NORTEL

Nortel Ethernet Routing Switch 5000 Series

Configuration — Security

Release: 6.1
Document Revision: 05.01

www.nortel.com

NN47200-501

Nortel Ethernet Routing Switch 5000 Series
Release: 6.1
Publication: NN47200-501
Document release date: 20 May 2009

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OFANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Contents

New in this release

The following sections detail what’s new in *Nortel Ethernet Routing Switch 5000 Series Configuration — Security* (NN47200-501) for Release 6.1.

Features

See the following sections for information about feature changes::

- “User name and password support” (page 11)
- “Extended password history” (page 11)
- “802.1X dynamic authorization extension” (page 12)

User name and password support

The Ethernet Routing Switch 5000 Series now features the ability to create user names and passwords for switch or stack access. This feature extends the current access method of one read-only or read-write password for switch or stack access. For more information, see:

- “Password security features” (page 51)
- “Creating user names and passwords” (page 164)

Extended password history

The Ethernet Routing Switch 5000 Series now features an extended password history. For more information, see:

- “Password security features” (page 51)
- “Configuring password history” (page 165)
- “Defaulting password history” (page 165)
- “Displaying password history settings” (page 165)

802.1X dynamic authorization extension

The Ethernet Routing Switch 5000 Series now supports 802.1X dynamic authorization extensions. The support allows third-party devices to dynamically change VLANs or close user sessions. For more information, see:

- “802.1X dynamic authorization extension” (page 42)
- “802.1X dynamic authorization extension configuration” (page 130)

Introduction

This document describes security features and how to configure security services for the Nortel Ethernet Routing Switch 5000 Series.

NNCLI command modes

NNCLI provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration
- Router Configuration

Mode access is determined by access permission levels and password protection.

If no password is set, you can enter NNCLI in User EXEC mode and use the **enable** command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

With sufficient permission, you can use the rules in the following table to move between the command modes.

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC `ERS5000>`	No entrance command, default mode	**exit** or **logout**
Privileged EXEC `ERS5000#`	**enable**	**exit** or **logout**

Command mode and sample prompt	Entrance commands	Exit commands

Global Configuration
`ERS5000(config)#`
	From Privileged EXEC mode, type:
	`configure terminal`
		To return to Privileged EXEC mode, type:
		`end`
		or
		`exit`
		To exit NNCLI completely, type:
		`logout`

Interface Configuration
`ERS5000(config-if)#`
	From Global Configuration mode:
	To configure a port, type:
	`interface fastethernet <port number>`
	To configure a VLAN, type:
	`interface fastethernet <vlan number>`
		To return to Global Configuration mode, enter:
		`exit`
		To return to Privileged EXEC mode, type:
		`end`
		To exit NNCLI completely, type:
		`logout`

Router Configuration
`ERS5000(config-router)#`
	From Global Configuration mode:
	To configure router OSPF, type:
	`router ospf`
	To configure router RIP, type:
	`router rip`
	To configure router VRRP, type:
	`router vrrp`
		To return to Global Configuration mode, enter:
		`exit`
		To return to Privileged EXEC mode, type:
		`end`
		To exit NNCLI completely, type:
		`logout`

For more information about the NNCLI command modes, see *Nortel Ethernet Routing Switch 5000 Series Fundamentals* (NN47200-104).

Navigation

- "Security fundamentals" (page 17)
- "Configuring and managing security using NNCLI" (page 91)
- "Configuring and managing security using the Web-based management interface" (page 197)

Security fundamentals

This chapter provides conceptual information to help you understand the security features supported by the Ethernet Routing Switch 5000 Series to restrict access to your network.

Navigation

MAC address-based security

The Media Access Control (MAC) address-based security feature is based on Nortel BaySecure local area network (LAN) Access for Ethernet, a real-time security system that safeguards Ethernet networks from unauthorized surveillance and intrusion. MAC address-based security can be derived from:

- Destination MAC address (mac-da-filtering)
- Source MAC address

  The list of authorized hosts is populated in one of the following ways:

  - Static (manual)

    Addresses are manually added by the user by specifying the address and the ports it is authorized on.

  - Learning

    Addresses are added by enabling learning, waiting for all MAC addresses on the network to be learned, and then disabling learning.

  - Auto-learning

    Addresses are added by setting a maximum of allowed addresses on a port (1 - 25). The switch allows only the addresses first learned up to the port maximum.

The MAC address-based security feature can be used to configure network access control, based on the source MAC addresses of authorized stations.

Use MAC address-based security to perform the following tasks:

- Create a list of up to 10 destination MAC addresses the system uses to drop all packets that contain one of the specified MAC addresses as the destination address regardless of the ingress port, source address intrusion, or VLAN membership.

  ATTENTION
  Ensure that you do not enter the MAC address for the stack or the units that you use.

- Create a list of up to 448 MAC source addresses and specify the source addresses authorized to connect to the switch or stack. There are three ways to populate this list:

  - Manual configuration

    When MAC address-based security is configured, the ports each MAC source address can access is specified. The options for allowed port access include NONE, ALL, and single or multiple ports specified in a list. A list can include a single port, 1/6 for example, or multiple ports, 1/1-4 for example. Manually added MAC addresses are referred to as being static.

— MAC address security learning

When activating MAC address learning on ports, security is temporarily disabled and all learned MAC addresses will be added to the list. When learning is deactivated, security is enabled and only the MAC addresses in the list are allowed to connect through the port.

— MAC address-based security auto-learning

Auto-learning populates the list without user intervention. The user sets a maximum number of allowed MAC addresses (1-25) for a specific port, and the switch only passes traffic from the addresses learned by the switch up to the maximum value.

Optional actions for the switch to perform if the software detects a source address security violation can be configured. Actions include sending a SNMP trap, turn on destination address filtering for the specified source addresses, disabling the port, or a combination of these options.

> **ATTENTION**
> Up to 32 MAC source addresses for each port can be configured on the 5520 and 5530 models. This limitation does not exist on any other switch models. 448 entries can be freely distributed across the system.

When you configure MAC-based security, you must specify the following items:

- Switch ports that each MAC SA can access.

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

- Optional actions for your switch to perform if the software detects an SA security violation.

  Responses include send a trap, turn on DA filtering for the specified SAs, disable the specific port, or a combination of these three options.

Use either Nortel Command Line Interface (NNCLI) or Web-based management system to configure MAC address-based security features.

MAC address-based security auto-learning

Use the MAC address-based security auto-learning feature 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 can specify the number of addresses to learn on the ports, to a maximum of 25 addresses for each 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 refresh in the MAC Security Address Table. If you set the aging time value to 0, the entries never age out; you must reset the MAC Security Address Table for the specified port to force it to learn new addresses.
- Auto-learned entries associated in the MAC Security Address Table to 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 Non-Volatile Random Access Memory (NVRAM) but learned after the bootup sequence. The aging time and the allowed number of auto-learned MAC addresses for each port save in nonvolatile 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 modifies to associate that MAC address with the new port (port y). The aging timer for the entry resets.
- If you disable auto-learning on a port, the system removes all the auto-learned MAC entries associated with that port in the MAC Security Address Table.
- 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. User settings take priority over auto-learning.

RADIUS-based network security

Remote Authentication Dial-In User Service (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.

Navigation

- "How RADIUS works" (page 21)
- "RADIUS password fallback" (page 22)
- "Configuring RADIUS authentication" (page 22)

How RADIUS works

A RADIUS application has two components:

- RADIUS server—a computer equipped with server software (for example, a UNIX workstation) located at a central office or campus. It has authentication and access information in a form compatible with the client.
- RADIUS client—a switch, router, or 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 that attempt to log on to the switch from a local console or Telnet.

Nortel recommends that you include two RADIUS servers in the Ethernet Routing Switch 5000 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 the primary and secondary server when you configure the RADIUS servers on the switch.

RADIUS allows three retries for service requests to each RADIUS server in the network. You can configure the timeout interval between each retry.

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 5000 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 configure the following user name attributes:

- For read-write access, configure the Service-Type field value to `Administrative`.
- For read-only access, configure 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, see 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 NNCLI, Web-based management interface or Java Device Manager (JDM).

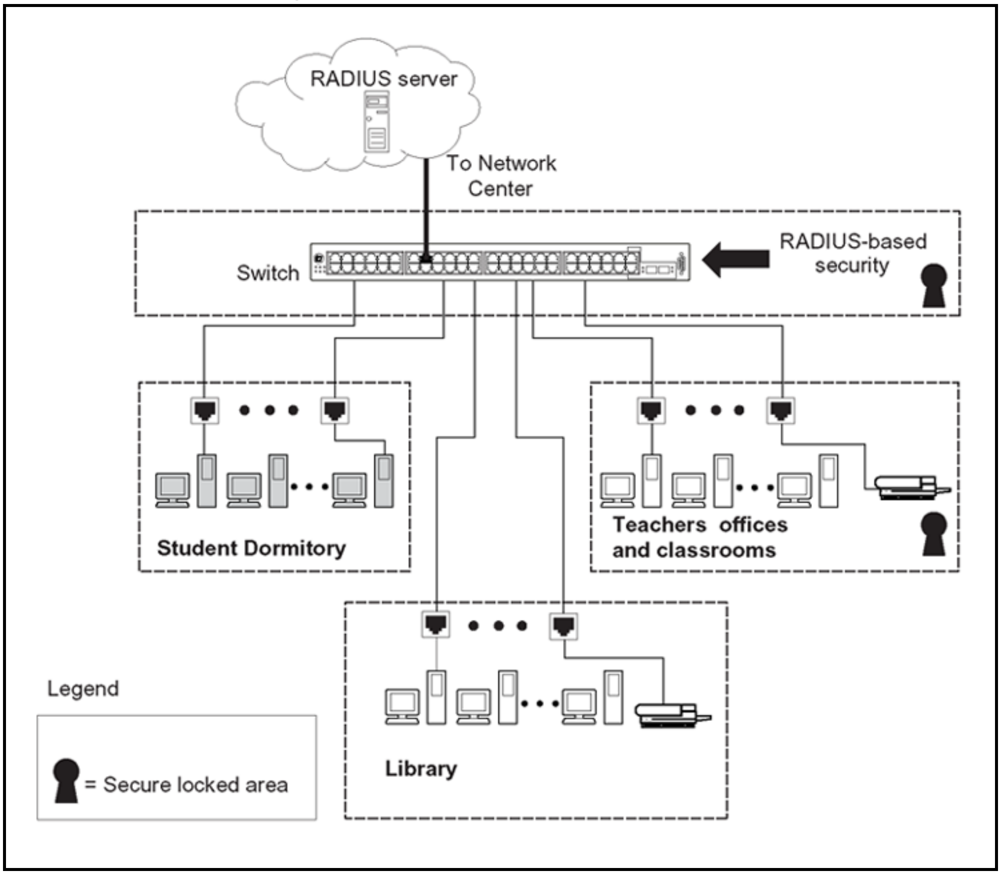
For more information about configuring RADIUS authentication using NNCLI, see "Configuring RADIUS authentication using NNCLI" (page 100). For more information about configuring RADIUS authentication using Web-based management, see "Configuring RADIUS security using the Web-based management interface" (page 227). For more information about configuring RADIUS authentication using the JDM, see "RADIUS Server security configuration using Device Manager" (page 253).

Campus security example

The following figure shows a typical campus configuration using the RADIUS-based and MAC address-based security features for the Ethernet Routing Switch 5000 Series.

This example assumes that the switch, teacher offices, classrooms, and library are physically secured. You can also physically secure the student dormitory.

Figure 1
Nortel Ethernet Routing Switch 5000 Series security features



In the previous configuration example, the security measures are implemented in the following locations:

- The switch

  The configuration example uses RADIUS-based security to limit administrative access to the switch through user authentication. See "RADIUS-based network security" (page 20).

  The configuration example uses MAC address-based security to allow up to 448 authorized stations access to one or more switch ports. See "MAC address-based security" (page 18).

  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 pre-wired with two RJ-45 jacks.

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

- Teacher offices and classrooms

The PCs that are located in the teacher 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, which prevents unauthorized access to the switch.

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

PCs are password protected and classrooms and offices are physically secured.

- Library

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

  PCs are password protected and access to the library is physically secured.

EAPOL-based security

The Ethernet Routing Switch 5000 Series uses an encapsulation mechanism to provide security, 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.

The EAP allows the exchange of authentication information between an 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 Ethernet Routing Switch 5000 Series, configured with the EAPOL-based security feature, reacts 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 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 can access the switch and the network.

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

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

The Authenticator communicates with the Supplicant using the EAPOL encapsulation mechanism.

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 controlled port on the switch, the controlled port 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 state is changed accordingly. If the authorization is successful, the controlled port 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 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-Volative 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 NVRAM.
- If an EAPOL connection is active on a port, 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 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 customized for your user ID and previously stored on the Authentication server.

To set up the Authentication server, configure the following Return List attributes for all user configurations. For more information about, see 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 (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 (used to indicate the port priority value assigned to the specified user)

System requirements

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

- At least one Ethernet Routing Switch 5000 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 Ethernet Routing Switch 5000 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 currently configured for:
  - Shared segments
  - MultiLink Trunking
  - MAC address-based security
  - IGMP (Static Router Ports)
  - Port mirroring (as long as port mirroring on EAP ports is disabled in Global Configuration mode)
  - IP Source Guard
- With EAPOL SHSA (the simplest EAPOL port operating mode), you can connect only a single client on each port 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 logons.

Advanced EAPOL features

EAPOL supports the following advanced features:

- Single Host with Single Authentication (SHSA) and Guest VLAN. For more information, see "Single Host with Single Authentication and Guest VLAN" (page 28).
- Multihost (MH) support:
  - Multiple Host with Multiple Authentication (MHMA) (see "Multiple Host with Multiple Authentication" (page 30))
  - Non-EAP hosts on EAP-enabled ports (see "Non-EAP hosts on EAP-enabled ports" (page 36))
  - Multiple Host with Single Authentication (MHSA) (see "Multiple Host with Single Authentication" (page 39))

> **ATTENTION**
> EAPOL supports only untagged traffic when the multihost features are used.

Single Host with Single Authentication and Guest VLAN

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 can access that port for traffic. Tagged ingress packets are sent to the PVID of that port. Exceptions include reserved addresses.

You can configure a guest VLAN to allow nonauthenticated 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 placed in a Guest VLAN.

    PVID of the port = Guest VLAN ID
  - If Guest VLAN is not enabled, the port services only EAPOL packets until successful authentication.
- During EAP authentication:

  - If Guest VLAN is enabled, the port is placed in a Guest VLAN.
  - If Guest VLAN is not enabled, the port services EAPOL packets only.
- If authentication succeeds:
  - The port is placed 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 placed 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 placed 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 for each 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 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 occur:
  - A message is sent to the syslog.
  - The port is blocked.
- When an authentication failure occurs, a port is placed back in the Guest VLAN.
- This Guest VLAN feature affects ports with 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.

- Guest VLAN 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 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.

In the MHMA mode, RADIUS-assigned VLAN values are ignored, and VLAN configuration changes are committed to NVRAM.

RADIUS-assigned VLAN values are allowed in the MHMA mode. For more information about RADIUS-assigned VLANs in the MHMA mode, see “RADIUS-assigned VLAN use in MHMA mode” (page 31).

MHMA support is on a for each 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. 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 disabled for ports in MHMA mode. Only preconfigured VLAN assignment for the port is used. Upon successful authentication, untagged traffic is put it in a VLAN configured for the 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 for each port and not for each 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 on to the port.
- EAP accounting, when enabled, displays the octet and packet counts for each physical port.
- Configuration settings are saved across resets.

RADIUS-assigned VLAN use in MHMA mode

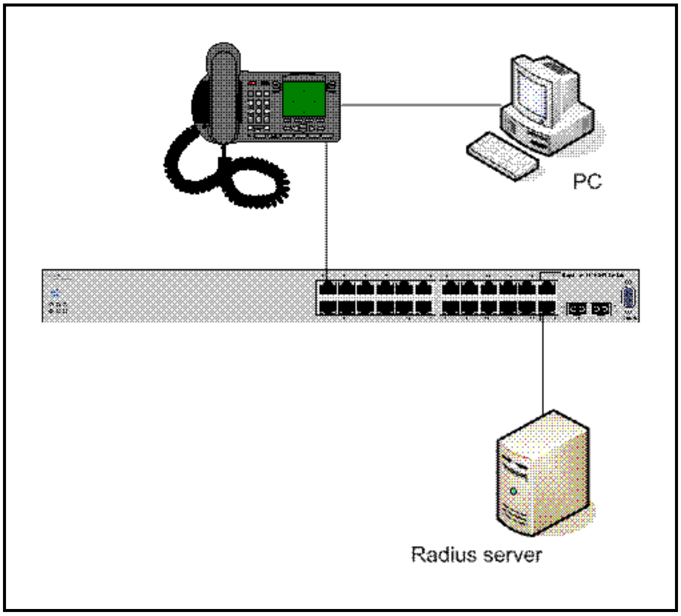
RADIUS-assigned VLAN use in the MHMA mode is allowed to give you greater flexibility and a more centralized assignment than existed. This feature is also useful in an IP Phone set up, when the phone traffic can be directed to the Voice over IP (VoIP) VLAN and the PC Data traffic can be directed to the 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.

ATTENTION
All VLAN movement in an EAP-enabled state is dynamic and is not saved across resets.

Consider the following setup in the figure:

- Ethernet Routing Switch 5510-24T stand-alone 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)

Figure 2
RADIUS-assigned VLAN use in MHMA mode



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 authenticate using MD5 credentials, but any other available type of authentication could be used (TLS, PEAP-MSCHAPv2, PEAP-TLS, and TTLS). 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 the Non-EAP IP Phone authentication in Global Configuration 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 Configuration and Interface Configuration 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). All EAP supplicants cannot support this operating mode.

      Following are the steps to enable the enhancement:

      – Enable unicast EAP requests in Global Configuration 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 Configuration and Iinterface Configuration modes, for all switch ports. You need to set the EAP packet mode to Unicast in both global an interface modes, for a switch port, in order to enable this feature. Any other combination (for example, multicast in global, unicast in interface mode) selects 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. Radius assigned VLANs is 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 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 Configuration 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-assigne
d-vlan
```

By default, the RADIUS- assigned VLANs in MHMA enhancement is disabled in Global Configuration and Interface Configuration 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 38).

    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 and also fails RADIUS authentication, the host is counted as an intruder. Data packets from that MAC address are dropped.
  - — 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 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, 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 32, 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.

ATTENTION
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 more information about configuring non-EAPOL host support, see "Configuring support for non-EAPOL hosts on EAPOL-enabled ports" (page 119).

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.
- The password is a string that combines the MAC address, switch IP address, unit, and port.

  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 for each 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, 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, 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.

Table 1
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 RADI US 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 5000 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 restart.

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.

Table 2
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

Event	Accounting information logged at server
	• Account status type • User name • Account session time • Account terminate cause • Input octet count for the session (see "Attention" (page 42)) • Output octet count for the session (see "Attention" (page 42)) • Input packet count for the session (see "Attention" (page 42)) • Output packet count for the session (see "Attention" (page 42)) **ATTENTION** 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.

Table 3
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 more information about configuring RADIUS accounting using NNCLI, see “Configuring RADIUS accounting using NNCLI” (page 158).

802.1X dynamic authorization extension

The 802.1X dynamic authorization extension enables the ability to dynamically change VLANs or close user sessions through a third-party device. This feature pertains to EAP clients only and does not impact non-EAP clients. When in use this feature allows for the closing of user sessions or the modification of the Guest VLAN, RADIUS VLAN for EAP clients, or RADIUS VLAN for non-EAP clients. This feature functions when either of the RADIUS VLAN assignment features are active on a port and with SHSA, MHMA, and MHSA port operating modes

This process uses the following entities in the network:

- The Ethernet Routing Switch 5000 Series device that authenticates each 802.1X client at a RADIUS server.
- The RADIUS server that sends requests to the Ethernet Routing Switch 5000 Series device. There are two RADIUS server requests that directly pertain to this feature:
  - The Disconnect command ends a user session.
  - The Change of Authorization (CoA) command modifies user session authorization attributes.

  > **ATTENTION**
  > Some literature now refers to the RADIUS server as the Dynamic Authorization Client (DAC) and the network device it interacts with as the Direct Authorization Server (DAS). In this instance the Ethernet Routing Switch 5000 Series device is the DAS.

- The 802.1X client that is authenticated by the RADIUS server and uses the Ethernet Routing Switch 5000 Series device services.

The key aspect of this feature is the receipt and processing of Disconnect and CoA commands from the RADIUS server. An Ethernet Routing Switch 5000 Series can receive and process these commands under the following conditions:

- A user authenticated session exists on a port. A single user session for single-host configuration or multiple user sessions for multiple host configuration.
- The port maintains the original VLAN membership.
- The port is added to a RADIUS-assigned VLAN.

> **ATTENTION**
> Commands are ignored on ports where this feature is not enabled.

During the process of listening for traffic requests from the RADIUS server, the switch can copy and send a UDP packet. This can cause a user to become disconnected. Nortel recommends implementing reply protection by including the Event Timestamp attribute in both requests and responses. Synchronize the RADIUS server and switch using an SNTP server to ensure the correct processing of the Event Timestamp attribute.

The RADIUS server must use the source IP address of the RADIUS UDP packet to determine which shared secret to accept for RADIUS requests to be forwarded by a proxy. When a proxy forwards RADIUS requests the NAS-IP-Address or NAS-IPv6-Address attributes do not match the source IP address observed by the RADIUS server. The RADIUS server cannot resolve the NAS-Identifier attribute whether a proxy is present or not. The authenticity check performed by the RADIUS server does not verify the switch identification attributes and an unauthorized switch can forge identification attributes and impersonate an authorized switch in the network. To prevent these vulnerabilities, Nortel recommends proxy configuration to confirm that the NAS identification attributes match the source IP address of the RADIUS UDP packet.

To enable the 802.1X dynamic authorization extension feature on the Ethernet Routing Switch 5000 Series, perform the following procedure.

Step	Action
1	Enable EAP globally.
2	Enable EAP on each applicable port.
3	Enable this feature globally.
4	Enable this feature on each applicable port.

--End--

TACACS+

Ethernet Routing Switch 5000 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).

> **ATTENTION**
> 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 NNCLI.

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

For more information about TACACS+ protocol, see ftp://ietf.org.

ATTENTION
TACACS+ is not compatible with 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)—a client, such as an Ethernet Routing Switch 5000 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 5000 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 5000 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 and 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.

ATTENTION

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 more information about configuration required on the TACACS+ server, see "TACACS+ server configuration example" (page 48) .

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.

> **ATTENTION**
> If authorization is enabled for a privilege level to which a user is assigned, the TACACS+ server denies 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.

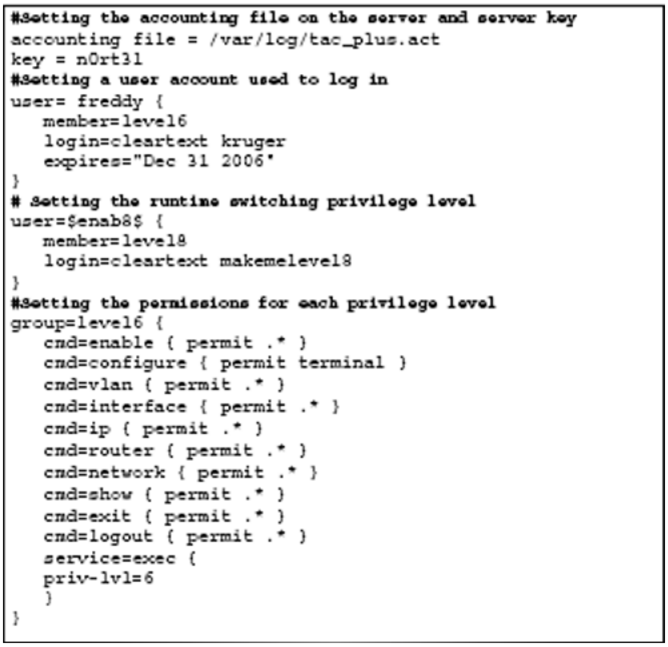
To return to the original privilege level, the user uses the following command on the switch:

```
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 more information about the configuration required on the TACACS+ server, see "TACACS+ server configuration example" (page 48) .

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.

Figure 3
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 317).

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 NNCLI terminal sessions within serial, Telnet, or SSH shells (from NNCLI 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 5000 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 NNCLI to configure TACACS+ on the Ethernet Routing Switch 5000 Series. You cannot configure TACACS+ using Device Manager or Web-based management.

For more information about configuring TACACS+ server information and TACACS+ authentication, authorization, and accounting using NNCLI, see "Configuring TACACS+ using NNCLI" (page 158).

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 Ethernet Routing Switch 5000 Series by defining the IP addresses that are allowed access to the switch.

The IP Manager allows you to do the following:

- Define a maximum of 50 Ipv4 and 50 Ipv6 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, SSH, and 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.

> **ATTENTION**
> 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 Ethernet Routing Switch 5000 Series provides password security through a variety of mechanisms. It supports both default and customized user names and passwords for accessing a switch or stack in read-only or read-write access. In addition, it supports password security for RADIUS shared secrets and SNMP access.

The following is a list of the types of password security provided by the device:

- default switch and stack read-only user name and password
- default switch and stack read-write user name and password
- customized user names and passwords for read-only switch and stack access
- customized user names and passwords for read-write switch and stack access
- 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 password security features are available:

- “Custom user names and passwords” (page 51)
- “Password length and valid characters” (page 52)
- “Password retry” (page 52)
- “Password history” (page 52)
- “Password display” (page 52)
- “Password verification” (page 52)
- “Password aging time” (page 52)
- “Log on failure timeout” (page 53)

Custom user names and passwords

The Ethernet Routing Switch 5000 Series device provides the ability to create custom user names and passwords for accessing the switch or stack. User names and associated passwords can be defined at any time but only come into effect when password security is enabled. User names and passwords are created only by a user with read-write privileges.

Custom users and passwords cannot have specialized access conferred to them. Custom users have the same privileges as the default read-only or read-write access user. The read-only and read-write passwords cannot be the same.

Password length and valid characters

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

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

Passwords are 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 NNCLI. For more information, see "Configuring password retry attempts" (page 165).

Password history

The Ethernet Routing Switch 5000 Series stores a maximum of the last 10 passwords used. Stored passwords are not reusable.

Password display

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

Password verification

New passwords must be verified before use. If the two passwords do not match, the password update process fails. In this case, the password change process starts over. There is no limit to the number of password change attempts.

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 read-write password can create a new password.

Log on failure timeout

Log on failure timeouts prevent brute force hacking. Following three consecutive password log on failures all password log on interfaces are disabled for 60 seconds. Log on failure timeouts disable the serial port, Telnet, and Web interfaces.

Log on failure timeouts affects only new log on sessions and do not interfere with sessions already in progress.

Default password and default password security

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

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 is enabled from the NNCLI 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 has the capacity to store up to 10 previously used passwords.
- Password verification is required.

Password security is disabled from the NNCLI 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 more information about NNCLI commands to enable or disable password security, see “Configuring password security using NNCLI” (page 163).

Password security features and requirements

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

Table 4
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: lowercase letters, capital letters, numbers, and special symbols such as !@#$%^&*().
Password length	The password must consist of between 10 and 15 characters.
log on 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 switch can be configured to store up to 10 previously used passwords. The passwords stored in the password history 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 NNCLI, 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.

NNCLI audit

NNCLI audit provides a means for tracking NNCLI commands.

The command history is stored in a special area of flash reserved for NNCLI 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 NNCLI 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)
- NNCLI command itself

NNCLI audit is enabled by default and cannot be disabled.

For more information about displaying NNCLI audit log, see "Displaying NNCLI Audit log using NNCLI" (page 165).

Simple Network Management Protocol

The Ethernet Routing Switch 5000 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

The following sections describes the various SNMP versions supported in the Ethernet Routing Switch 5000 Series.

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 an 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.

Ethernet Routing Switch 5000 Series support for SNMP

The SNMP agent in the Ethernet Routing Switch 5000 Series supports SNMPv1, SNMPv2c, and SNMPv3. Support for SNMPv2c introduces a standards-based GetBulk retrieval capability using SNMPv1 communities.

SNMPv3 support in the Ethernet Routing Switch 5000 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 Ethernet Routing Switch 5000 Series allows you to configure SNMPv3 using the Device Manager, Web-based management, or NNCLI.

SNMP MIB support

The Ethernet Routing Switch 5000 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 more information about the MIBs supported by the Ethernet Routing Switch 5000 Series, see "Supported SNMP MIBs and traps" (page 333).

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 Ethernet Routing Switch 5000 Series supports both industry-standard SNMP traps, as well as private Nortel enterprise traps.

For more information about the MIBs and traps supported by the Ethernet Routing Switch 5000 Series, see "Supported SNMP MIBs and traps" (page 333).

Feature interactions

If DHCP global is disabled, no SNMP traps for DHCP Snooping can be generated.

The SNMP trap for Dynamic ARP Inspection `bsaiArpPacketDroppedOnUntrustedPort` cannot be generated in the following circumstances:

- If the DHCP global is disabled.
- An ARP packet is received on a non-existent Vlan.
- An ARP inspection is not enabled on the management Vlan.

If a port is not IP Source Guard enabled, the SNMP trap for IP Source Guard, `bsSourceGuardReachedMapIpEntries`, cannot be generated.

If enabling IP Source Guard on a port fails due to insufficient resources available, the `bsSourceGuardCannotEnablePort` SNMP trap is generated.

SNMP trap port configuration

This feature provides information on how to configure the SNMP trap port. Using NNCLI, the user has the ability to specify a custom SNMP trap port when a new host receiver is added. The SNMP trap port is stored in NVRAM so that it is saved across switch and stack reboots. The SNMP trap port value is shared among all the units in the stack.

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

An SSL certificate is generated when

- The system is powered up for the first time and the NVRAM does not contain a certificate that can be used to initialize the SSL server.
- The management interface (NNCLI/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 (NNCLI/SNMP) can configure the Web server to operate in a secure or nonsecure 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 nonsecure connections with the browser are closed down.

In the nonsecure 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 Ethernet Routing Switch 5000 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):
40e04e564bcfe8b7febf1f7139b0fde9f5289f01020d5a59b66ce72078955
45f
b3abd694f836a9243651fd8cee502f665f47de8da44786e0ef292a3309862
273
d36644561472bb8eac4d1db9047c35ad40c930961b343dd03f77cd88e8ddd
3dd
a02ae29189b4690a1f47a5fa71b75ffcac305fae37c56ca87696dd9986
aa7d19
```

SSL configuration and management

For more information about configuring and managing SSL services, see "Configuring Secure Socket Layer services using NNCLI" (page 166).

Secure Shell protocol

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

There are two versions of the SSH protocol: SSH1 and SSH2. The SSH implementation in the Ethernet Routing Switch 5000 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 and password) 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 NNCLI 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 nonsecured 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 Ethernet Routing Switch 5000 Series is password authentication.

- Password authentication enable or disable

  If password authentication is not enabled, you are not allowed to initiate a 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 Ethernet Routing Switch 5000 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, for each port feature that works closely with information in the Dynamic Host Control Protocol (DHCP) snooping binding table. For more information about DHCP snooping, see "DHCP snooping" (page 62). 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.

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:

Table 5
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 more information about configuring IP Source Guard through NNCLI, see “IP Source Guard configuration using NNCLI” (page 191). For more information about configuring IP Source Guard through the JDM, see “IP Source Guard configuration using Device Manager” (page 265).

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.

    ATTENTION
    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.

ATTENTION
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 more information about the QoS DHCP snooping application, see *Nortel Ethernet Routing Switch 5000 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
- time until expiration of current entry
- 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.

The Ethernet Routing Switch 5000 Series supports IP Source Guard, which works closely with DHCP snooping. IP Source Guard can be enabled for each 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 for each VLAN.

Configure and manage DHCP snooping using the Nortel Networks Command Line Interface (NNCLI), Java Device Manager (JDM), and SNMP. For more information about configuring DHCP snooping through NNCLI, see "Configuring DHCP snooping using NNCLI" (page 172). For more information about configuring DHCP snooping through JDM, see "DHCP snooping configuration using Device Manager" (page 260).

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.

ATTENTION
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 63).

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 62) and “Configuring DHCP snooping using NNCLI” (page 172).

Dynamic ARP inspection is configured for each VLAN.

Configure and manage dynamic ARP inspection using NNCLI. For more information about configuring this feature with NNCLI, see “Configuring dynamic ARP inspection using NNCLI” (page 183). For more information about configuring this feature with Web-based management or the JDM, see *Nortel Ethernet Routing Switch 5000 Series Configuration — IP Routing Protocols* () (NN47200-503).

Feature limitations

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 antivirus 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).

The Ethernet Routing Switch 5000 Series supports Nortel SNA v2.0 and a lightweight version of SNAS Communication Protocol (SSCP-Lite). With SSCP-Lite, the Secure Network Access Switch (SNAS) can control simple VLAN transition for Ethernet switches and other policy enforcement points, using SNMP based VLAN assignments. You can use SSCP-Lite to deploy admission control policy server without 802.1X supplicant requirements for a non-SSCP enabled Packet Exchange Protocol (PEP) and when simple VLAN transition is a suitable enforcement mechanism.

You can configure the Ethernet Routing Switch 5000 Series as a network access device for 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 Nortel Health Agent applet, provides host integrity checking. Nortel Health Agent can be configured to run once, continuously, or never. Integrity checking is performed on hosts that support Windows operating systems when Nortel Health Agent is set to run once or continuously.
4. If the Nortel Health Agent 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 SNA requires the secure runtime image of the Ethernet Routing Switch 5000 Series software.

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 pre-specified 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, see *Nortel Secure Network Access Solution Guide* () (320817-A). For more information about configuring the Nortel SNAS 4050, see *Nortel Secure Network Access Switch 4050 User Guide* () (320818-A).

For more information about configuring the Ethernet Routing Switch 5000 Series for the Nortel SNA solution, see "Configuring Nortel Secure Network Access using NNCLI" (page 287)or "Configuring Nortel Secure Network Access using Device Manager" (page 303).

Navigation

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 through 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 TunnelGuard (TG) 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 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 Nortel Health Agent applet. Prior knowledge of the client PC is not required on the switch and the client does not require a 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.

ATTENTION
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 more information about modifying the filter sets, see *Nortel Ethernet Routing Switch 5000 Series Configuration — Quality of Service* () (NN47200-504). For more information about the current default Nortel SNA filter set rules, see “Default Nortel SNA filters” (page 339).

ATTENTION
When the Nortel SNA filters are applied to a port, an 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 83) and "Nortel SNA solution in an active network deployment" (page 80) 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 startup 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 startup 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.

ATTENTION
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 292))

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).

ATTENTION
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. For more information, see "Topologies" (page 75).

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.

With Ethernet Routing Switch 5000 Series, 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.

ATTENTION
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.

Table 6
Default Nortel SNA filter consumption

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

Filter parameters

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 339).

> **ATTENTION**
> If you plan to use the default filters, it is not necessary to configure filters before enabling Nortel SNA.

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

Table 7
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.

For more information about configuring the filters for Novell Netware log on, see “Configuring filters for Novell Netware log on” (page 74) . If you use any other log on controller, you must modify the filter set to allow the log on to work

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 289).

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
```

See *Nortel Ethernet Routing Switch 5000 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 5000 Series to function in either Layer 2 or Layer 3 for the Nortel SNA solution. In Layer 2, routing is disabled in the Ethernet Routing Switch 5000 Series switch. In Layer 3, routing is enabled in the switch.

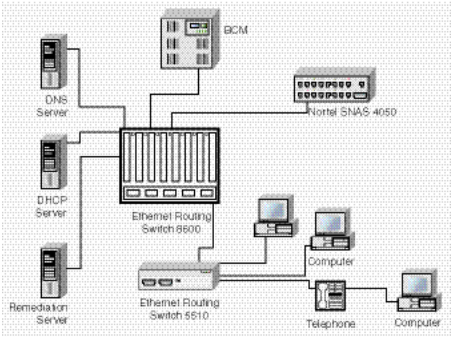
Layer 2

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.

Figure 4
Network access device-Layer 2 mode



Layer 3

In Layer 3 mode, DHCP-relay is enabled on the Ethernet Routing Switch 5000 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 Ethernet Routing Switch 5000 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 a port as a Nortel SNA uplink while the switch is in Layer 3 mode).

Fail Open

A Status Quo time interval applies to all Nortel Secure Network Access Server (NSNAS) connections to the Ethernet Routing Switch 5000 Series. The expiration of this interval indicates that the NSNAS connection with the switch has failed. When Fail Open is enabled on the switch and the connection to the NSNAS fails or is never established, the following apply:

- New clients connecting on ports without pre-authenticated clients will be moved to the Fail Open VLAN and filter. If the Fail Open filter is the red or yellow VLAN, the clients cannot gain full access to the network.
- New clients cannot connect on ports that already have authenticated clients connected (nonphone).
- Network access is not interrupted for devices pre-authenticated with MAC-authentication, TG-authentication, or 802.1x authentication.

If the NSNAS reconnects, ports are moved to the red vlan and red filter and all MACs on the ports are aged out. Any previous blocked MACs are unblocked.

If a connection to a NSNAS is never established on switch startup and Fail Open is enabled, Fail Open actions apply to all new clients.

Basic switch configuration for Nortel SNA

> **ATTENTION**
> 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.

> **ATTENTION**
> Nortel SNA requires the secure runtime image of the Ethernet Routing Switch 5000 Series software.

Configuring the network access device

To configure the Ethernet Routing Switch 5000 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 more information about NNCLI commands to configure the Nortel SNA solution on the switch, see “Configuring Nortel Secure Network Access using NNCLI” (page 287). For more information about configuring the Nortel SNA solution using Device Manager, see “Configuring Nortel Secure Network Access using Device Manager” (page 303).

- Configure static routes to all the networks behind the core routing device.

  This can be automated, as RIP and OSPF routing protocols are supported.
- Configure the switch management VLAN, if necessary.
- Configure SSH (see “Configuring SSH on the 5000 Series switch for Nortel SNA” (page 79)).

  a. Download the Nortel SNAS 4050 SSH public key to the switch.

  b. Enable SSH on the switch.

> **ATTENTION**
> 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).

- Configure the Nortel SNAS 4050 portal IP address (pVIP)/subnet (see "Configuring the Nortel SNAS 4050 subnet " (page 287)for NNCLI, or "Configuring the Nortel SNAS 4050 subnet using Device Manager" (page 304) for Device Manager).
- Configure port tagging, if applicable.

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

- Create the port-based VLANs.

  The VLANs are configured as VoIP, Red, Yellow, and Green VLANs later.
- Configure DHCP-relay and IP routing if the switch is used in Layer 3 mode.
- (Optional) Configure the filters (Red, Yellow, Green, and VoIP).

  > **ATTENTION**
  > 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.

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

- Configure the VoIP VLANs (see "Configuring Nortel SNA per VLAN " (page 289) for NNCLI, or "Configuring Nortel SNA per VLAN using Device Manager" (page 306) for Device Manager).
- Configure the Red, Yellow, and Green VLANs, associating each with the applicable filters (see "Configuring Nortel SNA per VLAN " (page 289)for NNCLI, or "Configuring Nortel SNA per VLAN using Device Manager" (page 306) 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.

- Configure the Nortel SNA ports (see "Enabling Nortel SNA on ports " (page 292) for NNCLI, or "Enabling Nortel SNA on ports using Device Manager" (page 308) 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.

  > **ATTENTION**
  > 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.

  > **ATTENTION**
  > You can configure Nortel SNA ports (both dynamic and uplink) after Nortel SNA is enabled globally.

- Enable Nortel SNA globally (see "Enabling Nortel SNA" (page 298) for NNCLI, or "Configuring Nortel SNA using Device Manager" (page 310) for Device Manager).

Configuring SSH on the 5000 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.

Configure SSH communication between the Ethernet Routing Switch 5000 Series and the Nortel SNAS 4050, by following this procedure:

Procedure steps

Step **Action**

1 Download the SSH public key from the Nortel SNAS 4050 to the switch:

> **ATTENTION**
> 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 5000 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 5000 Series switch, enable SSH using the following command from the Global Configuration mode:

```
ssh
```

3 On the Nortel SNAS 4050, import the 5000 Series switch public key:

```
/cfg/domain #/switch #/sshkey/import
apply
```

For more information about, see *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--

Nortel SNA solution in an active network deployment

You can deploy the Nortel SNA solution on an existing, active Ethernet Routing Switch 5000 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 Ethernet Routing Switch 5000 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 83)).

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 293)).

ATTENTION
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 5000 Series Configuration — Quality of Service* () (NN47200-504) and "Default Nortel SNA filters" (page 339) for more information).

When the Nortel SNA filters are applied to a port, an existing QoS filters on that port are disabled, and the Nortel SNA filters are applied (the earlier 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. With the Ethernet Routing Switch 5000 Series, 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 Ethernet Routing Switch 5000 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 5000 Series Configuration — Quality of Service* () (NN47200-504) and "Configuration example: Configuring the default Nortel SNA filters" (page 339) 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 5000 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.

Summary of security features

Table 8 "MAC security" (page 84) through Table 12 "SNMPv3 security" (page 86) provide an overview of some of the security features available on the Ethernet Routing Switch 5000 Series.

Table 8
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	For each 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	

Table 9
Password Authentication security

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

Table 10
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 for each port.
Layer	Layer 2.
Level of Security	Network access encryption.
Violations	The switch blocks a port if intruder is seen on that port. The administrator has to re-enable the 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.

Table 11
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), SSH (SSH On/Off), SNMP (SNMP On/Off) and Web Page Access (Web On/Off) with or without a list of 50 Ipv4 and 50 Ipv6 addresses and masks.
What is being secured	User access to the switch through Telnet, SSH, SNMP, or Web.
Per-Port or Per Switch	For each 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, SSH, SNMP, or Web Page.
Configuring using interfaces	Web, console, and NNCLI.
Restrictions and Limitations	Not applicable.

Table 12
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	For each 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 are incremented when any kind of violation occurs. (These can be monitored to detect intrusions, for example, by using RMON alarms.)
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.

Table 13
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	For each port.
Layer	Layer 2 and 3.

Table 13
DHCP snooping security (cont'd.)

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.

Table 14
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	For each 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	Due to VLAN changes, routed and tagged ARP packets can bypass dynamic ARP Inspection filters when a packet is rerouted in the Layer 3 mode.

Table 15
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	For each 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.

Table 16
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	For each port.
Layer	Layer 2-7.
Level of Security	Network access.
Violations	For nonauthenticated 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 NNCLI

This chapter describes the methods and procedures necessary to configure security on the Nortel Ethernet Routing Switch 5000 Series using the Nortel Networks Command Line Interface (NNCLI).

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

Navigation

Setting user access limitations using NNCLI

For more information about the configuration and management of user access limitations using NNCLI, see *Nortel Ethernet Routing Switch 5000 Series Overview — System Configuration* () (NN47200-500).

Configuring MAC address-based security using NNCLI

The following NNCLI commands allow for the configuration of the BaySecureapplication using Media Access Control (MAC) addresses.

> **ATTENTION**
> 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 more information about QoS policies, see *Nortel Ethernet Routing Switch 5000 Series Configuration — Quality of Service* () (NN47200-504).

NNCLI commands for MAC address security

The NNCLI 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.

Table 17
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

Table 17
show mac-security parameters (cont'd.)

Parameter	Description
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|disabl
e}] [snmp-lock {enable|disable}] [snmp-trap {enable|disable}]
```

The following table outlines the parameters for this command.

Table 18
mac-security parameters

Parameter	Description
disable|enable	Disables or enables MAC address-based security.
filtering {enable|disable}	Enables or disables DA filtering on intrusion detected.

Table 18
mac-security parameters (cont'd.)

Parameter	Description
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
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 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 the 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.

Table 19
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 executes in the Global Configuration 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.

Table 20
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 executes in the Global Configuration 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 executes 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.

Table 21
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 executes in the Global Configuration 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 executes in the Global Configuration 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.

Table 22
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

Parameter	Description
	the list of ports for which MAC address learning is being performed • 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 executes in the Interface Configuration 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 executes 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 also allows you 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 executes in the Global Configuration mode.

NNCLI commands for MAC address auto-learning

The NNCLI 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 executes in the Global Configuration 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 executes in the Global Configuration 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 executes in the Global Configuration 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.

Table 23
mac-security auto-learning parameters

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

Table 23
mac-security auto-learning parameters (cont'd.)

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 learns. The default is 2.

The **`mac-security auto-learning`** command executes in the Interface Configuration 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 executes in the Interface Configuration 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.

Table 24
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 learns. The default is 2.

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

Configuring RADIUS authentication using NNCLI

For more information about the function and operation of RADIUS in a Ethernet Routing Switch 5000 Series network, see "RADIUS-based network security" (page 20).

Configure RADIUS to perform authentication services for system users by doing the following:

- Configure the RADIUS server itself. For specific configuration procedures, see the vendor documentation. 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 100)).
- (Optional) Enable the RADIUS password fallback feature (see "Enabling RADIUS password fallback" (page 101)).

Configuring RADIUS server settings

Add a RADIUS server using 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.

Delete a RADIUS server and restore default RADIUS settings by using one of the following commands in Global or Interface Configuration mode:

```
no radius-server
```

```
default radius-server
```

Enabling RADIUS password fallback

Enable the RADIUS password fallback feature by using 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 you enable RADIUS password fallback, you cannot disable it without erasing all other RADIUS server settings.

ATTENTION
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.

Disable the RADIUS password fallback feature by using 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

Display RADIUS configuration status by using 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 using NNCLI

The following NNCLI 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 executes in the Global Configuration 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.

Table 25
eapol parameters

Parameter	Description
port <portllist>	Specifies the ports to configure for EAPOL; enter the desired port numbers. If this parameter is omitted, the system uses the port number specified when the interface command was issued.
init	Reinitiates 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 reauthentication.
re-authentication-period <1-604800>	Enter the desired number of seconds between reauthentication attempts.
re-authenticate	Specifies an immediate reauthentication.
quiet-interval <num>	Enter the desired number of seconds between an authentication failure and the start of a new authentication attempt; range is 1–65535.
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.
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 executes in the Interface Configuration 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.

Table 26
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 for each port Guest VLAN settings.
auth-diags {interface}	Displays the EAPOL authentication diagnostics interface.
auth-stats {interface}	Displays the authentication statistics interface.

The **show eapol** command executes 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:

Table 27
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 executes 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 executes in the Global Configuration mode.

The following table outlines the parameters for this command:

Table 28
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 executes in the Global Configuration mode.

The following table outlines the parameters for this command:

Table 29
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 executes in the Global Configuration mode.

The following table outlines the parameters for this command:

Table 30
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 executes in the Global Configuration mode.

The following table outlines the parameters for this command:

Table 31
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 executes in the Global Configuration mode.

The following table outlines the parameters for this command:

Table 32
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 executes in the Global Configuration mode.

The following table outlines the parameters for this command:

Table 33
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 executes in the Privileged Exec command mode.

The following table outlines the parameters for this command:

Table 34
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 using NNCLI

The Ethernet Routing Switch 5000 Series 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 28).

This section provides information about configuring the following features:

- Single Host with Single Authentication (SHSA) and Guest VLAN (see “Configuring guest VLANs” (page 109))
- Multiple Host with Multiple Authentication (MHMA) (see “Configuring multihost support” (page 110))
- Non-EAPOL hosts on EAPOL-enabled ports (see “Configuring support for non-EAPOL hosts on EAPOL-enabled ports” (page 119))
- Multiple Host with Single Authentication (MHSA) (see “Configuring MHSA” (page 128))

SHSA is the default configuration.

Configuring guest VLANs

Configure guest VLAN support by following this procedure:

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.

Table 35
eapol guest-vlan parameters

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

The **eapol guest-vlan** command executes in the Global Configuration 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 executes in the Global Configuration 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 executes in the Global Configuration mode.

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

Configuring multihost support

Configure multihost support by following this procedure:

1. Enable multihost support for the interface. The relevant command executes 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}] [use-most-recent-radius-vlan] }
```

The following table outlines the parameters for this command.

Table 36
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.

Table 36
eapol multihost parameters (cont'd.)

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.
use-most-recent-radius-vlan	Enables the use of the most recent RADIUS VLAN.

no eapol multihost command

The `no eapol multihost` command disables EAPOL multihost. This command executes 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-m
hsa-enable] [non-eap-phone-enable] [use-radius-assigned-vlan]
[eap-packet-mode] [use-most-recent-radius-vlan]
```

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.

Table 37
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.

Table 37
no eapol multihost parameters (cont'd.)

Parameter	Description
eap-packet-mode	Disables the EAP packet mode request feature.
use-most-recent-radius-vlan	Disables the use of the most recent RADIUS VLAN.

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] [use-most-recent-radius-vlan]
```

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.

Table 38
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.

Table 38
default eapol multihost parameters (cont'd.)

Parameter	Description
eap-packet-mode	Resets the EAP packet mode to the default (multicast).
use-most-recent-radius-vlan	Disables the use of the most recent RADIUS VLAN.

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 executes 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]
[use-most-recent-radius-vlan]
```

Table 39
no eapol multihost command parameters

Variable	Description
<portlist>	Specifies 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.

Table 39
no eapol multihost command parameters (cont'd.)

enable	Disables eapol on the desired port.
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.
use-most-recent-radius-vlan	Disables the use of the most recent RADIUS 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 executes 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 executes in the Interface Configuration mode.

eapol multihost use radius-assigned-vlan command

Enable RADIUS-assigned VLAN use in the MHMA mode by using the following command in the Global Configuration mode:

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

The following table outlines the parameters for this command:

Table 40
eapol multihost [use-radius-assigned-vlan] parameters

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

Enable RADIUS-assigned VLAN use in the MHMA mode for the desired interface by using the following command:

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

The following table outlines the parameters for this command:

Table 41
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

Globally disable RADIUS-assigned VLAN use in MHMA mode by using 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

Table 42
no eapol multihost [use-radius-assigned-vlan] parameters

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

Table 43
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.

Disable RADIUS-assigned VLAN use in the MHMA mode for the desired interface by using 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

Table 44
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.

Table 45
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.

Configuring last assigned VLAN

This section describes the procedures for the configuration of 802.1X non-EAP last assigned VLAN using NNCLI.

eap multihost use-most-recent-radius-vlan command

Enable the most recent RADIUS VLAN by using the following command in the Global Configuration mode:

```
eap multihost use-most-recent-radius-vlan
```

The following table defines variable parameters that you enter with the **`eap multihost use-most-recent-radius-vlan`** command.

Variable	Value
use-most-recent-radius-vlan	Allows the use of most recent RADIUS VLAN.

no eap multihost use-most-recent-radius-vlan command

Disable the use of most recent RADIUS VLAN by using the following command in the Global Configuration mode:

```
no eap multihost use-most-recent-radius-vlan
```

The following table defines variable parameters that you enter with the **`no eap multihost use-most-recent-radius-vlan`** command.

Variable	Value
use-most-recent-radius-vlan	Disables the use of most recent RADIUS VLAN.

default eap multihost use-most-recent-radius-vlan command

Restore the default EAPol multihost settings by using the following command:

```
default eap multihost use-most-recent-radius-vlan
```

The following table defines variable parameters that you enter with the **`default eap multihost use-most-recent-radius-vlan`** command.

Variable	Value
use-most-recent-radius-vlan	Disables the use of most recent RADIUS VLAN.

Selecting the packet mode for EAP requests

With EAP support, 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. With Release 5.1 and later, you can select the packet mode. This feature prevents repeated EAP responses from an EAP-capable device that is already authenticated.

Globally select the packet mode for EAP requests by using the following command:

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

The following table outlines the parameters for this command

Table 46
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.

Select the packet mode on the desired interface or on specific ports by using the following command:

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

The following table outlines the parameters for this command

Table 47
eapol multihost [eap-packet-mode {multicast | unicast}] parameters: Interface mode

Parameter	Description
<portlist>	Specifies 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.

Globally disable the selection of packet mode by using one of the following command:

```
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

Table 48
no eapol multihost [eap-packet-mode {multicast | unicast}] parameters

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

Table 49
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.

Disable the selection of packet mode on the desired interface by using one of the following command:

```
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

Table 50
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.

Table 51
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

Configure support for non-EAPOL hosts on EAPOL-enabled ports by doing the following:

1. Ensure that

   a. EAPOL is enabled globally and locally (for the desired interface ports) (see "Configuring Extensible Authentication Protocol security using NNCLI" (page 102))
   b. the desired ports have been enabled for multihost mode (see "Configuring multihost support" (page 110))
   c. guest VLAN is disabled locally (for the desired interface ports) (see "Configuring guest VLANs" (page 109))

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 120))
   b. RADIUS authentication (see "Enabling RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports" (page 121))
3. Specify the maximum number of non-EAPOL MAC addresses allowed on a port (see "Specifying the maximum number of non-EAPOL hosts allowed" (page 122)).
4. 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 123)).

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.

Enable local authentication of non-EAPOL hosts globally on the switch by using the following command in Global Configuration mode

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

Enable local authentication of non-EAPOL hosts for a specific port or for all ports on an interface by using 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.
```

Discontinue local authentication of non-EAPOL hosts on EAPOL-enabled ports by using 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.

Enable RADIUS authentication of non-EAPOL hosts globally on the switch by using the following command in Global Configuration mode:

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

The following table outlines the parameters for this command

Table 52
eapol multihost radius-non-eap-enable command

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

Enable RADIUS authentication of non-EAPOL hosts for a specific port or for all ports on an interface by using the following command in Interface Configuration mode:

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

The following table outlines the parameters for this command:

Table 53
eapol multihost radius-non-eap-enable command: Interface mode

Parameter	Description
<portlist>	Specifies 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 feature 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

Configure the format of the RADIUS password when authenticating non-EAP MAC addresses using RADIUS by using 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

Table 54
eapol multihost non-eap-pwd-fmt parameters

Parameter	Description
<ip-addr>	Specifies the IP address of the non-EAP client.
<mac-addr>	Specifies the MAC address of the non-EAP client.
<port-number>	Specifies 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

Configure the maximum number of non-EAPOL hosts allowed for a specific port or for all ports on an interface by using 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.

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

Creating the allowed non-EAPOL MAC address list

Specify the MAC addresses of non-EAPOL hosts allowed on a specific port or on all ports on an interface, for local authentication by using 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 124))
- port settings (see “Viewing port settings for non-EAPOL hosts” (page 124))
- allowed MAC addresses, for local authentication (see “Viewing allowed MAC addresses” (page 124))
- current non-EAPOL hosts active on the switch (see “Viewing current non-EAPOL host activity” (page 124))
- status in the Privilege Exec mode (see “show eapol multihost status command” (page 104)).

Viewing global settings for non-EAPOL hosts View global settings for non-EAPOL hosts on EAPOL-enabled ports by using 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 View non-EAPOL support settings for each port by using 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 View the MAC addresses of non-EAPOL hosts allowed to access ports on an interface by using 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 View information about non-EAPOL hosts currently active on the switch by using 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. Enable Nortel IP Phone clients on an EAP-enabled port by doing the following:

1. Ensure that
   - EAP is enabled globally and locally (on the desired interface ports). (For more information, see "Configuring Extensible Authentication Protocol security using NNCLI" (page 102)).
   - Multihost is enabled on the desired ports. (For more information, see "Configuring multihost support" (page 110)).
   - NonEAP is enabled globally and locally (on the desired interface ports). (For more information, see "Configuring support for non-EAPOL hosts on EAPOL-enabled ports" (page 119)).
   - 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. (For more information, see "Globally enabling Nortel IP Phone clients as a non-EAP type" (page 126)).
3. Enable Nortel IP Phone clients locally or for specific ports on the interface. (For more information, see "Enabling Nortel IP Phone clients in the interface mode" (page 127)).
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

Globally enable Nortel IP Phone clients as a non-EAP type by using the following command in the Global Configuration mode:

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

The following table outlines the parameters for this command:

Table 55
eapol multihost non-eap-phone-enable parameters

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

Globally disable Nortel IP Phone clients as a non-EAP type by using 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:

Table 56
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.

Table 57
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

Enable Nortel IP Phone clients in the interface mode by using the following command:

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

Table 58
eapol multihost non-eap-phone-enable parameters: Interface mode

Parameter	Description
<portlist>	Specifies 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.

Disable Nortel IP Phone clients in the interface mode by using one of the following commands:

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

or

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

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

Table 59
no eapol multihost non-eap-phone-enable parameters: Interface mode

Parameter	Description
<portlist>	Specifies 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.

Table 60
default eapol multihost non-eap-phone-enable parameters: Interface mode

Parameter	Description
<portlist>	Specifies 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

Configure MHSA support by doing the following:

1. Ensure that
   a. EAP is enabled globally and locally (for the desired interface ports) (For more information, see “Configuring Extensible Authentication Protocol security using NNCLI” (page 102))
   b. The desired ports are enabled for Multihost (For more information, see “Configuring multihost support” (page 110))
   c. The guest VLAN is disabled locally (for the desired interface ports) (For more information, see “Configuring guest VLANs” (page 109))
2. Enable MHSA globally on the switch (For more information, see “Globally enabling support for MHSA” (page 129)).
3. Configure MHSA settings for the interface or for specific ports on the interface (For more information, see “Configuring interface and port settings for MHSA” (page 129)):
   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

Enable support for MHSA globally on the switch by using 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

Configure MHSA settings for a specific port or for all ports on an interface by using 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. Disable MHSA by using 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. **ATTENTION** The configurable maximum number of non-EAPOL clients for each port is 32, but Nortel expects that the usual maximum allowed for each port is lower. Nortel expects that the combined maximum is approximately 200 for each box and 800 for a stack.

Viewing MHSA settings and activity

For more information about the commands to view MHSA settings and non-EAPOL host activity, see "Viewing non-EAPOL host settings and activity" (page 123).

802.1X dynamic authorization extension configuration

This feature provides functionality for third-party devices to dynamically change VLANs and close user sessions. For more information on this feature see "802.1X dynamic authorization extension" (page 42).

802.1X dynamic authorization extension configuration navigation

- "Configuring 802.1X dynamic authorization extension" (page 130)
- "Disabling 802.1X dynamic authorization extension" (page 131)
- "Viewing 802.1X dynamic authorization extension configuration" (page 132)
- "Viewing 802.1X dynamic authorization extension statistics" (page 133)
- "Enabling 802.1X dynamic authorization extension on EAP ports" (page 133)
- "Disabling 802.1X dynamic authorization extension on EAP ports" (page 134)
- "Enabling 802.1X dynamic authorization extension default on EAP ports" (page 135)

Configuring 802.1X dynamic authorization extension

Configure RADIUS dynamic authorization extension to allow a RADIUS server to send a Change of Authorization (CoA) or Disconnect command.

Prerequisites

- Enable EAP globally and on each applicable port.
- Enable the dynamic authorization extensions globally and on each applicable port.

  ATTENTION
  Disconnect or CoA commands are ignored if they are sent to a port this feature is not enabled on.

- Log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure RADIUS dynamic authorization extension by using the following command: `radius dynamic-server client A.B.C.D [secret] [port <1024-65535> ] [enable] [process-disconnect-requests] [process-change-of-auth-requests]`

--End--

Variable definitions

The following table defines parameters of the **radius dynamic-server** command.

Variable	Value
`<A.B.C.D>`	Adds a new RADIUS dynamic authorization client or changes the configuration of an existing RADIUS dynamic authorization client. <A.B.C.D.> is an IP address.
`enable`	Enables packet receiving from the RADIUS Dynamic Authorization Client.
`port`	Configures the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1024 to 65535.
`process-change-of-auth-requests`	Enables CoA request processing.
`process-disconnect-requests`	Enables Disconnect request processing.
`secret`	Configures the RADIUS Dynamic Authorization Client secret word.

Disabling 802.1X dynamic authorization extension

Disable RADIUS dynamic authorization extension to prevent a RADIUS server from sending a Change of Authorization or Disconnect command.

Procedure steps

Step	Action
1	Disable RADIUS dynamic authorization extension by using the following command: `no radius dynamic-server client <A.B.C.D.> enable`

--End--

Variable definitions

The following table defines parameters of the **`no radius dynamic-server`** command.

Variable	Value
`<A.B.C.D.>`	Adds a new RADIUS dynamic authorization client or changes the configuration of an existing RADIUS dynamic authorization client. <A.B.C.D.> is an IP address.

Viewing 802.1X dynamic authorization extension configuration

View RADIUS dynamic authorization client configuration to display and confirm the configuration of RADIUS dynamic authorization client parameters.

Prerequisites

- Log on to the Privileged EXEC mode in the NNCLI.

Procedure steps

Step	Action
1	View RADIUS dynamic authorization client configuration using the following command: `show radius dynamic-server [client <A.B.C.D.>]`

--End--

Variable definitions

The following table defines the parameters of the **`show radius dynamic-server`** command.

Variable	Value
`<A.B.C.D.>`	Identifies the IP address of the RADIUS dynamic authorization client.

Viewing 802.1X dynamic authorization extension statistics

View RADIUS dynamic authorization client statistics to display RADIUS dynamic authorization client statistical information.

Prerequisites

- Log on to the Privileged EXEC mode in the NNCLI.

Procedure steps

Step	Action
1	View RADIUS dynamic authorization client configuration by using the following command: `show radius dynamic-server statistics client <A.B.C.D.>`

--End--

Variable definitions

The following table defines the parameters of the `show radius dynamic-server statistics` command.

Variable	Value
`<A.B.C.D.>`	Identifies the IP address of the RADIUS dynamic authorization client.

Enabling 802.1X dynamic authorization extension on EAP ports

Enable 802.1X dynamic authorization extension on EAP ports for the ports to process CoA and Disconnect requests from the RADIUS server.

Prerequisites

- Log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Enable 802.1X dynamic authorization extension on an EAP port by using the following command: `eapol radius-dynamic-server enable`
2	Enable 802.1X dynamic authorization extension on a specific EAP port or a list of EAP ports by using the following command: `eapol port <LINE> radius-dynamic-server enable`

--End--

Variable definitions

The following table defines the parameters of the `eapol port <LINE> radius-dynamic-server enable` command.

Variable	Value
`<LINE>`	Indicates an individual port or list of ports.

Disabling 802.1X dynamic authorization extension on EAP ports

Disable 802.1X dynamic authorization extension on EAP ports to discontinue the ports from processing CoA and Disconnect requests from the RADIUS server.

Prerequisites

- Log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Disable 802.1X dynamic authorization extension (RFC 3576) on an EAP port by using the following command: `no eapol radius-dynamic-server enable`
2	Disable 802.1X dynamic authorization extension (RFC 3576) on a specific EAP port or a list of EAP ports by using the following command: `no eapol port <LINE> radius-dynamic-server enable`

--End--

Variable definitions

The following table defines variable parameters that you enter with the **`no eapol port <LINE> radius-dynamic-server enable`** command.

Variable	Value
`<LINE>`	Indicates an individual port or list of ports.

Enabling 802.1X dynamic authorization extension default on EAP ports

Enable the 802.1X dynamic authorization extension default on EAP ports to return the ports to the default configuration for processing CoA and Disconnect requests from the RADIUS server.

Prerequisites

- Log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step **Action**

1 Enable 802.1X dynamic authorization extension (RFC 3576) default on an EAP port by using the following command:

```
default eapol radius-dynamic-server enable
```

2 Enable 802.1X dynamic authorization extension (RFC 3576) default on a specific EAP port or a list of EAP ports by using the following command:

```
default eapol port <LINE> radius-dynamic-server
enable
```

--End--

Variable definitions

The following table defines the parameters of the **`default eapol port <LINE> radius-dynamic-server enable`** command.

Variable	Value
`<LINE>`	Indicates an individual port or list of ports.

SNMP configuration using NNCLI

This section describes how you can configure SNMP using NNCLI, to monitor devices running software that supports the retrieval of SNMP information.

Configuring SNMP v1, v2c, v3 Parameters using NNCLI

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 Ethernet Routing Switch 5000 Series support for SNMPv3, you can configure SNMP using the new standards-based method of configuring SNMP communities, users, groups, views, and trap destinations.

ATTENTION
You must configure views and users using NNCLI before SNMPv3 can be used. For more information, see "Configuring SNMP using NNCLI" (page 137).

ATTENTION
You must have the secure version of the software image installed on your switch before you can configure SNMPv3.

The Ethernet Routing Switch 5000 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 Ethernet Routing Switch 5000 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 following list shows the number of nonvolatile entries (entries stored in NVRAM) allowed in the SNMPv3 tables. The system does not allow you to create more entries marked nonvolatile when you reach these limits:

- snmpCommunityTable: 20
- vacmViewTreeFamilyTable: 60
- vacmSecurityToGroupTable: 40
- vacmAccessTable: 40
- usmUserTable: 20
- snmpNotifyTable: 20
- snmpTargetAddrTabel: 20
- snmpTargetParamsTable: 20

Configuring SNMP using NNCLI

You can use the commands detailed in this section 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 executes in the Privileged EXEC command mode.

Table 61 "show snmp-server command parameters and variables" (page 138) describes the parameters and variables for the **`show snmp-server`** command.

Table 61
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 executes in the Global Configuration mode.

Table 62 "snmp-server authentication-trap command parameters and variables" (page 138) describes the parameters and variables for the snmp-server authentication-trap command.

Table 62
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 executes in the Global Configuration 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`** executes in the Global Configuration 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 executes in the Global Configuration mode.

Table 63 "snmp-server community for read/write command" (page 139) describes the parameters and variables for the **`snmp-server community`** for read/write command.

Table 63
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. If ro nor rw are not 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 executes in the Global Configuration mode.

Table 64 "snmp-server community command parameters and variables" (page 140) describes the parameters and variables for the **snmp-server community** command.

Table 64
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 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.

Table 65 "no snmp-server community command parameters and variables" (page 141) describes the parameters and variables for the no **`snmp-server community`** command.

Table 65
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 executes in the Global Configuration 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.

describes the parameters and variables for the **`default snmp-server community`** command.

Table 66
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 executes in the Global Configuration mode.

Table 67 "snmp-server contact command parameters and variables" (page 142) describes the parameters and variables for the **`snmp-server contact`** command.

Table 67
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 executes in the Global Configuration 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 executes in the Global Configuration 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 executes in the Global Configuration mode.

Table 68 "snmp-server command parameters and variables" (page 143) describes the parameters and variables for the **`snmp-server`** command.

Table 68
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 executes in the Global Configuration mode.

The **`no snmp-server`** command has no parameters or variables.

ATTENTION
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 SNMPv3 MIBs. Each can generate v1, v2c, or v3 traps.

> **ATTENTION**
> Before using the desired community string or user in this command, ensure that it is 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 executes in the Global Configuration mode.

Table 69 "snmp-server host command parameters and variables" (page 144) describes the parameters and variables for the **snmp-server host** command.

Table 69
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>	Enter a value for the SNMP trap port between 1 and 65535.

Table 69
snmp-server host command parameters and variables (cont'd.)

Parameters and variables	Description
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.
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.

show snmp-server host command

The **`show snmp-server host`** command displays the current SNMP host information including the configured trap port.

The syntax for the **`show snmp-server host command`** is

```
show snmp-server host
```

The show snmp-server host executes in the Privileged EXEC mode.

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, a 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|<co
mmunity-string>}
```

The **no snmp-server host** command executes in the Global Configuration mode.

If you do not specify any parameters, this command deletes all trap destinations from the s5AgTrpRcvrTable and from SNMPv3 tables.

Table 70 "no snmp-server host command parameters and variables" (page 146) describes the parameters and variables for the **no snmp-server host** command.

Table 70
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, all hosts are cleared, proprietary and standards-based. 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 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 mode.

Table 71 "snmp-server location command parameters and variables" (page 147) describes the parameters and variables for the **snmp-server location** command.

Table 71
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 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 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 mode.

Table 72 "snmp-server name command parameters and variables" (page 148) describes the parameters and variables for the **snmp-server name** command.

Table 72
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 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 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 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.

Table 73 "snmp-server user parameters" (page 150) describes the parameters and variables for the `snmp-server user` command.

Table 73
snmp-server user parameters

Parameters	Description
username	Specifies the user name. Enter an alphanumeric string of up to 255 characters.
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 nonalphanumeric 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 nonalphanumeric 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.

> **ATTENTION**
> 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 mode.

> **ATTENTION**
> If you do not specify any parameters, this command deletes all snmpv3 users from the SNMPv3 tables.

Table 74 "no snmp-server user command parameters and variables" (page 151) describes the parameters and variables for the **`no snmp-server user`** command.

Table 74
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 mode.

Table 75 "snmp-server view command parameters and variables" (page 152) describes the parameters and variables for the **`snmp-server view`** command.

Table 75
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 • +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, the set of MIB objects accessible using this view. 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 mode.

Table 76 "no snmp-server view command parameters and variables" (page 153) describes the parameters and variables for the **no snmp-server view** command.

Table 76
no snmp-server view command parameters and variables

Parameters and variables	Description
viewname	Specifies the name of the view to be removed. This is not an optional parameter.

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.

> **ATTENTION**
> 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 mode.

Table 77 "snmp-server bootstrap command parameters and variables" (page 153) describes the parameters and variables for the **`snmp-server bootstrap`** command.

Table 77
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. **ATTENTION** In this configuration, view restricted matches view internet.

Table 77
snmp-server bootstrap command parameters and variables (cont'd.)

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. **ATTENTION** In this configuration, restricted contains a smaller subset of views than internet view. The subsets are defined according to RFC 3515 Appendix A.
<very-secure>	Specifies a maximum security configuration that allows no access to the users.

show snmp-server notification-control

The **`show snmp-server notification-control`** command shows the current state of the applicable notifications.

The syntax for the **`show snmp-server notification-control`** command is

```
show snmp-server notification-control
```

The **`show snmp-server notification-control`** command executes in Privileged EXEC mode.

snmp-server notification-control command

The **`snmp-server notification-control`** command enables the notification identified by the command parameter. The notification options are:

- DHCP Snooping: bsDhcpSnoopingBindingTableFull, bsDhcpSnoopingTrap
- Dynamic ARP Inspection: bsaiArpPacketDroppedOnUntrustedPort
- IP Source Guard: bsSourceGuardReachedMaxIpEntries, bsSourceGuardCannotEnablePort

The syntax for the **`snmp-server notification-control`** command is

```
snmp-server notification-control <WORD/1-128>
```

The **`snmp-server notification-control`** command executes in Global Configuration mode.

Table 78 "snmp-server notification-control command parameters and variables" (page 155)describes the parameters and variables for the `snmp-server notification-control` command.

Table 78
snmp-server notification-control command parameters and variables

Parameters and variables	Description
<WORD/1-128>	Can either be the English description or the OID of a supported notification type.

no snmp-server notification-control

The `no snmp-server notification-control` command disables the notification identified by the command parameter. The notification options are:

- DHCP Snooping: bsDhcpSnoopingBindingTableFull, bsDhcpSnoopingTrap
- Dynamic ARP Inspection: bsaiArpPacketDroppedOnUntrustedPort
- IP Source Guard: bsSourceGuardReachedMaxIpEntries, bsSourceGuardCannotEnablePort

The syntax for the `no snmp-server notification-control` command is

```
no snmp-server notification-control <WORD/1-128>
```

The `no snmp-server notification-control` command executes in Global Configuration mode.

Table 79 "no snmp-server notification-control command parameters and variables" (page 155)describes the parameters and variables for the `no snmp-server notification-control` command.

Table 79
no snmp-server notification-control command parameters and variables

Parameters and variables	Description
<WORD/1-128>	Can either be the English description or the OID of a supported notification type.

default snmp-server notification-control

The **`default snmp-server notification-control`** command returns the notification identified by the command parameter to its default state.

The syntax for the default snmp-server notification-control command is

```
default snmp-server notification-control <WORD/1-128>
```

The **`default snmp-server notification-control`** command executes in Global Configuration mode.

Table 80 " default snmp-server notification-control command parameters and variables" (page 156)describes the parameters and variables for the **`default snmp-server notification-control`** command.

Table 80
default snmp-server notification-control command parameters and variables

Parameters and variables	Description
<WORD/1-128>	Can either be the English description or the OID of a supported notification type.

spanning-tree rstp traps command

The RSTP traps feature provides notifications for the following events:

- RSTP instance up/down (not applicable at this time since Baystack products do not support runtime spanning-tree operation mode to be changed)
- RSTP core memory allocation error
- RSTP core buffer allocation error
- New root bridge
- Port protocol migration

The default settings of RSTP traps are enabled. The events are notified as SNMP traps and as system log messages.

The following messages for the RSTP traps will be logged into the system log:

- Trap: RSTP General Event (Up/Down)
- Trap: RSTP Error Event (Mem Fail / Buff Fail)
- Trap: RSTP New Root tt:tt:tt:tt:tt:tt:tt:tt

- Trap: RSTP Topology Change
- Trap: RSTP Protocol Migration Type: Send (RSTP/STP) for Port: t

If the traps are not received on the traps receiver host (should be configured) but the traps are logged into the system log, the network connectivity should be checked.

The **spanning-tree rstp traps command** enables RSTP traps.

The syntax for the **spanning-tree rstp traps** command is

```
spanning-tree rstp traps
```

The **spanning-tree rstp traps** command executes in the Global Configuration mode.

no spanning-tree rstp traps command

The **no spanning-tree rstp traps** command disables RSTP traps.

The syntax for the **no spanning-tree rstp traps** is

```
no spanning-tree rstp traps
```

The **no spanning-tree rstp traps** command executes in the Global Configuration mode.

default spanning-tree rstp traps command

The **default spanning-tree rstp traps** command returns RSTP traps to their default state.

The syntax for the **default spanning-tree rstp traps** is

```
default spanning-tree rstp traps
```

The **default spanning-tree rstp traps** command executes in the Global Configuration mode.

show spanning-tree rstp traps config conmmand

The **show spanning-tree rstp traps config** command shows the current state of the RSTP trap.

The syntax for the **show spanning-tree rstp traps config** command is

```
show spanning-tree rstp traps config
```

The **show spanning-tree rstp traps config** command executes in the Privileged EXEC mode.

Configuring RADIUS accounting using NNCLI

RADIUS accounting utilizes the same network server settings used for RADIUS authentication. For more information about the commands to configure the RADIUS server settings for the Ethernet Routing Switch 5000 Series, see "Configuring RADIUS server settings" (page 100).

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 101).

Configuring TACACS+ using NNCLI

For more information about the function and operation of TACACS+ in a Ethernet Routing Switch 5000 Series network, see "TACACS+" (page 44).

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

1. Configure the TACACS+ server itself. For more information, see the vendor documentation for your server for specific configuration procedures. For sample configurations, see "TACACS+ server configuration examples" (page 317).
2. Configure TACACS+ server settings on the switch (see "Configuring TACACS+ server settings" (page 159)).
3. Enable TACACS+ services over serial or Telnet connections (see "Enabling remote TACACS+ services" (page 160).

4. Enable TACACS+ authorization and specify privilege levels (see "Enabling TACACS+ authorization" (page 160)).

5. Enable TACACS+ accounting (see "Enabling TACACS+ accounting" (page 161)).

> **ATTENTION**
> You can enable TACACS+ authorization without enabling TACACS+ accounting, and you can enable TACACS+ accounting without enabling TACACS+ authorization.

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. **ATTENTION** 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 more information about configuring the primary TACACS+ server and shared secret, see "Configuring TACACS+ server settings" (page 159).

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 using NNCLI

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, SSH, or HTTP access, use the following command in Global Configuration mode:

ipmgr {telnet|snmp|web|ssh}

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 Web-based management system
ssh enables the IP Manager list check for SSH access

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> <Ipv4addr> [mask <mask>] for Ipv4 entries with list ID between 1-50.

ipmgr source-ip <list ID> <Ipv6addr/prefix> for Ipv6 entries with list ID between 51-100.

where

<list ID> is an integer in the range 1-50 for Ipv4 entries and 51-100 for Ipv6 entries 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
<Ipv4addr>	Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation.
<Ipv6addr/prefix>	Specifies the source IPv6 address and prefix from which access is allowed.
[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 for Ipv4 addresses and range 51-100 for Ipv6 addresses, 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 for Ipv4 entries, and to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 for Ipv6 entries. 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, SSH, and Web access are enabled
- whether the IP Manager list is being used to control access to Telnet, SNMP, SSH, and Web-based management system
- the current IP Manager list configuration

Configuring password security using NNCLI

The NNCLI 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.

Navigation

Enabling password security

The **password security** command enables the Password Security feature on the Ethernet Routing Switch 5000 Series.

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

```
password security
```

Disabling password security

The **no password security** command disables the Password Security feature on the Ethernet Routing Switch 5000 Series.

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

```
no password security
```

Creating user names and passwords

Use the **username** command to create custom user names and assign switch and stack read-only and read-write passwords to them. These custom user names apply to local authentication only.

The syntax of this command is as follows:

```
username <user_name> {switch | stack} {ro | rw}
```

After entering this command the user is prompted to enter the password for the new user. For more information about rules regarding password length and composition, see "Password length and valid characters" (page 52).

Custom users cannot have custom access rights and limitations. Use of the associated read-only password confers the same rights and limitations as the default read-only user. Use of the associated read-write password confers the same rights and limitation as the default read-write user. For more information on these default users, see “Default password and default password security” (page 53) and Table 4 "Summary of password security features and requirements" (page 54).

Configuring password retry attempts

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 to 100 that specifies the allowed number of failed log on attempts. The default is 3.

Configuring password history

Use the **password password-history** command to configure the number of passwords stored in the password history table. This command has the following syntax:

```
password password-history <3-10>
```

The parameter **<3-10>** represents the number of passwords to store in the history table. Use the appropriate value when configuring the feature.

Defaulting password history

Use the **default password password-history** command to return the number of passwords stored in the password history table to the default value of 3.

Displaying password history settings

The **show password password-history** command is used to display the number of passwords currently stored in the password history table.

Displaying NNCLI Audit log using NNCLI

The NNCLI audit provides a means for tracking NNCLI 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.

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

Configuring Secure Socket Layer services using NNCLI

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

Table 81
SSL commands

Command	Description
[no] ssl	Enables or disables SSL. The Web server operates in a secure mode when SSL is enabled and in nonsecure 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 nonsecure connection is also closed and the nonsecure operation resumes.
show ssl	Shows the SSL server configuration and SSL server state. See Table 82 "Server state information" (page 166) 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.

Table 82
Server state information

Field	Description
WEB Server SSL secured	Shows whether the Web server is using an SSL connection.

Table 82
Server state information (cont'd.)

Field	Description
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 NNCLI 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 NNCLI user has deleted the certificate.

Configuring Secure Shell protocol using NNCLI

Secure Shell protocol is used to improve Telnet and provide a secure access to NNCLI interface. There are two versions of the SSH Protocol. The Ethernet Routing Switch 5000 Series SSH supports SSH2.

The following NNCLI 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}
```

Table 83 "show ssh parameters" (page 167) outlines the parameters for this command.

Table 83
show ssh parameters

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

Table 83
show ssh parameters (cont’d.)

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

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 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 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 [address] [<key-name>] [usb]
```

Table 84 "ssh download-auth-key parameters" (page 169) outlines the parameters for this command.

Table 84
ssh download-auth-key parameters

Parameter	Description
address	Specify the TFTP server IP address.
key-name	Specify the TFTP/USB file name.
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 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 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 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}
```

Table 85 "no ssh parameters" (page 170) outlines the parameters for this command.

Table 85
no ssh parameters

Parameter	Description
dsa-auth	Disable SSH DSA authentication.
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 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 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 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 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 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 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 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 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 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 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 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 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 mode.

Configuring DHCP snooping using NNCLI

For more information about the function and operation of DHCP snooping in a Ethernet Routing Switch 5000 Series network, see “DHCP snooping” (page 62).

To configure DHCP snooping, do the following:

1. Enable DHCP snooping globally (see “Enabling DHCP snooping globally” (page 173)).
2. Enable DHCP snooping on the VLANs (see “Enabling DHCP snooping on the VLANs” (page 173)).
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 174)).

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 the VLANs enabled and disabled 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:

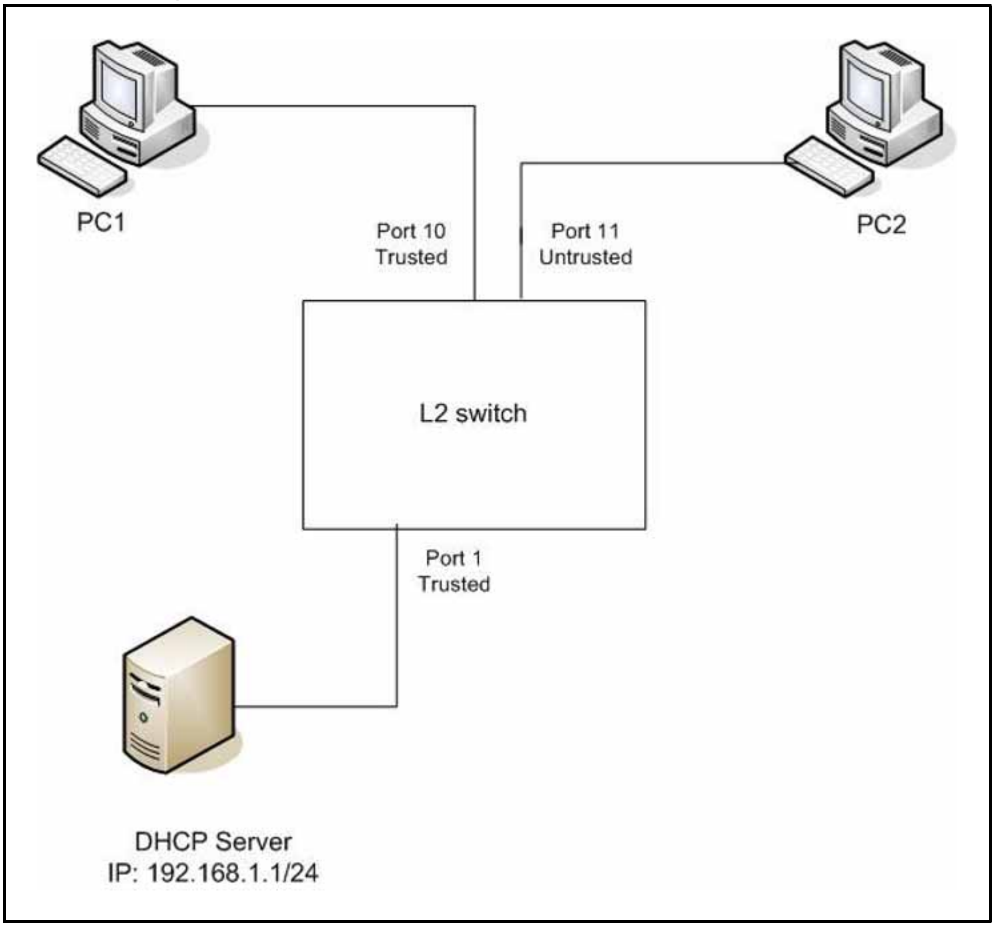
```
show ip dhcp-snooping binding
```

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

Figure 5 "Layer 2 configuration example" (page 176)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.

Figure 5
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 NNCLI 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) Time-to-Expiry  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
! ...
```

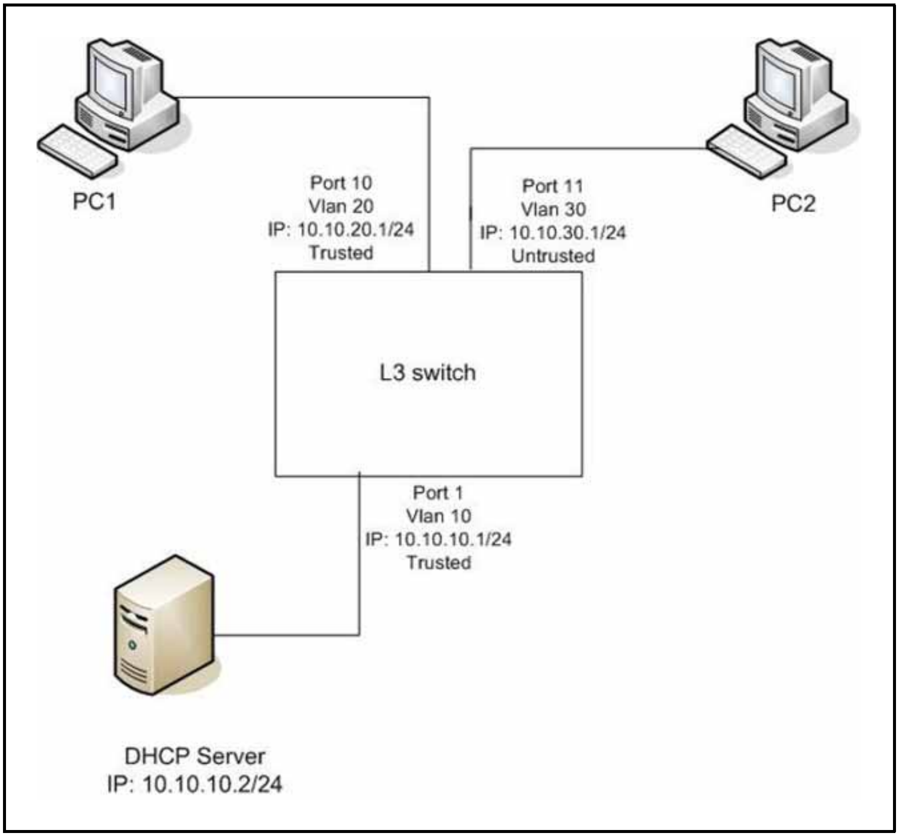
Renew the IP addresses for PC1 and PC2. Both PCs obtain IP addresses from the DHCP server. A DHCP binding entry for PC2 appears in the DHCP binding table . No binding entry for PC1 exists because port10 is DHCP Trusted.

```
(config)#show ip dhcp-snooping binding
MAC              IP           Lease (sec)   Time-to-Expiry   VID       Port
-------------------------------------------------------------------------
----------------------------------------------------
00-02-44-ab-2    10.10.30.2   86460          86580           1         11
d-f4
Total Entries:
1
```

DHCP snooping layer 3 configuration example

Figure 6 "Layer 3 configuration example" (page 179)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.

Figure 6
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.

Perform the following tasks to configure the preceding example:

Procedure steps

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 NNCLI commands required to configure DHCP snooping for this example.

```
>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

(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

(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 = v6.0.0.155
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 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 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 entry for PC1 exists because port10 is DHCP Trusted.

```
(config)#show ip dhcp-snooping binding
MAC                IP            Lease (sec)    Time-to-Expiry    VID    Port
--------------------------------------------------------------------------------
00-02-44-ab-2d-f4  10.10.30.2    86460          86580             30     11
Total Entries: 1
```

Configuring dynamic ARP inspection using NNCLI

For more information about the function and operation of dynamic Address Resolution Protocol (ARP) inspection in a Ethernet Routing Switch 5000 Series network, see "Dynamic ARP inspection" (page 64).

Configure dynamic ARP inspection by following this procedure.

Procedure steps

Step	Action
1	Enable dynamic ARP inspection on the VLANs (see "Enabling dynamic ARP inspection on the VLANs" (page 183)).
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 184)).

--End--

ATTENTION
For dynamic ARP inspection to function, DHCP snooping must be globally enabled. For more information about configuring DHCP snooping, see "Configuring DHCP snooping using NNCLI" (page 172).

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 the VLANs enabled and disabled 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 using NNCLI” (page 172) section and illustrated by the Figure 5 "Layer 2 configuration example" (page 176). 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.

ATTENTION

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 using NNCLI” (page 172) 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 entry 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 using NNCLI" (page 172)section and illustrated by the Figure 6 "Layer 3 configuration example" (page 179). 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/nonlocal/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 using NNCLI" (page 172) 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 using NNCLI

This section describes how you configure IP Source Guard using the Nortel Networks Command Line Interface (NNCLI).

ATTENTION
Nortel recommends that you do not enable IP Source Guard on trunk ports.

Prerequisites

- Ensure that dynamic Host Control Protocol (DHCP) snooping is globally enabled. (See "Enabling DHCP snooping globally" (page 173)).
- 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: bsSourceGuardConfigM ode

  This MIB 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 using NNCLI navigation

- “Enabling IP Source Guard using NNCLI” (page 192)
- “Viewing IP Source Guard port configuration information using NNCLI” (page 193)
- “Viewing IP Source Guard-allowed addresses using NNCLI” (page 194)
- “Disabling IP Source Guard using NNCLI” (page 194)

Enabling IP Source Guard using NNCLI

Enable IP Source Guard to add a higher level of security to the desired port by preventing IP spoofing by following this procedure.

Prerequisites

- Log on to the Ethernet, FastEthernet, or GigabitEthernet Interface Configuration mode in NNCLI.

> **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

The following table defines variables that you enter with the **`ip verify source [interface {[<interface type>] [<interface id>]}`** command.

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 configuration information using NNCLI

View IP Source Guard port configuration information to display IP Source Guard configuration settings for interfaces .

Prerequisites

- Log on to the Privileged Exec mode in NNCLI.

Procedure steps

Step Action

1 View IP Source Guard port configuration information by using the following command:

```
show ip verify source [interface {[ <interface type>]
[<interface id>]}
```

--End--

Variable definitions

The following table defines variables that you enter with the **`show ip verify source [interface {[ <interface type>] [<interface id>]}`** command.

Variable	Value
<interface id>	Identifies the ID of the interface for which you want to view IP Source Guard information.
<interface type>	Identifies the interface for which you want to view IP Source Guard information.

Viewing IP Source Guard-allowed addresses using NNCLI

View IP Source Guard-allowed addresses to display a single IP address or a group of IP addresses that IP Source Guard allowed.

Prerequisites

- Log on to the Privileged Exec mode in NNCLI.

Procedure steps

Step	Action
1	View IP Source Guard-allowed addresses by using the following command:

```
show ip source binding [<A.B.C.D.>] [interface
{[<interface type>] [<interface id>]}]
```

--End--

Variable definitions

The following table defines variables that you enter with the `show ip source binding [<A.B.C.D.>] [interface {[<interface type>] [<interface id>]}]` command.

Variable	Value
<A.B.C.D>	Identifies the IP address or group of addresses that IP Source Guard allowed.
<interface id>	Identifies the ID of the interface for which you want IP Source Guard-allowed addresses displayed.
<interface type>	Identifies the type of interface for which you want IP Source Guard-allowed addresses displayed.

Disabling IP Source Guard using NNCLI

Disable IP Source Guard to allow all IP traffic to go through without being filtered.

Prerequisites

- Log on to the Ethernet, FastEthernet, or GigabitEthernet Interface Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Disable IP Source Guard by using the following command:

```
no ip verify source interface {[<interface type>]
[<interface id>]}
```

--End--

Variable definitions

The following table defines variables that you enter with the **`no ip verify source interface {[<interface type>] [<interface id>]}`** command.

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 5000 Series using the Web-based management interface.

Configuring and managing security using the Web-based management interface navigation

Setting user access limitations using the Web-based management interface

For a complete explanation of the configuration and management of user access limitations using Web-based Management interface, see the *Nortel Ethernet Routing Switch 5000 Series Overview — System Configuration* () (NN47200-500).

Configuring EAPOL-based security using the Web-based management interface

Use the following procedure to configure and manage the Extensible Authentication Protocol over LAN (EAPOL) security with Web-based Management interface.

Prerequisite: Ensure that IP Source Guard is not enabled. (IP Source Guard and EAPOL are mutually exclusive).

Configure EAPOL-based security by following this procedure:

Procedure steps

Step	Action
1	Open the **EAPOL Security Configuration** window by choosing **Applications, EAPOL Security** from the menu.
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 **Submit** 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 appear in the **EAPOL Security Setting** section. Links to those ports not listed are provided at the bottom of the screen.
5	Click **Submit** under the **EAPOL Security Setting** section.

--End--

Variable definitions

Use the data in the following table to configure EAPOL-based security.

Variable	Value
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 the EAPOL state of this port to be initialized.

Variable	Value
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.
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.

SNMP configuration using the Web-based management interface

This section describes how you can configure SNMP using Web-based management, to monitor devices running software that supports the retrieval of SNMP information.

SNMP configuration using the Web-based management interface navigation

SNMP v1, v2c, v3 parameter configuration using the Web-based management interface

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 Ethernet Routing Switch 5000 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 Ethernet Routing Switch 5000 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 Ethernet Routing Switch 5000 Series software supports MD5 and SHA authentication, and AES, DES, and 3DES 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 using the Web-based management interface

The number of nonvolatile 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 nonvolatile when you reach these limits:

- snmpCommunityTable: 20
- vacmViewTreeFamilyTable: 60
- vacmSecurityToGroupTable: 40
- vacmAccessTable: 40
- usmUserTable: 20
- snmpNotifyTable: 20
- snmpTargetAddrTabel: 20
- snmpTargetParamsTable: 20

Configuring SNMPv1 using the Web-based management interface

You can configure SNMPv1 read-write and read-only community strings, enable or disable trap mode settings or the Autotopology feature or both. The Autotopology feature, when enabled, performs a process that recognizes device on the managed network and defines and maps its relation to other network devices in real time.

Configure the community string, trap mode, and Autotopology settings and features by following this procedure:

Procedure steps

Step	Action
1	Open the **SNMPv1** screen by choosing **Configuration, SNMPv1** from the menu.
2	Type information in the boxes, or select from a list.
3	Click **Submit** in section to save the changes.

--End--

Variable definitions

Use the data in the following table to configure SNMPv1.

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.

Section	Item	Range	Description
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.

SNMPv3 configuration using the Web-based management interface

This section describes the steps to build and manage SNMPv3 in Web-based management user interface.

Prerequisites

- You must configure views and users using NNCLI before SNMPv3 can be used. For more information, see “Configuring SNMP using NNCLI” (page 137).
- Ensure you have the secure version of the software image installed on your switch.

SNMPv3 configuration using the Web-based management interface navigation

- “Viewing SNMPv3 system information using the Web-based management interface” (page 204)
- “User access to SNMPv3 configuration using the Web-based management interface” (page 205)
- “SNMPv3 system user group membership configuration using the Web-based management interface” (page 208)
- “SNMPv3 group access rights configuration using the Web-based management interface ” (page 210)
- “SNMPv3 management information view configuration using the Web-based management interface” (page 212)
- “SNMPv3 system notification entry configuration using the Web-based management interface” (page 214)
- “SNMPv3 management target address configuration using the Web-based management interface” (page 216)
- “SNMPv3 management target parameter configuration using the Web-based management interface” (page 219)

Viewing SNMPv3 system information using the Web-based management interface

You can view information about the SNMPv3 engine that exists and the private protocols supported in the network configuration. You can also view information about packets received by the system having particular errors, such as unavailable contexts, unknown contexts, decrypting errors, or unknown user names.

View SNMPv3 system information by following this procedure:

Procedure steps

Step	Action
1	Open the **System Information** screen by choosing **Configuration, SNMPv3, System Information** from the menu.

--End--

Variable definitions Use the data in the following table to view and understand the System Information section of the SNMPv3 System Information screen.

Variable	Value
SNMP Engine ID	Specifies the SNMP engine identification number.
SNMP Engine Boots	Specifies the number of times that the SNMP engine has reinitialized itself since its initial configuration.
SNMP Engine Time	Specifies the number of seconds since the SNMP engine last incremented the snmpEngineBoots object.
SNMP Engine Maximum Message Size	Specifies 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	Specifies the SNMP dialect the engine recognizes. The dialects are: SNMPv1, SNMPv2C, and SNMPv3.

Variable	Value
Authentication Protocols Supported	Specifies 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	Specifies the registration point for standards-track privacy protocols used in SNMP Management Frameworks. The registration points are: DES, AES, 3DES, or None.

Use the data in the following table to view and understand the SNMPv3 Counters section of the SNMPv3 System Information screen.

Item	Description
Unavailable Contexts	Specifies the total number of packets dropped by the SNMP engine because the context contained in the message was unavailable.
Unknown Contexts	Specifies the total number of packets dropped by the SNMP engine because the context contained in the message was unknown.
Unsupported Security Levels	Specifies 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	Specifies the total number of packets dropped by the SNMP engine because they appeared outside of the window of authoritative SNMP engine.
Unknown User Names	Specifies the total number of packets dropped by the SNMP engine because they referenced an unknown user.
Unknown Engine IDs	Specifies the total number of packets dropped by the SNMP engine because they referenced an snmpEngineID that was not known to the SNMP engine.
Wrong Digest s	Specifies the total number of packets dropped by the SNMP engine because they did not contain the expected digest value.
Decryption Errors	Specifies the total number of packets dropped by the SNMP engine because they cannot be decrypted.

User access to SNMPv3 configuration using the Web-based management interface

You can view information about all current SNMPv3 user security parameters such as authentication/privacy protocols in use or create and delete SNMPv3 system user configurations.

Create an SNMPv3 system user configuration by following this procedure:

Procedure steps

Step	Action
1	Open the User Specification screen by choosing **Configuration, SNMPv3, User Specification** from the menu.
2	In the **User Specification Creation Table** section, **Action** column, type information in the boxes, or select from a list.
3	Click **Submit**. The new configuration appears in the User Specification Table.

--End--

Variable definitions Use the data in the following table to view and understand the User Specification Table section of the User Specification screen.

Variable and MIB association	Value
☒	Deletes the row.
User Name (usmUserSecurityName)	Specifies the name of an existing SNMPv3 user.
Authentication Protocol (usmUserAuthProtocol)	Indicates whether the message sent on behalf of this user to or 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 appears, information is dropped (lost) when you turn the power off. If Non-Volatile appears, information is saved in NVRAM when you turn the power off.

Use the data in the following table to create an SNMPv3 system user configuration.

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 or SHA protocols.
Authentication Passphrase (usmUserAuthPassword)	1..32	Type a string of character to create a password to use in conjunction with the authorization protocol.
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 eight 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 drops is dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

Deleting an SNMPv3 system user configuration using the Web-based management interface Delete an existing SNMPv3 user configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **User Specification** screen by choosing **Configuration, SNMPv3, User Specification** from the menu.
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--

SNMPv3 system user group membership configuration using the Web-based management interface

You can view information 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 using the Web-based management interface" (page 208)
- "Deleting an SNMPv3 group membership configuration using the Web-based management interface" (page 209)

Map an SNMPv3 system user to a group by following this procedure:

Procedure steps

Step	Action
1	Open the **Group Membership** screen by choosing **Configuration, SNMPv3, Group Membership** from the menu.
2	In the **Group Membership Creation** section, type information in the boxes, or select from a list.
3	Click **Submit**. The new entry appears in the **Group Membership Table**.

--End--

Variable definitions Use the data in the following table to map an SNMPv3 system user to a group.

Variable and MIB association	Range	Value
☒		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.
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.

Deleting an SNMPv3 group membership configuration using the Web-based management interface Delete an SNMPv3 group membership configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **Group Membership** screen by choosing **Configuration, SNMPv3, Group Membership** from the menu.
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**.

> **ATTENTION**
> This Group Membership Table section of the Group Membership page contains hyperlinks to the SNMPv3 User Specification and Group Access Rights screens.

--End--

SNMPv3 group access rights configuration using the Web-based management interface

You can view, create, or delete SNMPv3 group access right configurations using Web-based Management interface.

- “Creating an SNMPv3 group access rights configuration using the Web-based management interface” (page 210)
- “Deleting an SNMPv3 group access rights configuration using the Web-based management interface” (page 211)

Create SNMPv3 system-level access right configuration of a group by following this procedure:

Procedure steps

Step	Action
1	Open the **Group Access Rights** screen by choosing **Configuration, SNMPv3, Group Access Rights** from the menu.
2	In the **Group Access Creation** section, type information in the boxes, or select from a list.
3	Click **Submit**. The new entry appears in the **Group Access Table**.

--End--

Variable definitions Use the data in the following table to create SNMPv3 group access rights.

Variable and MIB association	Range	Value
☒	—	Deletes the row.

Variable and MIB association	Range	Value
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 (3) authPriv	Choose the minimum level of security required to gain the access rights allowed to the group. Only SSH images support authPriv level.
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.

Deleting an SNMPv3 group access rights configuration using the Web-based management interface Delete an SNMPv3 group access configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **Group Access Rights** screen by choosing **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**. **ATTENTION** This Group Access Table section of the Group Access Rights screen contains hyperlinks to the Management Information View screen.

--End--

SNMPv3 management information view configuration using the Web-based management interface

You can view a table of existing SNMPv3 management information view configurations, and create or delete SNMPv3 management information view configurations.

> **ATTENTION**
> 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 using the Web-based management interface" (page 212)
- "Deleting an SNMPv3 management information view configuration using the Web-based management interface" (page 214)

Create an SNMPv3 management information view configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **Management Info View** screen by choosing **Configuration, SNMPv3, Management Info View** from the menu.
2	In the **Management Information Creation** section, type information in the boxes, or select from a list.
3	Click **Submit**. The new entry appears in the **Management Information Table**.

--End--

Variable definitions Use the data in the following table to create an SNMPv3 management information view configuration.

Variable and MIB association	Range	Value
☒		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. **ATTENTION** 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

Variable and MIB association	Range	Value
		when you turn the power off.

Deleting an SNMPv3 management information view configuration using the Web-based management interface Delete an existing SNMPv3 management information view configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **Management Info View** screen by choosing **Configuration, SNMPv3, Management Info View** from the menu.
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--

SNMPv3 system notification entry configuration using the Web-based management interface

You can view, configure, and delete SNMPv3 system notification configurations and system notification types.

- "Creating an SNMPv3 system notification configuration using the Web-based management interface" (page 214)
- "Deleting an SNMPv3 system notification configuration using the Web-based management interface" (page 216)

Create an SNMPv3 system notification configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **Notification** screen by choosing **Configuration, SNMPv3, Notification** from the menu.

2 In the **Notification Creation** section, type information in the boxes, or select from a list.

3 Click **Submit**.

The new entry appears in the Notification Table section.

--End--

ATTENTION
This Notification Table section of the Notification screen contains hyperlinks to the Target Parameter screen.

Variable definitions Use the data in the following table to create an SNMPv3 system notification configuration.

Variable and MIB association	Range	Value
☒		Deletes the row.
Notify Name(snmpNotifyRowStatus)	1–32	Type a character string to identify the entry.
Notify Tag(snmpNotifyTag)	1–32	Type a value to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value equal to the value of an instance of this object is selected. If this object carries a zero length, no entries are selected.
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.

Deleting an SNMPv3 system notification configuration using the Web-based management interface Delete an SNMPv3 notification configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **Notification** screen by choosing **Configuration, SNMPv3, Notification** from the menu.
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--

SNMPv3 management target address configuration using the Web-based management interface

You can view, configure, and delete SNMPv3 management target configurations and management target address configurations.

- “Creating an SNMPv3 target address configuration using the Web-based management interface” (page 216)
- “Deleting an SNMPv3 target address configuration using the Web-based management interface” (page 218)

Create an SNMPv3 target address configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **Target Address** screen by choosing **Configuration, SNMPv3, Target Address** from the menu.
2	In the **Target Address Creation** section, type information in the boxes, or select from a list.
3	Click **Submit**. The new entry appears in the **Target Address Table**.

--End--

ATTENTION
This Target Address Table section of the Target Address screen contains hyperlinks to the Target Parameter screen.

Variable definitions Use the data in the following table to create an SNMPv3 target address configuration.

Variable and MIB association	Range	Value
☒		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.
Target Address (snmpTargetAddrTAddress)	XXX.XXX.XXX.XXX:XXX	Type a network address in this field. IPv4 and IPv6 are supported. For IPv4, use the format <IPv4_addr>:port. For IPv6, use the [<IPv6_addr>]:port format or the <IPv6_addr>:port format. The port number is an optional value. If you do not type a port number value, the switch automatically assigns a value of 162 for the port number. For example: 10.30.31.99:162
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.

Variable and MIB association	Range	Value
Target Retry Count (snmpTargetAddrRetryCount)	0–255	Type the default number of retries 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.

Deleting an SNMPv3 target address configuration using the Web-based management interface Delete an SNMPv3 target address configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **Target Address** screen by choosing **Configuration, SNMPv3, Target Address** from the menu.
2	In the **Target Address Table**, click the **Delete** icon for the entry you want to delete.

3	A message prompts for confirmation of the request. Click **OK**.

--End--

SNMPv3 management target parameter configuration using the Web-based management interface

SNMPv3 management target parameters are used during notification generation to specify the communication parameters used for exchanges with notification recipients.

You can view a table of existing SNMPv3 target parameter configurations, create SNMPv3 target parameters that associate notifications with particular recipients, and delete existing SNMPv3 target parameter configurations.

- "Creating an SNMPv3 target parameter configuration using the Web-based management interface" (page 219)
- "Deleting an SNMPv3 target parameter configuration using the Web-based management interface" (page 220)

Create an SNMPv3 target parameter configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **Target Parameter** screen by choosing **Configuration, SNMPv3, Target Parameter** from the menu.
2	In the **Target Parameter Creation** section, type information in the boxes, or select from a list.
3	Click **Submit**. The new entry appears in the Target Parameter Table.

--End--

Variable definitions Use the data in the following table to create an SNMPv3 target parameter configuration.

Variable	Range	Value
☒	—	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 (snmpTargetParamsSecurityName)	1–32	Type the principal on whose behalf SNMP messages are generated using this entry
Security Level (snmpTargetParamsSecurityLevel)	(1) noAuthNoPriv (2) authNoPriv (3) authPriv	Choose the level of security to be used when generating SNMP messages using this entry. AuthPriv is available only for compatible principal (Security Name) on SSH images.
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.

Deleting an SNMPv3 target parameter configuration using the Web-based management interface Delete an SNMPv3 target parameter configuration by following this procedure:

Procedure steps

Step	Action
1	Open the **Target Parameter** screen by choosing **Configuration, SNMPv3, Target Parameter** from the menu.
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--

SNMP trap receiver configuration using the Web-based management interface

You can view, configure, and delete SNMP trap receivers in Web-based Management interface.

The SNMP Trap Receiver Table is an alternative to using the SNMPv3 tables; Target, Notify and Parameter. Only SNMPv1 traps can be received with configurations performed on the SNMP trap receiver page.

IPv6 is not supported on the SNMP Trap receiver page. Use the SNMPv3 Target Table to specify an IPv6 network address.

SNMP trap receiver configuration using the Web-based management interface navigation

- “Creating an SNMP trap receiver configuration using the Web-based management interface” (page 221)
- “Deleting an SNMP trap receiver configuration using the Web-based management interface” (page 222)

Creating an SNMP trap receiver configuration using the Web-based management interface

Create an SNMP trap receiver configuration by following this procedure:

Procedure steps

Step	Action
1	Open the SNMP Trap Receiver screen by choosing **Configuration, SNMP Trap**.
2	In the **Trap Receiver Creation** section, type information in the boxes, or select from a list.
3	Click **Submit**. The new entry appears in the Trap Receiver Table.

--End--

Variable definitions Use the data in the following table to create an SNMP trap receiver configuration.

Variable	Range	Value
☒	—	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 traps. Only IPv4 is supported. For IPv6, use the SNMPv3 Target Table.
Community	0–32	Type the community string for the specified trap receiver.

Deleting an SNMP trap receiver configuration using the Web-based management interface

Delete SNMP trap receiver configurations by following this procedure:

Procedure steps

Step	Action
1	Open the **SNMP Trap Receiver** screen by choosing **Configuration, SNMP Trap**.
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--

MAC address-based security configuration using the Web-based management interface

The following sections outline how to configure and manage MAC Address-based security in Web-based Management interface.

MAC address-based security configuration using the Web-based management interface navigation

Configuring MAC Address-based security using the Web-based management interface

Configure the MAC Address-based security by following this procedure:

Procedure steps

Step	Action
1	Open the **Security Configuration** screen by choosing **Applications, MAC Address Security, Security Configuration** from the menu.
2	The **MAC Address Security Setting** section is used to configure the security settings. Use the fields in this section to perform initial configuration.
3	Click **Submit** 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** Clear ports from MAC Address security participation by following this procedure: • In the **Clear by Ports** row, click the icon in the **Action** column. This opens the Ports List View screen. Clear the ports to be removed from participation. • Click **Submit**. **b** Allow ports to learn MAC Addresses by following this procedure:

- In the **Learn by Ports** row, click the icon in the **Action** column. This opens the Ports List View screen. Select the ports that participates in MAC Address learning.
- Click **Submit**.

5 Set the state of port learning by choosing a value from the **Current Learning Mode** list.

6 Click the **Submit** under the **MAC Security Table** section.

--End--

Variable definitions

Use the data in the following table to configure the MAC Address-based security.

Variable	Value
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. The default value is Disabled.
Partition Time	Sets the time to partition a port on intrusion. **ATTENTION** Use this field only if the Partition Port on Intrusion Detected field is set to Enabled. There is no default for this field.

Variable	Value
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.

Enabling port security using the Web-based management interface

Enable MAC security on a port by following this procedure:

Procedure steps

Step	Action
1	Open the **Port Configuration** screen by choosing **Applications, MAC Address Security, Port Configuration** from the menu.
2	Select the options from the lists that enable the MAC security to be set for that port.
3	Click **Submit**.

--End--

Variable definitions

Use the data in the following table to enable MAC security on a port.

Variable	Value
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.

Configuring port Lists using the Web-based management interface

Add or delete ports in a list by following this procedure:

Procedure steps

Step	Action
1	Open the **Port Lists** screen by choosing **Applications, MAC Address Security, Port Lists** in the menu.
2	Click the icon in the **Action** column of the row containing the list to be edited.
3	A Port Lists screen appears. Select the ports to add to the list or cler those ports that are to be removed from the list.
4	Click **Submit**.

--End--

Adding MAC Addresses using the Web-based management interface

Add a MAC Address to the MAC Address-based security table by following this procedure:

Procedure steps

Step	Action
1	Open the **Security Table** screen by choosing **Applications, MAC Address Security, Security Table** from the menu.
2	In the **MAC Address Security Table Entry Creation** section, enter the MAC address information to enter in the table.
3	Click **Submit**.

--End--

Variable definitions

Use the data in the following table to add a MAC Address to the MAC Address-based security table.

Variable	Value
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.

Configuring DA MAC Filtering using the Web-based management interface

Drop all packets from a specified MAC destination address (DA) by performing this procedure:

Procedure steps

Step	Action
1	Open the **DA MAC Filtering** screen by choosing **Applications, MAC Address Security, DA MAC Filtering** from the menu.
2	Enter the MAC Address in the **DA MAC Address** field.
3	Click **Submit**.

--End--

Deleting MAC DAs using the Web-based management interface

Delete a MAC DA by following this procedure:

Procedure steps

Step	Action
1	Open the **DA MAC Filtering** screen by choosing **Applications, MAC Address Security, DA MAC Filtering** from the menu.
2	In the **Destination MAC Address Filtering Table**, click the **Delete** icon for the entry to be deleted. A message appears prompting you to confirm the request.
3	Click **Yes** to delete the MAC DA.

--End--

Configuring RADIUS security using the Web-based management interface

Configure and manage RADIUS-based security with Web-based Management interface by following this procedure.

Procedure steps

Step	Action
1	Open the **RADIUS** screen by choosing **Administration, Security, RADIUS** from the menu.

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.

3 Click **Submit** under the **RADIUS Authentication Setting** section.

--End--

Variable definitions

Use the data in the following table to configure and manage RADIUS-based security.

Variable	Value
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.

Configuring and managing security using Device Manager

This chapter describes the methods and procedures necessary to configure security on the Nortel Ethernet Routing Switch 5000 Series using Device Manager.

Navigation

EAPOL Configuration using Device Manager

This section describes how you can configure network access control on an internal Local Area Network (LAN) with Extensible Authentication Protocol over LAN (EAPOL), using Device Manager:

EAPOL Configuration using Device Manager navigation

- “Configuring EAPOL globally using Device Manager” (page 230)
- “Configuring port-based EAPOL using Device Manager” (page 231)
- “Configuring advanced port-based EAPOL using Device Manager” (page 234)
- “Viewing Multihost status information using Device Manager” (page 235)
- “Viewing Multihost session information using Device Manager” (page 236)
- “Allowed non-EAP MAC address list configuration using Device Manager” (page 237)
- “Graphing EAPOL statistics using Device Manager” (page 239)

Configuring EAPOL globally using Device Manager

Configure EAPOL globally to configure EAPOL parameters for the switch.

Procedure steps

Step	Action
1	Open the **Security** screen by choosing **Edit, Security, Security** from the menu.
2	Click the **EAPOL** tab.
3	In the fields provided, edit the EAPOL information.
4	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure EAPOL globally.

Variable	Value
SystemAuthControl	Enables or disables port access control on the switch.

Variable	Value
UserBasedPolicies Enabled	Enables or disables EAPOL user-based policies. For more information about user-based policies, see *Nortel Ethernet Routing Switch 5000 Series Configuration — Quality of Service* (NN47200-504).
UserBasedPoliciesFilterOnMac	Enables or disables the filter on MAC addresses for user-based policies.
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.
MultiHostAllowRadiusAssignedVlan	Enables or disables the use of RADIUS-assigned VLAN values in the Multihost mode.
MultiHostAllowNonEapRadiusAssignedVlan	Enables or disables the use of non-EAP RADIUS-assigned VLAN values in the Multihost mode.
MultiHostUseMostRecentRadiusAssignedVlan	Enables or disables the use of the most recent VLAN values assigned by the RADIUS server.
MultiHostEapPacketMode	Enables or disables the choice of packet mode (unicast or multicast) in the Multihost mode.
NonEapRadiusPasswordAttributeFormat	Enables or disables setting the format of the Remote Authentication Dial-In User Service (RADIUS) Server password attribute for non-EAP clients.
NonEapUserBasedPoliciesEnabled	Enables or disables non-EAP user-based policies.
NonEapUserBasedPoliciesFilterOnMac	Enables or disables the filter on MAC addresses for non-EAP user-based policies.

Configuring port-based EAPOL using Device Manager

Configure port-based EAPOL to configure EAPOL security parameters for an individual port or multiple ports.

Procedure steps

Step	Action
1	Select the port to edit from the **Device View**.
2	Select **Edit, Port** from the menu.
3	Click the **EAPOL** tab.
4	Click **Apply** after making changes.

--End--

Variable definitions

Use the data in the following table to configure port-based EAPOL.

Variable	Value
PortProtocolVersion	Specifies the EAP Protocol version running on this port.
PortCapabilities	Specifies the PAE functionality implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Initializes the port EAPOL state. **ATTENTION** Set this attribute to True to initialize the port EAPOL state.
PortReauthenticateNow	Reauthenticates the client. **ATTENTION** 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.

Variable	Value
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 reauthentications. The default is 3600 seconds. The time interval can be between 1 and 604800 seconds.
ReAuthenticationEnabled	Specifies if reauthentication is required. **ATTENTION** 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 KeyTranmissio nEnabled 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.

Configuring advanced port-based EAPOL using Device Manager

Configure advanced port-based EAPOL to configure advanced EAPOL security parameters for an individual port or multiple ports.

Procedure steps

Step	Action
1	Select the port to edit from the **Device View**.
2	Select **Edit, Port** from the menu.
3	Click the **EAPOL Advance** tab.
4	Click **Apply** after making changes.

--End--

Variable definitions

Use the data in the following table to configure advanced port-based EAPOL.

Variable	Value
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. **ATTENTION** 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.
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.

Variable	Value
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.
MultiHostNonEapAllowRadiusAssigned Vlan	Enables or disables support for non-EAP VLAN values assigned by the RADIUS server.
MultiHostUseMostRecentRadiusAssig nedVlan	Enables or disables the use of the most recent VLAN values assigned by the RADIUS server.
MultiHostEapPacketMode	Specifies the mode of EAPOL packet transmission (multicast or unicast).
ProcessRadiusRequestsServerPackets	Enables or disables the processing of RADIUS request server packets.

Viewing Multihost status information using Device Manager

View Multihost status information to display multiple host status for a port.

ATTENTION
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, you can select only one port.

Procedure steps

Step	Action
1	Select the port to edit from the **Device View**.
2	Select **Edit, Port** from the menu.
3	Click the **EAPOL Advance** tab.
4	Click **Multi Hosts** .

--End--

Variable definitions

Use the data in the following table to view Multihost status information.

Variable	Value
PortNumber	Specifies the port number in use.
ClientMACAddr	Specifies the MAC address of the client.
PaeState	Specifies the current state of the authenticator PAE state machine.
BackendAuthState	Specifies the current state of the backend authentication state machine.
Reauthenticate	Specifies the value used to reauthenticate the EAPOL client.

Viewing Multihost session information using Device Manager

View Multihost session information to display multiple host session information for a port.

> **ATTENTION**
> 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, you can select only one port.

Procedure steps

Step	Action
1	Select the port to edit from the **Device View**.
2	Select **Edit, Port** from the menu.
3	Click the **EAPOL Advance** tab.
4	Click the **Multi Hosts** tab.
5	Click **Multi Host Session**.

--End--

Variable definitions

Use the data in the following table to view Multihost session information.

Variable	Value
PortNumber	Specifies the port number in use.
ClientMACAddr	Specifies the MAC address of the client.
Id	Specifies a unique identifier for the session, in the form of a printable ASCII string of at least three characters.

Variable	Value
AuthenticMethod	Specifies the authentication method used to establish the session.
Time	Specifies the elapsed time of the session.
TerminateCause	Specifies the cause of the session termination.
UserName	Specifies the user name representing the identity of the supplicant PAE machine.

Allowed non-EAP MAC address list configuration using Device Manager

Configure the allowed non-EAP MAC address list to view and configure the list of MAC addresses for non-EAPOL clients authorized to access the port.

Allowed non-EAP MAC address list configuration using Device Manager navigation

- "Adding a MAC address to the allowed non-EAP MAC address list using Device Manager" (page 237)
- "Deleting a MAC address from the allowed non-EAP MAC address list using Device Manager" (page 238)
- "Viewing port non-EAP host support status using Device Manager" (page 238)

Adding a MAC address to the allowed non-EAP MAC address list using Device Manager

Add a MAC address to the allowed non-EAP MAC address list to insert a new MAC address to the list of MAC addresses for non-EAPOL clients authorized to access the port.

Procedure steps

Step	Action
1	Select the port to edit from the **Device View**.
2	Select **Edit, Port** from the menu.
3	Click the **EAPOL Advance** tab.
4	Click **Non-EAP MAC**.
5	Click **Insert**.
6	In the **ClientMACAddr** box, type a MAC address to add to the list of allowed non EAPOL clients.

7 Click **Insert**.

--End--

To delete a MAC address from the allowed non-EAP MAC address list, see "Deleting a MAC address from the allowed non-EAP MAC address list using Device Manager" (page 238)

Deleting a MAC address from the allowed non-EAP MAC address list using Device Manager

Procedure steps

Step	Action
1	Select the port to edit from the **Device View**.
2	Select **Edit, Port** from the menu.
3	Click the **EAPOL Advance** tab.
4	Click **Non-EAP MAC**.
5	In the **ClientMACAddr** box click the MAC address to delete.
6	Click **Delete**.
7	Click **Yes**.

--End--

Variable definitions Use the data in the following table to delete a MAC address from the allowed non-EAP MAC address list.

Variable	Value
PortNumber	Specifies the port number in use.
ClientMACAddr	Specifies the MAC address of the client.

Viewing port non-EAP host support status using Device Manager

View port non-EAP host support status to display the status of non-EAP host support on the port.

Procedure steps

Step	Action
1	Select the port to edit from the **Device View**.
2	Select **Edit, Port** from the menu.
3	Click the **EAPOL Advance** tab.

4 Click **Non-EAP MAC**.

5 Click the **Non-EAP Status** tab.

--End--

Variable definitions Use the data in the following table to view port non-EAP host support status.

Variable	Value
PortNumber	Specifies the port number in use.
ClientMACAddr	Specifies the MAC address of the client.
State	Specifies 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.
Reauthenticate	Specifies the value used to reauthenticate the MAC address of the client on the port.

Graphing EAPOL statistics using Device Manager

EAPOL port-based statistics can be graphed and analyzed on the **Graph Port** screen. For more information about, see*Nortel Ethernet Routing Switch 5000 Series Configuration — System Monitoring* () (NN47200-505).

Configuring general switch security using Device Manager

Configure general switch security to configure and manage general security parameters for the switch.

Procedure steps

Step	Action
1	Open the **Security** screen by choosing **Edit, Security, Security** from the menu.
2	Click the **General** tab.
3	Configure general switch security parameters as required.
4	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure general switch security.

Variable	Value
AuthSecurityLock	If this parameter is listed as locked, the agent refuses all requests to modify the security configuration. Entries also include: • other • notlocked
AuthCtlPartTime	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	Specifies 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 for each port. • autoLearn—Indicates that the switch learns the MAC addresses on each port as allowed addresses of that port.

Variable	Value
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 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. *da* means destination addresses.
CurrNodesAllowed	Specifies the current number of entries of the nodes allowed in the AuthConfig tab.
MaxNodesAllowed	Specifies the maximum number of entries of the nodes allowed in the AuthConfig tab.
PortSecurityStatus	Specifies the set of ports for which security is enabled.
PortLearnStatus	Specifies the set of ports where auto-learning is enabled.

Variable	Value
CurrSecurityLists	Specifies the current number of entries of the Security listed in the SecurityList tab
MaxSecurityLists	Specifies the maximum entries of the Security listed in the SecurityList tab.
AutoLearningAgingTime	Specifies 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.

Security list configuration using Device Manager

Configure the security list to manage the port members in a security list.

Security list configuration using Device Manager navigation

- “Adding ports to a security list using Device Manager” (page 242)
- “Deleting specific ports from a security list using Device Manager” (page 243)
- “Deleting all ports from a security list using Device Manager” (page 244)

Adding ports to a security list using Device Manager

Add ports to the security list to insert new port members into a security list.

Procedure steps

Step	Action
1	Open the Security screen by choosing **Edit, Security, Security** from the menu.
2	Click the **SecurityList** tab.
3	Click **Insert**.
4	In the **SecurityListIndx** box, accept the default sequential security list number provided by the switch. **OR** Type a number for the security list.
5	Click the ellipsis **(...)** for **SecurityListMembers**.
6	In the **SecurityListMembers** dialog box, select ports to add to the security list. **OR** Click **All** to select all ports.

7 Click **Ok**.

8 Click **Insert**.

--End--

Variable definitions

Use the data in the following table to add ports to the security list.

Variable	Value
SecurityListIndx	A numerical identifier for a security list. Values range from 1 to 32.
SecurityListMembers	Defines the security list port members.

Deleting specific ports from a security list using Device Manager

Delete specific ports from a security list to remove specific existing port members from a security list.

Procedure steps

Step **Action**

1 From the Device Manager menu bar, choose **Edit, Security, Security**.

2 Click the **SecurityList** tab.

3 Double-click the **SecurityListMembers** box for a security list.

4 Deselect security list port members as required.

5 Click **Ok**.

6 Click **Apply**.

--End--

Variable definitions

Use the data in the following table to delete specific ports from a security list.

Variable	Value
SecurityListIndx	A numerical identifier for a security list. Values range from 1 to 32.
SecurityListMembers	Defines the security list port members.

Deleting all ports from a security list using Device Manager

Delete all ports from a security list to remove all existing port members from a security list.

Procedure steps

Step	Action
1	From the Device Manager menu bar, choose **Edit, Security, Security**.
2	Click the **SecurityList** tab.
3	Click the **SecurityListMembers** box for a security list.
4	Click **Delete**.
5	Click **Yes**.

--End--

Variable definitions

Use the data in the following table to delete all ports from a security list.

Variable	Value
SecurityListIndx	A numerical identifier for a security list. Values range from 1 to 32.
SecurityListMembers	Defines the security list port members.

AuthConfig list configuration using Device Manager

The AuthConfig list consists of 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.

AuthConfig list configuration using Device Manager navigation

- "Adding entries to the AuthConfig list using Device Manager" (page 245)
- "Deleting entries from the AuthConfig list using Device Manager" (page 246)

Adding entries to the AuthConfig list using Device Manager

Procedure steps

Step	Action
1	Select **Edit, Security, Security** from the Device Manager menu.
2	Click the **AuthConfig** tab.
3	Click **Insert**.
4	In the Insert AuthConfig dialog box, type new entry information.
5	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to add entries to the AuthConfig list.

Variable	Value
BrdIndx	Index of the board. This corresponds to the unit. **ATTENTION** If this field is specified, the SecureList field is 0.
PortIndx	Index of the port. **ATTENTION** 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.
Source	Indicates the source of entries to the AuthConfig list.
Lifetime	Indicates the maximum time that entries remain in the AuthConfig list.

Deleting entries from the AuthConfig list using Device Manager

Delete entries from the AuthConfig list to remove information from the list of boards, ports and MAC addresses that have the security configuration.

Procedure steps

Step	Action
1	Select **Edit, Security, Security** from the Device Manager menu.
2	Click the **AuthConfig** tab.
3	Select a list entry.
4	Click **Delete**.
5	Click **Yes**.

--End--

Configuring MAC Address AutoLearn using Device Manager

Configure MAC Address AutoLearn to configure the MAC Address auto learning properties of switch ports.

Procedure steps

Step	Action
1	Open the **Security** screen by choosing **Edit, Security, Security** from the menu.
2	Click the **AutoLearn** tab.
3	Double-click the **Enabled** box for a port.
4	Select **true** to enable AutoLearn on the port. **OR** Select **false** to disable AutoLearn on the port.
5	Double-click the **MaxMacs** box for a port.
6	Type a value between 1 and 25.
7	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure MAC Address AutoLearn.

Variable	Value
Brd	Identifies the board.
Port	Identifies the port.
Enabled	Enables or disables AutoLearning on a port. Values are true or false.
MaxMacs	Defines the maximum number of MAC Addresses that the port can learn.

Vewing AuthStatus information using Device Manager

View AuthStatus information to display authorized boards and port status data collection information. Displayed information includes actions to be performed when an unauthorized station is detected and the current security status of a port.

Procedure steps

Step	Action
1	Open the **Security** screen by choosing **Edit, Security, Security** from the menu.
2	Click the **AuthStatus** tab.

--End--

Variable definitions

Use the data in the following table to view AuthStatus information.

Variable	Value
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.
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`.

Variable	Value
CurrentActionMode	A value representing the type of information contained, including: • noAction—Port does not have 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 filters 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. • If the port is partitioned, portPartition is returned.

Viewing AuthViolation information using Device Manager

View AuthViolation information to display a list of boards and ports where network access violations have occurred, and to display the identity of the offending MAC addresses.

Procedure steps

Step	Action
1	Open the Security screen by choosing **Edit, Security, Security** from the menu.
2	Click the **AuthViolation** tab.

--End--

Variable definitions

Use the data in the following table to view AuthViolation information.

Variable	Value
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).

Viewing MacViolation information using Device Manager

View MacViolation information to display a list of boards and ports where network access violations have occurred, and to display the identity of the offending MAC addresses.

Procedure steps

Step	Action
1	Open the **Security** screen by choosing **Edit, Security, Security** from the menu.
2	Click the **MacViolation** tab.

--End--

Variable definitions

Use the data in the following table to view MacViolation information.

Variable	Value
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.

Configuring the Secure Shell protocol using Device Manager

Configure the Secure Shell (SSH) protocol to replace Telnet and provide secure access to NNCLI interface.

Procedure steps

Step	Action
1	Select **Edit, Security, Security** from the Device Manager menu.
2	Click the **SSH** tab.
3	Configure SSH parameters as required.
4	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure SSH.

Variable	Value
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.

Variable	Value
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).
TftpServerInetAddressType	Indicates the type of address stored in the TFTP server.
TftpServerInetAddress	Specifies the IP address stored in the TFTP server for all TFTP operations.
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.
SshAuthKeyFilename	Specifies the SSH authentication key file to download.
UsbTargetUnit	Specifies the unit number of the USB port to use for file uploads and downloads. Values range from 1 to 9. Values 1 to 8 apply to a USB port in a switch stack. Value 9 applies to a stand-alone switch.
DnldSshAuthKeyFromUsb	Specifies to download the SSH authentication key using the USB port.
DnldSshAuthKeyFromUsbStatus	Indicates the status of the latest SSH authentication key download using the USB port. Values include the following: • other—no action taken since the switch startup • inProgress—authentication key download is in progress • success—authentication key download completed successfully • fail—authentication key download failed

Viewing SSH Sessions information using Device Manager

View SSH Sessions information to display currently active SSH sessions.

Procedure steps

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

2 Click the **SSH Sessions** tab.

--End--

Variable definitions

Use the data in the following table to configure an SSH Session.

Variable	Value
SshSessionInetAddressType	Indicates the type of IP address of the SSH client that opened the SSH session.
SshSessionInetAddress	Indicates the IP address of the SSH client that opened the SSH session.

Configuring SSL using Device Manager

Configure Secure Socket Layer (SSL) to provide your network with a secure Web management interface.

Procedure steps

Step **Action**

1 Select **Edit, Security, Security** from the Device Manager menu.

2 Click the **SSL** tab.

3 Configure SSL parameters as required.

4 Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure SSL.

Variable	Value
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.

Variable	Value
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 • success—the operation is complete • failure—the operation failed • other—the s5AgSslCertificateControl object was never set
ServerControl	Resets the SSL server. Values are reset and other. The default is other. **ATTENTION** You cannot reset the SSL server while creating the SSL certificate.

RADIUS Server security configuration using Device Manager

Configure RADIUS Server security to configure and manage RADIUS-based network security and 802.1X dynamic authorization extension (RFC 3576).

RADIUS Server configuration using Device Manager navigation

- “Configuring the RADIUS globals using Device Manager” (page 254)
- “Configuring the RADIUS server using Device Manager” (page 254)
- “Viewing RADIUS Dynamic Authorization server information using Device Manager” (page 255)
- “802.1X dynamic authorization extension (RFC 3576) configuration using Device Manager” (page 256)
- “Viewing RADIUS Dynamic Server statistics using Device Manager” (page 259)
- “Graphing RADIUS Dynamic Server statistics using Device Manager” (page 260)

Configuring the RADIUS globals using Device Manager

Configure the RADIUS globals to enable or disable RADIUS use of management IP.

Procedure 1
Procedure steps

Step	Action
1	From the Device Manager menu bar, choose **Edit > Security > RADIUS**.
2	Click the **Globals** tab.
3	Select the **RadiusUseMgmtIP** field to enable or disable RADIUS use of management IP.

--End--

Configuring the RADIUS server using Device Manager

Configure the RADIUS server to store client or user credentials, password, and access privileges.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Edit, Security, RADIUS**.
2	Click the **RADIUS Server** tab.
3	Configure RADIUS server parameters as required.
4	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure the RADIUS server.

Variable	Value
PrimaryRadiusServerAddressType	Specifies the type of primary IP address used by the Nortel SNAS 4050. Values are unknown, ipv4, and ipv6.

Variable	Value
PrimaryRadiusServer	Specifies the IP address of the primary RADIUS server (default: 0.0.0.0). **ATTENTION** If there is no primary RADIUS server, set the value of this field to 0.0.0.0 .
SecondaryRadiusServerAddressType	Specifies the type of secondary IP address used by the Nortel SNAS 4050. Values are unknown, ipv4, and ipv6.
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.
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. **ATTENTION** The shared secret key has a maximum of 16 characters.
ConfirmedSharedSecret(key)	Confirms the value of the shared secret key specified in the SharedSecret(Key) field. This field usually does not display anything (just a blank field), and is used when you are changing the SharedSecret(key) field. You must enter the value twice to confirm the string is entered in SharedSecret(Key).

Viewing RADIUS Dynamic Authorization server information using Device Manager

View RADIUS Dynamic Authorization server information to display RADIUS Dynamic Authorization server information for the switch.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Edit, Security, RADIUS**.

2 Click the **RADIUS Dynamic Auth. Server** tab.

--End--

Variable definitions

Use the data in the following table to view the number of Disconnect and CoA Requests received from unknown addresses.

Variable	Value
Identifier	Indicates the Network Access Server (NAS) identifier of the RADIUS Dynamic Authorization Server.
DisconInvalidClientAddresses	Indicates the number of Disconnect-Request packets received from unknown addresses.
CoAInvalidClientAddresses	Indicates the number of CoA-Request packets received from unknown addresses.

802.1X dynamic authorization extension (RFC 3576) configuration using Device Manager

Configure 802.1X dynamic authorization extension (RFC 3576) to enable the RADIUS server to send a change of authorization (CoA) or disconnect command to the Network Access Server (NAS)

802.1X dynamic authorization extension (RFC 3576) configuration using Device Manager navigation

- “Configuring 802.1X dynamic authorization extension (RFC 3576) client using Device Manager” (page 256)
- “Editing the 802.1X dynamic authorization extension (RFC 3576) client information using Device Manager” (page 257)
- “Editing the 802.1X dynamic authorization extension (RFC 3576) client secret word using Device Manager” (page 259)

Configuring 802.1X dynamic authorization extension (RFC 3576) client using Device Manager

Configure the RADIUS Dynamic Authorization client parameters for the switch.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Edit, Security, RADIUS**.
2	Click the **RADIUS Dynamic Auth. Client** tab.
3	Click **Insert**.
4	Configure RADIUS Dynamic Authorization client parameters as required.
5	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the RADIUS Dynamic Authorization client parameters.

Variable	Value
AddressType	Defines the IP address type for the RADIUS Dynamic Authorization Client.
Address	Defines the IP address of the RADIUS Dynamic Authorization Client.
Enabled	Enables packet receiving from the RADIUS Dynamic Authorization Client.
UdpPort	Configures the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1025 to 65535.
ProcessCoARequests	Enables change of authorization (CoA) request processing.
ProcessDisconnectRequests	Enables disconnect request processing.
Secret	Configures the RADIUS Dynamic Authorization Client secret word.
ConfirmedSecret	Confirms the RADIUS Dynamic Authorization Client secret word.

Editing the 802.1X dynamic authorization extension (RFC 3576) client information using Device Manager

Configure the RADIUS Dynamic Authorization client parameters for the switch.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Edit, Security, RADIUS**.
2	Click the **RADIUS Dynamic Auth. Client** tab.
3	Double-click a configurable RADIUS Dynamic Auth. Client dialog box .
4	Edit RADIUS Dynamic Authorization client parameters as required.
5	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure the RADIUS Dynamic Authorization client parameters.

Variable	Value
AddressType	Defines the IP address type for the RADIUS Dynamic Authorization Client. This is a read only value.
Address	Defines the IP address of the RADIUS Dynamic Authorization Client. This is a read only value.
Enabled	Enables or disables packet receiving from the RADIUS Dynamic Authorization Client. • enable—true • disable—false
UdpPort	Configures the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1025 to 65535.
ProcessCoARequests	Enables change of authorization (CoA) request processing.

Variable	Value
ProcessDisconnectRequests	Enables disconnect request processing.
Secret	The RADIUS Dynamic Authorization Client secret word. This box remains empty.

Editing the 802.1X dynamic authorization extension (RFC 3576) client secret word using Device Manager

Edit the RADIUS Dynamic Authorization client secret word to change the existing secret word.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Edit, Security, RADIUS**.
2	Click the **RADIUS Dynamic Auth. Client** tab.
3	Click **Change Secret**.
4	In the **Secret** dialog box, type a new secret word.
5	In the **Confirmed Secret** dialog box, retype the new secret word.
6	Click **Apply**.

--End--

Viewing RADIUS Dynamic Server statistics using Device Manager

View RADIUS Dynamic Server statistics to display and review RADIUS Dynamic Server statistical information.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Edit, Security, RADIUS**.
2	Click the **RADIUS Dynamic Server Stats** tab.

--End--

Variable definitions

Use the data in the following table to view RADIUS Dynamic Server statistics.

Variable	Value
ClientIndex	Indicates the RADIUS Dymanic Server client index.
ClientAddressType	Indicates the type of RADIUS Dymanic Server address. Values are ipv4 or ipv6.
ClientAddress	Indicates the IP address of the RADIUS Dymanic Server.
ServerCounterDiscontinuity	Indicates a count of RADIUS Dymanic Server discontinuity instances.

Graphing RADIUS Dynamic Server statistics using Device Manager

Graph RADIUS Dynamic Server statistics to display a graphical representation of statistics for a RADIUS Dynamic Server client.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Edit, Security, RADIUS**.
2	Click the **RADIUS Dynamic Server Stats** tab.
3	Click any box for a displayed RADIUS Dynamic Server client.
4	Click **Graph**.
5	Click and drag your cursor to highlight all RADIUS Dynamic Server statistical information to graph.
6	Click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

--End--

DHCP snooping configuration using Device Manager

Configure Dynamic Host Configuration Protocol (DHCP) snooping to provide security to your network by preventing DHCP spoofing.

DHCP snooping configuration using Device Manager navigation

- "Configuring DHCP snooping globally using Device Manager" (page 261)
- "Configuring DHCP snooping on a VLAN using Device Manager" (page 261)

- “Configuring DHCP snooping port trust using Device Manager” (page 262)
- “Viewing the DHCP binding information using Device Manager” (page 263)

Configuring DHCP snooping globally using Device Manager

Configure DHCP snooping globally to enable or disable DHCP snooping on the switch.

Procedure steps

Step	Action
1	Select **IP Routing, DHCP** from the Device Manager menu.
2	Click the **DHCP snooping** tab.
3	Select the **DhcpSnoopingEnabled** box to enable DHCP snooping globally. **OR** Deselect the **DhcpSnoopingEnabled** box to disable DHCP snooping globally.
4	Click **Apply** .

--End--

Configuring DHCP snooping on a VLAN using Device Manager

Configure DHCP snooping on a VLAN through to enable or disable DHCP snooping on the VLAN.

ATTENTION
You must enable DHCP snooping separately for each Vlan ID.

ATTENTION
If DHCP snooping is disabled on a VLAN, the switch forwards DHCP reply packets to all applicable ports, whether the port is trusted or untrusted.

Procedure steps

Step	Action
1	Select the port to edit from the **Device view**.
2	Select **IP Routing, DHCP** from the menu.
3	Click the **DHCP snooping-VLAN** tab.
4	Double-click on the **DhcpSnoopingEnabled** box for the Vlan.

5 Select **true** to enable DHCP snooping on the VLAN.

OR

Select **false** to disable DHCP snooping on the VLAN.

6 Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure DHCP snooping on a VLAN.

Variable	Value
VlanId	Indicates the VlanId on the VLAN.
DhcpSnoopingEnabled	Enables or disables DHCP snooping.

Configuring DHCP snooping port trust using Device Manager

Configure DHCP snooping port trust to specify whether a particular port or multiple ports are trusted or untrusted. Ports are untrusted by default.

Procedure steps

Step **Action**

1 Select **IP Routing,DHCP** from the menu.

2 Click the **DHCP snooping-port** tab.

3 Double-click on the **DhcpSnoopingIfTrusted** for a port.

4 Select **true** to configure the port to be trusted.

OR

Select **false** to configure the port to be untrusted.

5 Repeat steps **3** and **4** to configure additional ports as required.

6 Click **Apply**.

--End--

Variable definitions

Variable	Value
Port	Indicates the port on the switch.
DhcpSnoopingIfTrusted	Indicates whether the port is trusted or untrusted. Default is false.

Viewing the DHCP binding information using Device Manager

View the DHCP binding information to review current DHCP lease information.

Procedure steps

Step	Action
1	Select **IP Routing, DHCP** from the Device Manager menu.
2	Click the **DHCP Bindings** tab. The DHCP Bindings dialog box appears, displaying DHCP Binding information.

--End--

Variable definitions

Use the data in the following table to view the DHCP binding information.

Variable	Value
VlanId	Identifies the VLAN on the switch.
MacAddress	Indicates the MAC address of the DHCP client.
AddressType	Indicates the MAC address type of the DHCP client.
Address	Indicates IP address of the DHCP client.
Interface	Indicates the interface to which the DHCP client is connected.
LeaseTime(sec)	Indicates the lease time (in seconds) of the DHCP client binding.
TimeToExpiry(sec)	Indicates the time (in seconds) before a DHCP client binding expires.

Dynamic ARP inspection configuration using Device Manager

Use dynamic ARP inspection to validate ARP packets in a network.

Dynamic ARP inspection configuration using Device Manager navigation

- "Configuring dynamic ARP inspection on VLANs using Device Manager" (page 264)
- "Configuring dynamic ARP inspection on ports using Device Manager" (page 264)

Configuring dynamic ARP inspection on VLANs using Device Manager

Configure ARP inspection on a VLAN to enable or disable ARP inspection on one or more VLANs.

Procedure steps

Step	Action
1	Select **IP Routing,IP** from the menu.
2	Click the **ARP Inspection-VLAN** tab.
3	Double-click the **ARPInspectionEnabled** box for a VLAN.
4	Select **true** to enable ARP Inspection-VLAN. **OR** Select **false** to disable ARP Inspection-VLAN.
5	Repeat steps **3** and **4** for additional VLANs as required.
6	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure ARP inspection on a VLAN.

Variable	Value
VlanId	Identifies VLANs configured on the switch.
ARPInspectionEnabled	Enables or disables ARP inspection on a VLAN.

Configuring dynamic ARP inspection on ports using Device Manager

Configure ARP inspection on ports to enable or disable ARP inspection on one or more ports.

Procedure steps

Step	Action
1	Select **IP Routing,IP** from the menu.
2	Click the **ARP Inspection-port** tab.
3	Double-click on the **ARPInspectionIfTrusted** box for a port.
4	Select **true** to enable ARP Inspection-Port. **OR**

Select **false** to disable ARP Inspection-Port.

5 Repeat steps **3** and **4** for additional ports as required.

6 Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure ARP inspection ports.

Variable	Value
Port	Identifies ports on the switch, using the unit/port format.
ARPInspectionIfTrusted	Configures a port as trusted or untrusted for ARP inspection.

IP Source Guard configuration using Device Manager

This section describes how to configure IP Source Guard to add a higher level of security to a port or ports by preventing IP spoofing

ATTENTION
Nortel recommends that you do not enable IP Source Guard on trunk ports.

ATTENTION
Nortel recommends that you carefully manage the number of applications running on the Ethernet Routing Switch 8300 that use filters. For example, if you configure NSNA on ports and attempt to configure IP Source Guard on those same ports, the IP Source Guard configuration can fail due to the limited number of filters available.

Prerequisites

Before you can configure IP Source Guard, you must ensure the following:

- Dynamic Host Control Protocol (DHCP) snooping is globally enabled.

  For more information about, see “Configuring DHCP snooping globally using Device Manager” (page 261).
- The port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- The port is an untrusted DHCP snooping and dynamic ARP Inspection port.
- A minimum of 10 rules are available on the port.
- The bsSourceGuardConfigMode MIB object exists.

This MIB object is used to control the IP Source Guard mode on an interface.

- The following applications are not enabled:
  - IP Fix
  - Baysecure
  - Extensible Authentication Protocol over LAN (EAPoL)

> **ATTENTION**
> Hardware resources can run out if IP Source Guard is enabled on trunk ports with a large number of VLANs, which have DHCP snooping enabled. If this happens, traffic sending can be interrupted for some clients. Nortel recommends that IP Source Guard not be enabled on trunk ports.

IP Source Guard configuration using Device Manager navigation

- "Configuring IP Source Guard on a port using Device Manager" (page 266)
- "Filtering IP Source Guard addresses using Device Manager" (page 267)

Configuring IP Source Guard on a port using Device Manager

Configure IP Source Guard to enable or disable a higher level of security on a port or ports.

> **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.

Procedure steps

Step	Action
1	Select **IP Routing, DHCP** from the menu.
2	Cick the **IP Source Guard-port** tab.
3	In the IP Source Guard-port dialog box, double-click the **Mode** box for a port.
4	Select **ip** from the list to enable IP Source Guard. **OR** Select **disabled** from the list to disable IP Source Guard.
5	Click **Apply** after making changes.

6 Click **Refresh** to update the IP Source Guard-port dialog box display.

--End--

Variable definitions

Use the data in the following table to enable IP Source Guard on a port.

Variable	Value
Port	Identifies the port number.
Mode	Identifies the Source Guard mode for the port. The mode can be disabled or ip. The default mode is disabled.

Filtering IP Source Guard addresses using Device Manager

Filter IP Source Guard addresses to display IP Source Guard information for specific IP addresses.

Prerequisites

Before you can configure IP Source Guard, you must ensure the following:

- Dynamic Host Control Protocol (DHCP) snooping is globally enabled.

  For more information about, see "Configuring DHCP snooping globally using Device Manager" (page 261).
- The port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- The port is an untrusted DHCP snooping and dynamic ARP Inspection port.
- A minimum of 10 rules are available on the port.
- The bsSourceGuardConfigMode MIB object exists.

  This MIB object is used to control the IP Source Guard mode on an interface.
- The following applications are not enabled:
  - — IP Fix
  - — Baysecure
  - — Extensible Authentication Protocol over LAN (EAPoL)

ATTENTION
Hardware resources can run out if IP Source Guard is enabled on trunk ports with a large number of VLANs, which have DHCP snooping enabled. If this happens, traffic sending can be interrupted for some clients. Nortel recommends that IP Source Guard not be enabled on trunk ports.

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.

Procedure steps

Step	Action
1	Select **IP Routing, DHCP** from the menu.
2	Click the **IP Source Guard-addresses** tab.
3	Click **Filter**.
4	In the **IP Source Guard-addresses - Filter** dialog box, select the required parameters for displaying port IP Source Guard information.
5	Click **Filter**. IP Source Guard information for the specified IP addresses appears in the IP Source Guard-addresses dialog box.

--End--

Variable definitions

Use the data in the following table to filter IP Source Guard addresses.

Variable	Value
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.

Variable	Value
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.

Use the data in the following table to display IP Source Guard information for filtered addresses.

Variable	Value
Port	The port number.
Type	The internet address type.
Address	The IP address allowed by IP Source Guard.
Source	The source of the address.

SNMP configuration using Device Manager

This section describes how you can configure SNMP using Device Manager, to monitor devices running software that supports the retrieval of SNMP information.

SNMP configuration using Device Manager navigation

- “Setting SNMP v1, v2c, v3 Parameters” (page 270)
- “SNMPv3 and SNMP configuration using Device Manager” (page 271)

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 Ethernet Routing Switch 5000 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 Ethernet Routing Switch 5000 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 Ethernet Routing Switch 5000 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 following list contains the number of nonvolatile entries (entries stored in NVRAM) allowed in the SNMPv3 tables. The system does not allow you to create more entries marked nonvolatile when you reach these limits:

- snmpCommunityTable: 20
- vacmViewTreeFamilyTable: 60
- vacmSecurityToGroupTable: 40
- vacmAccessTable: 40
- usmUserTable: 20
- snmpNotifyTable: 20
- snmpTargetAddrTabel: 20
- snmpTargetParamsTable: 20

SNMPv3 and SNMP configuration using Device Manager

This section describes the configuration options available for SNMPv3 and SNMP.

SNMPv3 and SNMP configuration using Device Manager navigation

- “Configuring SNMPv3 using Device Manager” (page 271)
- “Configuring the switch to use SNMP using Device Manager” (page 283)

Configuring SNMPv3 using Device Manager

The Ethernet Routing Switch 5000 Series allows for configuration of SNMPv3 using the Device Manager, Web-based management, or NNCLI.

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.

- You must configure views and users using NNCLI before SNMPv3 can be used. For more information, see "Configuring SNMP using NNCLI" (page 137).
- Ensure you have the secure version of the software image installed on your switch.

- "Creating an SNMPv3 user using Device Manager" (page 272)
- "Viewing the details of an SNMPv3 user using Device Manager" (page 273)
- "Creating membership for a group using Device Manager" (page 274)
- "Viewing group membership using Device Manager" (page 275)
- "Creating access for a group using Device Manager" (page 275)
- "Viewing group access rights using Device Manager" (page 277)
- "Creating a new MIB view using Device Manager" (page 278)
- "Viewing MIBs assigned to an object using Device Manager" (page 279)
- "Creating a community using Device Manager" (page 280)
- "Creating a target table using Device Manager" (page 280)
- "Creating target parameters using Device Manager" (page 281)
- "Creating a Notify Table entry using Device Manager" (page 282)

To create an SNMPv3 user, you must clone and then modify the properties of an existing SNMPv3 user.

Create an SNMPv3 user by following this procedure:

Procedure steps

Step	Action
1	Open the **USM Table** screen by choosing **Edit, SnmpV3, USM Table** from the menu.
2	Click **Insert**. The Insert USM Table screen appears.
3	Type and select the required information in the **Insert USM Table** screen.

4 Click **Insert**.

--End--

Variable definitions Use the data in the following table to create an SNMPv3 user.

Variable	**Value**
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 the menu. If this field is selected, an old AuthPass and a new AuthPass must be entered.
Cloned User’s Auth Password	Specifies the authentication password of the user being cloned.
New User’s Auth Password	Specifies the new user authentication password.
Priv Protocol (Optional)	Assigns a privacy protocol (or no privacy) from menu. If this is selected, an old PrivPass and a new PrivPass must be entered.
Cloned User’s Priv Password	Specifies the privacy password of the user being cloned.
New User’s Priv Password	Specifies the name of the new privacy password.
StorageType	Specifies the type of storage: • volatile • nonVolatile • readOnly (not available)

To view SNMPv3 user details, see “Viewing the details of an SNMPv3 user using Device Manager” (page 273) .

View the details of an SNMPv3 user by following this procedure:

Procedure steps

Step	Action
1	Open the **USM Table** screen by choosing **Edit, SnmpV3, USM Table** from the menu.

--End--

Variable definitions Use the data in the following table to view the details of an SNMPv3 user.

Variable	**Value**
EngineID	Indicates the SNMP engine 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.

To create an SNMPv3 user, see "Creating an SNMPv3 user using Device Manager" (page 272) .

Create membership for a group by following this procedure:

Procedure steps

Step	Action
1	Open the **VACM** screen by choosing **Edit, SnmpV3, VACM Table...** from the menu.
2	Click **Insert**. The Insert Group Membership screen appears.
3	Select and type the required information.
4	Click **Insert**.

--End--

Variable definitions Use the data in the following table to create membership for a group.

Variable	**Value**
SecurityModel	Specifies the authentication checking to communicate to the switch.

Variable	Value
SecurityName	Specifies the security name assigned to this entry in the VACM table. The range is 1 to 32 characters.
GroupName	Specifies the name assigned to this group in the VACM table. The range is 1 to 32 characters.
StorageType	Specifies the selected type of storage. Options include: • volatile • nonVolatile • readOnly (not available)

To view existing SNMPv3 group membership details, see "Viewing group membership using Device Manager" (page 275) .

View group membership details in the view-based access control model (VACM) by following this procedure:

Procedure steps

Step	Action
1	Open the **VACM** screen by choosing **Edit, SnmpV3, VACM Table...** from the menu.

--End--

Variable definitions Use the data in the following table to view group membership details.

Variable	Value
SecurityModel	Specifies the security model currently in use.
SecurityName	Specifies the name representing the user in usm user. The range is 1 to 32 characters.
GroupName	Specifies the name of the group to which this entry (combination of securityModel and securityName) belongs.
StorageType	Specifies the storage type of the group to which this entry belongs.

Create new access for a group by following this procedure:

Procedure steps

Step	Action
1	Open the **VACM** screen by choosing **Edit, SnmpV3, VACM Table...** from the menu.
2	Click the **Group Access Right** tab.
3	Click **Insert**. The Insert Group Access Right screen appears.
4	Type and select the required information.
5	Click **Insert**.

--End--

Variable definitions Use the data in the following table to create new access for a group.

Variable	Value
vacmGroupName	Specifies 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 5000 Series switches, the ContextPrefix value should be an empty string.
SecurityModel	Specifies the security model of the entry. Values are SNMPv1, SNMPv2, and SNMPv3.
SecurityLevel	Specifies the minimum level of security required to gain access rights. The security levels are: • noAuthNoPriv • authNoPriv • AuthPriv

Variable	Value
ContextMatch (Optional)	Specifies the exact or prefix-only match to the contextName for an incoming SNMP packet. For 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.

To view SNMPv3 group access rights, see "Viewing group access rights using Device Manager" (page 277) .

View access rights for a group by following this procedure:

Procedure steps

Step	Action
1	Open the **VACM** screen by choosing **Edit, SnmpV3, VACM Table...** from the menu.
2	Click the **Group Access Right** tab.

--End--

Variable definitions Use the data in the following table to view access rights for a group.

Variable	Value
vacmGroupName	Specifies 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	Specifies the security model of the entry. Value are SNMPv1, SNMPv2, and SNMPv3.

Variable	Value
SecurityLevel	Specifies 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.

Create a new MIB view by following this procedure:

Procedure steps

Step	Action
1	Open the **VACM** screen by choosing **Edit, SnmpV3, VACM Table...** from the menu.
2	Click the **MIB View** tab.
3	Click **Insert**. The Insert MIB View screen appears.
4	Type and select the required information.
5	Click **Insert**.

--End--

Variable definitions Use the data in the following table to create a new MIB view.

Variable	Value
ViewName	Creates a new entry with this group name. The range is 1 to 32 characters.
Subtree	Specifies a valid object identifier that defines the set of MIB objects accessible by this SNMP entity, for example, 1.3.6.1.1.5

Variable	Value
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.

To view assigned MIB information, see "Viewing MIBs assigned to an object using Device Manager" (page 279) .

View MIBs assigned to an object by following this procedure:

Procedure steps

Step	Action
1	Open the **VACM** screen by choosing **Edit, SnmpV3, VACM Table...** from the menu.
2	Click the **MIB View** tab.

--End--

Variable definitions Use the data in the following table to view MIBs assigned to an object.

Variable	Value
ViewName	Creates a new entry with this group name. The range is 1 to 32 characters.
Subtree	Specifies a 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.

A community table contains objects for mapping between community strings and the security name created in VACM Group Member. Create a community by following this procedure:

Procedure steps

Step	Action
1	Open the **Community Table** screen by choosing **Edit, SnmpV3, Community Table** from the menu.
2	Click **Insert**. The Insert Community Table screen appears.
3	Type and select the required information.
4	Click **Insert**.

--End--

Variable definitions Use the data in the following table to create a community.

Variable	Value
Index	Specifies the unique index value of a row in this table. SnmpAdminString 1 to 32 characters.
Name	Specifies the community string for which a row in this table represents a configuration.
SecurityName	Specifies the security name assigned to this entry in the Community table. The range is 1 to 32 characters.
ContextEngineID	Specifies the context engine ID.
ContextName	Specifies the context name.
TransportTag	Specifies the transport tag.
StorageType	Specifies the storage type.

Create a Target Address table by following this procedure:

Procedure steps

Step	Action
1	Open the **Target Table** screen by choosing **Edit, SnmpV3, Target Table** from the menu.
2	Click **Insert**.
3	Type and select the required information.

4 Click **Insert**.

--End--

Variable definitions Use the data in the following table to create a Target Address table.

Variable	Value
Name	Specifies the name of the target table.
TDomain	Specifies the TDomain for the target table.
TAddress	Specifies the TAddress for the target table. This is the network address of the trap or notification receiver. IPv4 and IPv6 are supported.
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.

Create a target parameter by following this procedure:

Procedure steps

Step **Action**

1 Open the **Target Table** screen by choosing **Edit, SnmpV3, Target Table** from the menu.

2 Click the **Target Params Table** tab.

3 Click **Insert**.

4 Type and select the required information.

5 Click **Insert**.

--End--

Variable definitions Use the data in the following table to create a target parameter.

Variable	Value
Name	Specifies the name of the target parameters table.
MPModel	Specifies the Message Processing model, SNMPv1, SNMPv2c, or SNMPv3/USM.

Variable	Value
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, and authPriv.
Storage Type	Specifies the storage type: volatile or nonvolatile.

Create a Notify Table entry by following this procedure:

Procedure steps

Step	Action
1	Open the **Notify Table** screen by choosing **Edit, SnmpV3, Notify Table** from the menu.
2	Click **Insert**.
3	Type and select the required information.
4	Click **Insert**.

--End--

Variable definitions Use the data in the following table to create a Notify Table entry.

Variable	Value
Name	Specifies the unique identifier associated for the notify table.
Tag	Specifies the 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.

Variable	Value
Type	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 messages generated for selected rows contain SNMPv2-Trap PDUs. If the value of this object is inform, then messages generated for selected rows contain Inform PDUs. **ATTENTION** 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 nonvolatile.

Configuring the switch to use SNMP using Device Manager

This section describes how to configure SNMP on the switch.

- “Viewing SNMP information using Device Manager” (page 283)
- “Configuring trap receivers using Device Manager” (page 284)

Use the SNMP tab to display read-only information about the addresses that the agent software uses to identify the switch.

View the SNMP information by following this procedure:

Procedure steps

Step	Action
1	Select a chassis in the Device View.
2	Select **Edit, Chassis** from the Device Manager menu.
3	Click the **SNMP** tab.

--End--

Variable definitions Use the data in this table to display read-only information about the addresses that the agent software uses to identify the switch.

Variable	Value
LastUnauthenticatedInetAddressType	Specifies the type of IP address that was not authenticated by the device last.
LastUnauthenticatedInetAddress	Specifies the last IP address that was not authenticated by the device.
LastUnauthenticatedCommunityString	Specifies the last community string that was not authenticated by the device.
RemoteLoginInetAddressType	Specifies the type of IP address to last remotely log on to the system.
RemoteLoginInetAddress	Specifies the last IP address to remotely log on to the system.
TrpRcvrMaxEnt	Specifies the maximum number of trap receiver entries.
TrpRcvrCurEnt	Specifies the current number of trap receiver entries.
TrpRcvrNext	Specifies the next trap receiver entry to be created.

Configure trap receivers to view and edit information in the network traps table. The network traps table lists the devices that receive SNMP traps from the Ethernet Routing Switch 5000 Series.

Configure a trap receiver by following this procedure:

Procedure steps

Step	Action
1	Select the chassis in the Device View.
2	Select **Edit, Chassis** from the Device Manager menu.
3	Click the **Trap Receivers** tab. The network traps table appears.
4	Click **Insert**. The Insert Trap Receivers screen appears.
5	Type the **Index**, **NetAddr**, and **Community** information.

6 Click **Insert**.

--End--

Variable definitions Use the data in this table to list the devices that receive SNMP traps.

Variable	Value
Indx	Specifies the index of the entry in the table.
NetAddr	Specifies the IP address for the trap receiver.
Community	Specifies the community string used for trap messages to this trap receiver.

Configuring Nortel Secure Network Access using NNCLI

This chapter describes how to configure the Nortel Ethernet Routing Switch 5000 Series as a network access device in the Nortel Secure Network Access (Nortel SNA) solution using the Nortel Networks Command Line Interface (NNCLI).

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 77).

Navigation

Configuring the Nortel SNAS 4050 subnet

Configure the Nortel SNAS 4050 subnet by using 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.

ATTENTION

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

Configure the Nortel SNAS 4050 pVIP subnet of 10.40.40.0/24 by entering the following command:

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

Viewing Nortel SNAS 4050 subnet information

View information related to the Nortel SNAS 4050 pVIP subnet you configured by entering 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

Remove the Nortel SNAS 4050 pVIP subnet by using 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 69). For detailed information about configuring the filters, see *Nortel Ethernet Routing Switch 5000 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.

Configure the Nortel SNA VLANs by using 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 gives you the color to 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. If the filter set with this name does not already exist, the system creates the filter when you specify it with this command. If a filter set with the name you specify exists, that filter set is used. **ATTENTION** This parameter is not allowed for configuration of a VoIP VLAN. VoIP filters are part of the Red/Yellow filter sets.
yellow-subnet <ipaddr/mask>	Sets the Yellow VLAN subnet IP and mask (a.b.c.d/<0–32>). **ATTENTION**

	This parameter is only allowed for configuration of the Yellow VLAN.

Viewing Nortel SNA VLAN information

View information related to the Nortel SNA VLANs by using 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

Remove a Nortel SNA VLAN by using 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 more information about creating VLANs using the Ethernet Routing Switch 5000 Series, see *Nortel Ethernet Routing Switch 5000 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking* () (NN47200-502).

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

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

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

In this example, the following parameters are used:

VLAN	Parameters
Red	VLAN ID: 110 Color: Red Filter name: red
Yellow	VLAN ID: 120 Color: Yellow Filter name: yellow Subnet IP: 10.120.120.0/24
Green	VLAN ID: 130 Color: Green Filter name: green
VoIP	VLAN ID: 140 Color: VoIP

ATTENTION
If you do not configure filters manually 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

Configure the VoIP VLAN by using 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

Configure the Red VLAN by using 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

Configure the Yellow VLAN by using 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

Configure the Green VLAN by using 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 more information about port modes, see “Port modes” (page 69).

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

ATTENTION
The Ethernet Routing Switch 5530 has two 10-Gbit ports. You can configure these as uplink ports only. You cannot configure these ports 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.

Configure Nortel SNA on ports by using 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

View information related to the Nortel SNA interfaces by using 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

Remove a Nortel SNA port by using the following command from the Ethernet Interface Configuration mode:

```
no nsna
```

Example: Removing Nortel SNA ports

Disable Nortel SNA on ports 20–24 by using 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

Add the uplink port to the VLANs by using 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][,...]}

> **ATTENTION**
> 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. For more information, see *Nortel Ethernet Routing Switch 5000 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking* () (NN47200-502).

The membership of Nortel SNA uplink ports in non-Nortel SNA VLANs is not affected by globally enabling or disabling Nortel SNA. The Ethernet Routing Switch 5000 Series 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)#
```

ATTENTION
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 port changes its STP state to Fast Learning automatically. You can disable the Nortel SNA. You cannot set the state to Normal Learning for Nortel SNA.

Viewing information about Nortel SNA clients

View information about Nortel SNA clients by using 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

Specify Nortel IP phone signatures for the Nortel SNA solution by using 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

Remove a Nortel SNA phone signature by using 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

View configured Nortel SNA phone signatures by using the following command from the Privileged EXEC mode:

```
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 signatures that start with the string Nort.

Fail Open configuration using NNCLI

Configure Fail Open to control network access when the NSNA connection to the switch fails.

Fail Open configuration using NNCLI navigation

- “Configuring Fail Open using NNCLI” (page 296)
- “Disabling Fail Open using NNCLI” (page 297)

Configuring Fail Open using NNCLI

Configure Fail Open to enable and configure Fail Open on the switch.

Prerequisites

- Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure Fail Open globally by using the following command: **nsna fail-open**

--End--

Variable definitions

The following table defines optional parameters that you enter after the **nsna fail-open** command.

Variable	Value
enable	Enables Fail Open on the switch.

Variable	Value
filter-vlan-id <filter-id>	Identifies the unique identifier for the VLAN filter. Values range from 1 to 4094. If no value is selected, the switch applies a value of 0.
vlan-id <vlan-id>	Identifies the VLAN associated with Fail Open filters. Values range from 1 to 4094. If no value is selected, the switch applies a value of 0.

Example of configuring Fail Open using NNCLI

Procedure steps

Step	Action
1	Configure the Fail Open VLAN Id. `ERS-5520<config>#nsna fail-open vlan-id 120`
2	Configure the Fail Open VLAN filter ID. `ERS-5520<config>#nsna fail-open filter-vlan-id 120`
3	Enable Fail Open. `ERS-5520<config>#nsna fail-open enable`

--End--

Disabling Fail Open using NNCLI

Disable Fail Open to discontinue using Fail Open on the switch.

Prerequisites

- Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure Fail Open globally by using the following command:

```
no nsna fail-open
```

--End--

Enabling Nortel SNA

Enable Nortel SNA by using the following command from the Global Configuration mode:

```
nsna enable
```

ATTENTION
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 about SSH, see "Configuring SSH on the 5000 Series switch for Nortel SNA" (page 79).

Disabling Nortel SNA

Disable Nortel SNA by using the following command from the Global Configuration mode:

```
no nsna enable
```

Viewing the Nortel SNA state

View information about the state of Nortel SNA on the switch by using the following command from the Privileged EXEC configuration mode:

```
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 Ethernet Routing Switch 5000 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.

Default Nortel SNA filters are used in this example.

Scenario

Figure 7 "Basic network scenario" (page 300) 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.

Table 86
Network devices

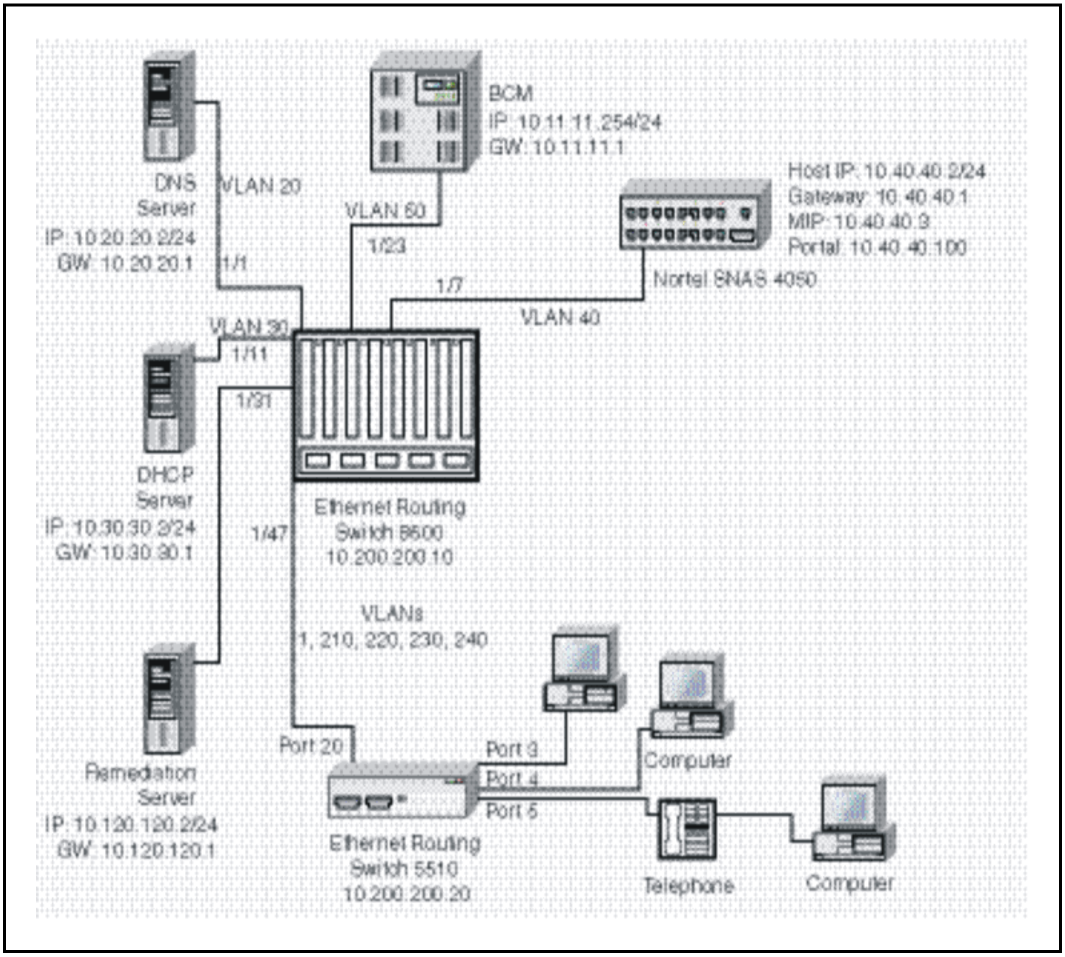
Device/Service	VLAN ID	VLAN IP	Device IP	Ethernet Routing Switch 8600 port
DNS	20	10.20.20.1	10.20.20.2	1/1
DHCP	30	10.30.30.1	10.30.30.2	1/11
Nortel SNAS 4050	40	10.40.40.1	10.40.40.2	1/7
Remediation server	120	10.120.120.1	10.120.120.2	1/31
Call server	50	10.11.11.1	10.11.11.254	1/23

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

Table 87
VLANs for the Ethernet Routing Switch 5510

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

Figure 7
Basic network scenario



Steps

The example illustrates the following required configuration steps:

1. “Setting the switch IP address” (page 301)
2. “Configuring SSH” (page 301)
3. “Configuring the Nortel SNAS 4050 pVIP subnet” (page 301)

4. “Creating port-based VLANs” (page 301)
5. “Configuring the VoIP VLANs” (page 301)
6. “Configuring the Red, Yellow, and Green VLANs” (page 302)
7. “Configuring the log on domain controller filters” (page 302)
8. “Configuring the Nortel SNA ports” (page 302)
9. “Enabling Nortel SNA globally” (page 302)

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 is already 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
```

ATTENTION
You must import the switch SSH key on the Nortel SNAS 4050 after enabling SSH on the Ethernet Routing Switch 5000 Series switch. For more information about, see “Configuring SSH on the 5000 Series switch for Nortel SNA” (page 79). Also, for more information about configuring SSH on the Nortel SNAS 4050, see *Nortel Secure Network Access Switch 4050 User Guide* () (320818-A).

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

ATTENTION
This step is optional.

ATTENTION
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 5000 Series as a network access device in the Nortel Secure Network Access (Nortel SNA) solution using Device Manager.

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 77).

Navigation

Configuring the Nortel SNAS 4050 subnet using Device Manager

ATTENTION
In Ethernet Routing Switch 5000 Series, software release 5.1 and later, supports only one entry for the Nortel SNAS 4050 subnet configuration.

Configure the Nortel SNAS 4050 portal Virtual IP (pVIP) subnet by following this procedure:

Procedure steps

Step	Action

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

The NASA dialog box appears with the NSNAS tab selected.

The following table describes the NSNAS tab fields.

Table 88
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.

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

> **ATTENTION**
> The default Red filter set uses pVIP address 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 associating 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--

Removing the Nortel SNAS 4050 subnet using Device Manager

Remove the currently configured Nortel SNAS 4050 by following this procedure:

Procedure steps

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 NSNA configuration.

--End--

Configuring QoS for the Nortel SNA solution using Device Manager

For general information about configuring filters and Quality of Service (QoS) in the Nortel SNA solution, see "Filters in the Nortel SNA solution" (page 69). For detailed information about configuring the filters, see *Nortel Ethernet Routing Switch 5000 Series Configuration — Quality of Service* () (NN47200-504).

Configuring Nortel SNA per VLAN using Device Manager

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

Configure the Nortel SNA VLANs by following this procedure:

Procedure steps

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 more information about creating the VLANs, see *Nortel Ethernet Routing Switch 5000 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking* () (NN47200-502).

Once you create a VLAN, the VLAN information appears in the Basic tab of the VLAN dialog box.

3 Click the **NSNA** tab.

The following table describes the VLAN NSNA tab fields.

Table 89
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. **ATTENTION** 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). **ATTENTION** This field is applicable only when the NsnaColor field is set to yellow.

Table 89
VLAN NSNA tab fields (cont'd.)

Field	Description
YellowSubnet	Specifies the subnet of the Yellow VLAN. **ATTENTION** This field is applicable only when the NsnaColor field is set to yellow.
YellowSubnetMask	Specifies the mask for the Yellow VLAN subnet. **ATTENTION** 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 menu.

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

6 Click **Apply**.

> **ATTENTION**
> Each switch must have only one, Red VLAN. Each switch can, however, have multiple Yellow, multiple Green, and multiple VoIP VLANs. Each Ethernet Routing Switch 5000 Series 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--

Removing a Nortel SNA VLAN

Remove a Nortel SNA VLAN by following this procedure:

Procedure steps

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.

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 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 changed the Nortel SNA color to none.

c Click **Delete**.

--End--

Enabling Nortel SNA on ports using Device Manager

Enable Nortel SNA on ports by following this procedure:

Procedure steps

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.

3 Click the **NSNA** tab.

The NSNA tab is selected.

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

Table 90
Port—NSNA tab fields

Field	Description
Mode	Specifies the Nortel SNA mode for the port. Options are the following: • disabled • dynamic • uplink **ATTENTION** 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. **ATTENTION** This field is only available when the port mode is dynamic.
UplinkVlans	Specifies the Nortel SNA uplink VLANs to which this port belongs. **ATTENTION** 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--

Configuring Nortel SNA using Device Manager

Configure Nortel SNA to globally enable or disable Nortel SNA, and to view Nortel SNA status information.

Prerequisites

- You must enable SSH before you can enable Nortel SNA globally. For more information about SSH, see "Configuring SSH on the 5000 Series switch for Nortel SNA" (page 79).

Procedure steps

Step	Action

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

2 Click the **Globals** tab.

The NSNA, Globals dialog box appears displaying NSNA status information.

3 To globally enable Nortel SNA, select the **Enabled** box.

OR

To globally disable Nortel SNA, deselect the **Enabled** box.

4 Click **Apply**.

> **ATTENTION**
> It can take 2–3 minutes to globally enable/disable Nortel SNA, especially on a fully populated stack.

--End--

Variable definitions

Use the data in the following table to configure Nortel SNA.

Variable	Value
Enabled	Enables or disables Nortel SNA on the network access device.
NsnasConnectionState	Displays the status of the connection between the network access device and the Nortel SNAS 4050.

Variable	Value
NsnasInetAddressType	Displays the type of IP address used by the Nortel SNAS 4050.
NsnasInetAddress	Displays the pVIP of the Nortel SNAS 4050.
NsnasSendHelloInterval	Displays the time interval, in seconds, 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, 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 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 Nortel SNAS has disconnected and the status-quo interval timer is running, this value will reflect the remaining time, until the status-quo timer expires. **ATTENTION**

Variable	Value
	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.

Viewing information about Nortel SNA clients using Device Manager

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

Procedure steps

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 Nsna Client tab. The Nsna Client tab is selected. Tab displays the clients currently connected to the network access device. The following table describes the **Nsna Client** fields.

Table 91
NSNA—Nsna client tab fields

Field	Description
IfIndex	Specifies 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	Specifies 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).

Table 91
NSNA—Nsna client tab fields (cont'd.)

Field	Description
Address	Specifies the IP address of the client.
Expired	Indicates whether this client has been aged-out.

--End--

Entering phone signatures for Nortel SNA using Device Manager

Specify IP phone signatures for Nortel SNA by following this procedure:

Procedure steps

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.
3	Click **Insert**. The NSNA, Insert IP Phone Signature dialog box appears.
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--

Removing Nortel SNA phone signatures

Remove a Nortel SNA phone signature by following this procedure:

Procedure steps

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.

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

4 Click **Delete**.

--End--

Configuring Nortel SNA static clients using Device Manager

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 more information, see *Nortel Secure Network Access Switch 4050 User Guide for NNCLI* () (NN47230-100).

Configuring Fail Open using Device Manager

Configure Fail Open to enable and configure or disable Fail Open on the switch.

Procedure steps

Step	Action
1	Select **Edit, Security, NSNA** from the Device Manager menu.
2	Click the **Fail Open** tab.
3	Select the **FailOpenEnabled** box to enable Fail Open.
4	In the **FailOpenVlan** dialog box, type a VLAN ID.
5	In the **FailOpenFilterVlan** dialog box, type a VLAN filter ID.
6	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure Fail Open.

Variable	Value
FailOpenEnabled	Enables or disables Fail Open on the switch.

Variable	Value
FailOpenVlan	Identifies the Fail Open VLAN. Values range from 1 to 4094. If no value is selected, the switch applies a value of 0.
FailOpenFilterVlan	Identifies the VLAN associated with Fail Open filters. Values range from 1 to 4094. If no value is selected, the switch applies a value of 0.

Appendixes

This section contains information about the following topics:

- "TACACS+ server configuration examples" (page 317)
- "Supported SNMP MIBs and traps" (page 333)
- "Default Nortel SNA filters" (page 339)

TACACS+ server configuration examples

See the following sections for basic configuration examples of the TACACS+ server:

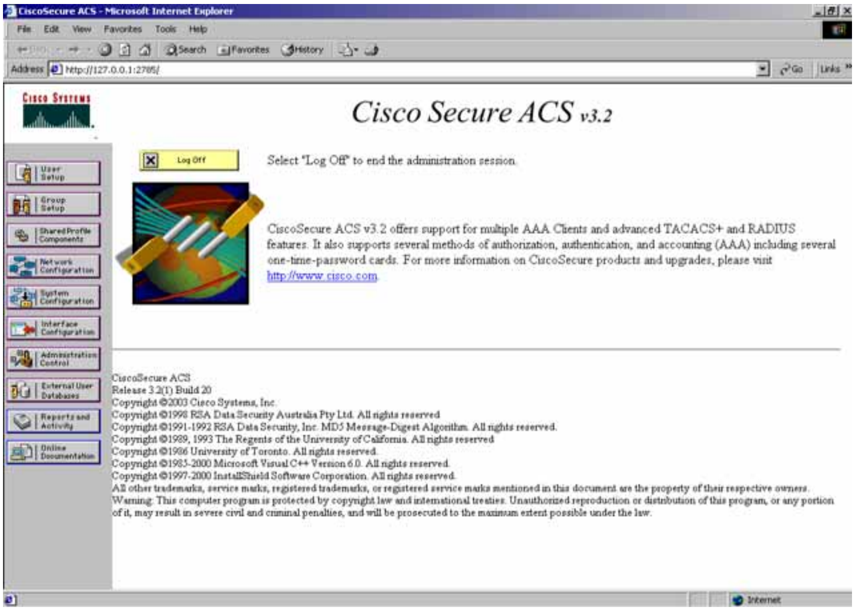
- "Configuration example: Cisco ACS (version 3.2) server" (page 317)
- "Configuration example: ClearBox server" (page 323)
- "Configuration example: Linux freeware server" (page 331)

See 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.

Figure 8
Cisco ACS (version 3.2) main administration window



Select "Log Off" to end the administration session.

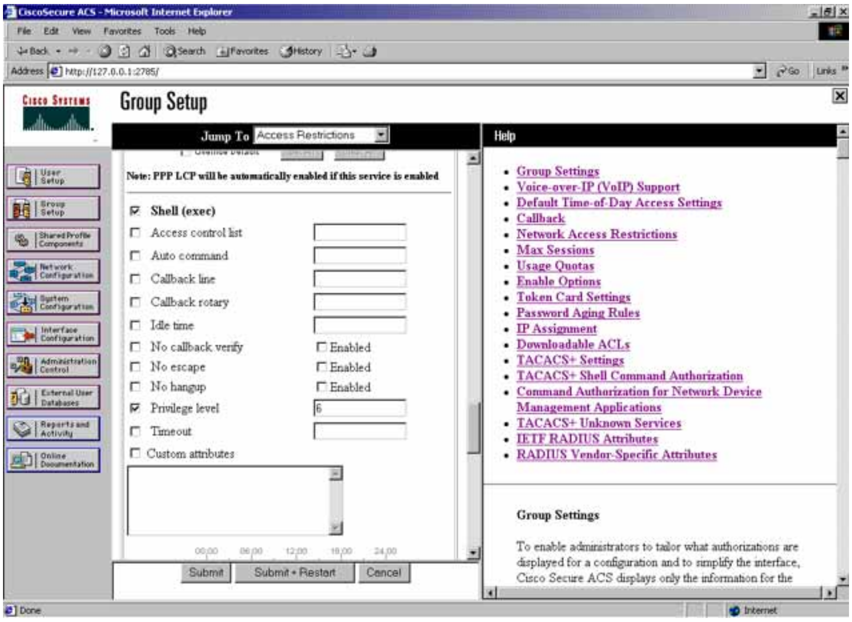
CiscoSecure ACS v3.2 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit 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.

Procedure steps

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.

Figure 9
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

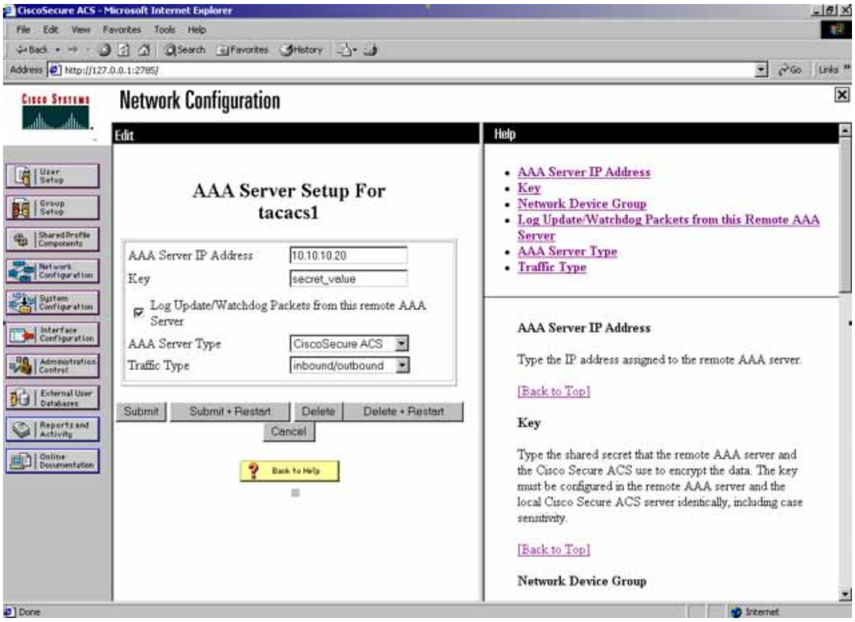
Group Settings

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+.

Figure 10
Network Configuration window - server setup



Network Configuration

Edit

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.

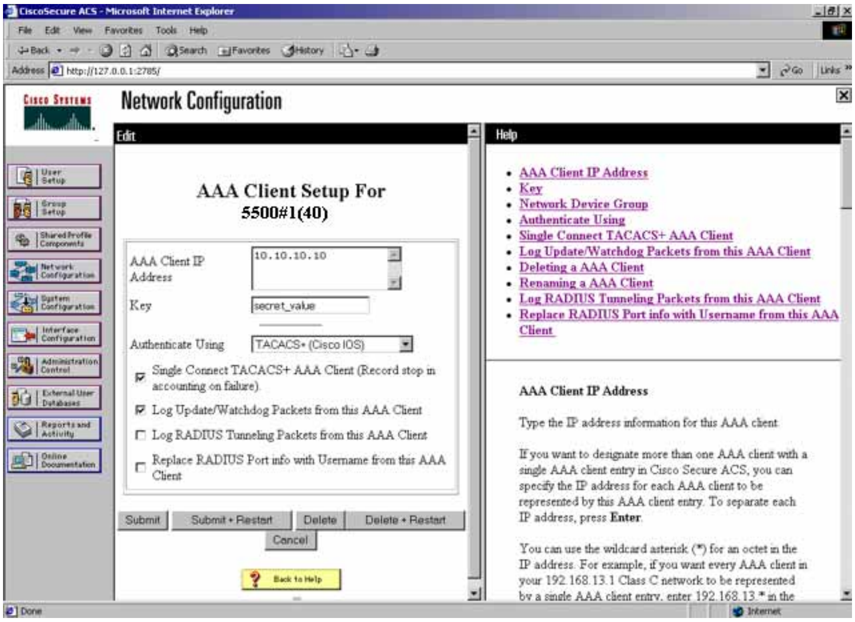
[Back to Top]

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 5000 Series.

Figure 11
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

- 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.

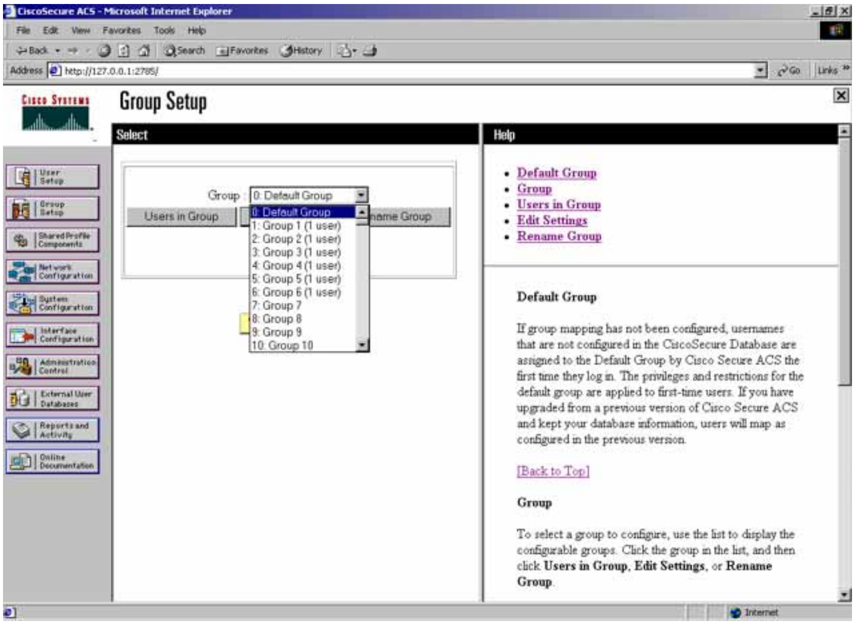
If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

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 and L1 accounts belong to group 2.

Figure 12
Group Setup window - viewing the group setup



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.

Group

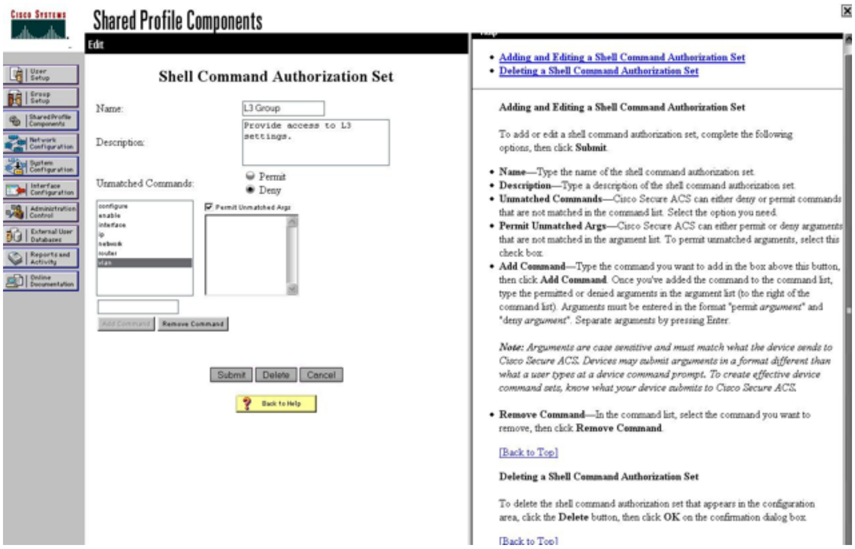
To select a group to configure, use the list to display the configurable groups. Click the group in the list, and then click **Users in Group**, **Edit Settings**, or **Rename Group**.

5 Specify the commands 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.

Figure 13
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

configure
enable
interface
ip
network
router
vlan

☑ 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

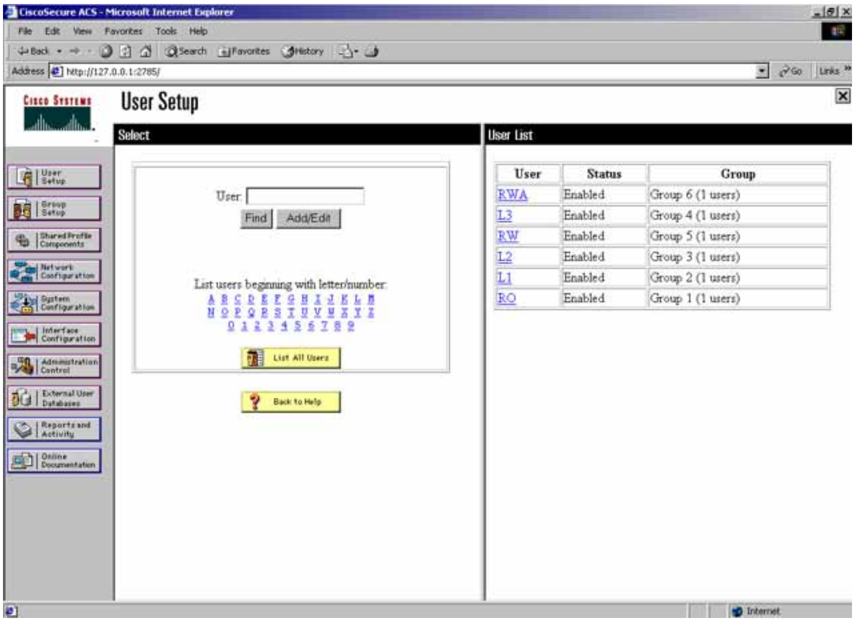
To delete the shell command authorization set that appears in the configuration area, click the **Delete** button, then click **OK** on the confirmation dialog box.

[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.

Figure 14
User Setup window - Cisco ACS server configuration



User:

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)

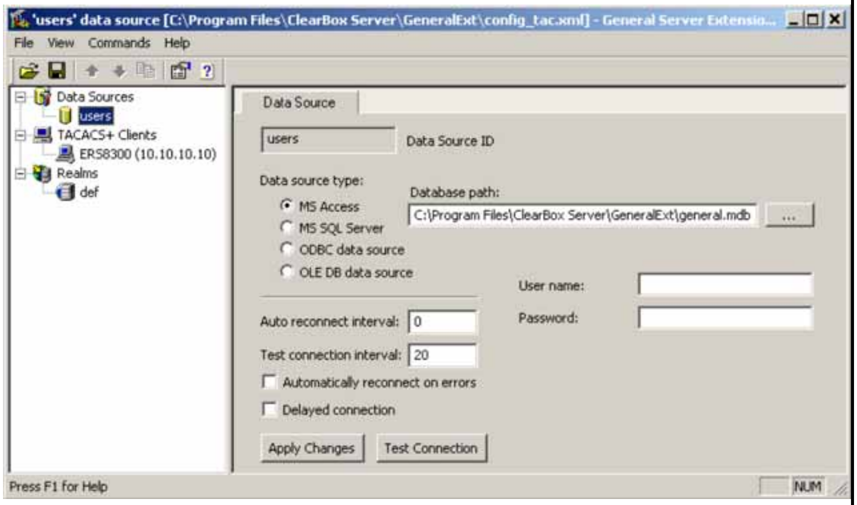
--End--

Configuration example: ClearBox server

Procedure steps

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.

Figure 15
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

users Data Source ID

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

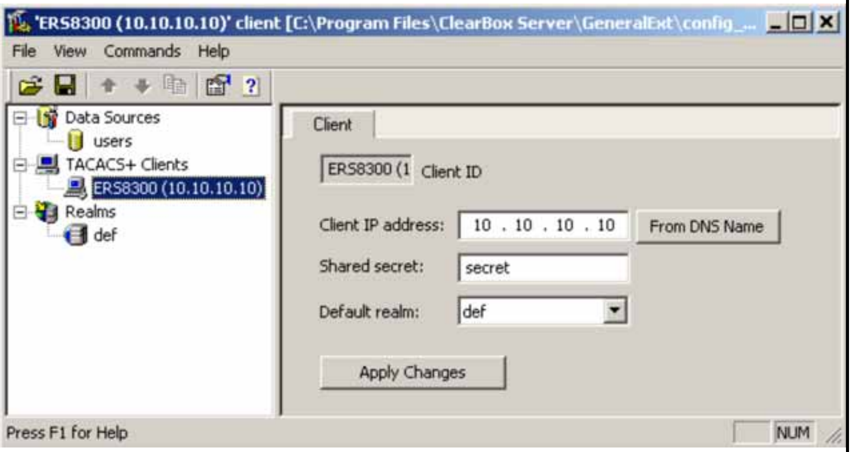
□ Automatically reconnect on errors

□ 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 Ethernet Routing Switch 5000 Series. Enter the appropriate information. The shared secret must match the value configured on the Ethernet Routing Switch 5000 Series.

Figure 16
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

ERS8300 (1 Client ID

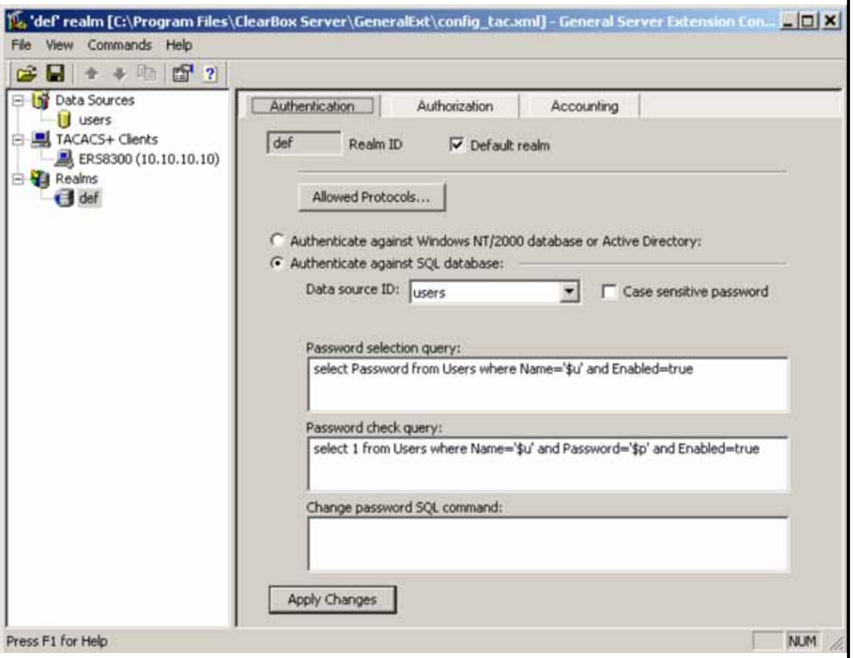
Client IP address: 10 . 10 . 10 . 10

Shared secret: secret

Default realm: def

The default realm Authentication tab looks like the following figure.

Figure 17
Default realm - Authentication tab



'def' realm [C:\Program Files\ClearBox Server\GeneralExt\config_tac.xml] - General Server Extension Con...

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

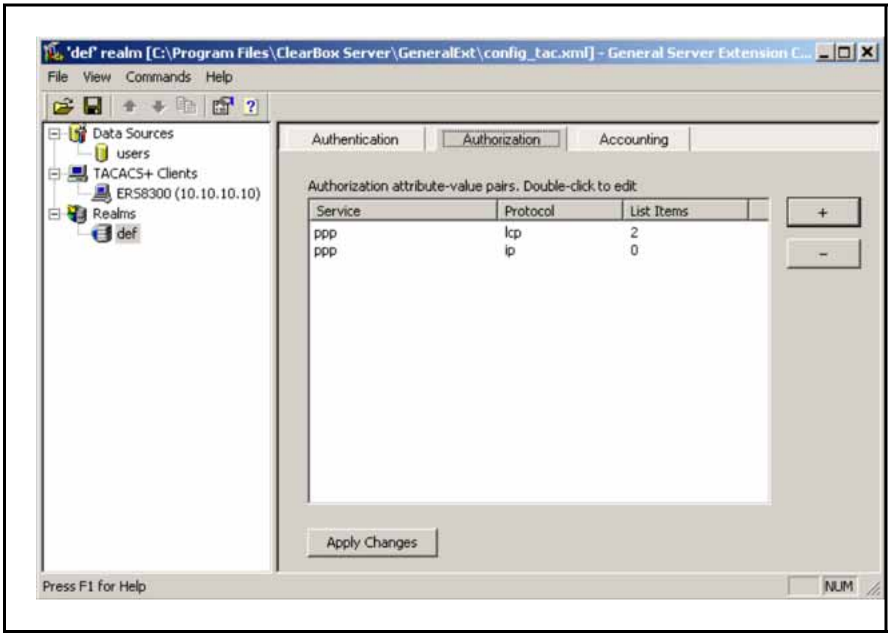
Change password SQL command:

3 Click **Realms, def, Authorization** tab.

A new service is required that allows the server to assign certain levels of access.

4 Click **+** to add an attribute-value pair for privilege levels (see the following figure).

Figure 18
Default realm - Authorization tab



Authorization attribute-value pairs. Double-click to edit

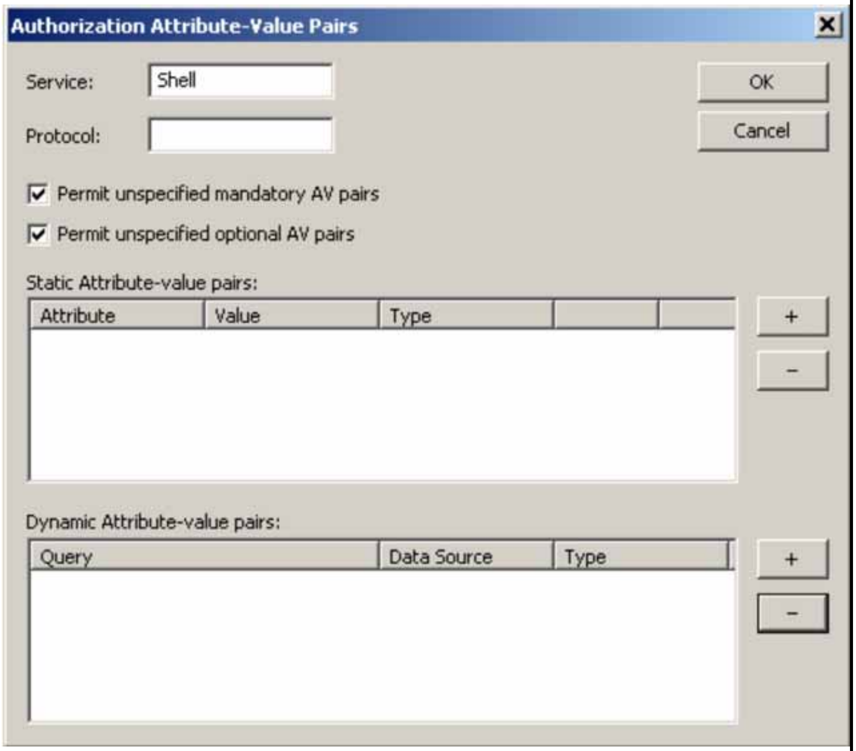
Service	Protocol	List Items
ppp	lcp	2
ppp	ip	0

5 Specify the query parameters.

a Enter information in the window as shown in the following figure.

b Click **+** to add the parameters to the query.

Figure 19
Adding parameters for the query



Authorization Attribute-Value Pairs
OK
Cancel
Static Attribute-value pairs:
Attribute
Value
Type
+
-
Dynamic Attribute-value pairs:
Query
Data Source
Type
+
-

Service: Shell

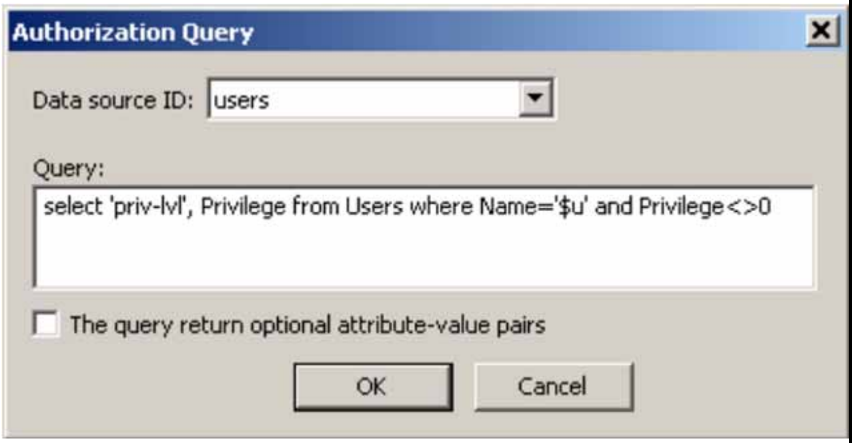
Protocol:

☑ Permit unspecified mandatory AV pairs

☑ Permit unspecified optional AV pairs

6 Use the string shown in the following figure for the authorization query.

Figure 20
Authorization Query window



Data source ID: users

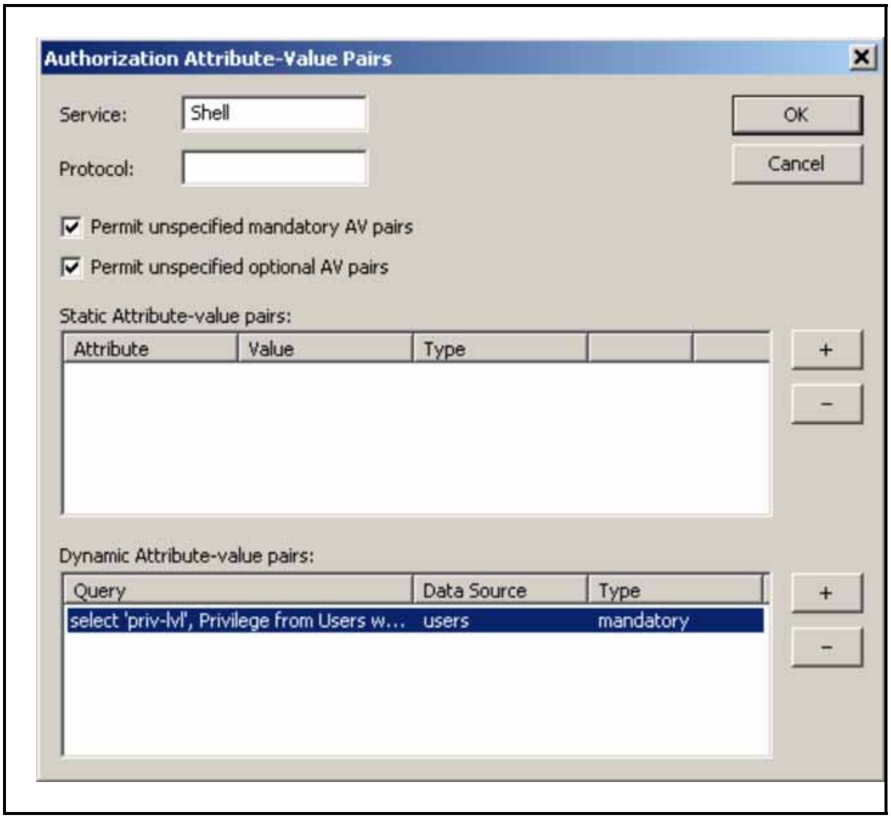
Query:

```
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.

Figure 21
Query parameters added to Authorization Attribute-Value Pairs window



Service: Shell

Protocol:

☑ Permit unspecified mandatory AV pairs

☑ Permit unspecified optional AV pairs

Static Attribute-value pairs:

Attribute	Value	Type		

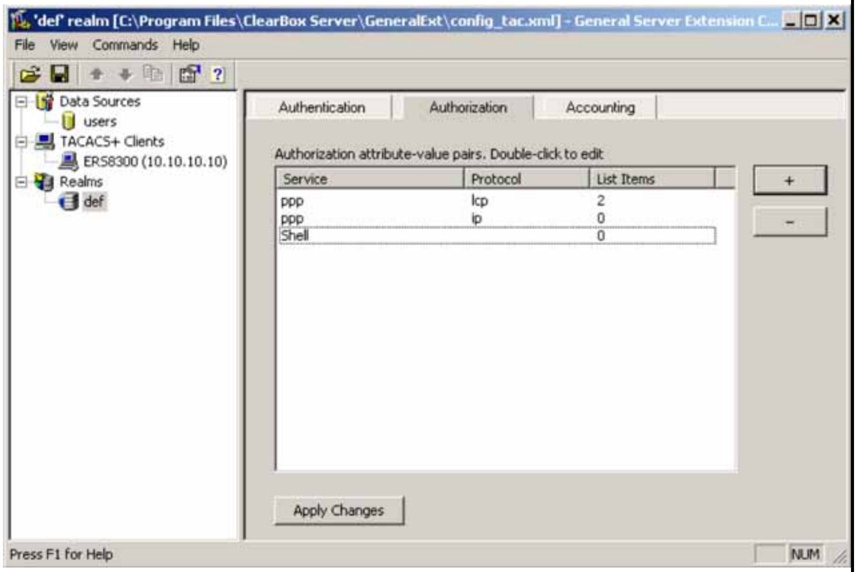
Dynamic Attribute-value pairs:

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).

Figure 22
Authorization attribute-value pairs added to Authorization tab



Authorization attribute-value pairs. Double-click to edit

Service	Protocol	List Items
ppp	lcp	2
ppp	ip	0
Shell		0

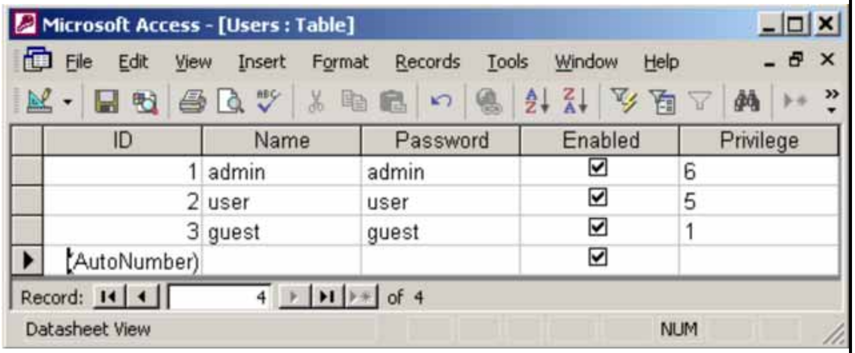
8 Navigate to the general.mdb file as specified earlier.

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.

Microsoft Access or third-party software is required to read this file.

> **ATTENTION**
> If you use the 30-day demo for ClearBox, the user names cannot be more than four characters in length.

Figure 23
Users table - Microsoft Access

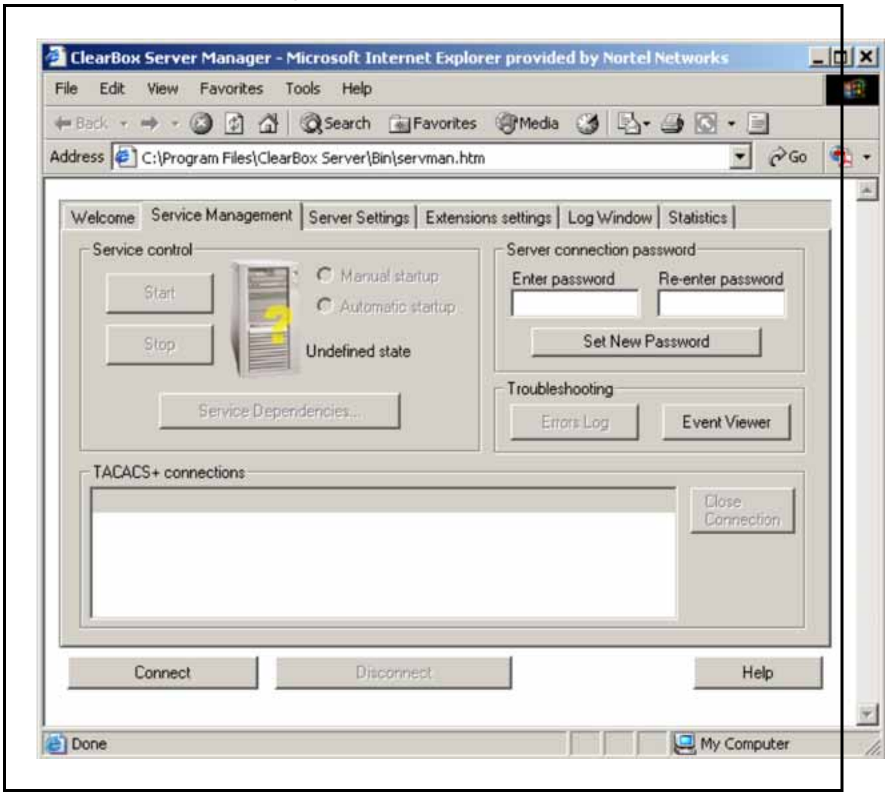

Microsoft Access - [Users : Table]
File Edit View Insert Format Records Tools Window Help
Record: 4 of 4
Datasheet View
NUM

ID	Name	Password	Enabled	Privilege
1	admin	admin	☑	6
2	user	user	☑	5
3	guest	guest	☑	1
(AutoNumber)			☑	

9 Start the server.

a Run the Server Manager (see the following figure).

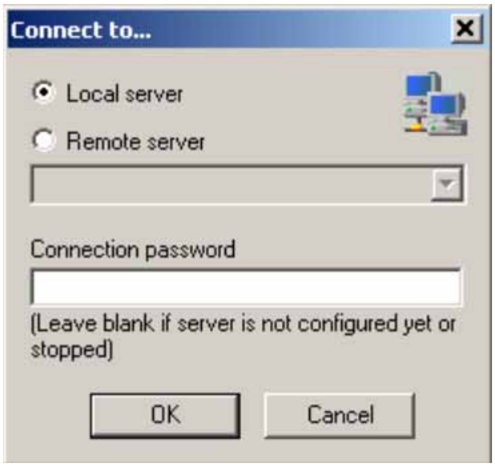
Figure 24
ClearBox Server Manager



b Click **Connect**.

The Connect to... dialog box appears (see the following figure).

Figure 25
Connect to... dialog box



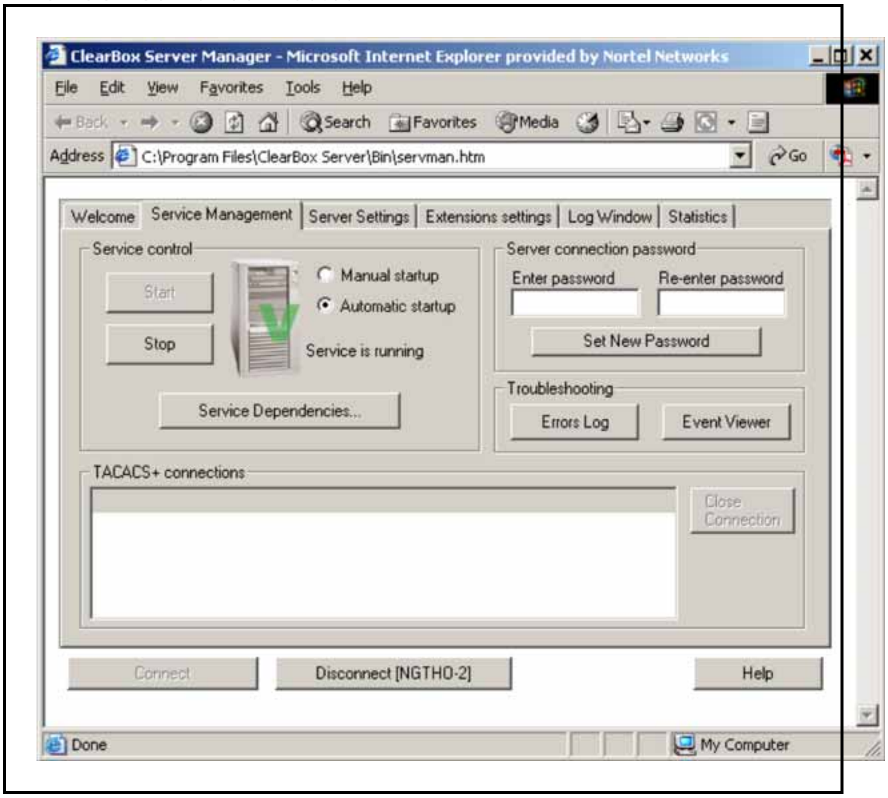
c Click **OK** (do not fill in fields).

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 restarting the server.

Figure 26
TACACS+ server connected



--End--

Configuration example: Linux freeware server

Procedure steps

Step	Action
1	After installing TACACS+ 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 configuration file. Add the following lines:

```
# 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 you configure on the switch while 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

<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 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 333)
- Table 95 "New MIBs" (page 335)
- “Supported traps” (page 335)

Supported MIBs

The following tables list supported SNMP MIBs.

Table 92
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

Table 93
SNMP proprietary MIB support

MIB name	File name
S5-AGENT-MIB	s5age.mib
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

Table 94
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

Table 94
Application and related MIBs (cont'd.)

Application	Related MIBs	File name
Policy management	NTN-QOS-POLICY-EVOL-PIB	pibNtnEvol.mib
RMON-MIB	RMON-MIB	rfc2819.mib
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:

Table 95
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.

Table 96
Supported SNMP traps

Trap name	Configurable	Sent when
RFC 2863 (industry standard):		
linkUp	For each port	A port link state changes to up.
linkDown	For each port	A port link state changes to down.
RFC 3418 (industry standard):		
authenticationFailure	System wide	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	A stack is configured.
BAY-STACK-ADAC-MIB:		
bsAdacPortConfiguration	For each port	Auto-configuration status changes on the port.
LLDP-MIB; LLDP-EXT-MED-MIB:		

Table 96
Supported SNMP traps (cont'd.)

Trap name	Configurable	Sent when
lldpRemTablesChange	System-wide	The value of lldpStatsRemTableLas t ChangeTime changes.
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 of connection close is provided.
nsnaStatusQuoIntervalExpired	System-wide	The status-quo interval expires after the connection to the Nortel SNAS 4050 closes.
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	For each 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.

Table 96
Supported SNMP traps (cont'd.)

Trap name	Configurable	Sent when
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.
nnMstProtocolMigration	For each 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 is transitioned to Master state.
vrrpTrapAuthFailure	System-wide	A packet is received from a router whose authentication key or authentication type conflicts with this router authentication key or authentication type. Implementation of this trap is optional.
bsveVrrpTrapStateTransition	For each port	A state transition is occurred on a particular VRRP interface. Implementation of this trap is optional.
bsDhcpSnoopingBindingTableFull	System-wide	DHCP binding table is full. Additional untrusted DHCP packets will not be added to the binding table and will be dropped.
bsDhcpSnoopingTrap	System-wide	DHCP REQUEST, RELEASE/DECLINE, REPLY, OFFER, ACK, NAK and LEASEQUERY dropped on untrusted port.
bsaiArpPacketDroppedOnUntrustedPort	System-wide	An ARP packet is dropped on untrusted port due to invalid IP/MAC binding.
bsSourceGuardReachedMaxIpEntries	System-wide	The maximum IP entries on the port has been reached.
bsSourceGuardCannotEnable Port	System-wide	Insufficient resources are available to enable IPSG on the port.
nnRstGenNotificationType	System-wide	Any of the general events like protocol up or protocol down occur.

Table 96
Supported SNMP traps (cont'd.)

Trap name	Configurable	Sent when
nnRstErrNotificationType	System-wide	Any of the error events like memory failure, buffer failure, protocol migration, new root topology or topology change occur.
nnRstDot1wOldDesignatedRoot	System-wide	A new root bridge is selected in the topology.
nnRstTopologyChange	System-wide	A topology change is detected.
nnRstPortNotificationMigrationType	System-wide	A port migration happens in the port.

Default Nortel SNA filters

This section includes the following topics:

- "Default filter configuration" (page 339)
- "Default filter parameters" (page 341)

Default filter configuration

The following example shows the default Nortel SNA filters created automatically by the switch. If you use the default filters created by the switch, must 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

```
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

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

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

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

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

```
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

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

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

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
```

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

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.

Table 97
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 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	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 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	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 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

Red filter set	Yellow filter set	Green filter set
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 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: 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 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	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	

Red filter set	Yellow filter set	Green filter set
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	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	
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	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	

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

Red filter set	Yellow filter set	Green filter set
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 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: 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 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:	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:	

Red filter set	Yellow filter set	Green filter set
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	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 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	

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: 0 Kbps Commit Burst: 0 Bytes Out-Profile Action: None Non-Match Action: Drop Storage Type: NonVolatile	

Index

Nortel Ethernet Routing Switch 5000 Series

Configuration — Security

Release: 6.1
Publication: NN47200-501
Document revision: 05.01
Document release date: 20 May 2009

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OFANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

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

www.nortel.com