes to all the networks behind the core routing device.

   This can be automated, as RIP and OSPF routing protocols are supported.
2. Configure the switch management VLAN, if necessary.
3. Configure SSH (see "Configuring SSH on the 5500 Series switch for Nortel SNA" (page 278)).
   a. Download the Nortel SNAS 4050 SSH public key to the switch.
   b. Enable SSH on the switch.

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

   c. Import the switch SSH public key on the Nortel SNAS 4050 (note that this step is performed on the Nortel SNAS 4050, not on the edge switch).
4. Configure the Nortel SNAS 4050 portal IP address (pVIP)/subnet (see "Configuring the Nortel SNAS 4050 subnet " (page 283)for CLI, or "Configuring the Nortel SNAS 4050 subnet" (page 297) for Device Manager).
5. Configure port tagging, if applicable.

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

6. Create the port-based VLANs.

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

7. Configure DHCP-relay and IP routing if the switch is used in Layer 3 mode.

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

   > ***Note:*** Manual configuration of the filters is optional. The filters are configured automatically as predefined defaults when you configure the Red, Yellow, Green, and VoIP VLANs.
   >
   > You can modify default filter sets and manually created filter sets after Nortel SNA is enabled.

9. Configure the VoIP VLANs (see "Configuring Nortel SNA per VLAN " (page 285) for CLI, or "Configuring Nortel SNA per VLAN" (page 300) for Device Manager).

10. Configure the Red, Yellow, and Green VLANs, associating each with the applicable filters (see "Configuring Nortel SNA per VLAN " (page 285)for CLI, or "Configuring Nortel SNA per VLAN" (page 300) for Device Manager).

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

11. Configure the Nortel SNA ports (see "Enabling Nortel SNA on ports " (page 288) for CLI, or "Enabling Nortel SNA on ports" (page 304) for Device Manager).

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

    > ***Note 1:*** If the network access device itself is the DHCP relay agent (that is, functioning in Layer 3 mode) for any of the Red, Yellow, Green, or VoIP VLANs, it is not necessary to configure an uplink port in that VLAN.
    >
    > ***Note 2:*** You can configure Nortel SNA ports (both dynamic and uplink) after Nortel SNA is enabled globally.

12. Enable Nortel SNA globally (see "Enabling Nortel SNA" (page 292) for CLI, or "Enabling Nortel SNA" (page 312) for Device Manager).

Configuring SSH on the 5500 Series switch for Nortel SNA

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

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

Step Action

1 Download the SSH public key from the Nortel SNAS 4050 to the switch:

> ***Note:*** Ensure you have generated the Nortel SNAS 4050 key. Use the following command on the Nortel SNAS 4050 to generate the SSH public and private keys for the Nortel SNAS 4050: **`cfg/domain #/sshkey/generate`**

a. On the Nortel SNAS 4050, use the **`/cfg/domain #/sshkey/export`** command to upload the key to a TFTP server, for manual retrieval from the switch.

b. On the 5500 Series switch, load the Nortel SNAS 4050 public key to the switch using the following commands from the Global configuration mode:

```
ssh download-auth-key address <ipaddr> key-name
<filename>
```

where

`<ipaddr>` is the IP address of the server (entered as A.B.C.D) where you placed the key.

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

```
ssh
```

3 On the Nortel SNAS 4050, import the 5500 Series switch public key:

```
/cfg/domain #/switch #/sshkey/import
apply
```

For more information, refer to *Nortel Secure Network Access Switch 4050 User Guide (320818-A)*.

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

—End—

Deploying the Nortel SNA solution in an active network

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

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

About the ports

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

- Nortel SNA
- non-Nortel SNA

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

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

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

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

If you subsequently disable Nortel SNA, the port returns to the pre-Nortel SNA state (see "Rolling back Nortel SNA mode to default mode" (page 282)).

When the port is a Nortel SNA uplink port and Nortel SNA is enabled, the port can be a member of Nortel SNA and non-Nortel SNA VLANs (see "Configuration example: Adding the uplink port" (page 289)).

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

You can configure multiple Nortel SNA uplink ports.

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

The PVID of the uplink port can be modified.

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

About the VLANs and filters

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

Nortel SNA enforcement zones have corresponding default Nortel SNA filter sets. Nortel recommends that you use the default filter sets. You can, however, create customized filters sets and attach these to the Nortel SNA VLANs. You can also modify the default filters, if necessary, after you have enabled them (see *Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service* (NN47200-504) and "Default Nortel SNA filters" (page 334) for more information).

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

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

- Red

- Yellow
- Green
- VoIP

Each network access device must have one, and only one, Red VLAN. Each switch can, however, have multiple Yellow and multiple Green VLANs. In Ethernet Routing Switch 5500 Series, Software Release 5.1, you can configure no more than five Yellow, five Green, and five VoIP VLANs on each switch.

Updating the filter sets

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

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

1. Manually update them using the **`qos nsna`** command (see *Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service* (NN47200-504) and "Configuration example: Configuring the default Nortel SNA filters" (page 334) for specific information).
2. Remove the filters and reconfigure:
   a. Disable Nortel SNA globally.
   b. Disable Nortel SNA on the ports.
   c. Mark the VLANs as non-Nortel SNA (mark VoIP VLANs last).
   d. Delete the filters using one of the following methods:
      i. Delete all the filters at once:
      ```
      enable
      con ter
      qos agent reset-default
      ```
      ii. Delete the filters one by one:
      ```
      no qos nsna name <filter-name-red>
      no qos nsna name <filter-name-yellow>
      no qos nsna name <filter-name-green>
      ```
   e. Remove the Nortel SNAS 4050 (**`no nsna nsnas`**).
   f. Reconfigure Nortel SNA.

Rolling back Nortel SNA mode to default mode

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

- VLAN settings
- QoS parameters
- Spanning Tree configuration

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

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

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

Configuring Nortel Secure Network Access using the CLI

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

This chapter includes the following topics:

For an overview of the steps required to configure a network access device in the Nortel SNA solution, see "Basic switch configuration for Nortel SNA" (page 275).

Configuring the Nortel SNAS 4050 subnet

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

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

where

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

This command includes the following parameters:

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

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

Configuration example: Adding a Nortel SNAS 4050 subnet

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

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

Viewing Nortel SNAS 4050 subnet information

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

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

Removing the Nortel SNAS 4050 subnet

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

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

where

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

Configuring QoS for the Nortel SNA solution

For general information about configuring filters and Quality of Service (QoS) in the Nortel SNA solution, see "Filters in the Nortel SNA solution" (page 268). For detailed information about configuring the filters, see *Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service* (NN47200-504).

Configuring Nortel SNA per VLAN

Ensure that:

- the VLANs that you plan to configure as Nortel SNA VLANs have no port numbers assigned.
- no non-Nortel SNA ports are associated with Nortel SNA VLANs.
- the filter name does not begin with a number.

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

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

where

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

This command includes the following parameters:

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

Viewing Nortel SNA VLAN information

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

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

where

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

Removing a Nortel SNA VLAN

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

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

where

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

Configuration example: Configuring the Nortel SNA VLANs

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

> ***Note:*** You must configure the Nortel SNAS 4050 pVIP subnet before you configure the Nortel SNA VLANs.
>
> VoIP VLANs are optional. If you are using VoIP VLANs, you must configure them before configuring the Red, Yellow, and Green VLANs.

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

In this example, the following parameters are used:

VLAN	Parameters
Red	VLAN ID: 110 Color: Red Filter name: red

VLAN	Parameters
Yellow	VLAN ID: 120 Color: Yellow Filter name: yellow Subnet IP: 10.120.120.0/24
Green	VLAN ID: 130 Color: Green Filter name: green
VoIP	VLAN ID: 140 Color: VoIP

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

Configuring the VoIP VLAN

To configure the VoIP VLAN, use the following command:

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

Configuring the Red VLAN

To configure the Red VLAN, use the following command:

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

Configuring the Yellow VLAN

To configure the Yellow VLAN, use the following command:

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

```
---------------------------------------------------------
120         Yellow      yellow              10.120.120.0/24
```

Configuring the Green VLAN

To configure the Green VLAN, use the following command:

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

Enabling Nortel SNA on ports

The following sections describe how to enable Nortel SNA on the ports. For information about port modes, refer to "Port modes" (page 268).

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

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

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

`nsna`

This command includes the following parameters:

nsna followed by:	
port <portlist>	Identifies a port other than that specified when entering the Ethernet Interface configuration mode. The parameter <portlist> uses the convention {port[–port][,...]}.

dynamic voip-vlans <vidlist>	Sets the Nortel SNAS 4050 dynamic port configuration, where <vidlist> is the VoIP VLAN IDs (vlan-id[-vlan-id][,...]).
uplink vlans <vidlist>	Defines the Nortel SNAS 4050 uplink VLAN list, where <vidlist> is the Nortel SNA VLAN IDs (vlan-id[-vlan-id][,...]).

Viewing Nortel SNA port information

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

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

where

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

Removing a Nortel SNA port

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

```
no nsna
```

Example: Removing Nortel SNA ports

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

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

Configuration example: Adding the uplink port

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

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

where

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

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

The membership of Nortel SNA uplink ports in non-Nortel SNA VLANs is not affected by globally enabling or disabling Nortel SNA. Nortel Ethernet Routing Switch 5500 Series Software Release 5.1 supports multiple Nortel SNA uplink ports.

In this example, the following parameters are used:

- uplink port is 20
- Nortel SNA VLAN IDs are 110, 120, 130, 140

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

Configuration example: Adding client ports

In this example, the following parameters are used:

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

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

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

Viewing information about Nortel SNA clients

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

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

where

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

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

```
5510-48T(config)# show nsna client interface 5
Total Number of Clients: 2
Unit/  Client MAC          Device Type  VLAN Id   Filter    IP Address       Exp
Port                                              VLAN Id
---------------------------------------------------------------------------------
5      00:0a:e4:0b:47:44   IP Phone     140 (V)   110 (R)   10.100.140.11    No
5      00:0f:ea:88:be:7a   PC           110 (R)   110 (R)   10.100.110.116   No
```

Entering phone signatures for Nortel SNA

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

```
nsna phone-signature <LINE>
```

where

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

Removing Nortel SNA phone signatures

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

```
no nsna phone-signature <LINE>
```

where

`<LINE>` is the phone signature string

Viewing Nortel SNA phone signatures

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

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

where

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

Enabling Nortel SNA

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

```
nsna enable
```

Note: You must enable SSH before you enable Nortel SNA globally. The command to enable Nortel SNA fails if SSH is not enabled. For more information, see "Configuring SSH on the 5500 Series switch for Nortel SNA" (page 278).

Disabling Nortel SNA

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

```
no nsna enable
```

Viewing the Nortel SNA state

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

```
show nsna
```

Display NSNA Configuration

Example:

```
show nsna
NSNA Enabled:  Yes
NSNAS Connection State:  Connected
NSNAS Address:  10.200.200.2
NSNAS Hello Interval:  60
NSNAS Inactivity Interval:  180
NSNAS Connection Version:  SSCPv1
NSNAS Status-Quo Interval:  60
```

Example: Viewing Nortel SNA and Nortel SNAS 4050 information

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

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

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

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

Configuration example

The configuration example is based on the following assumptions:

- You are starting with an installed switch that is not currently configured as part of the network.
- You have installed Nortel Ethernet Routing Switch 5500 Series, Software Release 5.1 or higher.
- You have configured basic switch connectivity.
- You have initialized the switch and it is ready to accept configuration.

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

Scenario

"Basic network scenario" (page 294) shows the basic network configuration used in this example. The Ethernet Routing Switch 8600 functions as the core router.

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

Network devices

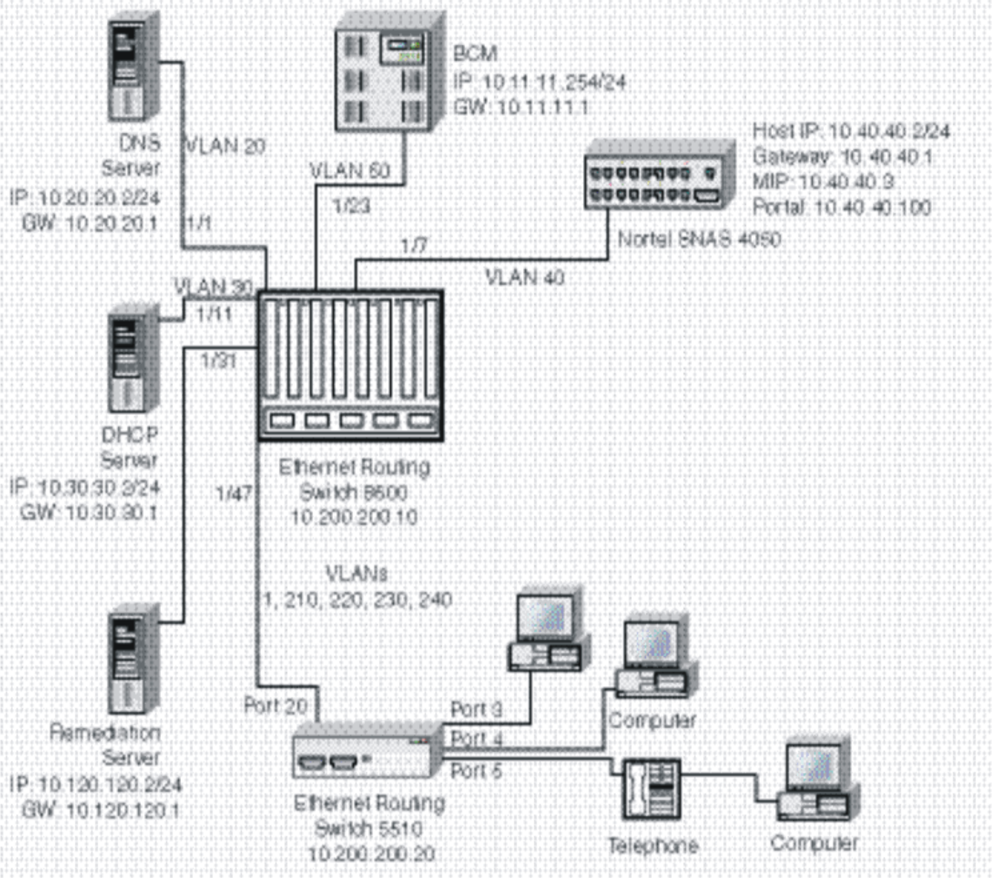
Device/Service	VLAN ID	VLAN IP	Device IP	Ethernet Routing Switch 8600 port
DNS	20	10.20.20.1	10.20.20.2	1/1
DHCP	30	10.30.30.1	10.30.30.2	1/11
Nortel SNAS 4050	40	10.40.40.1	10.40.40.2	1/7
Remediation server	120	10.120.120.1	10.120.120.2	1/31
Call server	50	10.11.11.1	10.11.11.254	1/23

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

VLANs for the Ethernet Routing Switch 5510

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

Basic network scenario



Steps

The example illustrates the following required configuration steps:

1. "Setting the switch IP address" (page 295)
2. "Configuring SSH" (page 295)
3. "Configuring the Nortel SNAS 4050 pVIP subnet" (page 295)
4. "Creating port-based VLANs" (page 295)

5. "Configuring the VoIP VLANs" (page 295)
6. "Configuring the Red, Yellow, and Green VLANs" (page 295)
7. "Configuring the log on domain controller filters" (page 296)
8. "Configuring the Nortel SNA ports" (page 296)
9. "Enabling Nortel SNA globally" (page 296)

Setting the switch IP address

```
5510-48T(config)#ip address 10.200.200.20 netmask
255.255.255.0
5510-48T(config)# ip default-gateway 10.200.200.10
```

Configuring SSH

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

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

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

> ***Note:*** You must import the switch SSH key on the Nortel SNAS 4050 after enabling SSH on the Nortel Ethernet Routing Switch 5500 Series switch. For more information, see "Configuring SSH on the 5500 Series switch for Nortel SNA" (page 278). Also, refer to *Nortel Secure Network Access Switch 4050 User Guide (320818-A)* for more information about configuring SSH on the Nortel SNAS 4050.

Configuring the Nortel SNAS 4050 pVIP subnet

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

Creating port-based VLANs

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

Configuring the VoIP VLANs

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

Configuring the Red, Yellow, and Green VLANs

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

Configuring the log on domain controller filters

Note: This step is optional.

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

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

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

Configuring the Nortel SNA ports

Add the uplink port:

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

Add the client ports:

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

Enabling Nortel SNA globally

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

Configuring Nortel Secure Network Access using Device Manager

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

This chapter includes the following topics:

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

For an overview of the steps required to configure a network access device in the Nortel SNA solution, see "Basic switch configuration for Nortel SNA" (page 275).

Configuring the Nortel SNAS 4050 subnet

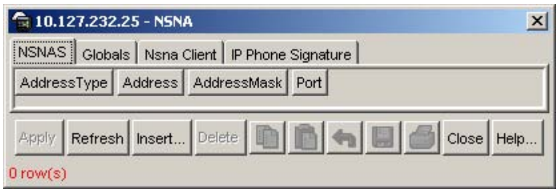
Note: In Ethernet Routing Switch 5500 Series, Software Release 5.1, only one entry for the Nortel SNAS 4050 subnet can be configured.

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

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

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

NSNA -- NSNAS tab



0 row(s)

The following table describes the NSNAS tab fields.

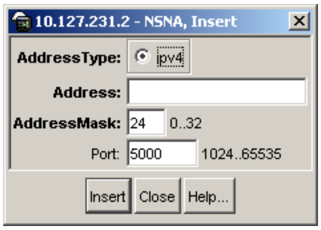
NSNA -- NSNAS tab fields

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

2 Click **Insert**.

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

NSNA, Insert dialog box



AddressType: ● ipv4

Address:

AddressMask: 24 0..32

Port: 5000 1024..65535

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

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

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

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

5 Click **Insert**.

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

—End—

See also:

- "Removing the Nortel SNAS 4050 subnet" (page 299)
- "Configuring QoS for the Nortel SNA solution" (page 300)
- "Configuring Nortel SNA per VLAN" (page 300)
- "Enabling Nortel SNA on ports" (page 304)
- "Viewing Nortel SNA settings" (page 307)
- "Viewing information about Nortel SNA clients" (page 309)
- "Entering phone signatures for Nortel SNA" (page 310)
- "Enabling Nortel SNA" (page 312)

Removing the Nortel SNAS 4050 subnet

To remove the currently configured Nortel SNAS 4050:

Step Action

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

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

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

3 Click **Delete**.

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

—End—

See also:

- "Configuring the Nortel SNAS 4050 subnet" (page 297)
- "Configuring QoS for the Nortel SNA solution" (page 300)
- "Configuring Nortel SNA per VLAN" (page 300)
- "Enabling Nortel SNA on ports" (page 304)
- "Viewing Nortel SNA settings" (page 307)
- "Viewing information about Nortel SNA clients" (page 309)
- "Entering phone signatures for Nortel SNA" (page 310)
- "Enabling Nortel SNA" (page 312)

Configuring QoS for the Nortel SNA solution

For general information about configuring filters and Quality of Service (QoS) in the Nortel SNA solution, see "Filters in the Nortel SNA solution" (page 268). For detailed information about configuring the filters, see *Nortel Ethernet Routing Switch 5500 Series Configuration - Quality of Service* (NN47200-504).

Configuring Nortel SNA per VLAN

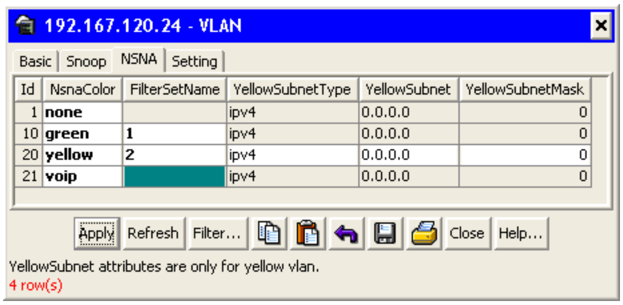
ATTENTION

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

To configure the Nortel SNA VLANs:

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

VLAN -- NSNA tab



192.167.120.24 - VLAN

Id	NsnaColor	FilterSetName	YellowSubnetType	YellowSubnet	YellowSubnetMask
1	**none**		ipv4	0.0.0.0	0
10	**green**	**1**	ipv4	0.0.0.0	0
20	**yellow**	**2**	ipv4	0.0.0.0	0
21	**voip**		ipv4	0.0.0.0	0

YellowSubnet attributes are only for yellow vlan.

4 row(s)

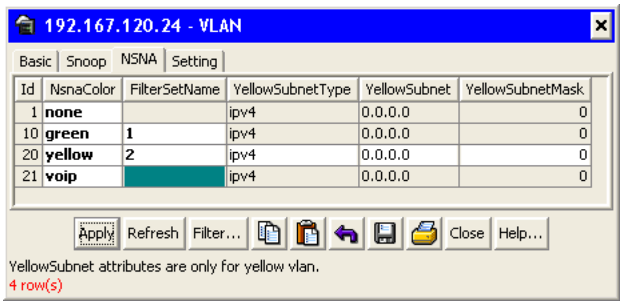
The following table describes the VLAN NSNA tab fields.

VLAN NSNA tab fields

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

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

Example of configured VLAN -- NSNA tab



Id	NsnaColor	FilterSetName	YellowSubnetType	YellowSubnet	YellowSubnetMask
1	**none**		ipv4	0.0.0.0	0
10	**green**	**1**	ipv4	0.0.0.0	0
20	**yellow**	**2**	ipv4	0.0.0.0	0
21	**voip**		ipv4	0.0.0.0	0

YellowSubnet attributes are only for yellow vlan.
4 row(s)

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

6 Click **Apply**.

ATTENTION

ATTENTION
Each switch must have one, and only one, Red VLAN. Each switch can, however, have multiple Yellow, multiple Green, and multiple VoIP VLANs. In Ethernet Routing Switch 5500 Series, Software Release 5.1, each switch supports up to five Yellow, five Green, and five VoIP VLANs. If IP Phones are intended for use in the system, create the VoIP VLAN first and then create the Red, Green, and Yellow VLANs.

—End—

See also:

- "Removing a Nortel SNA VLAN" (page 302)
- "Configuring the Nortel SNAS 4050 subnet" (page 297)
- "Configuring QoS for the Nortel SNA solution" (page 300)
- "Enabling Nortel SNA on ports" (page 304)
- "Viewing Nortel SNA settings" (page 307)
- "Viewing information about Nortel SNA clients" (page 309)
- "Entering phone signatures for Nortel SNA" (page 310)
- "Enabling Nortel SNA" (page 312)

Removing a Nortel SNA VLAN

To remove a Nortel SNA VLAN:

Step **Action**

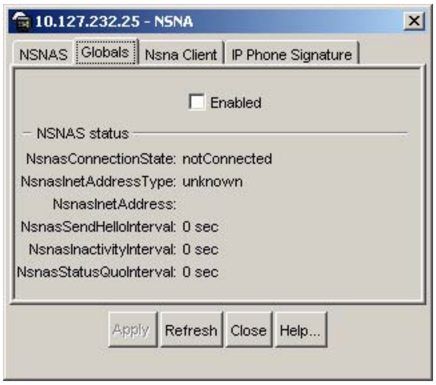
1 Select **Edit > Security > NSNA** from the Device Manager menu.

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

2 Click the **Globals** tab.

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

NSNA -- Globals



□ Enabled

NSNAS status

NsnasConnectionState: notConnected
NsnasInetAddressType: unknown
NsnasInetAddress:
NsnasSendHelloInterval: 0 sec
NsnasInactivityInterval: 0 sec
NsnasStatusQuoInterval: 0 sec

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

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

4 Click **Close**.

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

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

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

b. Click the **NSNA** tab.

The **NSNA** tab is selected.

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

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

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

7 Click **Apply**.

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

a. Click the **Basics** tab.

The **Basics** tab is selected.

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

c. Click **Delete**.

—End—

See also:

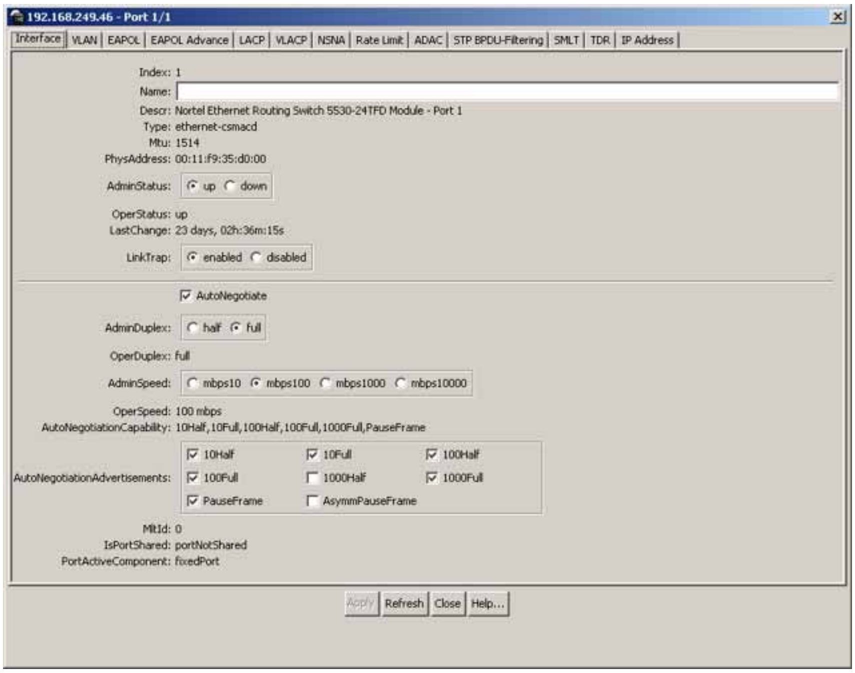
- "Configuring Nortel SNA per VLAN" (page 300)
- "Configuring the Nortel SNAS 4050 subnet" (page 297)
- "Configuring QoS for the Nortel SNA solution" (page 300)
- "Enabling Nortel SNA on ports" (page 304)
- "Viewing Nortel SNA settings" (page 307)
- "Viewing information about Nortel SNA clients" (page 309)
- "Entering phone signatures for Nortel SNA" (page 310)
- "Enabling Nortel SNA" (page 312)

Enabling Nortel SNA on ports

To enable Nortel SNA on ports:

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

Port -- Interface tab



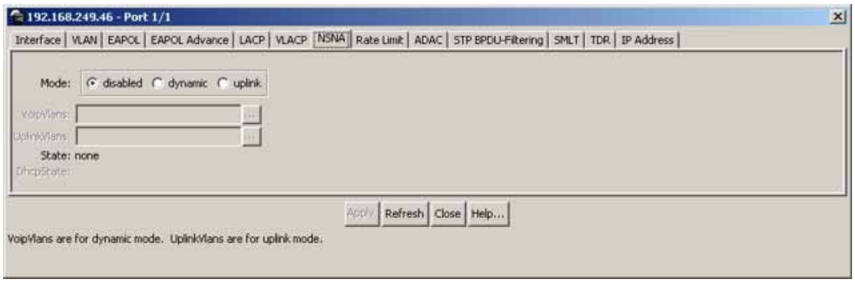
Index: 1
Name:
Descr: Nortel Ethernet Routing Switch 5530-24TFD Module - Port 1
Type: ethernet-csmacd
Mtu: 1514
PhysAddress: 00:11:f9:35:d0:00
AdminStatus: ● up ○ down
OperStatus: up
LastChange: 23 days, 02h:36m:15s
LinkTrap: ● enabled ○ disabled

☑ AutoNegotiate
AdminDuplex: ○ half ● full
OperDuplex: full
AdminSpeed: ○ mbps10 ● mbps100 ○ mbps1000 ○ mbps10000
OperSpeed: 100 mbps
AutoNegotiationCapability: 10Half,10Full,100Half,100Full,1000Full,PauseFrame
AutoNegotiationAdvertisements: ☑ 10Half ☑ 10Full ☑ 100Half ☑ 100Full □ 1000Half ☑ 1000Full ☑ PauseFrame □ AsymmPauseFrame
MltId: 0
IsPortShared: portNotShared
PortActiveComponent: fixedPort

3 Click the **NSNA** tab.

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

Port -- NSNA tab



Mode: ● disabled ○ dynamic ○ uplink
VoipVlans:
UplinkVlans:
State: none
DhcpState:

VoipVlans are for dynamic mode. UplinkVlans are for uplink mode.

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

Port -- NSNA tab fields

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

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

4 Configure the port:

a. Select the port mode.

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

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

5 Click **Apply**.

—End—

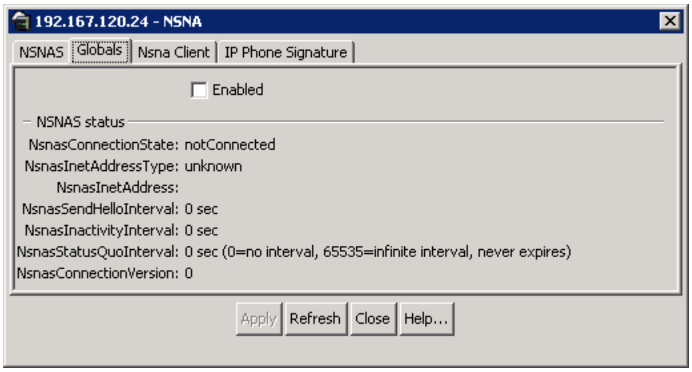
See also:

- "Configuring the Nortel SNAS 4050 subnet" (page 297)
- "Configuring QoS for the Nortel SNA solution" (page 300)

- "Configuring Nortel SNA per VLAN" (page 300)
- "Viewing Nortel SNA settings" (page 307)
- "Viewing information about Nortel SNA clients" (page 309)
- "Entering phone signatures for Nortel SNA" (page 310)
- "Enabling Nortel SNA" (page 312)

Viewing Nortel SNA settings

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



□ Enabled

NSNAS status

NsnasConnectionState: notConnected
NsnasInetAddressType: unknown
NsnasInetAddress:
NsnasSendHelloInterval: 0 sec
NsnasInactivityInterval: 0 sec
NsnasStatusQuoInterval: 0 sec (0=no interval, 65535=infinite interval, never expires)
NsnasConnectionVersion: 0

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

NSNA -- Globals tab fields

Field	Description
Enabled	When checked, enables Nortel SNA on the network access device (for more information, see "Enabling Nortel SNA" (page 312).
NsnasConnectionState	Displays the status of the connection between the network access device and the Nortel SNAS 4050.
NsnasInetAddressType	Displays the type of IP address used by the Nortel SNAS 4050.
NsnasInetAddress	Displays the pVIP of the Nortel SNAS 4050.

Field	Description
NsnasSendHelloInterval	Displays the time interval, in seconds (s), for the hello (healthcheck) messages sent by the Nortel SNAS 4050 to verify connectivity with the network access device. The interval is configured on the Nortel SNAS 4050. The valid configurable range for the interval is 60s (1m) to 64800s (18h). If there is no current connection between the network access device and the Nortel SNAS 4050, the field displays a value of zero.
NsnasInactivityInterval	Displays the switch inactivity interval, in seconds (s), after which the switch enters status-quo mode. The switch inactivity interval is the hello (healthcheck) interval x the number of retries (deadcount) configured on the Nortel SNAS 4050. If there is no current connection between the network access device and the Nortel SNAS 4050, the field displays a value of zero.
NsnasStatusQuoInterval	Displays the status-quo interval time, in seconds(s) for the current or last SSCP connection. The valid configurable range for the status-quo interval is 0 to 65535s (18h approx). • If the solution has been configured so that no status-quo interval is used, the field displays a value of 65535. This means that the network access device does not move Nortel SNA-enabled ports to the Red VLAN even though the connection between the Nortel SNAS 4050 and the network access device may have been interrupted. • If the NSNAS has disconnected and the status-quo interval timer is running, this value will reflect the remaining time, until the status-quo timer expires. ***Note:*** A status-quo interval value of 0 indicates that the network access device will move Nortel SNA-enabled ports to the Red VLAN immediately, when the connection between the Nortel SNAS 4050 and the network access device is interrupted.
NsnasConnectionVersion	The version of the Nsnas Connection.

—End—

See also:

- "Configuring the Nortel SNAS 4050 subnet" (page 297)
- "Configuring QoS for the Nortel SNA solution" (page 300)

- "Configuring Nortel SNA per VLAN" (page 300)
- "Enabling Nortel SNA on ports" (page 304)
- "Viewing information about Nortel SNA clients" (page 309)
- "Entering phone signatures for Nortel SNA" (page 310)
- "Enabling Nortel SNA" (page 312)

Viewing information about Nortel SNA clients

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

Step Action

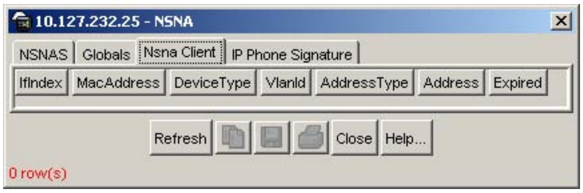
1 Select **Edit > Security > NSNA** from the Device Manager menu.

The **NSNA** dialog box appears with the **NSNAS** tab selected (see "NSNA -- NSNAS tab" (page 298)).

2 Click the **Nsna Client** tab.

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

NSNA -- Nsna client tab



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

NSNA -- Nsna client tab fields

Field	Description
IfIndex	the ifIndex of the port on which the client is attached.
MacAddress	Specifies the MAC address of the client.
Device Type	Specifies the type of client device (pc, ipPhone, or a passive device).
VlanId	The Vlan ID of the client.
FilterVlanId	Specifies the Vlan ID whose associated filter set is installed in the selected port.
AddressType	Specifies the type of IP address used by this client (IPv4 is currently the only option available).

Field	Description
Address	Specifies the IP address of the client.
Expired	Indicates whether this client has been aged-out.

—End—

See also:

- "Configuring the Nortel SNAS 4050 subnet" (page 297)
- "Configuring QoS for the Nortel SNA solution" (page 300)
- "Configuring Nortel SNA per VLAN" (page 300)
- "Enabling Nortel SNA on ports" (page 304)
- "Viewing Nortel SNA settings" (page 307)
- "Entering phone signatures for Nortel SNA" (page 310)
- "Enabling Nortel SNA" (page 312)

Entering phone signatures for Nortel SNA

To specify IP phone signatures for Nortel SNA:

Step Action

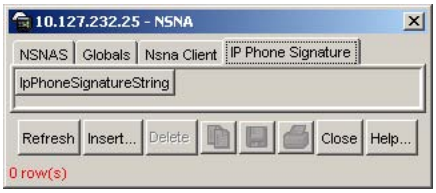
1 Select **Edit > Security > NSNA** from the Device Manager menu.

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

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

The **IP Phone Signature** tab is selected (see the following figure).

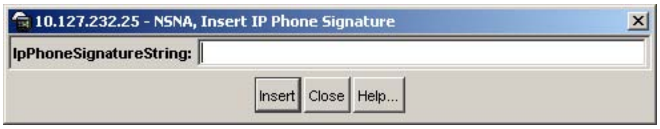
NSNA -- IP Phone Signature tab



3 Click **Insert**.

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

NSNA, Insert IP Phone Signature dialog box



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

5 Click **Insert**.

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

—End—

See also:

- "Removing Nortel SNA phone signatures" (page 311)
- "Configuring the Nortel SNAS 4050 subnet" (page 297)
- "Configuring QoS for the Nortel SNA solution" (page 300)
- "Configuring Nortel SNA per VLAN" (page 300)
- "Enabling Nortel SNA on ports" (page 304)
- "Viewing Nortel SNA settings" (page 307)
- "Viewing information about Nortel SNA clients" (page 309)
- "Enabling Nortel SNA" (page 312)

Removing Nortel SNA phone signatures

To remove a Nortel SNA phone signature:

Step	Action
1	Select **Edit > Security > NSNA** from the Device Manager menu. The **NSNA** dialog box appears with the **NSNAS** tab selected.
2	Click the **IP Phone Signature** tab. The **IP Phone Signature** tab is selected (see "NSNA -- IP Phone Signature tab" (page 310)).
3	Select the row containing the IP phone signature you want to remove.
4	Click **Delete**.

—End—

See also:

- "Entering phone signatures for Nortel SNA" (page 310)
- "Configuring the Nortel SNAS 4050 subnet" (page 297)
- "Configuring QoS for the Nortel SNA solution" (page 300)
- "Configuring Nortel SNA per VLAN" (page 300)
- "Enabling Nortel SNA on ports" (page 304)
- "Viewing Nortel SNA settings" (page 307)
- "Viewing information about Nortel SNA clients" (page 309)
- "Enabling Nortel SNA" (page 312)

Configuring Nortel SNA static clients

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

Enabling Nortel SNA

ATTENTION

You must enable SSH before you enable Nortel SNA globally. The command to enable Nortel SNA fails if SSH is not enabled. Refer to "Configuring SSH on the 5500 Series switch for Nortel SNA" (page 278) for detailed information.

To globally enable Nortel SNA:

Step	Action
1	Select **Edit > Security > NSNA** from the Device Manager menu. The **NSNA** dialog box appears with the **NSNAS** tab selected.
2	Click the **Globals** tab. The **Globals** tab is selected (see "NSNA -- Globals" (page 303)).
3	Select the **Enabled** check box.
4	Click **Apply**.

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

—End—

See also:

- "Configuring the Nortel SNAS 4050 subnet" (page 297)
- "Configuring QoS for the Nortel SNA solution" (page 300)
- "Configuring Nortel SNA per VLAN" (page 300)
- "Enabling Nortel SNA on ports" (page 304)
- "Viewing Nortel SNA settings" (page 307)
- "Viewing information about Nortel SNA clients" (page 309)
- "Entering phone signatures for Nortel SNA" (page 310)

Appendixes

This section contains information about the following topics:

- "TACACS+ server configuration examples" (page 315)
- "Supported SNMP MIBs and traps" (page 329)
- "Default Nortel SNA filters" (page 334)

TACACS+ server configuration examples

Refer to the following sections for basic configuration examples of the TACACS+ server:

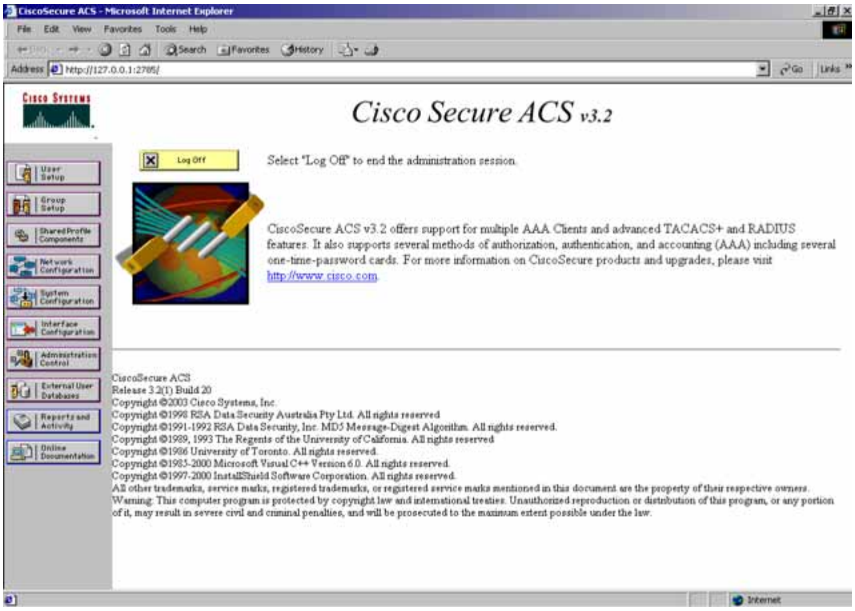
- "Configuration example: Cisco ACS (version 3.2) server" (page 315)
- "Configuration example: ClearBox server" (page 320)
- "Configuration example: Linux freeware server" (page 327)

Refer to vendor documentation for your server for specific configuration procedures.

Configuration example: Cisco ACS (version 3.2) server

The following figure shows the main administration window.

Cisco ACS (version 3.2) main administration window



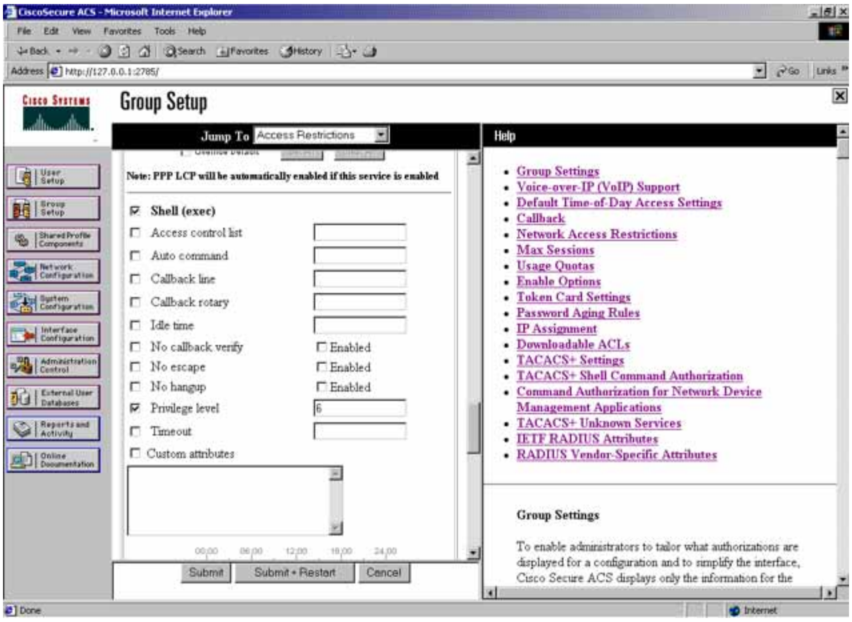
Select "Log Off" to end the administration session.

CiscoSecure ACS v3.2 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com

CiscoSecure ACS
Release 3.2(1) Build 20
Copyright ©2003 Cisco Systems, Inc.
Copyright ©1998 RSA Data Security Australia Pty Ltd. All rights reserved
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners.
Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Step	Action
1	Define the users and the corresponding authorization levels. If you map users to default group settings, it is easier to remember which user belongs to each group. For example, the rwa user belongs to group 15 to match Privilege level 15. All rwa user settings are picked up from group 15 by default. The following figure shows a sample Group Setup window.

Group Setup window - Cisco ACS server configuration



Group Setup

Jump To: Access Restrictions

Note: PPP LCP will be automatically enabled if this service is enabled

- ☑ Shell (exec)
- □ Access control list
- □ Auto command
- □ Callback line
- □ Callback rotary
- □ Idle time
- □ No callback verify □ Enabled
- □ No escape □ Enabled
- □ No hangup □ Enabled
- ☑ Privilege level: 6
- □ Timeout
- □ Custom attributes

Help

- Group Settings
- Voice-over-IP (VoIP) Support
- Default Time-of-Day Access Settings
- Callback
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Enable Options
- Token Card Settings
- Password Aging Rules
- IP Assignment
- Downloadable ACLs
- TACACS+ Settings
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

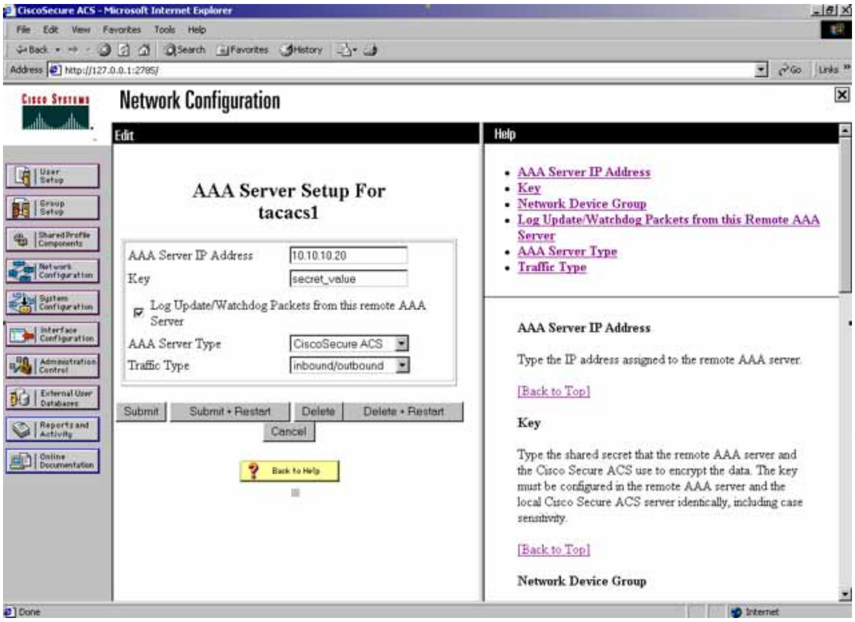
Group Settings

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, Cisco Secure ACS displays only the information for the

2 Configure the server settings.

The following figure shows a sample Network Configuration window to configure the authentication, authorization, and accounting (AAA) server for TACACS+.

Network Configuration window - server setup



Network Configuration

AAA Server Setup For tacacs1

- AAA Server IP Address: 10.10.10.20
- Key: secret_value
- ☑ Log Update/Watchdog Packets from this remote AAA Server
- AAA Server Type: CiscoSecure ACS
- Traffic Type: inbound/outbound

Help

- AAA Server IP Address
- Key
- Network Device Group
- Log Update/Watchdog Packets from this Remote AAA Server
- AAA Server Type
- Traffic Type

AAA Server IP Address

Type the IP address assigned to the remote AAA server.

[Back to Top]

Key

Type the shared secret that the remote AAA server and the Cisco Secure ACS use to encrypt the data. The key must be configured in the remote AAA server and the local Cisco Secure ACS server identically, including case sensitivity.

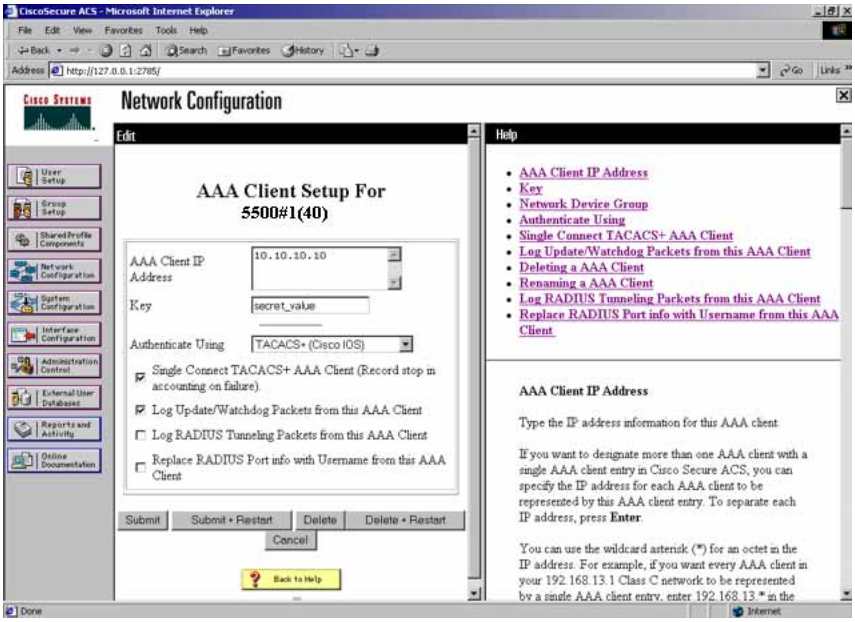
[Back to Top]

Network Device Group

3 Define the client.

The following figure shows a sample Network Configuration window to configure the client. Authenticate using TACACS+. Single-connection can be used, but this must match the configuration on the Nortel Ethernet Routing Switch 5500 Series.

Network Configuration window - client setup



Network Configuration

AAA Client Setup For 5500#1(40)

AAA Client IP Address: 10.10.10.10

Key: secret_value

Authenticate Using: TACACS+ (Cisco IOS)

☑ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

☑ Log Update/Watchdog Packets from this AAA Client

☐ Log RADIUS Tunneling Packets from this AAA Client

☐ Replace RADIUS Port info with Username from this AAA Client

Submit | Submit + Restart | Delete | Delete + Restart | Cancel

Back to Help

- AAA Client IP Address
- Key
- Network Device Group
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update/Watchdog Packets from this AAA Client
- Deleting a AAA Client
- Renaming a AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

AAA Client IP Address

Type the IP address information for this AAA client.

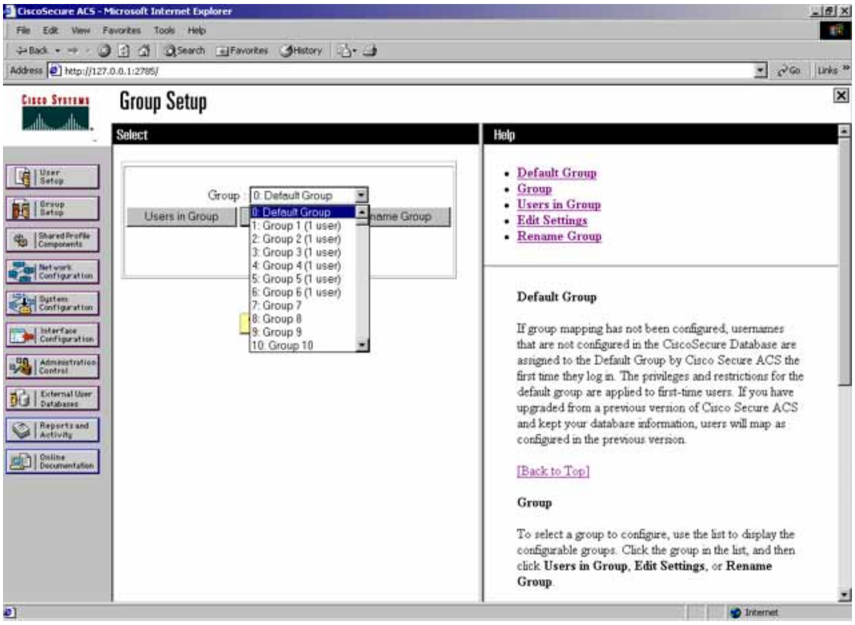
If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the

4 Verify the groups you have configured.

In this example, the user is associated with a user group (see the following figure). The rwa account belongs to group 15, and its privilege level corresponds to the settings for group 15. The ro accounts belong to group 0, L1 accounts belong to group 2, and so on.

Group Setup window - viewing the group setup



- Default Group
- Group
- Users in Group
- Edit Settings
- Rename Group

Default Group

If group mapping has not been configured, usernames that are not configured in the CiscoSecure Database are assigned to the Default Group by Cisco Secure ACS the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, users will map as configured in the previous version.

[Back to Top]

Group

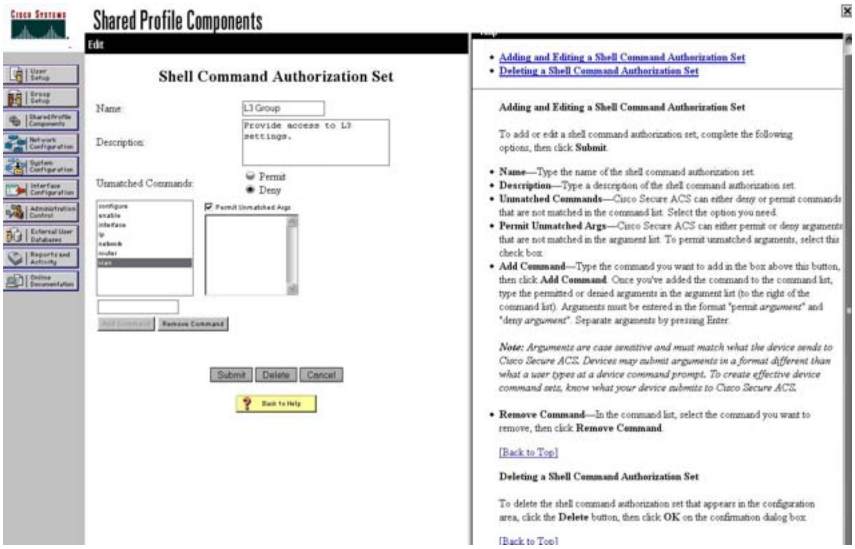
To select a group to configure, use the list to display the configurable groups. Click the group in the list, and then click **Users in Group**, **Edit Settings**, or **Rename Group**.

5 Specify the commands that are allowed or denied for the various groups.

a. Go to **Shared Profile Components > Shell Command Authorization Set**. The Shell Command Authorization Set screen appears (see the following figure).

b. Select the commands to be added to the command set, and specify whether the action is permit or deny.

Shared Profile Components window - defining the command set



Shell Command Authorization Set

Name: L3 Group

Description: Provide access to L3 settings.

Unmatched Commands: ○ Permit ● Deny

☑ Permit Unmatched Args

- Adding and Editing a Shell Command Authorization Set
- Deleting a Shell Command Authorization Set

Adding and Editing a Shell Command Authorization Set

To add or edit a shell command authorization set, complete the following options, then click **Submit**.

- **Name**—Type the name of the shell command authorization set.
- **Description**—Type a description of the shell command authorization set.
- **Unmatched Commands**—Cisco Secure ACS can either deny or permit commands that are not matched in the command list. Select the option you need.
- **Permit Unmatched Args**—Cisco Secure ACS can either permit or deny arguments that are not matched in the argument list. To permit unmatched arguments, select this check box.
- **Add Command**—Type the command you want to add in the box above this button, then click **Add Command**. Once you've added the command to the command list, type the permitted or denied arguments in the argument list (to the right of the command list). Arguments must be entered in the format "permit *argument*" and "deny *argument*". Separate arguments by pressing Enter.

Note: Arguments are case sensitive and must match what the device sends to Cisco Secure ACS. Devices may submit arguments in a format different than what a user types at a device command prompt. To create effective device command sets, know what your device submits to Cisco Secure ACS.

- **Remove Command**—In the command list, select the command you want to remove, then click **Remove Command**.

[Back to Top]

Deleting a Shell Command Authorization Set

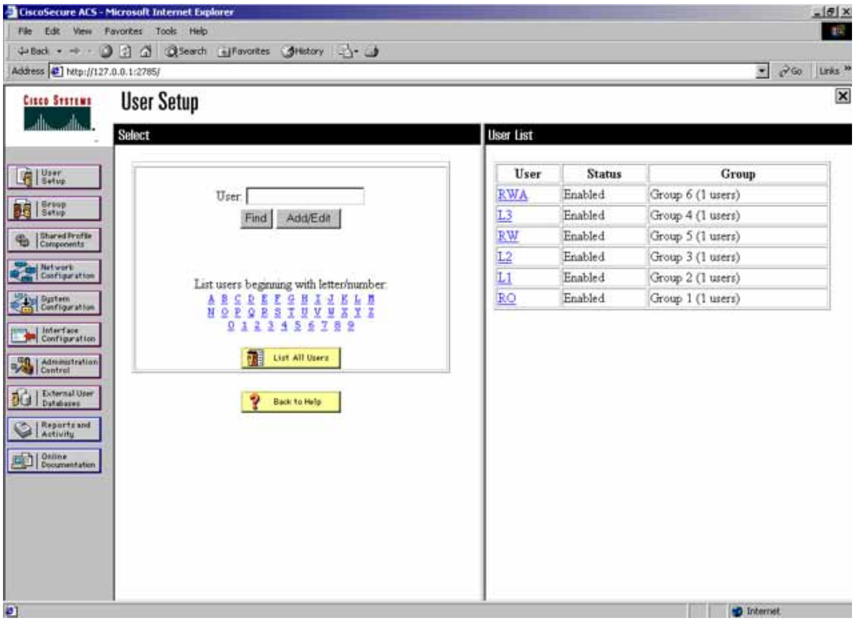
To delete the shell command authorization set that appears in the configuration area, click the **Delete** button, then click **OK** on the confirmation dialog box.

[Back to Top]

6 View users, their status, and the corresponding group to which each belongs.

The following figure shows a sample User Setup window. You can use this window to find, add, edit, and view users settings.

User Setup window - Cisco ACS server configuration



User	Status	Group
RWA	Enabled	Group 6 (1 users)
L3	Enabled	Group 4 (1 users)
RW	Enabled	Group 5 (1 users)
L2	Enabled	Group 3 (1 users)
L1	Enabled	Group 2 (1 users)
RO	Enabled	Group 1 (1 users)

—End—

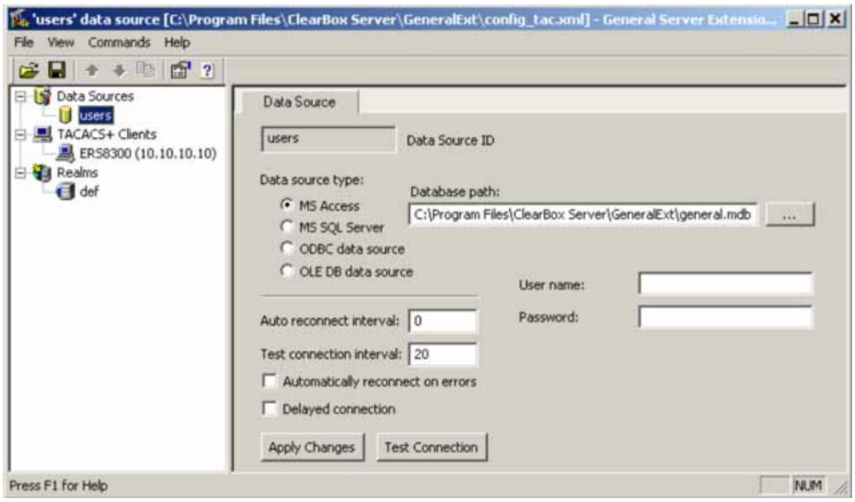
Configuration example: ClearBox server

Step	Action

1 Run the General Extension Configurator and configure the user data source (see the following figure).

In this example, Microsoft Access was used to create a database of user names and authorization levels; the general.mdb file needs to include these users.

General Extension Configurator



'users' data source [C:\Program Files\ClearBox Server\GeneralExt\config_tac.xml] - General Server Extensio...

Data Sources
- users

TACACS+ Clients
- ERS8300 (10.10.10.10)

Realms
- def

Data Source ID: users

Data source type:
- ● MS Access
- ○ MS SQL Server
- ○ ODBC data source
- ○ OLE DB data source

Database path: C:\Program Files\ClearBox Server\GeneralExt\general.mdb

User name:

Password:

Auto reconnect interval: 0

Test connection interval: 20

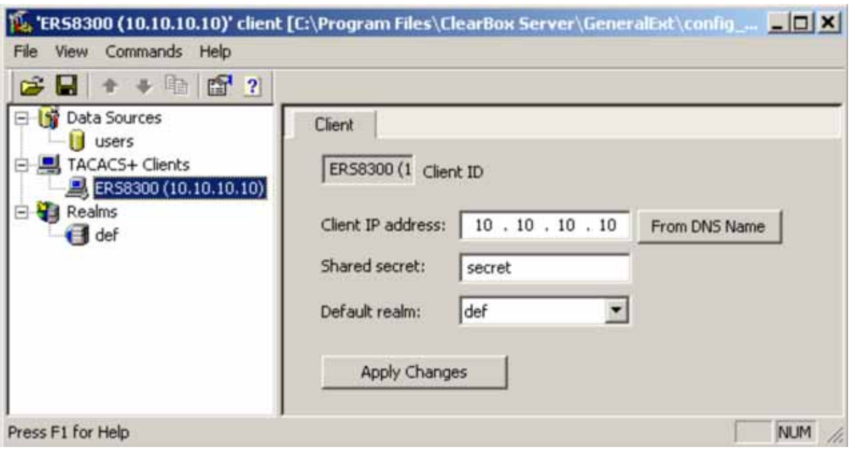
□ Automatically reconnect on errors

□ Delayed connection

2 Create a Client entry for the switch management IP address by right-clicking the **TACACS+ Clients** item.

In this case, the TACACS+ Client is the Nortel Ethernet Routing Switch 5500 Series. Enter the appropriate information. The shared secret must match the value configured on the Nortel Ethernet Routing Switch 5500 Series.

Creating a client entry



'ERS8300 (10.10.10.10)' client [C:\Program Files\ClearBox Server\GeneralExt\config_...

Data Sources
- users

TACACS+ Clients
- ERS8300 (10.10.10.10)

Realms
- def

Client ID: ERS8300 (1

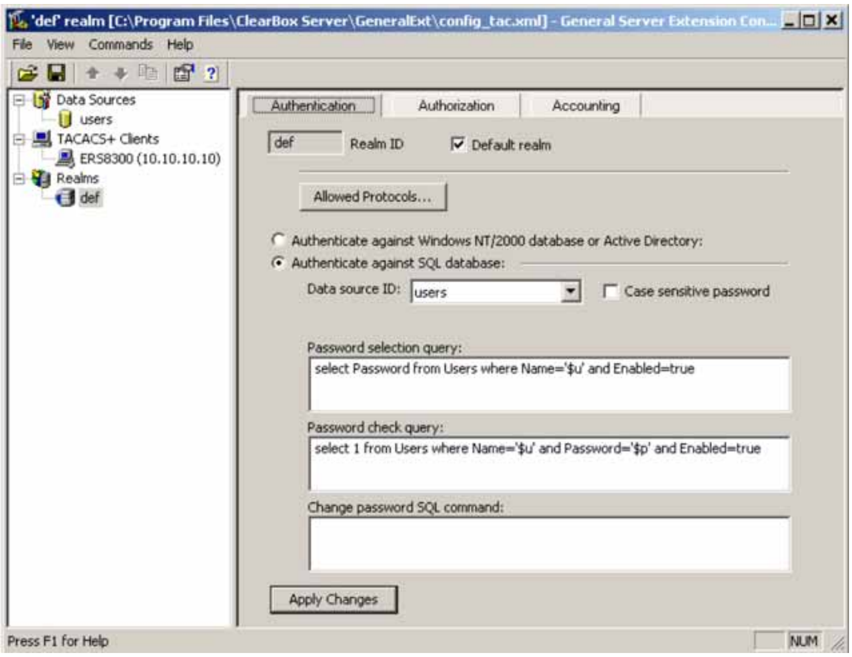
Client IP address: 10 . 10 . 10 . 10

Shared secret: secret

Default realm: def

The default realm Authentication tab looks like the following figure.

Default realm - Authentication tab



Realm ID: def

☑ Default realm

○ Authenticate against Windows NT/2000 database or Active Directory:

● Authenticate against SQL database:

Data source ID: users

☐ Case sensitive password

Password selection query:

select Password from Users where Name='$u' and Enabled=true

Password check query:

select 1 from Users where Name='$u' and Password='$p' and Enabled=true

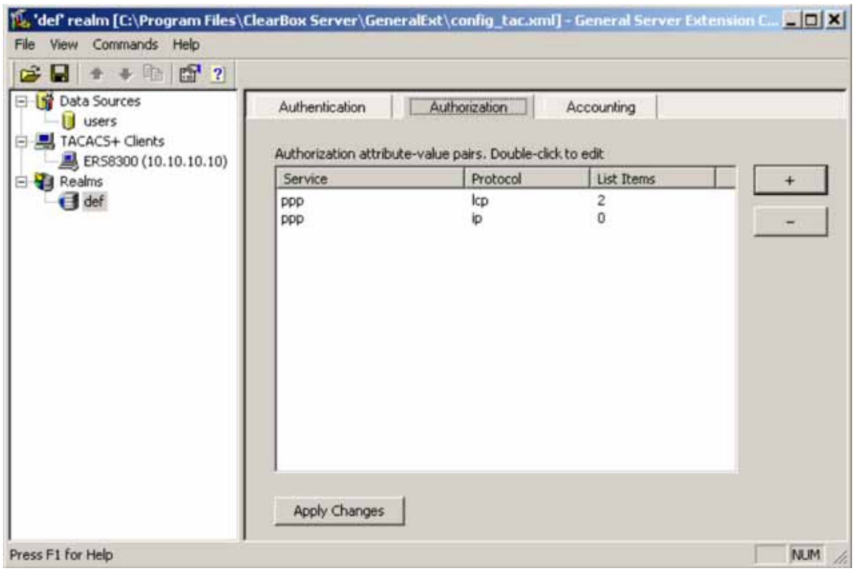
Change password SQL command:

3 Select **Realms > def > Authorization** tab.

A new service is required that allows the server to assign certain levels of access.

4 Click the **+** button to add an attribute-value pair for privilege levels (see the following figure).

Default realm - Authorization tab



Authorization attribute-value pairs. Double-click to edit

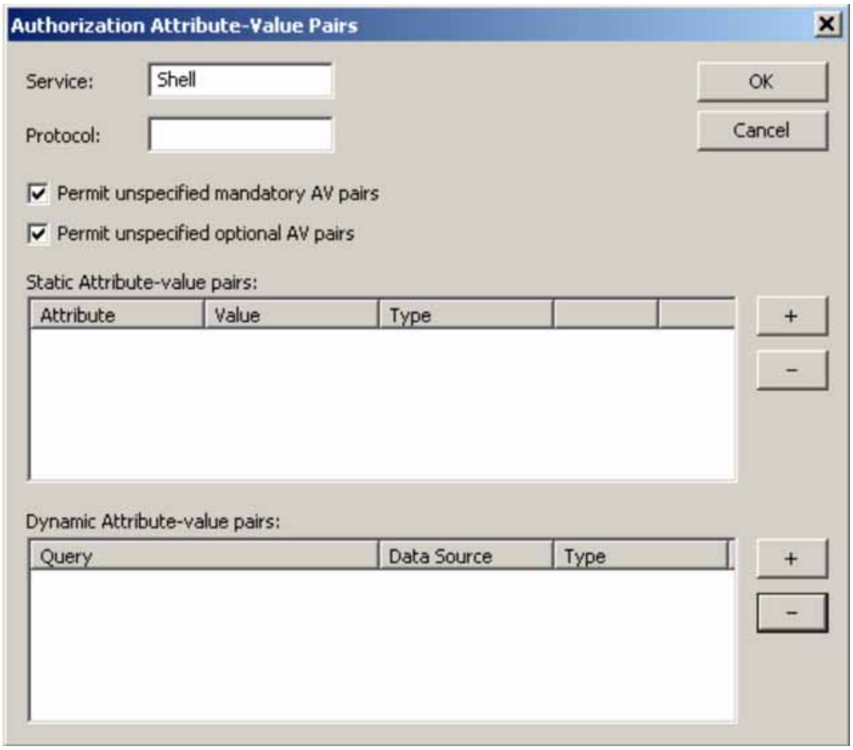
Service	Protocol	List Items
ppp	lcp	2
ppp	ip	0

5 Specify the query parameters.

a. Enter information in the window as shown in the following figure.

b. Click the **+** button to add the parameters to the query.

Adding parameters for the query



Authorization Attribute-Value Pairs

Service: Shell

Protocol:

☑ Permit unspecified mandatory AV pairs

☑ Permit unspecified optional AV pairs

Static Attribute-value pairs:

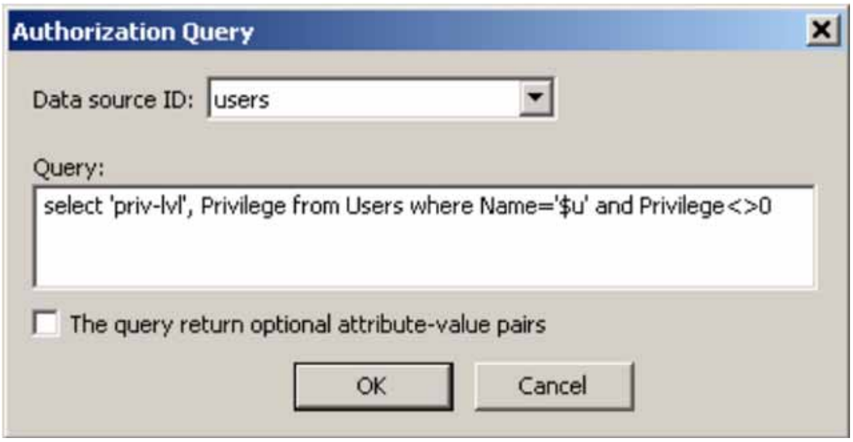
Attribute	Value	Type		

Dynamic Attribute-value pairs:

Query	Data Source	Type

6 Use the string shown in the following figure for the authorization query.

Authorization Query window



Authorization Query

Data source ID: users

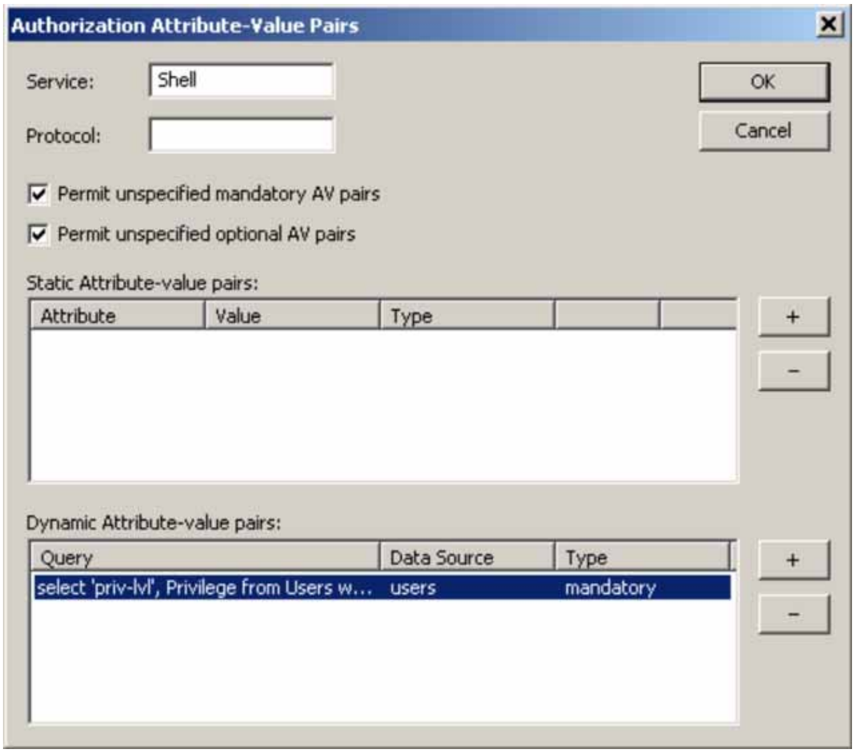
Query:

```
select 'priv-lvl', Privilege from Users where Name='$u' and Privilege<>0
```

□ The query return optional attribute-value pairs

The final window looks like the following figure.

Query parameters added to Authorization Attribute-Value Pairs window



Authorization Attribute-Value Pairs

Service: Shell

Protocol:

☑ Permit unspecified mandatory AV pairs

☑ Permit unspecified optional AV pairs

Static Attribute-value pairs:

Attribute	Value	Type		

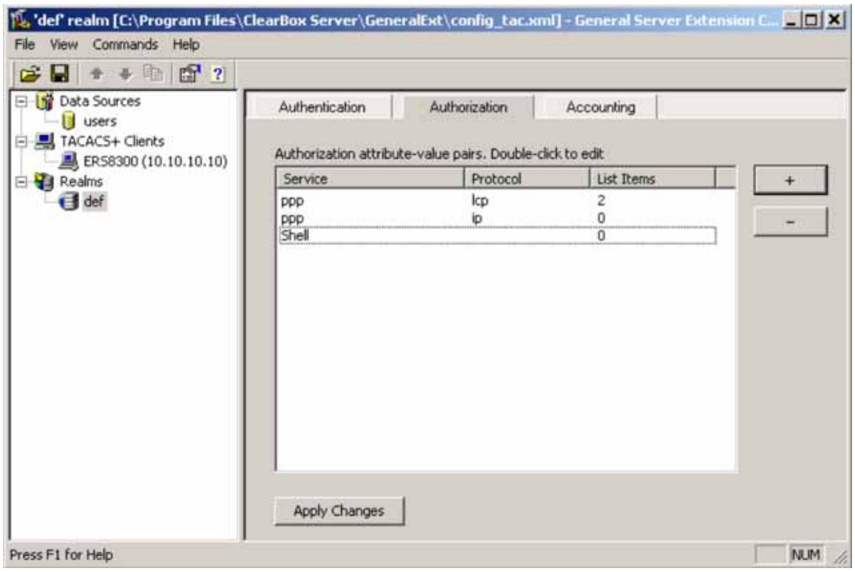
Dynamic Attribute-value pairs:

Query	Data Source	Type
select 'priv-lvl', Privilege from Users w...	users	mandatory

7 Click **OK**.

The information appears on the **Authorization** tab (see the following figure).

Authorization attribute-value pairs added to Authorization tab



'def' realm [C:\Program Files\ClearBox Server\GeneralExt\config_tac.xml] - General Server Extension C...

Authorization attribute-value pairs. Double-click to edit

Service	Protocol	List Items
ppp	lcp	2
ppp	ip	0
Shell		0

Press F1 for Help

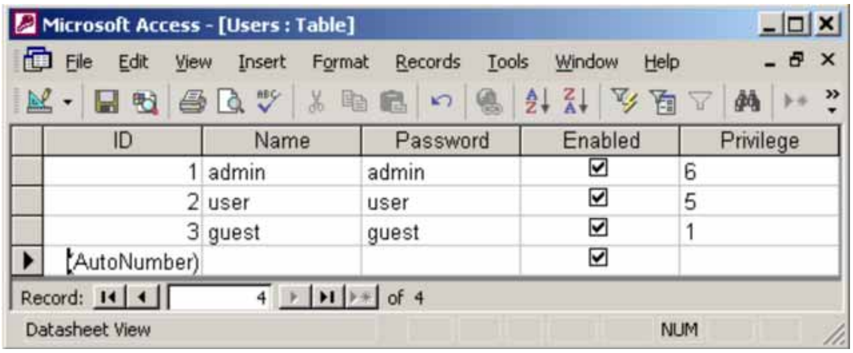
8 Navigate to the general.mdb file as specified earlier.

The user table should look like the one shown in the following figure. If the `Privilege` column does not exist, create one and populate it according to the desired access level.

Note that Microsoft Access or third-party software is required to read this file.

> ***Note:*** If you use the 30-day demo for ClearBox, the user names cannot be more than four characters in length.

Users table - Microsoft Access



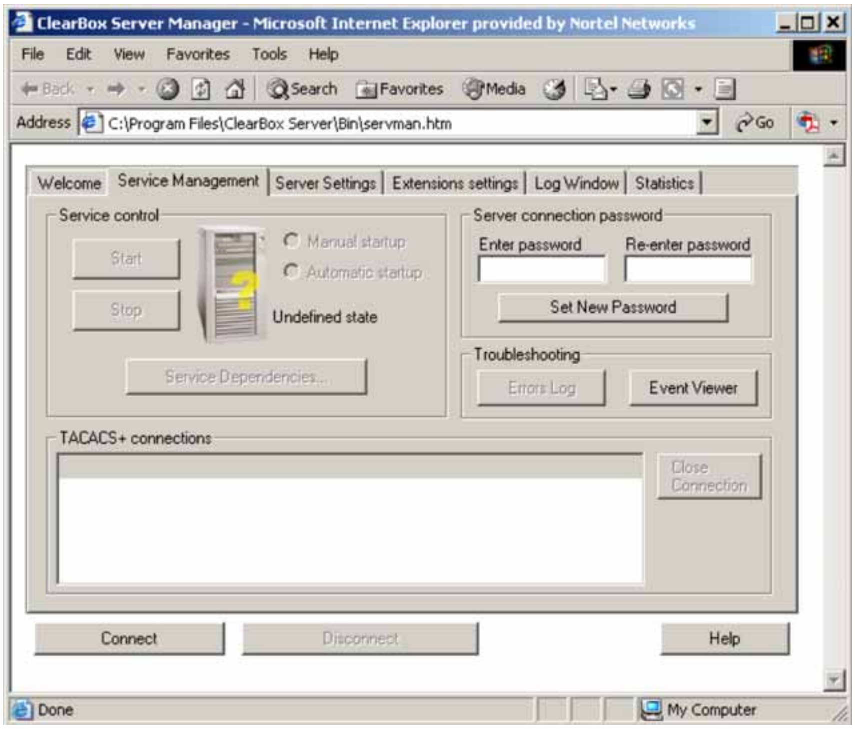
ID	Name	Password	Enabled	Privilege
1	admin	admin	☑	6
2	user	user	☑	5
3	guest	guest	☑	1
(AutoNumber)			☑	

Record: 4 of 4

9 Start the server.

a. Run the Server Manager (see the following figure).

ClearBox Server Manager



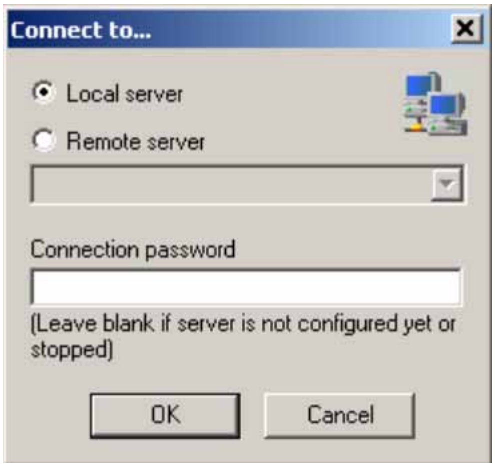
Address: C:\Program Files\ClearBox Server\Bin\servman.htm

Undefined state

b. Click the **Connect** button.

The **Connect to...** dialog box appears (see the following figure).

Connect to... dialog box



● Local server

○ Remote server

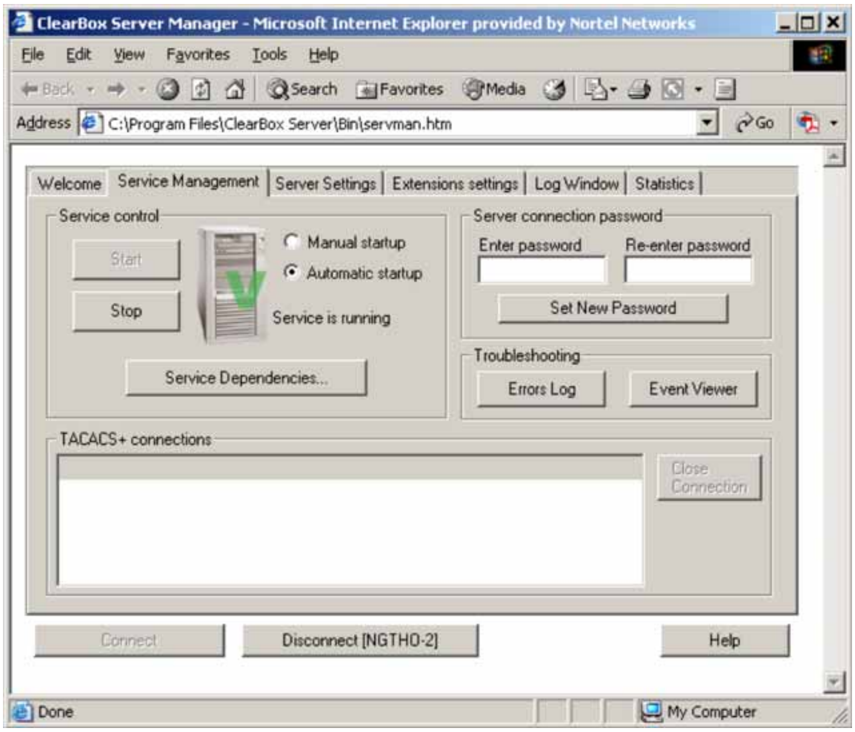
c. Click **OK** (do not fill in any fields).

d. Click **OK** at the warning message.

e. Click **Start**.

The Server Manager should now look like the following figure. Any changes to the General Server Extension Configurator require that the server be restarted.

TACACS+ server connected



ClearBox Server Manager - Microsoft Internet Explorer provided by Nortel Networks

Address: C:\Program Files\ClearBox Server\Bin\servman.htm

Service control: ○ Manual startup ● Automatic startup

Service is running

—End—

Configuration example: Linux freeware server

Step	Action

1 After TACACS+ is installed on the Linux server, change the directory to:

```
$cd /etc/tacacs
```

2 Open the configuration file tac_plus.cfg:

```
$vi tac_plus.cfg
```

3 Comment out all the existing lines in the config file. Add new lines similar to the following:

```
# Enter your NAS key and user name
key = <secret key>
user = <user name> {
        default service = permit
           service = exec {
                 priv-lvl = <Privilege level 1 to 15>
}
       login = <Password type> <password>
}
# Set the location to store the accounting records
```

where

`<secret key>` is the key that is to be configured on the switch when creating the TACACS+ server entry
`<user name>` is the user name used to log on to the switch
`<Privilege level>` specifies the privilege level (for example rwa = 6; rw = 5; ro = 1)
`<Password type>` specifies the type of password -- for example, the password can be clear text or from the Linux password file, and so on
`<Password>` if the password type is clear text, the password itself

The following is a sample config file.

```
$vi tac_plus.cfg

# Created by Joe SMITH(jsmit@isp.net)
# Read user_guide and tacacs+ FAQ for
more information
#
# Enter your NAS key
key = secretkey
user = smithJ {
default service = permit
service = exec {
priv-lvl = 15
}
login = cleartext M5xyH8
```

4 Save the changes to the tac_plus.cfg file

5 Run the TACACS+ daemon using the following command:

```
$/usr/local/sbin/tac_plus -C /etc/tacacs/tac_plus.cfg &
```

where

- tac_plus is stored under /usr/local/sbin
- the config file you just edited is stored at /etc/tacacs/

The TACACS+ server on Linux is ready to authenticate users.

—End—

Supported SNMP MIBs and traps

This section includes information about:

- "Supported MIBs" (page 329)
- "New MIBs" (page 331)
- "Supported traps" (page 331)

Supported MIBs

The following tables list supported SNMP MIBs.

SNMP Standard MIB support

MIB name	RFC	File name
RMON-MIB	2819	rfc2819.mib
RFC1213-MIB	1213	rfc1213.mib
IF-MIB	2863	rfc2863.mib
SNMPv2-MIB	3418	rfc3418.mib
EtherLike-MIB	2665	rfc2665.mib
ENTITY-MIB	2737	rfc2737.mib
BRIDGE-MIB	4188	rfc4188.mib
P-BRIDGE-MIB	4363	rfc4363-p.mib
Q-BRIDGE-MIB	4363	rfc4363-q.mib
IEEE8021-PAE-MIB	n/a	eapol-d10.mib
SMIv2-MIB	2578	rfc2578.mib
SMIv2-TC-MIB	2579	rfc2579.mib
SNMPv2-MIB	3418	rfc3418.mib
SNMP-FRAMEWORK-MIB	3411	rfc3411.mib
SNMP-MPD-MIB	3412	rfc3412.mib
SNMP-NOTIFICATION-MIB	3413	rfc3413-notif.mib
SNMP-TARGET-MIB	3413	rfc3413-tgt.mib
SNMP-USER-BASED-MIB	3414	rfc3414.mib
SNMP-VIEW-BASED-ACM-MIB	3415	rfc3415.mib
SNMP-COMMUNITY-MIB	3584	rfc3584.mib

SNMP proprietary MIB support

MIB name	File name
S5-AGENT-MIB	s5age.mib

MIB name	File name
S5-CHASSIS.MIB	s5cha.mib
S5-CHASSIS-TRAP.MIB	s5ctr.trp
S5-ETHERNET-TRAP.MIB	s5etr.trp
RAPID-CITY-MIB	rapidCity.mib
S5-SWITCH-BAYSECURE-MIB	s5sbs.mib
BN-IF-EXTENSIONS-MIB	s5ifx.mib
BN-LOG-MESSAGE-MIB	bnlog.mib
S5-ETH-MULTISEG-TOPOLOGY-MIB	s5emt.mib
NTN-QOS-POLICY-EVOL-PIB	pibNtnEvol.mib
BAY-STACK-NOTIFICATIONS-MIB	bsn.mib

Application and related MIBs

Application	Related MIBs	File name
Auto-detection and auto-configuration of IP Phones (ADAC)	BAY-STACK-ADAC-MIB	bayStackAdac.mib
Autotopology	S5-ETH-MULTISEG-TOPOLOGY-MIB	s5emt.mib
BaySecure	S5-SWITCH-BAYSECURE-MIB	s5sbs.mib
Extensible Authentication Protocol over LAN (EAPOL)	IEEE8021-PAE-MIB	eapol-d10.mib
IP multicast (IGMP snooping/proxy)	RAPID-CITY-MIB (rcVlanIgmp group)	rcVlan.mib
Link Aggregation Control Protocol (LACP)	IEEE8023-LAG-MIB; BAY-STACK-LACP-EXT-MIB	ieee8023-lag.mib; bayStackLacpExt.mib
Link Layer Discovery Protocol (LLDP)	LLDP-MIB; LLDP-EXT-DOT1-MIB; LLDP-EXT-DOT3-MIB; LLDP-EXT-MED-MIB	lldp.mib; lldpExtDot1.mib; lldpExtDot3.mib; lldpExtMed.mib
MIB-2	RFC1213-MIB	rfc1213.mib
MultiLink Trunking (MLT)	RAPID-CITY-MIB (rcMlt group)	rcMlt.mib
Nortel Secure Network Access (Nortel SNA)	NORTEL-SECURE-NETWORK-ACCESS-MIB	nortelSecureNetworkAccess.mib
Open Shortest Path First (OSPF)	OSPF-MIB; RAPID-CITY-MIB (ospf group); BAY-STACK-OSPF-EXT-MIB	rfc1850.mib; rapidCity.mib; bayStackOspfExt.mib
Policy management	NTN-QOS-POLICY-EVOL-PIB	pibNtnEvol.mib
RMON-MIB	RMON-MIB	rfc2819.mib

Application	Related MIBs	File name
Routing Information Protocol (RIP)	RIPv2-MIB	rfc1724.mib
SNMPv3	SNMP-FRAMEWORK-MIB	rfc3411.mib
	SNMP-MPD-MIB	rfc3412.mib
	SNMP-NOTIFICATION-MIB	rfc3413-notif.mib
	SNMP-TARGET-MIB	rfc3413-tgt.mib
	SNMP-USER-BASED-SM-MIB	rfc3414.mib
	SNMP-VIEW-BASED-ACM-MIB	rfc3415.mib
	SNMP-COMMUNITY-MIB	rfc3584.mib
Spanning Tree	BRIDGE-MIB	rfc4188.mib
for MSTP	NORTEL-NETWORKS-MULTIPLE-SPANNING-TREE-MIB	nnmst.mib
for RSTP	NORTEL-NETWORKS-RAPID-SPANNING-TREE-MIB	nnrst.mib
System log	BN-LOG-MESSAGE-MIB	bnlog.mib
VLAN	RAPID-CITY-MIB (rcVlan group)	rcVlan.mib
Virtual Router Redundancy Protocol (VRRP)	VRRP-MIB; BAY-STACK-VRRP-EXT-MIB	rfc2787.mib; bayStackVrrpExt.mib

New MIBs

The following table lists the new MIBs:

New MIBs

MIB name	RFC	File name
BAY-STACK-ERROR-MESSAGE-MIB	1271	Rfc1271.mib
BAY-STACK-DHCP-SNOOPING-MIB		
BAY-STACK-ARP-INSPECTION-MIB		

Supported traps

The following table lists supported SNMP traps.

Supported SNMP traps

Trap name	Configurable	Sent when
RFC 2863 (industry standard):		
linkUp	Per port	A port’s link state changes to up.

Trap name	Configurable	Sent when
linkDown	Per port	A port’s link state changes to down.
RFC 3418 (industry standard):		
authenticationFailure	System wide	There is an SNMP authentication failure.
coldStart	Always on	The system is powered on.
warmStart	Always on	The system restarts due to a management reset.
s5CtrMIB (Nortel proprietary traps):		
s5CtrUnitUp	Always on	A unit is added to an operational stack.
s5CtrUnitDown	Always on	A unit is removed from an operational stack.
s5CtrHotSwap	Always on	A unit is hot-swapped in an operational stack.
s5CtrProblem	Always on	• Base unit fails • AC power fails or is restored • RPSU (DC) power fails or is restored • Fan fails or is restored
s5EtrSbsMacAccessViolation	Always on	A MAC address security violation is detected.
entConfigChange	Always on	Any hardware change--unit added or removed from stack, GBIC inserted or removed.
risingAlarm fallingAlarm	Always on	An RMON alarm threshold is crossed.
bsnConfigurationSavedToNvram	Always on	Each time the system configuration is saved to NVRAM.
bsnEapAccessViolation	Always on	An EAP access violation occurs.
bsnStackManagerReconfiguration	System-wide	There has been a stack configuration.
BAY-STACK-ADAC-MIB:		
bsAdacPortConfiguration	Per port	Auto-configuration status changes on the port.
LLDP-MIB; LLDP-EXT-MED-MIB:		
lldpRemTablesChange	System-wide	The value of lldpStatsRemTableLast ChangeTime changes.

Trap name	Configurable	Sent when
lldpXMedTopologyChangeDetected	System-wide	The local device senses a topology change indicating either that a new remote device has been attached a local port or that a remote device disconnected or moved from one port to another.
NORTEL-SECURE-NETWORK-ACCESS-MIB:		
nsnaClosedConnectionToSnas	System-wide	The device closes the connection to the Nortel Secure Network Access Switch 4050 (Nortel SNAS 4050). The reason the connection was closed is provided.
nsnaStatusQuoIntervalExpired	System-wide	The status-quo interval expires after the connection to the Nortel SNAS 4050 has closed.
nsnaInvalidMessageFromSnas	System-wide	The device receives an invalid (usually corrupted) message from the Nortel SNAS 4050. The error notification provides as much of the invalid message header as is available.
NORTEL-NETWORKS-RAPID-SPANNING-TREE-MIB:		
nnRstGeneralEvent	Always on	Any general event, such as protocol up or protocol down, occurs.
nnRstErrorEvent	System-wide	Any error event occurs. Error events include memory failure, buffer failure, protocol migration, new root, and topology change.
nnRstNewRoot	System-wide	A new root bridge is selected in the topology.
nnRstTopologyChange	System-wide	A topology change is detected.
nnRstProtocolMigration	Per port	Port protocol migration occurs.
NORTEL-NETWORKS-MULTIPLE-SPANNING-TREE-MIB:		
nnMstGeneralEvent	Always on	Any general event, such as protocol up or protocol down, occurs.
nnMstErrorEvent	System-wide	Any error event occurs. Error events include memory failure, buffer failure, protocol migration, new root, and topology change.
nnMstNewRoot	System-wide	A new root bridge is selected in the topology.
nnMstTopologyChange	System-wide	A topology change is detected.

Trap name	Configurable	Sent when
nnMstProtocolMigration	Per port	Port protocol migration occurs.
nnMstRegionConfigChange	System-wide	The MST region configuration identifier changes.
VRRP-MIB; BAY-STACK-VRRP-EXT-MIB:		
vrrpTrapNewMaster	System-wide	The sending agent has transitioned to Master state.
vrrpTrapAuthFailure	System-wide	A packet has been received from a router whose authentication key or authentication type conflicts with this router’s authentication key or authentication type. Implementation of this trap is optional.
bsveVrrpTrapStateTransition	Per port	A state transition has occurred on a particular VRRP interface. Implementation of this trap is optional.

Default Nortel SNA filters

This section includes the following topics:

- "Default filter configuration" (page 334)
- "Default filter parameters" (page 336)

Default filter configuration

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

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

Configuration example: Configuring the default Nortel SNA filters

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

Green filter

The Green filter allows all traffic:

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

qos nsna set name GREENFILTER
```

Red filter

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

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

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

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

ARP traffic

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

UDP traffic and ICMP traffic for the VoIP VLAN

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

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

ICMP traffic

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

Enable Red filter set

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

Yellow filter

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

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

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

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

ARP traffic

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

Yellow subnet traffic

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

UDP traffic and ICMP traffic for the VoIP VLAN

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

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

ICMP traffic

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

Enable Yellow filter set

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

Default filter parameters

The following table lists the default Nortel SNA filter set parameters. The filter set name varies depending on the configuration.

Default Nortel SNA filter sets

Red filter set	Yellow filter set	Green filter set
Id: 1 Unit/Port: 0 (TEMPLATE) Name: Red Block: NsnaDefRedBlk1 Eval Order: 5 Address Type: IPv4 Destination Addr/Mask: 10.40.40.0/24 Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: TCP Destination L4 Port Min: 80	Id: 2 Unit/Port: 0 (TEMPLATE) Name: Yellow Block: NsnaDefYelBlk1 Eval Order: 5 Address Type: IPv4 Destination Addr/Mask: 10.40.40.0/24 Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: TCP Destination L4 Port Min: 80	Id: 3 Unit/Port: 0 (TEMPLATE) Name: Green Block: Eval Order: 1 Address Type: Ignore Destination Addr/Mask: Ignore Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: Ignore Destination L4 Port Min: Ignore Destination L4 Port Max: Ignore

Red filter set	Yellow filter set	Green filter set
Destination L4 Port Max: 80 Source L4 Port Min: Ignore Source L4 Port Max: Ignore IPv6 Flow Id: Ignore Destination MAC Addr: Ignore Destination MAC Mask: Ignore Source MAC Addr: Ignore Source MAC Mask: Ignore VLAN: Ignore VLAN Tag: Ignore EtherType: 0x0800 802.1p Priority: All Action Drop: No Action Update DSCP: Ignore Action Update 802.1p Priority: Ignore Action Set Drop Precedence: Low Drop Commit Rate: 1000 Kbps Commit Burst: 4096 Bytes Out-Profile Action: Drop Non-Match Action: Drop Storage Type: NonVolatile	Destination L4 Port Max: 80 Source L4 Port Min: Ignore Source L4 Port Max: Ignore IPv6 Flow Id: Ignore Destination MAC Addr: Ignore Destination MAC Mask: Ignore Source MAC Addr: Ignore Source MAC Mask: Ignore VLAN: Ignore VLAN Tag: Ignore EtherType: 0x0800 802.1p Priority: All Action Drop: No Action Update DSCP: Ignore Action Update 802.1p Priority: Ignore Action Set Drop Precedence: Low Drop Commit Rate: 0 Kbps Commit Burst: 0 Bytes Out-Profile Action: None Non-Match Action: Drop Storage Type: NonVolatile	Source L4 Port Min: Ignore Source L4 Port Max: Ignore IPv6 Flow Id: Ignore Destination MAC Addr: Ignore Destination MAC Mask: Ignore Source MAC Addr: Ignore Source MAC Mask: Ignore VLAN: Ignore VLAN Tag: Ignore EtherType: Ignore 802.1p Priority: All Action Drop: No Action Update DSCP: Ignore Action Update 802.1p Priority: Ignore Action Set Drop Precedence: Low Drop Commit Rate: 0 Kbps Commit Burst: 0 Bytes Out-Profile Action: None Non-Match Action: Defer Storage Type: NonVolatile
Id: 1 Unit/Port: 0 (TEMPLATE) Name: Red Block: NsnaDefRedBlk1 Eval Order: 6 Address Type: IPv4 Destination Addr/Mask: 10.40.40.0/24 Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: TCP Destination L4 Port Min: 443 Destination L4 Port Max: 443 Source L4 Port Min: Ignore Source L4 Port Max: Ignore IPv6 Flow Id: Ignore Destination MAC Addr: Ignore Destination MAC Mask: Ignore Source MAC Addr: Ignore Source MAC Mask: Ignore VLAN: Ignore VLAN Tag: Ignore EtherType: 0x0800 802.1p Priority: All	Id: 2 Unit/Port: 0 (TEMPLATE) Name: Yellow Block: NsnaDefYelBlk1 Eval Order: 6 Address Type: IPv4 Destination Addr/Mask: 10.40.40.0/24 Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: TCP Destination L4 Port Min: 443 Destination L4 Port Max: 443 Source L4 Port Min: Ignore Source L4 Port Max: Ignore IPv6 Flow Id: Ignore Destination MAC Addr: Ignore Destination MAC Mask: Ignore Source MAC Addr: Ignore Source MAC Mask: Ignore VLAN: Ignore VLAN Tag: Ignore EtherType: 0x0800 802.1p Priority: All	

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

Red filter set	Yellow filter set	Green filter set
Id: 1 Unit/Port: 0 (TEMPLATE) Name: Red Block: Eval Order: 12 Address Type: Ignore Destination Addr/Mask: Ignore Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: Ignore Destination L4 Port Min: Ignore Destination L4 Port Max: Ignore Source L4 Port Min: Ignore Source L4 Port Max: Ignore IPv6 Flow Id: Ignore Destination MAC Addr: Ignore Destination MAC Mask: Ignore Source MAC Addr: Ignore Source MAC Mask: Ignore VLAN: Ignore VLAN Tag: Ignore EtherType: 0x0806 802.1p Priority: All Action Drop: No Action Update DSCP: Ignore Action Update 802.1p Priority: Ignore Action Set Drop Precedence: Low Drop Commit Rate: 1000 Kbps Commit Burst: 4096 Bytes Out-Profile Action: Drop Non-Match Action: Drop Storage Type: NonVolatile	Id: 2 Unit/Port: 0 (TEMPLATE) Name: Yellow Block: Eval Order: 12 Address Type: Ignore Destination Addr/Mask: Ignore Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: Ignore Destination L4 Port Min: Ignore Destination L4 Port Max: Ignore Source L4 Port Min: Ignore Source L4 Port Max: Ignore IPv6 Flow Id: Ignore Destination MAC Addr: Ignore Destination MAC Mask: Ignore Source MAC Addr: Ignore Source MAC Mask: Ignore VLAN: Ignore VLAN Tag: Ignore EtherType: 0x0806 802.1p Priority: All Action Drop: No Action Update DSCP: Ignore Action Update 802.1p Priority: Ignore Action Set Drop Precedence: Low Drop Commit Rate: 0 Kbps Commit Burst: 0 Bytes Out-Profile Action: None Non-Match Action: Drop Storage Type: NonVolatile	
Id: 1 Unit/Port: 0 (TEMPLATE) Name: Red Block: NsnaDefRedBlk2 Eval Order: 17 Address Type: IPv4 Destination Addr/Mask: Ignore Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: UDP Destination L4 Port Min: Ignore Destination L4 Port Max: Ignore	Id: 2 Unit/Port: 0 (TEMPLATE) Name: Yellow Block: Eval Order: 17 Address Type: IPv4 Destination Addr/Mask: 10.120.120.0/24 Source Addr/Mask: Ignore DSCP: Ignore IPv4 Protocol / IPv6 Next Header: Ignore Destination L4 Port Min: Ignore	

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

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

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

Index

Nortel Ethernet Routing Switch 5500 Series

Configuration — Security

Publication: NN47200-501
Document status: Standard
Document version: 03.01
Document date: 27 August 2007

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

Sourced in Canada and the United States of America

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