Part No. 217104-A
June 2005

4655 Great America Parkway
Santa Clara, CA 95054

# Configuring and Managing Security

## Nortel Ethernet Switches 460 and 470
## Software Release 3.6


NORTEL

## International regulatory statements of conformity

This is to certify that the Nortel Ethernet Switches 460 and 470 were evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC - Electromagnetic Emissions – CISPR 22, Class A
- EMC - Electromagnetic Immunity – CISPR 24
- Electrical Safety – IEC 60950, with CB member national deviations

Further, the equipment has been certified as compliant with the national standards as detailed below.

## National electromagnetic compliance (EMC) statements of compliance

### FCC statement (USA only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

### ICES statement (Canada only)

#### Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Nortel Ethernet Switches 460 and 470) do not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

#### Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Nortel Ethernet Switches 460 and 470) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

### CE marking statement (Europe only)

#### EN 55 022 statements

This is to certify that the Nortel Ethernet Switches 460 and 470 are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

**Caution:** This device is a Class A product. In a domestic environment, this device can cause radio interference, in which case the user may be required to take appropriate measures.

### EN 55 024 statement

This is to certify that the Nortel Ethernet Switches 460 and 470 are shielded against the susceptibility to radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of
EN 55 024 (CISPR 24).

### CE Declaration of Conformity

This product conforms to the provisions of the R&TTE Directive 1999/5/EC.

## VCCI statement (Japan/Nippon only)

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

## BSMI statement for Ethernet Switches 460 and 470 (Taiwan only)

This is a Class A product based on the standard of the Bureau of Standards, Metrology and Inspection (BSMI) CNS 13438, Class A.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者 會被要求採取某些適當的對策。

## MIC notice for Ethernet Switches 460 and 470 (Republic of Korea only)

This device has been approved for use in Business applications only per the Class A requirements of the Republic of Korea Ministry of Information and Communications (MIC). This device may not be sold for use in a non-business application.

Observe the Regulatory Marking label on the bottom surface of the chassis for specific certification information pertaining to this model. Each model in the Ethernet Switch Series which is approved for shipment to/usage in Korea is labeled as such, with all appropriate text and the appropriate MIC reference number.

# National safety statements of compliance

## CE marking statement (Europe only)

### EN 60 950 statement

This is to certify that the Nortel Ethernet Switches 460 and 470 are in compliance with the requirements of EN 60 950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance.

## NOM statement Ethernet Switches 460 and 470 (Mexico only)

The following information is provided on the devices described in this document in compliance with the safety requirements of the Norma Oficial Méxicana (NOM):

| | |
|---|---|
| Exporter: | Nortel Networks, Inc.<br>4655 Great America Parkway<br>Santa Clara CA 95054 USA |
| Importer: | Nortel Networks de México, S.A. de C.V.<br>Avenida Insurgentes Sur #1605<br>Piso 30, Oficina<br>Col. San Jose Insurgentes<br>Deleg-Benito Juarez<br>México D.F. 03900 |
| Tel: | 52 5 480 2100 |
| Fax: | 52 5 480 2199 |
| Input: | Ethernet Switch 460, Ethernet Switch 470 |
| | 100 - 120 VAC 16A 50 to 60 Hz |
| | 200 - 240 VAC 12 A 50 to 60 Hz |

## Información NOM (unicamente para México)

La información siguiente se proporciona en el dispositivo o en los dispositivos descritos en este documento, en cumplimiento con los requisitos de la Norma Oficial Méxicana (NOM):

| | |
|---|---|
| Exportador: | Nortel Networks, Inc.<br>4655 Great America Parkway<br>Santa Clara, CA 95054 USA |
| Importador: | Nortel Networks de México, S.A. de C.V.<br>Avenida Insurgentes Sur #1605<br>Piso 30, Oficina<br>Col. San Jose Insurgentes<br>Deleg-Benito Juarez<br>México D.F. 03900 |
| Tel: | 52 5 480 2100 |
| Fax: | 52 5 480 2199 |
| Embarcar a: | Ethernet Switch 460, Ethernet Switch 470 |
| | 100 - 120 VAC 16A 50 to 60 Hz |
| | 200 - 240 VAC 12 A 50 to 60 Hz |

## Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

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

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

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

3. **Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. **General**

   a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government,

the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-Odd entities) and 48 C.F.R. 227.7202 (for Odd entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

## Revision History

| Date Revised | Version | Reason for revision |
|---|---|---|
| June 2005 | 1.0 | Created new document structure and incorporated new features for Ethernet Switch Release 3.6 software. |

# Contents

# Figures

# Tables

# Preface

## About this guide

This guide provides information about configuring and managing Quality of Service and IP Filtering features on the Nortel Ethernet Switch 460 and Nortel Ethernet Switch 470.

## Network management tools and interfaces

The following are the management tools and interfaces available with the switch (for basic instructions on these tools, refer to the *System Configuration Guide* (217105-A)):

- Console interface

  The console interface (CI) allows you to configure and manage the switch locally or remotely. Access the CI menu and screens locally through a console terminal attached to your Ethernet Switch, remotely through a dial-up modem connection, or in-band through a Telnet session.

- Web-based management

  You can manage the network from the World Wide Web and can access the Web-based Graphical User Interface (GUI) through the HTML-based browser located on your network. The GUI allows you to configure, monitor, and maintain your network through web browsers. You can also download software using the web.

- Java-based Device Manager

  The Device Manager is a set of Java-based graphical network management applications that is used to configure and manage Ethernet Switches 460 and 470.

- Command Line Interface (CLI)

  The CLI is used to automate general management and configuration of the Ethernet Switches 460 and 470. Use the CLI through a Telnet connection or through the serial port on the console.

- Any generic SNMP-based network management software

  You can use any generic SNMP-based network management software to configure and manage Ethernet Switches 460 and 470.

- Telnet

  Telnet allows you to access the CLI and CI menu and screens locally using an in-band Telnet session.

- SSH

  Secure Shell (SSH) is a client/server protocol that can provide a secure remote login with encryption of data, username, and password.

- Nortel Enterprise Policy Manager

  The Nortel Enterprise Policy Manager (formerly Optivity Policy Services) allows you to configure the Ethernet Switches 460 and 470 with a single system.

## Before you begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks, bridging, and IP
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies

Before using this guide, you must complete the installation procedures discussed in *Installing the Nortel Ethernet Switch 460-24T-PWR* (213318-C) or *Installing the Nortel Ethernet Switch 470* (217108-A).

# Text conventions

| | |
|---|---|
| angle brackets (< >) | Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.<br>Example: If the command syntax is<br>`ip default-gateway <XXX.XXX.XXX.XXX>`,<br>you enter<br>`ip default-gateway 192.32.10.12` |
| braces ({ }) | Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.<br>Example: If the command syntax is<br>`http-server {enable\|disable}`<br>the options are `enable` or `disable`. |
| brackets ([ ]) | Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.<br>Example: If the command syntax is<br>`show ip [bootp]`,<br>you can enter either:<br>`show ip` or `show ip bootp`. |
| `plain Courier text` | Indicates command syntax and system output.<br>Example:<br>`TFTP Server IP Address:  192.168.100.15` |
| vertical line \| | Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.<br>Example: If the command syntax is<br>`cli password <serial\|telnet>`,<br>you must enter either `cli password serial` or `cli password telnet`, but not both. |
| H.H.H. | Enter a MAC address in this format (XXXX.XXXX.XXXX). |

# Related publications

For more information about managing or using the switches, refer to the following publications:

- *Release Notes for the Ethernet Switch 460 and 470 Switch Software Version 3.6* (217103)
- *Installing the Nortel Ethernet Switch 460-24T-PWR* (213318-C)
- *Installing the Nortel Ethernet Switch 470* (217108-A)
- *System Configuration Guide* (217105-A)
- *Configuring Quality of Service, and IP Filtering* (217106-A)
- *System Monitoring Guide* (217107-A)
- *Configuring IP Multicast Routing Protocols* (217459-A)
- *Configuring VLANs, Spanning Tree, and MultiLink Trunking*
- *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* (312865-B)

You can print selected technical manuals and release notes free, directly from the Internet. Go to www.nortel.com/support. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems web site to download a free copy of the Adobe Acrobat Reader.

# Obtaining technical assistance

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

If you purchased a Nortel service program, contact one of the following Nortel Technical Solutions Centers:

| Technical Solutions Center | Telephone |
|---|---|
| Europe, Middle East, and Africa | (33) (4) 92-966-968 |
| North America | (800) 4NORTEL or (800) 466-7835 |
| Asia Pacific | (61) (2) 9927-8800 |
| China | (800) 810-5000 |

Additional information about the Nortel Technical Solutions Centers is available from www.nortel.com/callus.

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

# Chapter 1
# Using security in your network

This chapter describes the security features available with the Ethernet Switches 460 and 470, and their applicable Console Interface (CI) commands. This chapter discusses the following topics:



## IP manager list

You can limit access to the management features of the Ethernet Switches 460 and 470 by defining the IP addresses that are allowed to access the switch. The features provided by the IP manager list are:

- definitions of up to 50 allowed IP addresses and masks
- options to enable or disable access for Telnet, Simple Network Management Protocol (SNMP), and the Web-based management system

You must set the Telnet feature after the first power-up.

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

## Configuring Telnet/SNMP/Web access using the Console Interface

You must change the Telnet access field by connecting directly to the device through the serial port.

You cannot change the Telnet access field through a Telnet connection.

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

Configuring Telnet access does not affect any existing sessions. The changes in the configuration are enforced for all subsequent Telnet connections.

Figure 1 displays the TELNET/SNMP/Web Access Configuration screen.

**Figure 1** TELNET/SNMP/Web Access Configuration screen

```
                TELNET/SNMP/Web Access Configuration

 TELNET:                                |            Access:       Use List:
 Login Timeout      :[ 1 minute ]       |  TELNET: [ Enabled  ]     [ Yes ]
 Login Retries      :[ 3 ]              |  SNMP  : [ Enabled  ]     [ Yes ]
 Inactivity Timeout:[ 15 minutes ]      |  WEB   : [ Enabled  ]     [ Yes ]
 Event Logging      :[ All       ]      |

#          Allowed Source IP Address             Allowed Source Mask
--         -------------------------          -------------------------
 1            [ 0.0.0.0 ]                          [ 0.0.0.0 ]
 2            [ 255.255.255.255 ]                  [ 255.255.255.255 ]
 3            [ 255.255.255.255 ]                  [ 255.255.255.255 ]
 4            [ 255.255.255.255 ]                  [ 255.255.255.255 ]
 5            [ 255.255.255.255 ]                  [ 255.255.255.255 ]
 6            [ 255.255.255.255 ]                  [ 255.255.255.255 ]
 7            [ 255.255.255.255 ]                  [ 255.255.255.255 ]
 8            [ 255.255.255.255 ]                  [ 255.255.255.255 ]
 9            [ 255.255.255.255 ]                  [ 255.255.255.255 ]
 10           [ 255.255.255.255 ]                  [ 255.255.255.255 ]

Press Ctrl-N to display next screen.
Enter number, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main
Menu.
```

Table 4 describes the TELNET/SNMP/Web Access Configuration screen fields.

**Table 1** TELNET/SNMP/Web Access Configuration screen fields

| Field | Description |
|---|---|
| **TELNET Access** | Allows a user remote access to the management systems through a Telnet session.<br>Default Value: Enabled<br>Range: Enabled, Disabled |
| **Login Timeout** | Specifies the amount of time a user has to enter the correct password at the console-terminal prompt.<br>Default Value: 1 minute<br>Range: 0 to 10 minutes (0 indicates “no timeout”) |
| **Login Retries** | Specifies the number of times a user can enter an incorrect password at the console-terminal prompt before the switch terminates the session.<br>Default Value: 3<br>Range: 1 to 100 |
| **Inactivity Timeout** | Specifies the amount of time the session can be inactive before the switch terminates the session.<br>Default Value: 15 minutes<br>Range: 0 to 60 minutes (0 indicates “no timeout”) |
| **Event Logging** | Specifies the types of events that are displayed in the System Log screen (see *System Monitoring Guide* (217107-A)).<br>Default Value: All<br>Range: All, None, Accesses, Failures<br>Description: *None:* Indicates that no Telnet events will be logged in the Event Log screen.<br>*Accesses*: Logs only Telnet connect and disconnect events in the Event Log screen.<br>*Failures:* Logs only failed Telnet connection attempts in the Event Log screen.<br>*All:* Logs the following Telnet events to the Event Log screen:<br>• TELNET connect: Indicates the IP address and access mode of a Telnet session.<br>• TELNET disconnect: Indicates the IP address of the remote host and the access mode, due to either a logout or inactivity.<br>• Failed TELNET connection attempts: Indicates the IP address of the remote host whose IP address is not on the list of allowed addresses, or indicates the IP address of the remote host that did not supply the correct password. |

**Table 1** TELNET/SNMP/Web Access Configuration screen fields (Continued)

| Field | Description |
|---|---|
| **TELNET Access** | Specifies if Telnet access is allowed, and only to those IP addresses on the list.<br>Default Value: Access: Enabled; Use List: Yes<br>Range: Access: Enabled, Disabled; Use List: Yes, No |
| **SNMP Access** | Specifies if SNMP access is allowed, and only to those IP addresses on the list. (SNMP access includes the Device Manager.)<br>Default Value: Access: Enabled; Use List: Yes<br>Range: Access: Enabled, Disabled; Use List: Yes, No |
| **WEB Access** | Specifies if access to the Web-based management system is allowed, and only to those IP addresses on the list.<br>Default Value: Access: Enabled; Use List: Yes<br>Range: Access: Enabled, Disabled; Use List: Yes, No |
| **Allowed Source IP Address** | Specifies up to ten user-assigned host IP addresses that are allowed Telnet access to the management systems.<br>Default Value: 0.0.0.0 (no IP address assigned)<br>Range: Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point |
| **Allowed Source Mask** | Specifies up to ten user-assigned allowed source address masks. The remote IP address is masked with the Allowed Source Mask and, if the resulting value equals the Allowed Source IP address, the connection is allowed.<br>For example, a connection is allowed with the following settings:<br>Remote IP address = 192.0.1.5<br>Allowed Source IP Address = 192.0.1.0<br>Allowed Source Mask = 255.255.255.0<br>Default Value: 0.0.0.0 (no IP mask assigned)<br>Range: Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point |

## Restricted SSH access with IP Manager list

When Telnet is enabled and use list is also enabled, the IP Manager list restricts Secure Shell (SSH) access.

### Configuring IP Manager using the CLI

IP Manager is configured through the Command Line Interface (CLI) using the `ipmgr` command. For more information, see "Configuring the IP manager list" on page 89.

## Password authentication

This section discusses the following topics:

- "Management password: Local"
- "Management password: RADIUS" on page 41

### Management password: Local

The Console/Comm Port Configuration screen (Figure 2 on page 37) allows you to configure and modify the console/comm port parameters and security features of a switch.

To open the Console/Comm Port Configuration screen:

➨ Choose Console/Comm Port Configuration (or press o) from the main menu.

**Figure 2** Console/comm port configuration screen

```
Select C:\WINNT\system32\telnet.exe
                    Console/Comm Port Configuration

        Comm Port Data Bits:                  8 Data Bits
        Comm Port Parity:                     No Parity
        Comm Port Stop Bits:                  1 Stop Bit
        Console Port Speed:                   [ 9600 Baud   ]

        Console Switch Password Type:         [ None                    ]
        Console Stack Password Type:          [ None                    ]
        Telnet/WEB Switch Password Type:      [ None                    ]
        Telnet/WEB Stack Password Type:       [ None                    ]
        Console Read-Only Switch Password:    [ ***************** ]
        Console Read-Write Switch Password:   [ ***************** ]
        Console Read-Only Stack Password:     [ ***************** ]
        Console Read-Write Stack Password:    [ ***************** ]
        RADIUS Password Fallback:             [ No   ]
        Primary RADIUS Server:                [ 0.0.0.0 ]
        Secondary RADIUS Server:              [ 0.0.0.0 ]
        UDP RADIUS Port:                      [ 1645 ]
        RADIUS Shared Secret:                 [ ***************** ]
        RADIUS Timeout Period:                [ 2 seconds ]

Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 2 describes the Console/Comm Port Configuration screen fields used to configure local passwords for managing the switch.

**Table 2** Console/Comm Port Configuration screen fields

| Field | Description |
|---|---|
| Console Switch Password Type | Enables password protection for accessing the console interface (CI) of a *stand-alone switch* through a console terminal.<br><br>If you set this field to Required, you can use the Logout option to restrict access to the CI. You must specify the correct password at the console-terminal prompt. See field definitions for "Console Read-Only Switch Password" on page 38 and "Console Read-Write Switch Password" on page 39 in this table for more information.<br><br>Default Value: None<br><br>Range: None, Local Password, RADIUS Authentication |

**Table 2** Console/Comm Port Configuration screen fields (Continued)

| Field | Description |
|---|---|
| Console Stack Password Type | Enables password protection for accessing the console interface (CI) of a stack through a console terminal.<br>If you set this field to Required, you can use the Logout option to restrict access to the CI. You must specify the correct password at the console-terminal prompt. See field definitions for "Console Read-Only Stack Password" on page 39 and "Console Read-Write Stack Password" on page 39 in this table for more information.<br>Default Value: None<br>Range: None, Local Password, RADIUS Authentication |
| Telnet/WEB Switch Password Type | Enables password protection for accessing the console interface (CI) of a *stand-alone switch* through a Telnet session.<br>If you set this field to Required, you can use the Logout option to restrict access to the CI. Thereafter, you must specify the correct password at the console-terminal prompt. See field definitions for "Console Read-Only Switch Password" and "Console Read-Write Switch Password" in this table for more information.<br>Default Value: None<br>Range: None, Local Password, RADIUS Authentication |
| Telnet/WEB Stack Password Type | Enables password protection for accessing the console interface (CI) of a stack through a Telnet session.<br>If you set this field to Required, you can use the Logout option to restrict access to the CI. Thereafter, you must specify the correct password at the console-terminal prompt. See field definitions for "Console Read-Only Stack Password" on page 39 and "Console Read-Write Stack Password" on page 39 in this table for more information.<br>Default Value: None<br>Range: None, Local Password, RADIUS Authentication |
| Console Read-Only Switch Password | When the Console Switch Password Type field is set to Required (for Telnet, for Console, or for Both), this field allows read-only password access to the CI of a *stand-alone switch*. Users can access the CI using the correct password (see default), but cannot change parameters or use the Reset option or Reset to Default option.<br>Default Value: user<br>Range: An ASCII string of up to 15 printable characters |

**Table 2** Console/Comm Port Configuration screen fields (Continued)

| Field | Description |
|---|---|
| Console Read-Write Switch Password | When the Console Switch Password Type field is set to Required (for Telnet, for Console, or for Both), this field allows read-write password access to the CI of a stand-alone switch. Users can log in to the CI using the correct password (see default) and can change any parameter, except the passwords.<br>You can change the default passwords for read-only access and read-write access to a private password.<br>Default Value: secure<br>Range: Any ASCII string of up to 15 printable characters |
| Console Read-Only Stack Password | When the Console Stack Password Type field is set to Required (for Telnet, for Console, or for Both), this field allows read-only password access to the CI of a stack. Users can access the CI using the correct password (see default), but cannot change parameters or use the Reset option or Reset to Default option.<br>Default Value: user<br>Range: An ASCII string of up to 15 printable characters |
| Console Read-Write Stack Password | When the Console Stack Password Type field is set to Required (for Telnet, for Console, or for Both), this field allows read-write password access to the CI. Users can log in to the CI using the correct password (see default) and can change any parameter, except the passwords.<br>You can change the default passwords for read-only access and read-write access to a private password.<br>Default Value: secure<br>Range: Any ASCII string of up to 15 printable characters |

**Table 2** Console/Comm Port Configuration screen fields (Continued)

| Field | Description |
|---|---|
| Console Read-Write Password | When the Console Switch Password Type field is set to Local Password (for Telnet, for Console, or for Both), this field allows read-write password access to the CI. Users can log in to the CI using the correct password (see default), and can change any parameter, except the switch password.<br><br>You can change the default passwords for read-only access and read-write access to a private password.<br><br>Default Value: secure<br><br>Range: An ASCII string of up to 15 printable characters |
| | **Caution:** If you change the system-supplied default passwords, be sure to write the new passwords down and keep them in a safe place. If you forget the new passwords, you cannot access the console interface. In that case, contact Nortel for help. |
| | **Achtung:** Wenn Sie die für das System standardmäßig eingestellten Paßwörter ändern, notieren Sie sich die neuen Paßwörter, und bewahren Sie sie an einem sicheren Ort auf. Falls Sie die neuen Paßwörter vergessen, können Sie nicht mehr auf die Konsolenschnittstelle zugreifen. Wenden Sie sich in diesem Fall an Nortel, um Unterstützung zu erhalten. |
| | **Attention:** Si vous changez les mots de passe par défaut du système, assurez-vous de bien noter vos nouveaux mots de passe et de les conserver dans un endroit sûr. Si vous perdez vos nouveaux mots de passe, vous ne pourrez plus accéder à votre interface. Le cas échéant, veuillez contacter Nortel. |
| | **Precaución:** Si modifica las contraseñas predeterminadas asignadas por el sistema, asegúrese de anotar las nuevas contraseñas y guárdelas en un lugar seguro. Si olvida las nuevas contraseñas, no podrá acceder al interfaz de la consola. En ese caso, póngase en contacto con Nortel para obtener ayuda al respecto. |
| | **Attenzione:** In caso di modifica delle password predefinite nel sistema, assicurarsi di annotare le nuove password e di conservarle in un luogo sicuro. Nel caso in cui le nuove password vengano dimenticate, non sarà possibile accedere all'interfaccia della console. In tal caso, contattare la Nortel per avere assistenza. |
| | 注意：システム装備したデフォルトのパスワードを変更する場合、必ず新しいパスワードを書き留めて安全な場所に保管してください。新しいパスワードを忘れてしまうと、コンソール・インタフェイスにアクセスできません。この場合は、Bay Networksまでご連絡ください。 |

## Management password: RADIUS

The Console/Comm Port Configuration screen (Figure 2 on page 37) allows you to configure and modify the console/comm port parameters and security features of a switch.

To open the Console/Comm Port Configuration screen:

➨ Choose Console/Comm Port Configuration (or press o) from the main menu.

Table 3 describes the Console/Comm Port Configuration screen fields used to configure local passwords for managing the switch.

**Table 3** Console/Comm Port Configuration screen fields

| Field | Description |
|---|---|
| RADIUS Password Fallback | Allows you to configure password fallback as an option when using RADIUS authentication for login and password. When disabled, the RADIUS server must be configured and reachable in order to authenticate login and password. When enabled and the RADIUS server is unavailable or unreachable, you can use the local switch/stack password to log in to the switch/stack. |
| Primary RADIUS Server | Specifies the IP address of the primary RADIUS server. |
| Secondary RADIUS Server | Specifies the IP address of the secondary RADIUS server. |
| UDP RADIUS Port | Specifies the port number of the RADIUS server. |
| RADIUS Shared Secret | Your special switch security code that provides authentication to the RADIUS server.<br>Default: Null string (which will not authenticate)<br>Range: Any contiguous ASCII string that contains at least 10 printable characters, up to a maximum of 16 |
| RADIUS Timeout Period | Specifies the time in seconds that the RADIUS client waits for a response from a RADIUS server before timeout.<br>Range: 1-60 |

### RADIUS fallback enhancement

The system can use the local password of the switch or stack if the RADIUS server is unavailable to authenticate you for administrative access. This option is disabled by default.

RADIUS password fallback allows you to configure password fallback as an option when using RADIUS authentication for login and password.

When RADIUS password fallback is enabled and the RADIUS server is unavailable or unreachable, you can use the local switch or stack password to log in to the switch or stack.

When RADIUS password fallback is disabled, you must specify the RADIUS username and password from the NetLogin screen. You cannot log in to the switch or stack unless the RADIUS server is configured and reachable in order to authenticate the login and password.

You can use the following CLI commands to enable and disable this feature:

- radius-server password fallback
- no radius-server

### RADIUS access challenge

Release 3.6 software provides support for RADIUS access challenge as specified in RFC 2138. No configuration on the Ethernet Switches 460 or 470 is required.

RFC 2138 specifies that the RADIUS server can provide further security of authentication by challenging users with more levels of challenges and passwords.

## Password Security

The Password Security feature applies stricter rules to govern user passwords.

**Note:** The Password Security feature can be enabled only on an SSH-enabled image.

When the Password Security feature is running, the following password rules apply:

- A valid password must consist of at least 10, but not more than 15, printable characters. There is no requirement for the number of digits in a valid password. It is not required that a valid password must start with a letter. The password is case-sensitive.
- The system allows a user to try a password three consecutive times before the system resets the login process.
- The system keeps password history so that previously used passwords cannot be reused. The number of passwords kept in the history for each user is three. When the fourth new password is accepted, the switch obsoletes the first password.
- Passwords expire after a preset time period. After expiration, the user is prompted for a password update at login. The aging time can be configured using CLI from 1 day to 2730 days (or about 7.5 years).
- The user must log in as a Read-Write user to update the passwords.
- On an SSH-enabled image, default passwords become "userpasswd" for RO and "securepasswd" for RW. These new passwords are required because Password Security is enabled by factory default. Non-SSH-enabled images retain the standard default passwords (RO: user and RW: secure)
- The Password Security attributes are loaded from NVRAM. As a result, if an SSH image replaces a non-SSH image on a switch, Password Security is initially disabled, and the switch retains the standard default passwords (user and secure).
- Whenever a password or a community string or a RADIUS shared secret is displayed, it is not displayed in clear text. It is always displayed as 15 asterisks (*).
- Because passwords are not displayed in clear text, when a user is updating a password, the user must retype the new password to confirm the change. If the two passwords do not match, the update process fails and the user must try again. There is no limit to the number of times a user can try to update a password.

The rules listed here apply to the following passwords:

- Switch RO password
- Switch RW password
- Stack RO password
- Stack RW password

As for RADIUS Shared Secret and Community Strings, only display and verification requirements apply. The following do not expire:

- RADIUS Shared Secret
- Read-Only community string
- Read-Write community string

You can configure the Password Security feature using the CLI.

### Failed Login Attempt Trap

With Release 3.6 software, a new SNMP trap, bsnLoginFailure, sends a trap for each failed login attempt due to a user/password mismatch, provided that at least one trap receiver is configured on the switch or stack. Also, with an SSH-enabled image, the trap is generated when Digital Signature Algorithm (DSA) authentication fails due to key mismatch. No trap is generated when the login fails due to a wrong configuration of the RADIUS server, or when the client IP is not in the allowed IP list.

The bsnLoginFailure trap contains the IP address attempting the unsuccessful login, the type of connection used (Telnet, SSH, Web, serial connection) and the username.

## Secure Shell (SSH)

Secure Shell (SSH) is a client/server protocol that specifies the way to conduct secure communications over a network.

SSH can replace Telnet, FTP, and other remote logon utilities with encryption of the data, username, and password. In addition to standard username/password authentication, SSH supports a variety of the many different public/private key encryption schemes available. Using the public key of the host server, the client and server negotiate to generate a session key known only to the client and the server. This one-time key is used to encrypt all traffic between the client and the server.

Using a combination of host, server, and session keys, the SSH protocol can provide strong authentication and secure communication over an insecure network.

SSH provides protection from the following security risks:

- IP Spoofing
- IP source routing
- DNS spoofing
- Man-in-the-middle/TCP hijacking attacks
- Eavesdropping/Password sniffing

Even if network security is compromised, traffic cannot be played back or decrypted, and the connection cannot be hijacked. The secure channel of communication provided by SSH does not provide protection against break-in attempts or denial-of-service (DOS) attacks.

The SSH protocol supports the following security features:

- Authentication—This feature determines a way to identify the SSH client. During the login process, the SSH client is queried for a digital proof of identity. Supported authentications are DSA and passwords.
- Encryption—The SSH server uses encryption algorithms to scramble data and rendered it unintelligible except to the receiver. Supported encryption is 3DES only.
- Integrity—This feature guarantees that the data is transmitted from the sender to the receiver without any alteration. If any third party captures and modifies the traffic, the SSH server detects this alteration. The implementation of the SSH server on the Ethernet Switches 460 and 470 enables the SSH client to make a secure connection to Ethernet Switches 460 and 470 and works with commercially available SSH clients.

## SSH version 2 (SSH-2)

SSH protocol, version 2 (SSH-2) is a complete rewrite of the SSH-1 protocol. While SSH-1 contains multiple functions in a single protocol, in SSH-2 the functions are divided among three layers:

- SSH Transport Layer (SSH-TRANS)

The SSH transport layer manages the server authentication and provides the initial connection between the client and the server. Once established, the transport layer provides a secure, full-duplex connection between the client and server.

- SSH Authentication Protocol (SSH-AUTH)

  The SSH authentication protocol runs on top of the SSH transport layer and authenticates the client-side user to the server. SSH-AUTH defines three authentication methods: public key, host-based, and password. SSH-AUTH provides a single authenticated tunnel for the SSH connection protocol.

- SSH Connection Protocol (SSH-CONN)

  The SSH connection protocol runs on top of the SSH transport layer and user authentication protocols. SSH-CONN provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections. These richer services are multiplexed into the single encrypted tunnel provided by the SSH transport layer.

The modular approach of SSH-2 improves on the security, performance, and portability of the SSH-1 protocol.

**Note:** The SSH-1 and SSH-2 protocols are not compatible. The SSH implementation on the Ethernet Switches 460 and 470 supports the more secure version, the SSH-2 protocol. Ensure that your SSH client supports the SSH-2 protocol.

## Establishing a secure SSH connection

To establish a secure SSH connection to the Ethernet Switches 460 and 470, perform the following tasks.

1. Configure and enable the SSH service on the switch. For more information about configuring SSH using CLI, see Chapter 2, “Configuring security using the CLI,” on page 85.

**Note:** You must use the CLI to initially configure SSH. You can use Device Manager to change the SSH configuration parameters. However, Nortel recommends using the CLI.

By default, the SSH service, when enabled, listens for connections on port 22. It allows up to two simultaneous SSH connections. In the default configuration, sessions can be authenticated by either password or public key authentication.

**2** Connect to the switch using your SSH client.

Refer to the documentation that came with your selected SSH client for information about initiating a secure SSH connection to the switch.

**a** To connect to the switch using password authentication:

— Enter either the Console Read-Only switch password (default is *user*) or the Console Read-Write switch password (default is *secure*) when asked to enter the password.

When using password authentication, the user name is not required.

**Note:** Using the Console Read-Only or Console Read-Write password does not set read-only or read-write privileges. Either password will work to establish a secure SSH connection to the device.

**b** To connect to the switch using DSA public key authentication:

— Generate a DSA key pair (public and private keys) using your SSH client or key-gen tool and export your public key. Refer to the documentation that came with your selected SSH client or key-gen tool for information about generating a DSA key pair and exporting the public key.

— Download the DSA public key file to the switch using your TFTP server. For more information about configuring using the CLI, see Chapter 2, “Configuring security using the CLI,” on page 85.

— Connect to the switch using DSA public key authentication.

Refer to the documentation that came with your SSH client for information about establishing a secure SSH connection using DSA public key authentication.

## Syslog enhancements for SSH

The following event-triggered messages have been added to the system log to support SSH:

- Success Connection—Indicates that the client has successfully initiated an SSH session with the switch or stack
- Connection Logout—Indicates that the client has logged out of the device
- Inactivity Logout—Indicates that the client was logged out by the stack or switch due to inactivity
- Disallowed connection dues to host not allowed—Indicates that the client's connection request was not allowed due to the restrictions applied by the IP Manager Access Control List.
- Download DSA key completion—Indicates that the switch or stack has successfully downloaded the DSA key.
- SSH Enabled in secure mode—Indicates that the `ssh secure` command was invoked to initiate the SSH feature. Telnet, SNMP, and Web management are all disabled as a result of this command.
- SSH Enabled in non-secure mode—Indicates that the “ssh” command was invoked to initiate the SSH feature.
- SSH Disabled—Indicates that the SSH feature has been deactivated by the “no ssh” command.

# Secure Socket Layer browser-based management

Secure Socket Layer (SSL) browser-based management provides security for the web management interface.

SSL browser-based management allows the customer to access browser-based management using a secure https session. The user must enable SSL for the browser through the CLI. Once the SSL is enabled, the user can manage the switch or stack through secure http by entering the IP address for the host switch or stack through https, for example, https://10.30.31.105.

The capabilities of the secure web management interface are as follows:

- The web server can provide secure or non-secure http sessions. The user can specify session type using the CLI. The web server does not support both types of sessions concurrently.
- The web server can restart with a new digital certificate without resetting the system. This capability allows the web server to switch to a different host key in case the original key is stolen or compromised.
- The maximum number of concurrent SSL connections is equal to the maximum number of http sessions that are supported by the web server, which is four.

**Note:** The SSL feature can be enabled only on an SSH-enabled image.

SSL must be enabled first through the CLI on a switch/stack in order to be able to manage the switch/stack through a secure http connection.

For more information about configuring SSL using the CLI, see "Configuring Secure Socket Layer (SSL) Web-based management" on page 109.

# SNMPv3

Release 3.5 software and later support SNMPv3 in Device Manager, Web-based Management, or by using CLI commands. The SNMP agent supports exchanges using SNMPv1, SNMPv2c and SNMPv3.

SNMPv2c uses a standards-based GetBulk retrieval capability by using SNMPv1 communities.

SNMPv3 support introduces industrial-grade user authentication and message security, including MD5 and SHA-based user authentication and message integrity verification, as well as DES-based privacy encryption.

For information about configuring SNMPv3 using the CLI, see Chapter 2, "Configuring security using the CLI," on page 85.

For information about configuring SNMPv3 through the Device Manager, see the Chapter 3, "Configuring security using Device Manager," on page 157.

For information about configuring SNMPv3 using Web-based management, see Chapter 4, "Configuring security using Web-based management," on page 223.

## TELNET/SNMP/Web Access Configuration screen

The TELNET/SNMP/Web Access Configuration screen (Figure 3) allows a user at a remote console terminal to communicate with the Ethernet Switches 460 and 470 as if the console terminal were directly connected to it. You can have up to 50 active Telnet sessions at one time.

To open the TELNET/SNMP/Web Access Configuration screen:

**1** Choose TELNET/SNMP/Web Access Configuration (or press t) from the main menu.

**Figure 3** TELNET/SNMP/Web Access Configuration screen

```
                    TELNET/SNMP/Web Access Configuration

 TELNET:                                |            Access:        Use List:
 Login Timeout      :[ 1 minute ]       |  TELNET: [ Enabled  ]      [ Yes ]
 Login Retries      :[ 3 ]              |  SNMP  : [ Enabled  ]      [ Yes ]
 Inactivity Timeout:[ 15 minutes ]      |  WEB   : [ Enabled  ]      [ Yes ]
 Event Logging      :[ All       ]      |

#          Allowed Source IP Address              Allowed Source Mask
--         -------------------------            -------------------------
 1            [ 0.0.0.0 ]                           [ 0.0.0.0 ]
 2            [ 255.255.255.255 ]                   [ 255.255.255.255 ]
 3            [ 255.255.255.255 ]                   [ 255.255.255.255 ]
 4            [ 255.255.255.255 ]                   [ 255.255.255.255 ]
 5            [ 255.255.255.255 ]                   [ 255.255.255.255 ]
 6            [ 255.255.255.255 ]                   [ 255.255.255.255 ]
 7            [ 255.255.255.255 ]                   [ 255.255.255.255 ]
 8            [ 255.255.255.255 ]                   [ 255.255.255.255 ]
 9            [ 255.255.255.255 ]                   [ 255.255.255.255 ]
10            [ 255.255.255.255 ]                   [ 255.255.255.255 ]


Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 4 describes the TELNET/SNMP/Web Access Configuration screen fields.

**Table 4** TELNET/SNMP/Web Access Configuration screen fields

| Field | Description |
|---|---|
| TELNET Access | Allows a user remote access to the management systems through a Telnet session.<br>Default Value: Enabled<br>Range: Enabled, Disabled |
| Login Timeout | Specifies the amount of time a user has to enter the correct password at the console-terminal prompt.<br>Default Value: 1 minute<br>Range: 0 to 10 minutes (0 indicates “no timeout”) |
| Login Retries | Specifies the number of times a user can enter an incorrect password at the console-terminal prompt before terminating the session.<br>Default Value: 3<br>Range: 1 to 100 |
| Inactivity Timeout | Specifies the amount of time the session can be inactive before it is terminated.<br>Default Value: 15 minutes<br>Range: 0 to 60 minutes (0 indicates “no timeout”) |
| Event Logging | Specifies the types of events that are displayed in the Event Log screen (see the System Log screen in the *System Configuration Guide* (217105-A)).<br>Default Value: All<br>Range: All, None, Accesses, Failures<br>Description: All*:* Logs the following Telnet events to the Event Log screen:<br>• TELNET connect: Indicates the IP address and access mode of a Telnet session.<br>• TELNET disconnect: Indicates the IP address of the remote host and the access mode, due to either a logout or inactivity.<br>• Failed TELNET connection attempts: Indicates the IP address of the remote host whose IP address is not on the list of allowed addresses, or indicates the IP address of the remote host that did not supply the correct password.<br>*None:* Indicates that no Telnet events are logged in the Event Log screen.<br>*Accesses*: Logs only Telnet connect and disconnect events in the Event Log screen.<br>*Failures:* Logs only failed Telnet connection attempts in the Event Log screen. |

**Table 4** TELNET/SNMP/Web Access Configuration screen fields (Continued)

| Field | Description |
|---|---|
| TELNET Access | Specifies if Telnet access is allowed and only to those on the list.<br>Default Value: Access: Enabled; Use List: Yes |
| | Range: Access: Enabled, Disabled; Use List: Yes, No |
| SNMP Access | Specifies if SNMP access is allowed and only to those on the list. (SNMP access includes the Device Manager system.)<br>Default Value: Access: Enabled; Use List: Yes<br>Range: Access: Enabled, Disabled; Use List: Yes, No |
| WEB Access | Specifies if access to the Web-based management system is allowed and only to those on the list.<br>Default Value: Access: Enabled; Use List: Yes<br>Range: Access: Enabled, Disabled; Use List: Yes, No |
| Allowed Source IP Address | Specifies up to 50 user-assigned host IP addresses that are allowed Telnet access to the management systems.<br>Default Value: 0.0.0.0 (no IP address assigned)<br>Range: Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point |
| Allowed Source Mask | Specifies up to 50 user-assigned allowed source address masks. The remote IP address is masked with the Allowed Source Mask and, if the resulting value equals the Allowed Source IP address, the connection is allowed.<br>For example, a connection would be allowed with the following settings:<br>Remote IP address = 192.0.1.5<br>Allowed Source IP Address = 192.0.1.0<br>Allowed Source Mask = 255.255.255.0<br>Default Value: 0.0.0.0 (no IP mask assigned)<br>Range: Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point |

## SNMP Configuration screen

The SNMP Configuration screen (Figure 4) allows you to set or modify the SNMP configuration parameters.

To open the SNMP Configuration screen:

➨ Choose SNMP Configuration (or press m) from the main menu.

**Figure 4** SNMP Configuration screen

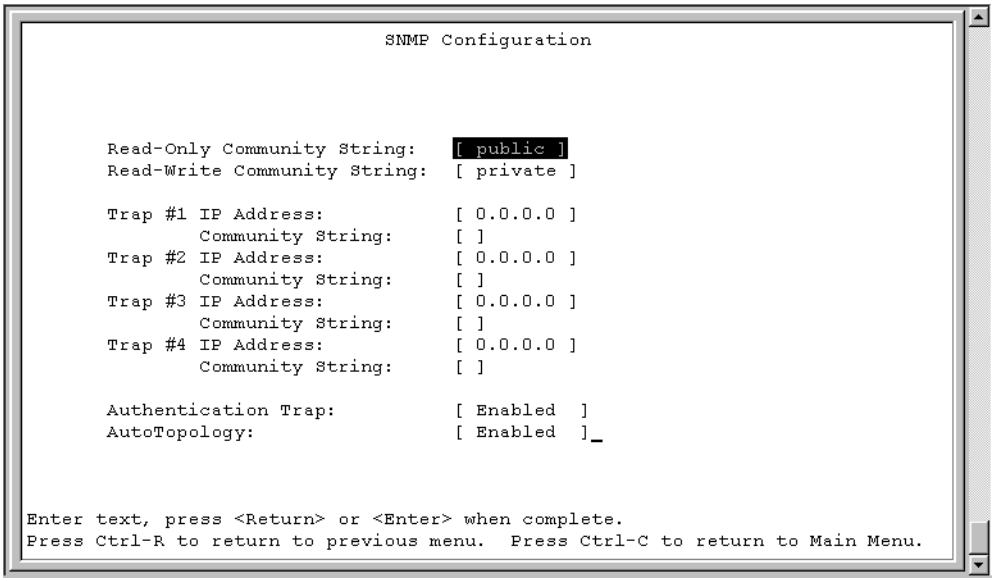



Table 5 describes the SNMP Configuration screen fields.

**Table 5** SNMP Configuration screen fields

| Field | Description |
|---|---|
| **Read-Only Community String** | The community string used for in-band read-only SNMP operations.<br>Default Value public<br>Range Any ASCII string of up to 32 printable characters |

**Table 5** SNMP Configuration screen fields (Continued)

| Field | Description |
|---|---|
| Read-Write Community String | The community string used for in-band read-write SNMP operations.<br>Default Value: private<br>Range: Any ASCII string of up to 32 printable characters |
| Trap #1 IP Address* | Number one of four trap IP addresses. Successive trap IP address fields are numbered 2, 3, and 4. Each trap address has an associated community string (see Community String).<br>Default Value: 0.0.0.0 (no IP address assigned)<br>Range: Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point |
| Community String | The community string associated with one of the four trap IP addresses (see field description for "Trap #1 IP Address").<br>Default Value: Zero-length string<br>Range: Any ASCII string of up to 32 printable characters |
| Authentication Trap | Determines whether a trap is sent when an SNMP authentication fails.<br>Default Value: Enabled<br>Range: Enabled, Disabled |
| Autotopology | Allows you to enable or disable the switch participation in Autotopology, which allows network topology mapping of other switches in your network.<br>Default Value: Enabled<br>Range: Disabled |

* The Trap IP Address and Community String fields can be set using a MIB table (in a Nortel proprietary MIB). The status of the row in the MIB table can be set to Ignore. If the row status is set to Ignore, the fields appear to be set when viewed from the console terminal; however, no traps are sent to that address until the row status is set to Valid.

# MAC address filtering-based security

## DA filtering using MAC address-based security

You can use the MAC address-based security feature (BaySecure*) to configure the Ethernet Switches 460 and 470 to drop all packets with specified MAC Destination Addresses (DA). You can enter up to 10 specific MAC DAs you want filtered. This is an enhancement to the current MAC address-based security system that allows you to filter MAC source addresses (SAs).

**Note:** You must use either the Web-based management system or the CLI to configure MAC DA filtering.

## MAC Address Table screen

The MAC Address Table screen (Figure 5 on page 57) allows you to view MAC addresses that the switch has discovered or to search for a specific MAC address.

➨ Choose MAC Address Table (or press m) from the Switch Configuration Menu screen to open the MAC Address Table screen (Figure 5 on page 57).

**Figure 5** MAC Address Table Screen (1 of 3)

```
Select C:\WINNT\system32\telnet.exe
                              MAC Address Table

                Aging Time:                  [ 300 seconds ]
                Find an Address:             [ 00-00-00-00-00-00 ]
                Select VLAN ID:              [     1 ]
                Number of addresses:           9


00-00-A2-0B-3D-45              Port: 24
00-02-E3-05-3B-B5              Port: 24
00-04-38-D2-6F-21              Port: 24
00-04-38-D4-FE-41              Port: 24
00-09-97-49-66-C0
00-80-2D-4B-73-83              Port: 24
00-80-2D-8C-4E-01              Port: 24
00-E0-7B-51-B5-57              Port: 24
00-E0-7B-CC-6C-A1              Port: 24
00-E0-7B-CC-7E-81              Port: 24



End of Address Table. Press Ctrl-P to see previous display.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 6 describes the MAC Address Table screen fields.

**Table 6** MAC Address Table screen fields

| Field | Description |
|---|---|
| Aging Time | Specifies how long a learned MAC address remains in the switch's forwarding database. If an entry is inactive for a period of time that exceeds the specified aging time, the address is removed.<br>Default Value 300 seconds<br>Range 10 to 1 000 000 seconds |
| Find an Address | Allows the user to search for a specific MAC address.<br>Default Value 00-00-00-00-00-00 (no MAC address assigned)<br>Range 00-00-00-00-00-00 to FE-FF-FF-FF-FF-FF |

**Table 6** MAC Address Table screen fields (Continued)

| Field | Description |
|---|---|
| Select VLAN ID | Enter the VLAN ID number for which you want to display the MAC addresses.<br>Default Value 1<br>Range 1-4094 |
| Number of addresses | Displays the total number of MAC addresses currently learned by the specified VLAN. This number updates dynamically when you press [Ctrl]-P or [Ctrl]-N to scroll through the list. |

## MAC Address Security Configuration Menu screen

The MAC Address Security Configuration Menu screen (Figure 6 on page 59) allows you to specify a range of system responses to unauthorized network access to your switch. The system response can range from sending a trap to disabling the port. The network access control is based on the MAC addresses of the authorized stations. You can specify a list of up to 448 MAC addresses that are authorized to access the switch. You can also specify the ports that each MAC address is allowed to access. The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, and so on. You must also include the MAC address of any router connected to any secure ports.

In addition, you can configure the Ethernet Switches 460 and 470 to drop all packets with specified MAC DAs. You can enter up to 10 specific MAC DAs you want filtered. The packet with the specified MAC DA is dropped regardless of the ingress port, source address (SA) intrusion, or VLAN membership.

**Note:** You must use either the Web-based management system or the CLI to configure MAC DA filtering.

When the switch software detects a security violation on the specified MAC SAs, the response can be to send a trap, turn on the DA filtering that is based on SA filtering, disable the specific port, or any combination of these three options.

To open the MAC Address Security Configuration screen:

➨ Choose MAC Address Security Configuration from the Switch Configuration Menu.

**Figure 6** MAC Address Security Configuration Menu screen

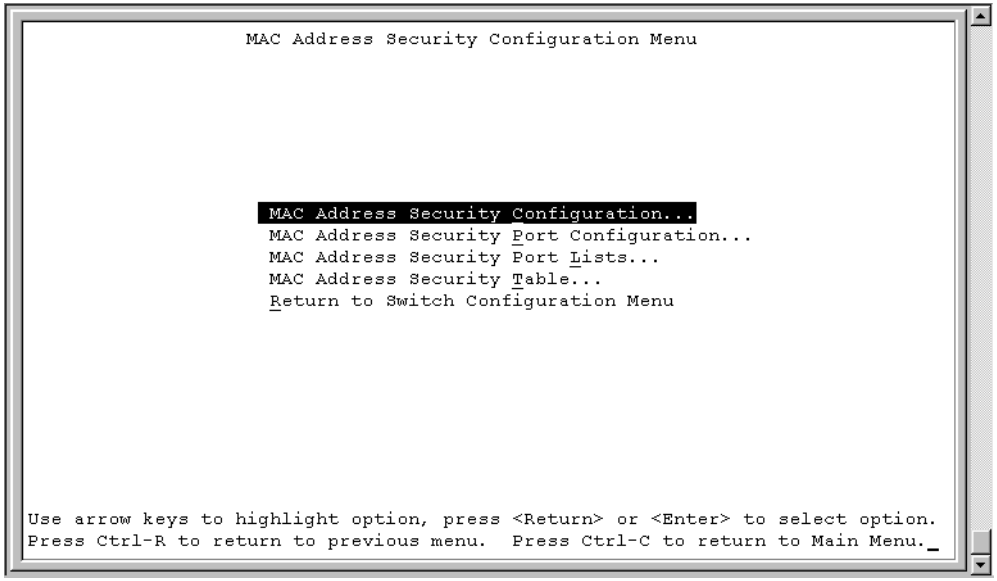



Table 7 describes the MAC Address Security Configuration Menu options.

**Table 7** MAC Address Security Configuration Menu Options

| Option | Description |
|---|---|
| MAC Address Security Configuration... | Displays the MAC Address Security Configuration screen (see "MAC Address Security Configuration Menu screen" on page 58). This screen allows you to enable or disable the MAC Address Security feature. |
| MAC Address Security Port Configuration... | Displays the MAC Address Security Port Configuration screen (see "MAC Address Security Port Configuration screen" on page 63). This screen allows you to enable or disable MAC Security for each port. |

**Table 7** MAC Address Security Configuration Menu Options (Continued)

| Option | Description |
|---|---|
| MAC Address Security Port Lists... | Displays the MAC Address Security Port Lists screen (see "MAC Address Security Port Lists screens" on page 65). This screen allows you to create port lists that can be used as an *allowed source port list* for a MAC address in the MAC Address Security Table screen. |
| MAC Address Security Table... | Displays the MAC Address Security Table screen (see "MAC Address Security Table screens" on page 68). This screen allows you to specify the MAC addresses that are allowed to access the switch. |

## MAC Address Security Configuration screen

The MAC Address Security Configuration screen (Figure 7 on page 61) allows you to enable or disable the MAC address security feature and to specify the appropriate system responses to any unauthorized network access to your switch.

➨ Choose MAC Address Security Configuration from the MAC Address Security Configuration Menu to open the MAC Address Security Configuration screen.

**Figure 7** MAC Address Security Configuration screen

```
Select C:\WINNT\system32\telnet.exe
                    MAC Address Security Configuration

      MAC Address Security:                          [ Disabled ]
      MAC Address Security SNMP-Locked:              [ Disabled ]
      Partition Port on Intrusion Detected:          [ Disabled ]

      DA Filtering on Intrusion Detected:            [ Disabled ]
      Generate SNMP Trap on Intrusion:               [ Disabled ]
      MAC Auto-Learning Aging Time:                  [ 60 minutes ]

 MAC Security Table:

 Clear by Ports: [    ]

 Learn by Ports: [ 1/3 ]

 Current Learning Mode:                    [ Disabled ]



Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 8 describes the MAC Address Security Configuration screen fields.

**Table 8** MAC Address Security Configuration fields

| Field | Description |
|---|---|
| MAC Address Security | When this field is set to enabled, the software checks source MAC addresses of packets that arrive on secure ports against MAC addresses listed in the MAC Address Security Table for allowed membership. If the software detects a source MAC address that is not an allowed member, the software registers a MAC intrusion event.<br>Default Disabled<br>Range Disabled, Enabled |
| MAC Address Security SNMP-Locked | When this field is set to enabled, the MAC address security screens cannot be modified using SNMP (SNMP includes the JDM management system).<br>Default Disabled<br>Range Disabled, Enabled |

**Table 8** MAC Address Security Configuration fields (Continued)

| Field | Description |
|---|---|
| Partition Port on Intrusion Detected | This field value determines how the switch reacts to an intrusion event. When an intrusion event is detected (see field description for "MAC Address Security" on page 61) the specified switch port is set to Disabled (partitioned from other switch ports).<br>When the field is set to:<br>• Disabled - the port remains enabled, even if an intrusion event is detected.<br>• Enabled - the port becomes disabled, then automatically resets to enabled depending on the value set in the Partition Time field.<br>• Forever - the port becomes disabled, and remains disabled (partitioned). The Partition Time field cannot be used to automatically to reset the port to Enabled if you set this field to Forever.<br>You can always manually set the port status field to enabled using the Port Configuration screen (see *System Configuration Guide* (217105-A)).<br>Default Disabled<br>Range Disabled, Enabled, Forever |
| Partition Time | This field appears only when the Partition Port on Intrusion Detected field is set to enabled. This field determines the length of time a partitioned port remains disabled. This field is not operational when the Partition Port on Intrusion Detected field is set to Forever.<br>Default 1 second (the value 0 indicates forever)<br>Range 0-65536 seconds |
| DA Filtering on Intrusion Detected | When set to enabled, this field isolates the intruding node by filtering (discarding) packets sent to that MAC address.<br>Default Disabled<br>Range Disabled, Enabled |
| MAC Auto-Learning Aging Time | This field sets the aging time, in minutes, for the auto-learned addresses in the MAC Security Table.<br>Default 60<br>Range 0-65535 An aging time of 0 specifies that the auto-learned addresses never age out. |
| Generate SNMP Trap on Intrusion | When set to enabled and a MAC intrusion event is detected, the software issues an SNMP trap message to all registered SNMP trap addresses (see "SNMP Configuration screen" on page 54).<br>Default Disabled<br>Range Disabled, Enabled |

**Table 8** MAC Address Security Configuration fields (Continued)

| Field | Description |
|---|---|
| Clear by Ports | This field clears the specified port (or ports) that are listed in the Allowed Source Port(s) field of the MAC Address Security Table screen (see "MAC Address Security Table screens" on page 68). When you specify a port (or ports) to be cleared using this field, the specific port (or ports) is cleared for each of the entries listed in the MAC Address Security Table. If you totally clear the allowed Source Port(s) field (leaving a blank field) for an entry, the associated MAC address for that entry is also cleared.<br>Default NONE<br>Range NONE, ALL, a port number list (for example, 1/1, 2/6, and so on) |
| Learn by Ports | All source MAC addresses of any packets received on the specified port (or ports) are added to the MAC Security Table when the Current Learning Mode field is set to Enabled. You cannot include any of the port values you have chosen for the secure ports field.<br>Default NONE<br>Range NONE, ALL, a port number list (for example, 1/1, 2/6, and so on) |
| Current Learning Mode | This field indicates the current learning mode for the switch ports. When this field is set to Learning in Progress, all source MAC addresses of any packets received on the specified port (or ports) are added to the MAC Security Table (maximum of 448 MAC address entries allowed). If you exceed the limit of 448 entries, the system prompts you with an alert message.<br>Default Disabled<br>Range Enabled, Disabled |

## MAC Address Security Port Configuration screen

The MAC Address Security Port Configuration screens (Figure 8 on page 64 and Figure 9 on page 65) allow you to set or modify your MAC address port security configuration on a per-port basis.

To open the MAC Address Security Port Configuration screen:

➨ Choose MAC Address Security Port Configuration from the MAC Address Security Configuration Menu.

**Figure 8** MAC Security Port Configuration screen

```
Select C:\WINNT\system32\telnet.exe

                              MAC Security Port Configuration
                                Unit:  [ 1 ]
  Port    Trunk     Security      Auto-Learning      MAC Address No.
  ----    -----   ------------   ---------------    -----------------
    1             [ Disabled ]    [ Disabled ]        [     2    ]
    2             [ Disabled ]    [ Disabled ]        [     2    ]
    3             [ Disabled ]    [ Disabled ]        [     2    ]
    4             [ Disabled ]    [ Disabled ]        [     2    ]
    5             [ Disabled ]    [ Disabled ]        [     2    ]
    6             [ Disabled ]    [ Disabled ]        [     2    ]
    7             [ Disabled ]    [ Disabled ]        [     2    ]
    8             [ Disabled ]    [ Disabled ]        [     2    ]
    9             [ Disabled ]    [ Disabled ]        [     2    ]
   10             [ Disabled ]    [ Disabled ]        [     2    ]
   11             [ Disabled ]    [ Disabled ]        [     2    ]
   12             [ Disabled ]    [ Disabled ]        [     2    ]
   13             [ Disabled ]    [ Disabled ]        [     2    ]
   14             [ Disabled ]    [ Disabled ]        [     2    ]
                                                                 More...

Press Ctrl-N to display next screen.
Use space bar to display choices or enter text.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 9 describes the MAC Security Port Configuration screen fields.

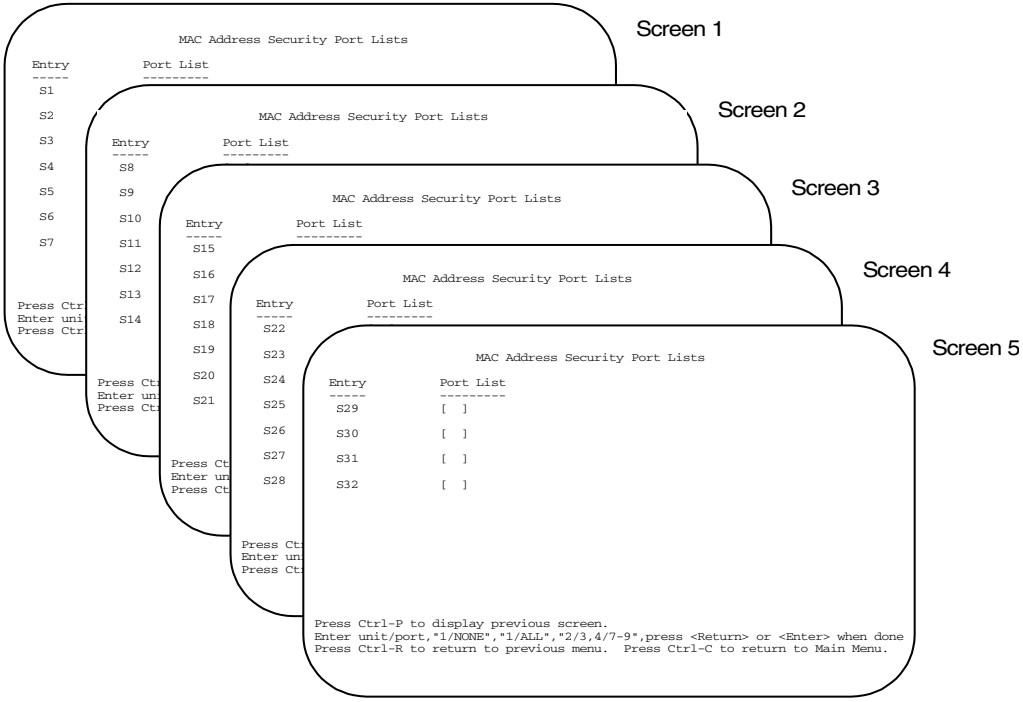
**Table 9** MAC Security Port Configuration screen fields

| Field | Description |
|---|---|
| Unit | Allows you to choose the unit number you want to display the ports for. |
| Port | Displays a numbered port list. |
| Trunk | Displays the trunk number if the port is a member of that trunk.<br>Default blank field |
| Security | Determines whether security is enabled or disabled on the port level or switch level.<br>Default Disabled<br>Range Disabled, Enabled |
| Auto-Learning | Determines whether auto-learning is enabled or disabled on the port.<br>Default Disabled |
| MAC Address No. | Specifies the maximum number of MAC addresses stored in the MAC Security Table for the port.<br>Default 2<br>Range 1-25 |

## MAC Address Security Port Lists screens

The MAC Address Security Port Lists screens allow you to create port lists that can be used as *allowed source port lists* for a specified MAC address in the MAC Address Security Table screen. You can create as many as 32 port lists, using up to five MAC Address Security Port Lists screens (see Figure 9).

**Figure 9** MAC Address Security Port Lists screens




To open the MAC Address Security Lists screen:

➨ Choose MAC Address Security Lists from the MAC Address Security Configuration Menu. (See Figure 10 on page 66.)

The options for allowed port access include: NONE, ALL, and ports that are specified in a list (for example, 1/1, 2/6, and so on).

**Figure 10** MAC Address Security Port Lists screen

```
                    MAC Address Security Port Lists

 Entry          Port List
 -----          ---------
  S1             [    ]

  S2             [    ]

  S3             [    ]

  S4             [    ]

  S5             [    ]

  S6             [    ]

  S7             [    ]

                                                          More...


Press Ctrl-N to display next screen.
Enter unit/port,"1/NONE","1/ALL","2/3,4/7-9",press <Return> or <Enter> when done
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 10 describes the MAC Address Security Port Lists screen fields.

**Table 10** MAC Address Security Port Lists screen fields

| Field | Description |
|---|---|
| Entry | This field indicates the port list number (S1 to S32) that corresponds to the values you set in the Port List field. |
| Port List | This field allows you to create a port list that you can use as an “Allowed Source” in the MAC Address Security Table screen. |

## Port list syntax

A unit/port number list is composed of one or more list items, each of which can be a single number or a range of numbers (where the numbers represent one or more ports).

## Accelerator keys for repetitive tasks

You can use certain keystrokes as accelerator keys to help speed up repetitive tasks. For example, suppose you want to modify the Port List field in the MAC Address Security Port List screen (Figure 10 on page 66). You can modify the port list in any of the following ways:

- Add a new port to an existing port number list.
- Remove a port from an existing port number list.
- Copy an existing field into an adjacent field.

### *Adding a new port to an existing port number list*

In the example shown in Figure 10 on page 66, S3 shows the Port List field values as:

1/3,2/7,3/1-4

If you want to add another port (for example, port 2/9) to the existing port number list, you could highlight the field and then type another port list, including the new port number 1/3,2/7,**2/9**,3/1-4 [Return]. This method can be cumbersome.

As an alternative method, you can highlight the field and then enter +2/9 [Return]. The existing field keeps the previous list and adds the new port number (2/9) between ports 2/7 and 3/14.

(If you choose to add port 2/8 to the existing port number list, the field accepts the new port 2/8 but shows the new port number list field as: 1/3,2/7-8,3/1-4.)

### *Removing a port from an existing port number list*

To remove a port from the port number list, use the minus sign (-) character instead of the plus sign (+) character as described in "Adding a new port to an existing port number list".

### *Copying an existing field into and adjacent field*

You can use the period (.) character to copy a previously entered field value into the field directly next to it. For example, to copy the Allowed Source S3 (shown in Figure 10 on page 66) into the next field (entry 6):

1. Enter a MAC address into the next MAC address field.
2. Highlight the (blank) Allowed Source field.
3. Enter the period (.) character and click Return.

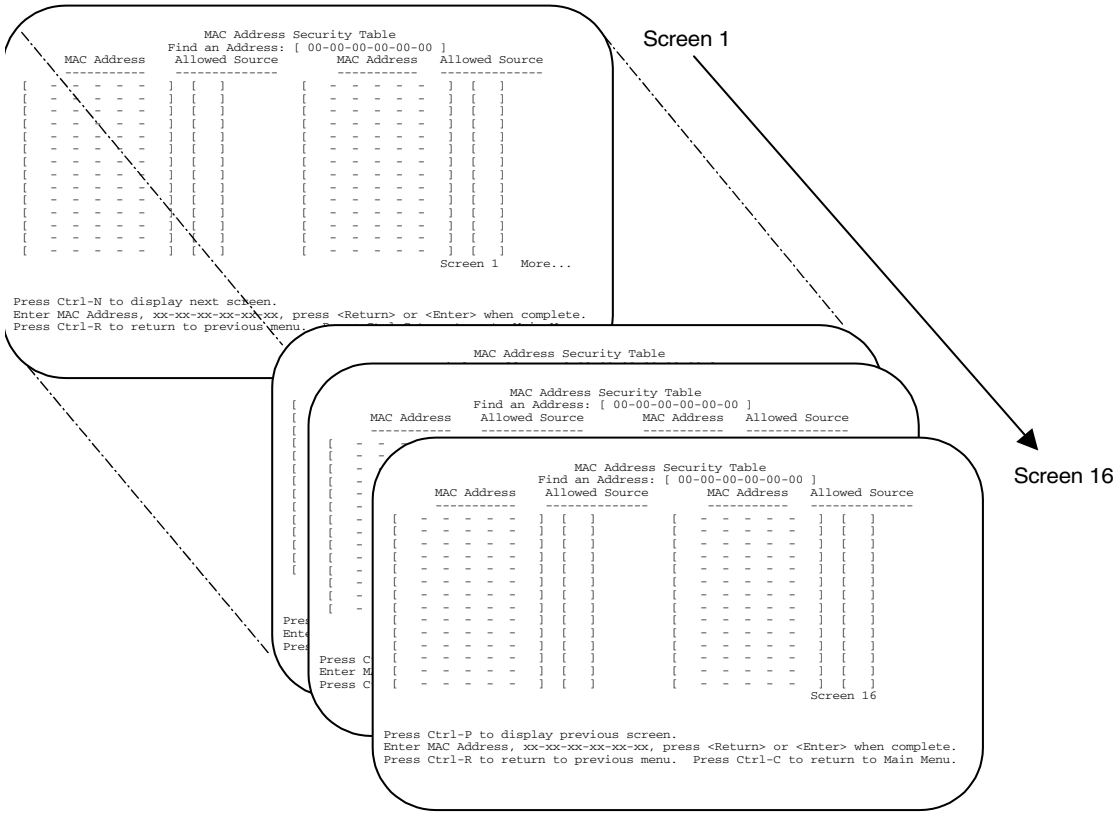
The port number list from the previous entry is copied into the new field.

## MAC Address Security Table screens

The MAC Address Security Table screens allow you specify the ports that each MAC address is allowed to access. You must also include the MAC addresses of any routers that are connected to any secure ports.

16 MAC Address Security Table screens are available (Figure 11 on page 69). You can use these screens to create up to 448 MAC address entries (28 per screen).

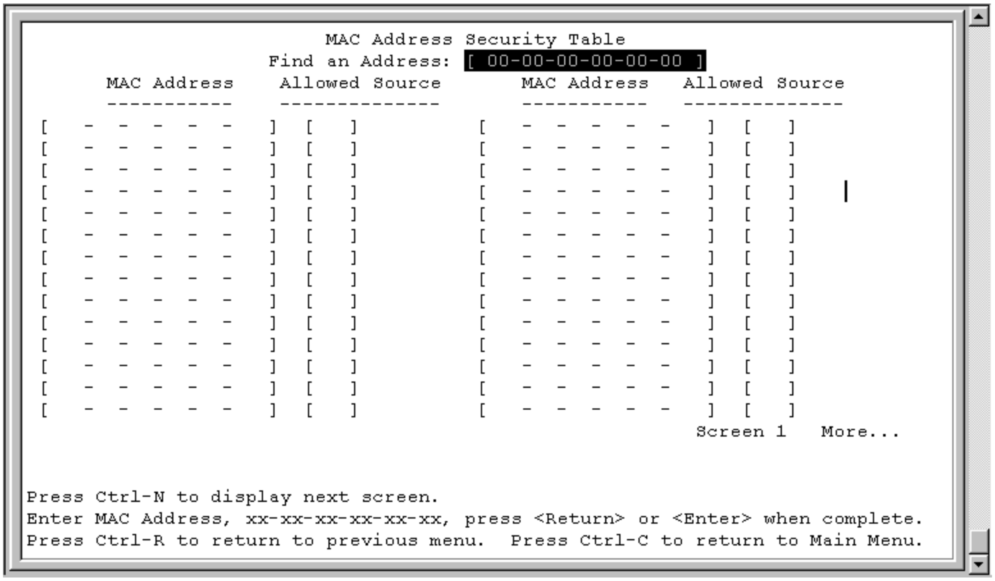
**Figure 11** MAC Address Security Table screens




To open the MAC Address Security Table screen:

➡ Choose MAC Address Security Table from the MAC Address Security Configuration Menu (Figure 12 on page 70).

**Figure 12** MAC Address Security Table screen



```
                              MAC Address Security Table
                          Find an Address: [ 00-00-00-00-00-00 ]
       MAC Address     Allowed Source          MAC Address    Allowed Source
       -----------     --------------          -----------    --------------
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]            [   -  -  -  -  -   ]  [   ]
                                                        Screen 1   More...


Press Ctrl-N to display next screen.
Enter MAC Address, xx-xx-xx-xx-xx-xx, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 11 describes the MAC Address Security Table screen fields.

**Table 11** MAC Address Security Table Screen Fields

| Field | Description |
|---|---|
| **Find an Address** | Allows you to search for a specific MAC address that is used in any of the MAC Address Security Table screens. |
| **MAC Address** | Allows you to specify up to 448 MAC addresses that are authorized to access the switch. You can specify the ports that each MAC address is allowed to access using the Allowed Source field (see next field description). The specified MAC address does not take effect until the Allowed Source field is set to some value (a single unit/port number or a port list value that you previously configured in the MAC Address Security Port Lists screen). You can clear an existing MAC address field by entering zero (0) in the field and pressing [Enter].<br>Default - - - - - (no address assigned)<br>Range A range of 6 Hex Octets, separated by dashes (multicast* and broadcast addresses are not allowed). |

**Table 11** MAC Address Security Table Screen Fields (Continued)

| Field | Description |
|---|---|
| **Allowed Source** | Allows you to specify the ports that each MAC address is allowed to access. The options for the Allowed Source field include a single unit/port number or a port list value that you previously configured in the MAC Address Security Port Lists screen.<br>Default - (Blank field)<br>Range A single unit/port or a port list value (for example, 1/3, 1/6, 3/4, S1, S5, and so on). |

* Multicast address -- Note that the first octet of any multicast address will always be an odd number.

For information about configuring MAC address-based DA filtering, see Chapter 2, "Configuring security using the CLI," on page 85 and Chapter 4, "Configuring security using Web-based management," on page 223.

## MAC address-based security auto-learning

The MAC address-based security auto-learning feature provides the ability to add allowed MAC addresses in the MAC Security Table automatically without user intervention. The user specifies the number of addresses to be added in the table, in intervals of 1 to 25 maximum addresses per port. The switch forwards traffic only for those MAC addresses on the specified ports.

The user can configure an aging time period in minutes after which the entries are refreshed in the MAC Security Table. If the value is set to 0, the entries will never age-out, and the user must reset the MAC Address Table for the specified port to force new addresses to be learned.

The user cannot modify the MAC addresses that were automatically learned (added to the MAC Security Tool).

The addresses added automatically are not saved in NVRAM but learned after the boot-up sequence. The aging time and the number of MAC addresses per port are saved in non-volatile memory.

The user can reset the MAC address table for a port by disabling the security on the port and then re-enabling it.

If a MAC is already learned on port x and the address later migrates to port y, the MAC entry port association is removed from port x and associated with port y in the MAC Security Address Table. The aging timer for this entry will be reset.

If a static MAC Address is associated with a port (configured or not with the auto-learning feature) and the same MAC address is learned on a different port, the specific address will never be associated with the second port in the MAC Security Address Table. This means that user settings have priority over automatic learning.

When the user disables auto-learning on a port, all the MAC entries associated with that port in the MAC Security Address Table are removed.

If a link-down event occurs on a port that is enabled with the auto-learning feature, the associated entries in the MAC Security Address Table are deleted.

## EAPOL-based security

Release 3.6 software provides support for security based on the Extensible Authentication Protocol over LAN (EAPOL), which uses the EAP as described in the IEEE Draft P802.1X to allow you to set up network access control on internal LANs.

For information about configuring EAPOL-based security using the Console Interface (CI) menus, refer to the "EAPOL Security Configuration screen" on page 79.

To configure this feature using the Web-based management system, refer to Chapter 4, "Configuring security using Web-based management," on page 223.

To use Device Manager (DM) to configure EAPOL-based security, see Chapter 3, "Configuring security using Device Manager," on page 157.

To configure this feature using CLI commands, refer to Chapter 2, "Configuring security using the CLI," on page 85.

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

The following example illustrates how the Ethernet Switches 460 and 470, configured with the EAPOL-based security feature, react to a new network connection:

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

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

- Supplicant—the device applying for access to the network.
- Authenticator—software with the sole purpose of authorizing a supplicant that is attached to the other end of a LAN segment.
- Authentication Server—a RADIUS server that provides authorization services to the Authenticator.
- Port Access Entity (PAE)—a software entity associated with each port that supports the Authenticator or Supplicant functionality. In the preceding example, the Authenticator PAE resides on the switch.
- Controlled Port—any switch port with EAPOL-based security enabled.

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

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

The Authenticator determines the controlled port's operational state. After the RADIUS server notifies the Authenticator PAE about the success or failure of the authentication, it changes the controlled port's operational state accordingly.

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

When the Authentication server returns a success or failure message, the controlled port's state is changed accordingly. If the authorization is successful, the controlled port's operational state is set to Forwarding. Otherwise, the controlled port's state 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. The controlled port's state is set to Blocking.
- 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 a port, and then the port is authorized, the EAPOL feature dynamically changes the port's VLAN configuration according to pre-configured values, and assigns a new VLAN. The new VLAN configuration values are applied according to previously stored parameters (based on the user_id) in the Authentication server.

The following VLAN configuration values are affected:

- Port membership

- PVID
- Port priority

When the EAPOL-based security is disabled on a port that was previously authorized, the port's VLAN configuration values are restored directly from the switch's Non-Volatile Random Access Memory (NVRAM).

The following exceptions apply to dynamic VLAN assignments:

- The dynamic VLAN configuration values assigned by EAPOL are **not** stored in the switch's NVRAM.
- You can override the dynamic VLAN configuration values assigned by EAPOL; however, ensure that the values you configure are not stored in NVRAM.
- When EAPOL is enabled on a port, and you configure values other than VLAN configuration values, those values are applied and stored in NVRAM.

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

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

To set up the Authentication server, set the following Return List attributes for all user configurations (refer to your Authentication server documentation):

- VLAN membership attributes:
  - Tunnel-Type: value 13, Tunnel-Type-VLAN
  - Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
  - Tunnel-Private-Group-Id: ASCII value 1 to 4094 (this value is used to identify the specified VLAN)
- Port priority (vendor-specific) attributes:
  - Vendor Id: value 562, Nortel vendor Id

— Attribute Number: value 1, Port Priority
— Attribute Value: value 0 (zero) to 7 (this value is used to indicate the port priority value assigned to the specified user)

### *System requirements*

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

- At least one of the following supported switches:
  — Ethernet Switch 460 or Ethernet Switch 470 (software version V3.0, or later)
- RADIUS server (Microsoft Windows.NET Server)
- Client software that supports EAPOL (Microsoft Windows XP Client)

You must specify the Microsoft 2001 IAS server (or any generic RADIUS server that supports EAP) as the primary RADIUS server for these devices.

You must also configure your Ethernet Switches 460 and 470 for port-based VLANs and EAPOL security.

**Note:** Windows XP* or Windows 2000* PCs running the built-in EAP client drop the first received EAP message. Therefore, the second message that the client receives appears to be the first. The interval that the client must wait for the second EAP message after the link is up is defined by the EAPOL quiet period value (default value: 60 seconds). As a result, the user typically does not see a password window until 60 seconds after the link is up.

To log out of EAP, the EAP client must explicitly send an EAP Logoff packet to the PAE. The built-in EAP client for MS Windows does not send this packet. Therefore, if you physically disconnect the client from the switch, the PAE will log out the client after a timeout period (typically about 1 minute).

### *EAPOL-based security configuration rules*

The following configuration rules apply to your Ethernet Switches 460 and 470 when using EAPOL-based security:

- Before configuring EAPOL-based security, you must assign a valid IP to the switch and configure the Primary RADIUS Server and Shared Secret fields.
- You cannot configure EAPOL-based security on ports that are currently configured for:
  - MultiLink Trunking
  - MAC address-based security
  - IGMP (Static Router Ports)
  - Port mirroring
- Using Multiple Host Multiple Authentication (MHMA), you can connect more than one client on each port that is configured for EAPOL-based security. (See "Multiple clients with EAPOL-based security" on page 77 and "Multiple Host Multiple Authentication (MHMA)" on page 78 for more information.)
- With the MHMA feature enabled, you can provide EAPOL-based security to ports configured for shared segments.

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

## Multiple clients with EAPOL-based security

Prior to the Release 3.6 software, EAP (802.1x) Authentication supported Port Based User Access. At any time, only one user (MAC) could be authenticated on a port, and the port could be assigned to only one Port-based VLAN. Only the MAC address of the device/user that completed the EAP negotiations on the port would have access to that port for traffic. Any tagging of ingress packets would be to the PVID of that port.

With Release 3.6 software, EAP allows for:

- Single Host with Single Authentication (SHSA) and Guest VLANs
- Multiple Host (MAC) with Multiple Authentication (MHMA) - EAP Clients only

## Single Host, Single Authentication (SHSA) with Guest VLANs

This is the default EAP configuration. For an EAP-enabled port, only one device/user on that port can complete EAP Authentication. When completed, only the MAC address of this device is allowed on that port for traffic. The only exceptions are reserved addresses. However, Guest VLANs can be configured for access to that port. Any active VLAN can be made a Guest VLAN.

## Multiple Host Multiple Authentication (MHMA)

For an EAP-Enabled port with Multiple Host (MAC) Multiple Authentication (MHMA), a finite number of users (that is, devices), each with a different MAC address, is allowed on a port. Each user must complete EAP Authentication for the port to allow traffic with the corresponding MAC address. Only traffic from the authorized hosts is allowed on that port.

In the current release, the MHMA support is provided for EAP clients only.

**Note:** EAPOL uses the Port Access Entity (PAE) group address of 01-80-C2-00-00-03. This PAE group address is one of the reserved group MAC addresses that are *not* forwarded by MAC bridges. As a result, when an EAP-enabled port has the MHMA feature enabled, you must use a hub to connect stations to the port.

**Note:** Users running Windows XP* can experience problems attempting to log in to the network if EAP MHMA is enabled (for example, if multiple computers are connected through a hub to the switch). Windows XP does not respond to EAP Request-Identity packets if it receives too many requests from the switch in a short period of time (which happens on multihost-enabled ports). The Windows XP client ignores further Request-Identity packets if the authentication fails two or more times for any reason. When this occurs, you must disable and re-enable the network connection on the Windows XP client.

Better performance with MHMA can be achieved by using a third-party EAP client, such as Funk Software Odyssey* client (for Windows) or Open1x Xsupplicant* client (for Linux).

## EAPOL Security Configuration screen

The EAPOL Security Configuration screen (Figure 13 on page 80) allows you to selectively limit access to the switch based on an authentication mechanism that uses Extensible Authentication Protocol (EAP) to exchange authentication information between the switch and an authentication server.

**Note:** Before you use the EAPOL Security Configuration screen, you must configure your Primary RADIUS Server and RADIUS Shared Secret.

You also need to set up specific user accounts on your RADIUS server:

- User names
- Passwords
- VLAN IDs (optional)
- Port priority (optional)

You can set up these parameters directly on your RADIUS server. For detailed instructions about configuring your RADIUS server, refer to your RADIUS server documentation.

**Note:** Do not enable EAPOL security on the switch port that is connected to the RADIUS server.

To open the EAPOL Security Configuration screen:

➨ Choose EAPOL Security Configuration (or press e) from the Switch Configuration Menu.

**Figure 13** EAPOL Security Configuration screen

```
                          EAPOL Security Configuration

                 EAPOL Administrative State:  [ Disabled ]

                         Unit: [  1  ] Port: [  1  ]

       Initialize:                      [ No  ]
       Administrative Status:           [ Force Authorized   ]
       Operational Status:                Authorized
       Administrative Traffic Control:[ Incoming and Outgoing ]
       Operational Traffic Control:       Incoming and Outgoing
       Re-authenticate Now:             [ No  ]
       Re-authentication:               [ Disabled ]
       Re-authentication Period:        [ 3600 seconds ]
       Quiet Period:                    [ 60 seconds ]
       Transmit Period:                 [ 30 seconds ]
       Supplicant Timeout:              [ 30 seconds ]
       Server Timeout:                  [ 30 seconds ]
       Maximum Requests:                [ 2 ]_


Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 12 describes the EAPOL Security Configuration screen options

**Table 12** EAPOL security configuration screen options

| Option | Description |
|---|---|
| EAPOL Administrative State | Allows you to enable or disable EAPOL for your switch or stack. When this field is set to disabled (the default state), the Operational Status for all of the switch/stack ports is set to Authorized (no security restriction).<br>Default Disabled<br>Range Disabled, Enabled |
| Unit | Allows you to select the unit number (when stacking is configured) to view or configure. To view or configure another unit, type its unit number and press [Enter], or press the spacebar to toggle the unit numbers. If you set this field value to All, other screen field values you modify apply to *all* stack ports.<br>Default 1<br>Range 1,2,3,4,5,6,7,8,ALL |

**Table 12** EAPOL security configuration screen options (Continued)

| Option | Description |
|---|---|
| Port | Allows you to select a specified unit's (see preceding Unit field) port number to view or configure. To view or configure another port, type its port number and press [Enter], or press the spacebar to toggle the port numbers. If you set this field value to All, other screen field values you modify apply to *all* ports for the specified unit.<br><br>When using the Ethernet Switches 460 and 470, the All value is also useful when you want to apply modified field values to most of, but not all of, your switch's ports. For example, if you want to apply modified field values to all but one of your switch's ports, it may be easier to apply the All value in the Port field, and then reconfigure the single port back to its original values.<br><br>Default 1<br><br>Range 1 to 28, ALL (Ethernet Switch 460-24T)<br>1 to 26, ALL (Ethernet Switch 470-24T)<br>1 to 48, ALL (Ethernet Switch 470-48T) |
| Initialize | Allows you to activate EAPOL authentication for the specified unit/port.<br><br>Default No<br><br>Range No, Yes |
| Administrative Status | Allows you to set the EAPOL authorization status for the specified unit/port.<br><br>Default Force Authorized<br><br>Range Force Authorized, Force Unauthorized, Auto<br><br>• Force Authorized means the specified unit/port authorization status is *always* authorized.<br>• Force Unauthorized means the specified unit/port authorization status is *always* Unauthorized.<br>• Auto means the specified unit/port authorization status depends on the EAP authentication results. |
| Operational Status | A read-only field that shows the current authorization status for the specified unit/port. This read-only field does not appear when the Unit/Port field value is set to All.<br><br>Default Authorized<br><br>Range Authorized, Unauthorized |

**Table 12** EAPOL security configuration screen options (Continued)

| Option | Description |
|---|---|
| Administrative Traffic Control | Allows you to choose whether EAPOL authentication is set for incoming and outgoing traffic or for incoming traffic only. For example, if you set the specified unit/port field value to Incoming and Outgoing, and the EAPOL authentication fails, then both incoming and outgoing traffic on the specified unit/port is blocked.<br>Default Incoming and Outgoing<br>Range Incoming and Outgoing, Incoming Only |
| Operational Traffic Control | A read-only field that indicates the current administrative traffic control configuration for the specified unit/port (see preceding field description). This read-only field does not appear when the Unit/Port field value is set to All.<br>Default Incoming and Outgoing<br>Range Incoming and Outgoing, Incoming Only |
| Re-authenticate Now | Allows you to activate EAPOL authentication for the specified unit/port immediately, without waiting for the Re-Authentication Period to expire.<br>Default No<br>Range No, Yes |
| Re-authentication | Allows you to repeat EAPOL authentication for the specified unit/port according to the time interval value configured in the Re-Authentication Period field (see next field description).<br>Default Enabled<br>Range Enabled, Disabled |
| Re-authentication Period | When the Re-Authentication field value (see preceding field) is set to enabled, this field allows you to specify the time period between successive EAPOL authentications for the specified unit/port.<br>Default 3600 seconds<br>Range 1 to 604800 seconds |
| Quiet Period | Allows you to specify the time period between any single EAPOL authentication failure and the start of a new EAPOL authentication attempt.<br>Default 60 seconds<br>Range 0 to 65535 seconds |
| Transmit Period | Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets.<br>Default 30 seconds<br>Range 1 to 65535 seconds |

**Table 12** EAPOL security configuration screen options (Continued)

| Option | Description |
|---|---|
| Supplicant Timeout | Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets.<br>Default 30 seconds<br>Range 1 to 65535 seconds |
| Server Timeout | Allows you to specify how long the switch waits for the RADIUS server to respond to all EAP packets.<br>Default 30 seconds<br>Range 1 to 65535 seconds |
| Maximum Requests | Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant.<br>Default 2 attempts<br>Range 1 to 10 attempts |
| User Based Policy | Allows you to enable or disable User-Based Policy (UBP) attributes.<br>Range Enable or disable |

# Chapter 2
# Configuring security using the CLI

This chapter describes the security commands available with the CLI. For more information about these security features, as well as using the console interface (CI) menus, refer to Chapter 1, “Using security in your network,” on page 31.

This chapter covers the following topics:



## Securing your system

To secure your system using the CLI, refer to the following sections:

## Setting the CLI password

You can set passwords using the `cli password` command for selected types of access using the CLI, Telnet, or RADIUS security.

For more information about Telnet access, refer to "Setting Telnet access" on page 95. For more information about using RADIUS security with the CLI, refer to "Configuring the RADIUS-based management password authentication" on page 135.

### cli password command

The `cli password` command is in two forms and performs the following functions for either the switch or the entire stack:

- changes the password for access through the serial console port and Telnet
- specifies changing the password for serial console port or Telnet access and whether to authenticate password locally or with the RADIUS server

The configurations are made for the current operation mode (either switch or stack). The syntax for the `cli password` command is:

```
cli password {ro|rw} <WORD>

cli password {serial|telnet} {none|local|radius}
```

The `cli password` command is in the config command mode.

Table 13 describes the parameters and variables for the `cli password` command.

**Table 13** cli password command parameters and variables

| Parameters and variables | Description |
|---|---|
| `ro\|rw` | Specifies you are modifying the read-only (ro) password or the read-write (rw) password. |
| <*WORD*> | Enter your password.<br>Note: This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password. |
| `serial\|telnet` | Specifies you are modifying the password for serial console access or for Telnet access. |
| `none\|local\|radius` | Specifies the password you are modifying:<br>• `none`—disables the password<br>• `local`—use the locally defined password for serial console or Telnet access<br>• `radius`—use RADIUS authentication for serial console or Telnet access |

## Setting Password Security

The following commands enable and configure Password Security:


- "password security command"
- "no password security command" on page 88
- "password aging-time day command" on page 88
- "show password aging-time day command" on page 88


### password security command

The `password security` command enables password security on the switch.

The syntax of the command is:

```
password security
```

The `password security` command has no parameters or variables.

The `password security` command is in the config command mode.

## no password security command

The `no password security` command disables password security on the switch.

The syntax of the command is:

```
no password security
```

The `no password security` command has no parameters or variables.

The `no password security` command is in the config command mode.

## password aging-time day command

The `password aging-time day` command sets the password aging time.

The syntax of the command is:

```
password aging-time day <aging-value>
```

where aging-value is between 0 - 2730. A value of 0 causes the password to age out immediately.

If a new aging time is set from the CLI, the password aging counters are not reset.

The `password aging-time day` command is in the config command mode.

## show password aging-time day command

The `show password aging-time day` command shows the password aging-time.

The syntax of the command is:

```
show password aging-time day
```

Sample output for this command is:

```
Aging time: 2730 days
```

The `show password aging-time day` command is in the config command mode.

## Configuring the IP manager list

When enabled, the IP manager list determines which source IP addresses are allowed access to the switch. No other source IP addresses have access to the switch. You configure the IP manager list using the following commands:


- "show ipmgr command"
- "ipmgr command for management system" on page 90
- "no ipmgr command for management system" on page 91
- "ipmgr command for source IP address" on page 92
- "no ipmgr command for source IP address" on page 93


### show ipmgr command

The `show ipmgr` command displays whether Telnet, SNMP, and Web access are enabled; whether the IP manager list is being used to control access to Telnet, SNMP, and the Web-based management system; and the current IP manager list configuration. The syntax for the `show ipmgr` command is:

```
show ipmgr
```

The `show ipmgr` command is in the privExec command mode.

The `show ipmgr` command has no parameters or variables.

Figure 14 displays sample output from the `show ipmgr` command.

**Figure 14** `show ipmgr` command output

```
470_24T#show ipmgr
TELNET Access: Enabled
SNMP Access:   Enabled
WEB Access:    Enabled
TELNET IP List Access Control: Enabled
SNMP IP List Access Control:   Enabled
WEB IP List Access Control:    Enabled
Allowed Source IP Address  Allowed Source Mask
-------------------------  -------------------
0.0.0.0                    0.0.0.0
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
```

## ipmgr command for management system

The `ipmgr` command for the management systems enables the IP manager list for Telnet, SNMP, or HTTP access. The syntax for the `ipmgr` command for the management systems is:

```
ipmgr {telnet|snmp|http} [source-ip <1-50> <XXX.XXX.XXX.XXX>
[mask <XXX.XXX.XXX.XXX>]]
```

The `ipmgr` command for the management systems is in the config mode.

Table 14 describes the parameters and variables for the `ipmgr` command.

**Table 14** ipmgr command for system management parameters and variables

| Parameters and variables | Description |
|---|---|
| `telnet\|snmp\|http` | Enables IP manager list checking for access to various management systems:<br>• `telnet`—provides list access using Telnet access<br>• `snmp`—provides list access using SNMP, including the Device Manager<br>• `http`—provides list access using the Web-based management system |
| `source-ip <1-50> <XXX.XXX.XXX.XXX>` | Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation. |
| `[mask <XXX.XXX.XXX.XXX>]` | Specifies the subnet mask from which access is allowed; enter IP mask in dotted-decimal notation. |

## no ipmgr command for management system

The `no ipmgr` command disables the IP manager list for Telnet, SNMP, or HTTP access. The syntax for the `no ipmgr` command for the management systems is:

```
no ipmgr {telnet|snmp|http}
```

The `no ipmgr` command is in the config mode.

Table 15 describes the parameters and variables for the `no ipmgr` command.

**Table 15** no ipmgr command for management system

| Parameters and variables | Description |
|---|---|
| `telnet\|snmp\|http` | Disables IP manager list checking for access to various management systems:<br>• `telnet`—disables list check for Telnet access<br>• `snmp`—disables list check for SNMP, including the Device Manager<br>• `http`—disables list check for the Web-based management system |

## ipmgr command for source IP address

The `ipmgr` command for source IP addresses allows you to enter the source IP addresses or address ranges that you allow to access the switch or the stack. The syntax for the `ipmgr` command for source IP addresses is:

```
ipmgr {source-ip <1-50> <XXX.XXX.XXX.XXX>
[mask <XXX.XXX.XXX.XXX>]}
```

The `ipmgr` command for the source IP addresses is in the config mode.

Table 16 describes the parameters and variables for the `ipmgr` command for the source IP addresses

**Table 16** ipmgr command for source IP addresses parameters and variables

| Parameters and variables | Description |
|---|---|
| `source-ip <1-50> <XXX.XXX.XXX.XXX>` | Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation. |
| `[mask <XXX.XXX.XXX.XXX>]` | Specifies the subnet mask from which access is allowed; enter IP mask in dotted-decimal notation. |

### no ipmgr command for source IP address

The `no ipmgr` command for source IP addresses disables access for specified source IP addresses or address ranges and denies them access to the switch or the stack. The syntax for the `no ipmgr` command for source IP addresses is:

```
no ipmgr {source-ip [<1-50>]}
```

The `no ipmgr` command for the source IP addresses is in the config mode.

Table 17 describes the parameters and variables for the `no ipmgr` command for the source IP addresses.

**Table 17** no ipmgr command for source IP addresses parameters and variables

| Parameters and variables | Description |
|---|---|
| `source-ip [<1-50>]` | When you specify an option, it sets the IP address and mask for the specified entry to 255.255.255.255 and 255.255.255.255.<br>When you omit the optional parameter, it resets the list to factory defaults. |

## Changing the http port number

Beginning with Release 3.1 software, you can configure the HTTP port. This feature provides enhanced security and network access. The default HTTP port typically used to communicate between the Web client and the server is port 80. With this feature, you can change the HTTP port.

You can configure this feature using the following commands:


- "show http-port command" on page 94
- "http-port command" on page 94
- "default http-port" on page 95

## show http-port command

The `show http-port` command displays the port number of the HTTP port. The syntax for the `show http-port` command is:

```
show http-port
```

The `show http-port` command is in the privExec command mode.

The `show http-port` command has no parameters or variables.

Figure 15 displays sample output from the `show http-port` command.

**Figure 15** `show http-port` command output

```
470_48T#show http-port
HTTP Port: 80
```

## http-port command

The `http-port` command sets the port number for the HTTP port. The syntax for the `http-port` command is:

```
http-port <1024-65535>
```

The `http-port` command is in the config command mode.

Table 18 describes the parameters and variables for the `http-port` command.

**Table 18** `http-port` command parameters and variables

| Parameters and variables | Description |
|---|---|
| <1024-65535> | Enter the port number you want to be the HTTP port. |

**Note:** To set the HTTP port to 80, use the `default http-port` command.

The default value for this parameter is port 80.

### default http-port

The `default http-port` command sets the port number for the HTTP port to the default value of 80. The syntax for the `default http-port` command is:

```
default http-port
```

The `default http-port` command is in the config command mode.

The `default http-port` command has no parameters or variables.

## Setting Telnet access

You can also access the CLI through a Telnet session. To access the CLI remotely, the management port must have an assigned IP address, and remote access must be enabled. You can log on to the switch using Telnet from a terminal that has access to the switch.

To open a Telnet session from Device Manager, click the Telnet icon on the toolbar (Figure 16) or click Action > Telnet on the Device Manager toolbar.

**Figure 16** Telnet icon on Device Manager toolbar

**Note:** Multiple users can access the CLI system simultaneously, through the serial port, Telnet, and modems. The maximum number of simultaneous users is four plus one each at the serial port for a maximum of 12 users. All users can configure simultaneously.

You can view the Telnet-allowed IP addresses and settings, change the settings, or disable the Telnet connection. This section covers the following topics:


- "show telnet-access command" on page 96
- "telnet-access command" on page 96
- "no telnet-access command" on page 97
- "default telnet-access command" on page 98

## show telnet-access command

The `show telnet-access` command displays the current settings for Telnet access. The syntax for the `show telnet-access` command is:

```
show telnet-access
```

The `show telnet-access` command is in the privExec command mode.

The `show telnet-access` command has no parameters or variables.

Figure 17 displays sample output from the `show telnet-access` command.

**Figure 17** `show telnet-access` command output

```
470_24T#show telnet-access
TELNET Access:       Enabled
Login Timeout:       1 minute(s)
Login Retries:       3
Inactivity Timeout:  15 minute(s)
Event Logging:       All
Allowed Source IP Address  Allowed Source Mask
-------------------------  -------------------
0.0.0.0                    0.0.0.0
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
```

## telnet-access command

The `telnet-access` command allows you to configure the Telnet connection used to manage the switch. The syntax for the `telnet-access` command is:

```
telnet-access [enable|disable] [login-timeout <1-10>]
[retry <1-100>] [inactive-timeout <0-60>]
[logging {none|access|failures|all}]
[source-ip <1-50> <XXX.XXX.XXX.XXX>[mask <XXX.XXX.XXX.XXX>]]
```

The `telnet-access` command is in the config command mode.

Table 19 describes the parameters and variables for the `telnet-access` command.

**Table 19** `telnet-access` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `enable\|disable` | Enables or disables Telnet connections. |
| `login-timeout <1-10>` | Specifies the time in minutes to wait between initial Telnet connection and accepted password before closing the Telnet connection; enter an integer between 1 and 10. |
| `retry <1-100>` | Specifies the number of times the user can enter an incorrect password before closing the connection; enter an integer between 1 and 100. |
| `inactive timeout <0-60>` | Specifies in minutes how long to wait before closing an inactive session; enter an integer between 0 and 60. |
| `logging {none\|access\|failures\|all}]` | Specifies what types of events you want to save in the event log:<br>• `none`—do not save access events in the log<br>• `access`—save access events in the log<br>• `failure`—save failed access events in the log<br>• `all`—save all access events in the log |
| `[source-ip <1-50> <XXX.XXX.XXX.XXX> [mask <XXX.XXX.XXX.XXX>]` | Specifies the source IP address that allow connections. Enter the IP address as an integer or in dotted-decimal notation. Specifies the subnet mask that allow connections; enter IP mask in dotted-decimal notation.<br><br>Note: These are the same source IP addresses as in the IP Manager list. For more information about the IP Manager list, see "Configuring the IP manager list" on page 89. |

## no telnet-access command

The `no telnet-access` command allows you to disable the Telnet connection. The syntax for the `no telnet-access` command is:

```
no telnet-access [source-ip [<1-50>]]
```

The `no telnet-access` command is in the config mode.

Table 20 describes the parameters and variables for the `no telnet-access` command.

**Table 20** `no telnet-access` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `source-ip [<1-50>]` | Disables the Telnet access.<br>When you do *not* use the optional parameter, the source-ip list is cleared, meaning the 1st index is set to 0.0.0.0./0.0.0.0. and the 2nd to 50th indexes are set to 255.255.255.255/255.255.255.255.<br>When you *do* specify a source-ip value, the specified pair is set to 255.255.255.255/255.255.255.255.<br><br>Note: These are the same source IP addresses as in the IP Manager list. For more information about the IP Manager list, see "Configuring the IP manager list" on page 89. |

### default telnet-access command

The `default telnet-access` command sets the Telnet settings to the default values. The syntax for the `default telnet-access` command is:

```
default telnet-access
```

The `default telnet-access` command is in the config command mode.

The `default telnet-access` command has no parameters or variables.

## Configuring Secure Shell (SSH)

**Note:** Refer to the release notes accompanying your software release for the latest information about how to download the SSH-enabled image file. The SSH server will not function without the use of this image.

The secure shell protocol provides secure access to the CLI interface. With the CLI system, you can use the following commands:

- "show ssh global command" on page 99

## show ssh global command

The `show ssh global` command displays the secure shell configuration information. The syntax for the `show ssh global` command is:

```
show ssh global
```

The `show ssh global` command is in the privExec command mode.

The `show ssh global` command has no parameters or variables.

Figure 18 on page 100 displays sample output from the `show ssh global` command.

**Figure 18** `show ssh global` command output

```
470_24T#show ssh global
Active SSH Sessions      :  2
Version                  :  Version 2 only
Port                     :  22
Max. Sessions            :  2
Timeout                  :  60
DSA Key Size             :  1024
DSA Authentication       :  True
Password Authentication  :  True
DSA Auth Key TFTP Server :  134.177.152.12
DSA Host Keys            :  pubkey.txt
Enabled                  :  True
```

## show ssh session command

The `show ssh session` command displays the secure shell session information. The session information includes the session ID and the host IP address. A host address of 0.0.0.0 indicates no connection for that session ID. The syntax for the `show ssh session` command is:

`show ssh session`

The `show ssh session` command is in the privExec command mode.

The `show ssh session` command has no parameters or variables.

Figure 19 displays sample output from the `show ssh session` command.

**Figure 19** `show ssh session` command output

```
470_24T#show ssh session
Session  Host
-------  ---------------
0        134.177.152.12
1        0.0.0.0
```

### show ssh download-auth-key command

The `show ssh download-auth-key` command displays the results of the most recent attempt to download the DSA public key from the TFTP server. The syntax for the `show ssh download-auth-key` command is:

```
show ssh download-auth-key
```

The `show ssh download-auth-key` command is in the privExec command mode.

The `show ssh download-auth-key` command has no parameters or variables.

Figure 20 displays sample output from the `show ssh session` command.

**Figure 20** `show ssh download-auth-key` command output

```
470_24T#show ssh download-auth-key
Public Key TFTP Server   :  134.177.152.12
Public Key File Name     :  pubkey.txt
Last Transfer Result     :  Success
```

### ssh dsa-key command

The `ssh dsa-key` command initiates generation of a DSA host key at the next system reboot. If a key size is specified, a key of this size (in bytes) is generated. If no key size is specified, the previous provisioned key size (or default of 1024) is used. This command can be executed only in the SSH disable mode. The syntax of the `ssh dsa-key` command is:

```
ssh dsa-key-gen [<512-1024>]
```

The `ssh dsa-key-gen` command is in the config command mode.

Table 21 describes the parameters and variables for the `ssh dsa-key-gen` command.

**Table 21** `ssh dsa-key-gen` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<512-1024>* | Sets the SSH host key size. Can be a value from 512 to 1-24. Default is 1024. |

## no ssh dsa-key command

The `no ssh dsa-key-gen` command deletes the DSA host key in the switch. The syntax of the `no ssh dsa-key-gen` command is:

```
no ssh dsa-key
```

The `no ssh dsa-key` command is in the config command mode.

There are no parameters or variables for the `no ssh dsa-key` command.

## ssh command

The `ssh` command enables the SSH server on the Ethernet Switch in non-secure mode. In addition to accepting SSH connections, the switch continues to accept Web, SNMP, and Telnet connections while in this mode. The syntax of the `ssh` command is:

```
ssh
```

The `ssh` command is in the config command mode.

There are no parameters or variables for the `ssh` command.

## no ssh command

The `no ssh` command disables the SSH server on the switch. The syntax of the `no ssh` command is:

```
no ssh
```

The `no ssh` command is in the config command mode.

There are no parameters or variables for the `no ssh` command.

## ssh secure command

The `ssh secure` command enables the SSH server on the switch in secure mode. In secure mode, the switch does not accept Web, SNMP, or Telnet connections. The syntax of the `ssh secure` command is:

```
ssh secure
```

The `ssh secure` command is in the config command mode.

There are no parameters or variables for the `ssh secure` command.

## no ssh secure command

The `no ssh secure` command disables the SSH server on the switch. The syntax of the `no ssh secure` command is:

```
no ssh secure
```

The `no ssh secure` command is in the config command mode.

There are no parameters or variables for the `no ssh secure` command.

## ssh max-sessions command

The `ssh max-sessions` command allows you to set the maximum number of simultaneous SSH sessions allowed. The syntax of the `ssh max-sessions` command is:

```
ssh max-sessions <0-2>
```

where the default value is 2.

The `ssh max-sessions` command is in the config command mode.

## ssh timeout command

The `ssh timeout` command sets the timeout value for session authentication. The syntax of the `ssh timeout` command is:

```
ssh timeout <1-120>
```

The `ssh timeout` command is in the config command mode.

Table 22 describes the parameters and variables for the `ssh timeout` command.

**Table 22** `ssh timeout` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<1-120>* | Specifies the timeout value for authentication. Default is 60. |

## ssh dsa-auth command

The `ssh dsa-auth` command enables DSA authentication. The syntax of the `ssh dsa-auth` command is:

```
ssh dsa-auth
```

The `ssh dsa-auth` command is in the config command mode.

There are no parameters or variables for the `ssh dsa-auth` command.

## no ssh dsa-auth command

The `no ssh dsa-auth` command disables DSA authentication. The syntax of the `no ssh dsa-auth` command is:

```
no ssh dsa-auth
```

The `no ssh dsa-auth` command is in the config command mode.

There are no parameters or variables for the `no ssh dsa-auth` command.

## ssh pass-auth command

The `ssh pass-auth` command enables password authentication. The syntax of the `ssh pass-auth` command is:

```
ssh pass-auth
```

The `ssh pass-auth` command is in the config command mode.

There are no parameters or variables for the `ssh pass-auth` command.

## no ssh pass-auth command

The `no ssh pass-auth` command disables password authentication. The syntax for the `no ssh pass-auth` command is:

```
no ssh pass-auth
```

The `no ssh pass-auth` command is in the config command mode.

There are no parameters or variables for the `no ssh pass-auth` command.

## ssh port command

The `ssh port` command sets the SSH connection port. The syntax of the `ssh port` command is:

```
ssh port <1-65535>
```

The `ssh port` command is in the config command mode.

Table 23 describes the parameters and variables for the `ssh port` command.

**Table 23** `ssh port` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<1-65535>* | Specifies the SSH connection port. Default is 22. |

## ssh download-auth-key

The `ssh download-auth-key` command downloads the client public key from the TFTP server to the switch. The syntax for the `ssh download-auth-key` command is:

```
ssh download-auth-key [address <XXX.XXX.XXX.XXX>]
[key-name <file>]
```

The `ssh download-auth-key` command is in the config command mode.

Table 24 describes the parameters and variables for the `ssh download-auth-key` command.

**Table 24** `ssh download-auth-key` command parameters and variables

| Parameters and variables | Description |
|---|---|
| address <*XXX.XXX.XXX.XXX*> | The IP address of the TFTP server. |
| key-name <*file*> | The name of the public key file on the TFTP server. |

## default ssh command

The `default ssh` command resets the specific secure shell configuration parameter to the default value. The syntax of the `default ssh` command is:

```
default ssh
[dsa-auth|dsa-key|max-sessions|pass-auth|port|timeout]
```

The `default ssh` command is in the config command mode.

Table 25 describes the parameters and variables for the `default ssh` command.

**Table 25** `default ssh` command parameters and variables

| Parameters and variables | Description |
|---|---|
| dsa-auth | Resets dsa-auth to the default value. Default is True. |
| dsa-key | Resets the dsa-key size to the default value of 1024 bits. |

**Table 25** `default ssh` command parameters and variables (Continued)

| Parameters and variables | Description |
|---|---|
| `max-sessions` | Resets the maximum number of simultaneous sessions to the default of 2. |
| `pass-auth` | Resets pass-auth to the default value. Default is True. |
| `port` | Resets the port number for SSH connections to the default. Default is 22. |
| `timeout` | Resets the timeout value for session authentication to the default. Default is 60. |

## Command history audit log

Starting with Release 3.6 software, Ethernet Switches 460 and 470 save the last 100 commands entered to a command history log in NVRAM. This history is periodically copied from NVRAM to the remote syslog server.

Each log entry consists of:

- a timestamp (sysUpTime or real clock time, if available)
- the source of the command (for example, console interface and unit or Telnet and IP)
- the text of the command itself

The command history is saved if a user resets the switch to factory defaults (in this case, the history would also contain the reset command).

You must configure a remote syslog server in order to save all of the command history (see *System Monitoring Guide* (217107-A)). If you do not configure a remote syslog server, the switch loses the commands when they begin to wrap in the NVRAM buffer.

## show audit log command

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 | ssh | telnet]
```

The `show audit log` command is in the privExec command mode.

Table 26 describes the parameters and variables for the `show audit log` command.

**Table 26** show audit log command parameters and variables

| Parameters and variables | Description |
|---|---|
| asccfg | Displays the audit log for ASCII configuration. |
| serial | Displays the audit log for serial connections. |
| ssh | Displays the audit log for SSH connections. |
| telnet | Displays the audit log for Telnet connections. |

Figure 21 displays sample output from the `show audit log` command.

**Figure 21** `show audit log` command output

```
470-24T#show audit log telnet
Idx Pri(/Timestamp/Host) Stat Source(Unit)   Uptime       Command
----------------------------------------------------------------
1  <30> :S telnet(192.168.10.2): 5 days, 05:50:09: configure
2  <30> :S telnet(192.168.10.2): 5 days, 05:50:30: interface FastEthernet all
3  <30>  :S telnet(192.168.10.2): 0 days, 03:54:47: enable
4  <30>  :S telnet(192.168.10.2): 0 days, 03:54:53: configure
5  <30>  :S telnet(192.168.10.2): 0 days, 03:55:00: interface FastEthernet all
6  <30>  :S telnet(192.168.10.2): 1 day, 00:31:24: enable
7  <30>  :S telnet(192.168.10.2): 1 day, 00:31:26: configure
8  <30>  :S telnet(192.168.10.2): 1 day, 00:31:47: show qos
interface-assignments
9  <30>  :S telnet(192.168.10.2): 1 day, 00:59:21: enable
10 <30>  :S telnet(192.168.10.2): 1 day, 00:59:24: configure
----More (q=Quit, space/return=Continue)----
```

## Enabling or disabling the server for Web-based management

You can enable or disable the Web server for the Web-based management system.

This section discusses the following commands:


- "web-server"
- "no web-server" on page 109


### web-server

The `web-server` command enables or disables the Web server that you can use for Web-based management. The syntax for the `web-server` command is:

```
web-server {enable|disable}
```

The `web-server` command is in the config mode.

Table 27 describes the parameters and variables for the `web-server` command.

**Table 27** `web-server` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `enable\|disable` | Enables or disables the Web server. |

### no web-server

The `no web-server` command disables the Web server that you use for Web-based management. The syntax for the `no web-server` command is:

```
no web-server
```

The `no web-server` command is in the config mode.

The `no web-server` command has no parameters or variables.

## Configuring Secure Socket Layer (SSL) Web-based management

You can enable or disable Secure Socket Layer (SSL) to provide security for the Web-based management system.

This section discusses the following commands:



## ssl command

The `ssl` command enables SSL on the switch. When SSL is enabled, the Web server operates in secure mode.

The syntax of the `ssl` command is:

```
ssl
```

The `ssl` command is in the config command mode.

There are no parameters or variables for the `ssl` command.

## no ssl command

This command disables SSL on the switch. When SSL is disabled, the Web server operates in non-secure mode.

The syntax of the `no ssl` command is:

```
no ssl
```

The `no ssl` command is in the config command mode.

There are no parameters or variables for the `no ssl` command.

## ssl certificate command

The `ssl certificate` command creates a certificate. On creation, this new certificate is used only on the next system reset or SSL server reset. The certificate generated is stored in NVRAM as file SSLCERT.DAT and replaces the existing file. This operation does not affect the ongoing SSL server operation.

The syntax of the `ssl certificate` command is:

```
ssl certificate
```

The `ssl certificate` command is in the config command mode.

There are no parameters or variables for the `ssl certificate` command.

## no ssl certificate command

The `no ssl certificate` command deletes a certificate. On deletion, the certificate in the NVRAM is deleted. The delete operation does not affect the ongoing SSL server operation.

The syntax of the `no ssl certificate` command is:

```
no ssl certificate
```

The `no ssl certificate` command is in the config command mode.

There are no parameters or variables for the `no ssl certificate` command.

## ssl reset command

The `ssl reset` command resets the SSL server. If SSL is enabled, The SSL server is restarted and initialized with the certificate stored in NVRAM. Existing SSL connections, if present, are closed. If SSL is not enabled, the existing non-secure connections are nevertheless closed, and the non-secure operation resumes.

The syntax of the `ssl reset` command is:

```
ssl reset
```

The `ssl reset` command is in the config command mode.

There are no parameters or variables for the `ssl reset` command.

## show ssl certificate command

The `show ssl certificate` command displays the certificate that is in use by the SSL server and what is in the NVRAM.

The syntax of the `show ssl certificate` command is:

```
show ssl certificate
```

The `show ssl certificate` command is in the config command mode.

There are no parameters or variables for the `show ssl certificate` command.

## show ssl command

The `show ssl` command shows the SSL server configuration and state.

The syntax for this command is:

```
show ssl
```

Table 28 describes the Server State Information that is output from the `show ssl` command:

**Table 28** show ssl command output description

| Field | Description |
|---|---|
| Web Server SSL secured | Indicates whether the Web server is using SSL connection. |
| SSL Server state | Indicates the SSL server state, which can be one of the following.<br>• Un-initialized: the server is not running.<br>• Certificate Initialization: the server is generating a certificate during its initialization phase.<br>• Active: the server is initialized and running. |
| SSL Certificate: Generation in progress | Indicates whether the SSL is in the process of generating a certificate.<br>The SSL server generates a certificate during the server start-up initialization and when the CLI user initiates a new certificate regeneration, providing a new public-private key pair. |
| SSL Certificate: Saved in non-volatile config | Indicates whether an SSL certificate exists in the NVRAM. The SSL certificate is not present if the system is initialized for the first time or a CLI user has deleted the certificate. |

## Common SNMP and SNMPv3 CLI commands

This section describes the common CLI commands for configuring SNMP and SNMPv3. For details on the SNMP CLI commands that are specific to SNMPv3, refer to "CLI commands specific to SNMPv3" on page 125.

The switch provides the following CLI commands to configure SNMP and SNMPv3:

## snmp-server command

The `snmp-server` command enables or disables the SNMP server. The syntax for the `snmp-server` command is:

```
snmp-server {enable|disable}
```

The `snmp-server` command is in the config command mode.

Table 29 describes the parameters and variables for the `snmp-server` command.

**Table 29** `snmp-server` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `enable\|disable` | Enables or disables the SNMP server. |

## no snmp-server command

The `no snmp-server` command disables SNMP access. The syntax for the `no snmp-server` command is:

```
no snmp-server
```

The `no snmp-server` command is in the config command mode.

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

**Note:** Disabling SNMP access also locks you out of the Device Manager management system.

## snmp-server authentication-trap command

The `snmp-server authentication-trap` command enables or disables the generation of SNMP authentication failure traps. The syntax for the `snmp-server authentication-trap` command is:

```
snmp-server authentication-trap {enable|disable}
```

The `snmp-server authentication-trap` command is in the config command mode.

Table 30 describes the parameters and variables for the `snmp-server authentication-trap` command.

**Table 30** `snmp-server authentication-trap` command

| Parameters and variables | Description |
|---|---|
| `enable\|disable` | Enables or disables the generation of authentication failure traps. |

## no snmp-server authentication-trap command

The `no snmp-server authentication-trap` command disables generation of SNMP authentication failure traps. The syntax for the `no snmp-server authentication-trap` command is:

```
no snmp-server authentication-trap
```

The `no snmp-server authentication-trap` command is in the config command mode.

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

## default snmp-server authentication-trap command

The `default snmp-server authentication-trap` command restores SNMP authentication trap configuration to the default settings. The syntax for the `default snmp-server authentication-trap` command is:

```
default snmp-server authentication-trap
```

The `default snmp-server authentication-trap` command is in the config command mode.

The `default snmp-server authentication-trap` command has no parameters or variables.

## snmp-server community for read/write command

The `snmp-server community` command for read/write modifies the community strings for SNMP v1 and SNMPv2c access. The syntax for the `snmp-server community` for read/write command is:

```
snmp-server community <community-string> [ro|rw]
```

The `snmp-server community` for read/write command is in the config command mode.

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.

This command affects community strings that were created prior to Release 3.0 software. These community strings have a fixed MIB view.

Table 31 describes the parameters and variables for the `snmp-server community` for read/write command.

**Table 31** `snmp-server community for read/write` command

| Parameters and variables | Description |
|---|---|
| *<community-string>* | Changes community strings for SNMP v1 and SNMPv2c access. Enter a community string that works as a password and permits access to the SNMP protocol. If you set the value to 'NONE', it is disabled.<br>Note: This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new community string. |
| `ro\|rw` | 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.<br><br>**Note**: If neither `ro` nor `rw` is specified, `ro` is assumed (default). |

## 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 in the config command mode.

If you do not specify a read-only or read-write community parameter, all community strings are removed, including all 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 32 describes the parameters and variables for the `no snmp-server community` command.

**Table 32** `no snmp-server community` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `ro\|rw\|` | Sets the specified old-style community string's value to NONE, thereby disabling it. |
| *<community-string>* | Deletes the specified community string from the SNMPv3 MIBs (that is, from the new-style configuration). |

## default snmp-server community command

The `default snmp-server community` command restores the community string configuration to the default settings. The syntax for the `default snmp-server community` command is:

```
default snmp-server community [ro|rw]
```

The `default snmp-server community` command is in the config command mode.

If the read-only or read-write parameter is omitted from the command, then all communities are restored to their default settings. The read-only community is set to Public, the read-write community is set to Private, and all other communities are deleted.

Table 33 describes the parameters and variables for the `default snmp-server community` command.

**Table 33** `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'. |

## show snmp-server community command

The `show snmp-server community` command displays the SNMP community string configuration. (The community strings are not displayed when Password Security is enabled.) The syntax for the `show snmp-server community` command is:

```
show snmp-server community
```

The `show snmp-server` command is in the privExec command mode.

## snmp-server contact command

The `snmp-server contact` command configures the SNMP sysContact value. The syntax for the `snmp-server contact` command is:

```
snmp-server contact <text>
```

The `snmp-server contact` command is in the config command mode.

Table 34 describes the parameters and variables for the `snmp-server contact` command.

**Table 34** `snmp-server contact` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<text>* | Specifies the SNMP sysContact value; enter an alphanumeric string. |

## no snmp-server contact command

The `no snmp-server contact` command clears the sysContact value. The syntax for the `no snmp-server contact` command is:

```
no snmp-server contact
```

The `no snmp-server contact` command is in the config command mode.

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

## default snmp-server contact command

The `default snmp-server contact` command restores the sysContact value to the default value. The syntax for the `default snmp-server contact` command is:

```
default snmp-server contact
```

The `default snmp-server contact` command is in the config command mode.

The `default snmp-server contact` 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 in the config command mode.

Table 35 describes the parameters and variables for the `snmp-server location` command.

**Table 35** `snmp-server location` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<text>* | Specifies 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 <text>
```

The `no snmp-server location` command is in the config command mode.

Table 36 describes the parameters and variables for the `no snmp-server location` command.

**Table 36** `no snmp-server location` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<text>* | Specifies the SNMP sysLocation value. Enter a string of up to 255 characters. |

## 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 in the config command mode.

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

## 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 in the config command mode.

Table 37 describes the parameters and variables for the `snmp-server name` command.

**Table 37** `snmp-server name` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<text>* | Specifies 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 <text>
```

The `no snmp-server name` command is in the config command mode.

Table 38 describes the parameters and variables for the `no snmp-server name` command.

**Table 38** `no snmp-server name` command parameters and variables

| Parameters and variables | Description |
|---|---|
| <text> | Specifies the SNMP sysName value; enter an alphanumeric string of up to 255 characters. |

## 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 in the config command mode.

Table 39 describes the parameters and variables for the `default snmp-server name` command.

**Table 39** `default snmp-server name` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `<text>` | Specifies the SNMP sysName value; enter an alphanumeric string of up to 255 characters. |

## snmp trap link-status command

The `snmp trap link-status` command enables the linkUp/linkDown traps for the port. The syntax of the command is:

```
snmp trap link-status [port <portlist>]
```

The `snmp trap link-status` command is in the config-if command mode.

Table 40 describes the parameters and variables for the `snmp trap link-status` command.

**Table 40** `snmp trap link-status` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `port <portlist>` | Specifies the port numbers to enable the linkUp/linkDown traps on. Enter the port numbers or All.<br><br>**Note**: If you omit this parameter, the system uses the port number specified with the `interface` command. |

## no snmp trap link-status command

The `no snmp trap link-status` command disables the linkUp/linkDown traps for the port. The syntax of the `no snmp trap link-status` command is:

```
no snmp trap link-status [port <portlist>]
```

The `no snmp trap link-status` command is in the config-if command mode.

Table 41 describes the parameters and variables for the `no snmp trap link-status` command.

**Table 41** `no snmp trap link-status` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `port <portlist>` | Specifies the port numbers to disable the linkUp/linkDown traps on. Enter the port numbers or all.<br><br>**Note**: If you omit this parameter, the system uses the port number specified with the `interface` command. |

## default snmp trap link-status command

The `default snmp trap link-status` command disables the linkUp/linkDown traps for the port. The syntax of the command is:

`default snmp trap link-status [port <portlist>]`

The `default snmp trap link-status` command is in the config-if command mode.

Table 42 describes the parameters and variables for the `default snmp trap link-status` command.

**Table 42** `default snmp trap link-status` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `port <portlist>` | Specifies the port numbers to disable the linkUp/linkDown traps on. Enter the port numbers or all.<br><br>**Note**: If you omit this parameter, the system uses the port number specified with the `interface` command. |

## CLI commands specific to SNMPv3

This section describes the unique CLI commands for configuring SNMPv3. For details on the CLI commands that are common to both SNMP and SNMPv3, refer to "Common SNMP and SNMPv3 CLI commands" on page 113.

The following SNMP commands are specific to SNMPv3:



## snmp-server user command

The `snmp-server user` command creates an SNMPv3 user. The syntax for the `snmp-server user` command 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 in the config command mode.

The `sha` and `des` parameters are available only if the switch image has full SHA/DES support.

The command shows three sets of read/write/notify views. The first set specifies unauthenticated access. The second set specifies authenticated access. The third set specifies authenticated and encrypted access.

You can specify authenticated access only if the `md5` or `sha` parameter is included. Likewise, you can specify authenticated and encrypted access only if the `des` parameter is included.

If you omit the authenticated view parameters, authenticated access uses the views specified for unauthenticated access. If you omit all the authenticated and encrypted view parameters, the authenticated and encrypted access uses the same views used for authenticated access. These views are the unauthenticated views, if all the authenticated ones are also omitted.

Table 43 describes the parameters and variables for the `snmp-server user` command.

**Table 43** `snmp-server user` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<username>* | Specifies the user names; enter an alphanumeric string of up to 255 characters. |
| `md5` *<password>* | Specifies the use of an md5 password.<br>• *password*—specifies the new user md5 password; enter an alphanumeric string.<br>If this parameter is omitted, the user is created with only unauthenticated access rights.<br>Note: This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password. |
| `read-view` *<view-name>* | Specifies the read view to which the new user has access:<br>• *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:<br>• *view-name*—specifies the viewname; enter an alphanumeric string of up to 255 characters. |

**Table 43** `snmp-server user` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `notify-view` *<view-name>* | Specifies the notify view to which the new user has access:<br>• *view-name*—specifies the viewname; enter an alphanumeric string of up to 255 characters. |
| `sha/des/3des/aes` | Specifies SHA authentication or one of the following: DES, 3DES, or AES privacy encryption.<br>Note: This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password. |

## 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 <username>
```

The `no snmp-server user` command is in the config command mode.

Table 44 describes the parameters and variables for the `no snmp-server user` command.

**Table 44** `no snmp-server user` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<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 that 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 in the config command mode.

Table 45 describes the parameters and variables for the `snmp-server view` command.

**Table 45** `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 MIB object English descriptor, a dotted form *OID,* or a mix of the two. Each *OID* may also be preceded by a '+' or '-' sign (if this is omitted, a '+' sign is implied). For the dotted form, a sub-identifier can be a '*' indicating a wildcard. Some examples of valid *OID* parameters are as follows:<br>• `sysName`<br>• `+sysName`<br>• `-sysName`<br>• `+sysName.0`<br>• `+ifIndex.1`<br>• `-ifEntry.*.1` (matches all objects in the if Table with an instance of 1, i.e., the entry for interface #1)<br>• `1.3.6.1.2.1.1.1.0` (dotted form of `sysDescr`)<br>The `'+'` or `'-'` indicates whether the specified *OID* is included in or excluded from, respectively, the set of MIB objects that are accessible using this view. For example, if you create a view like this:<br>• `snmp-server view myview +system -sysDescr`<br>And you use that view for the read-view of a user, then the user can read only the system group, except for `sysDescr`. |

## no snmp-server view command

The `no snmp-server view` command deletes the specified view. The syntax for the `no snmp-server view` command is:

```
no snmp-server view <viewname>
```

The `no snmp-server view` is in the config command mode.

Table 46 describes the parameters and variables for the `no snmp-server view` command.

**Table 46** `no snmp-server view` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<viewname>* | Specifies the name of the view to be removed. If no view is specified, all views are removed. |

## snmp-server host for old-style table command

The `snmp-server host` for old-style table command adds a trap receiver to the old-style trap-receiver table. The table has a maximum of four entries, and the 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 syntax for the `snmp-server host` for old-style table command is:

```
snmp-server host <host-ip> <community-string>
```

The `snmp-server host` for old-style table command is in the config command mode.

Table 47 describes the parameters and variables for the `snmp-server host` for old-style table command.

**Table 47** `snmp-server host` for old-style table command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<host-ip>* | Enter a dotted-decimal IP address of a host that is the trap destination. |
| *<community-string>* | Enter a community string that works as a password and permits access to the SNMP protocol. |

## snmp-server host for new-style table command

The `snmp-server host` for new-style table command adds a trap receiver to the new-style configuration (that is, to the SNMPv3 tables) You can create several entries in this table, and each can generate v1, v2c, or v3 traps. Note that you must have previously configured the community string or user that is specified, with a notify-view. The syntax for the `snmp-server host` for new-style table command is:

```
snmp-server host <host-ip> {v1 <community-string>|
v2c <community-string>| v3 {auth|no-auth|auth-priv}
<username>}
```

The `snmp-server host` for new-style table command is in the config command mode.

Table 48 describes the parameters and variables for the `snmp-server host` for new-style table command.

**Table 48** `snmp-server host` for new-style table command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<host-ip>* | Enter a dotted-decimal IP address of a host that will be the trap destination. |
| v1 *<community-string>* | Using v1 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels may be created. |
| v2c *<community-string>* | Using v2c creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels may be created. |
| v3 {auth\|no-auth\| auth-priv} | Using v3 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels may be created:<br>Enter the following variables:<br>• auth\|no-auth—specifies whether SNMPv3 traps should be authenticated<br>• auth-priv—this parameter is only available if the image has full SHA/DES support. |
| *<username>* | Specifies the SNMPv3 username for trap destination; enter an alphanumeric string. |

## no snmp-server host for old-style table command

The `no snmp-server host` for old-style table command deletes trap receivers from the old-style table. The syntax for the `no snmp-server host` for old-style table command is:

```
no snmp-server host [<host-ip> [<community-string>]]
```

The `no snmp-server host` for old-style table command is in the config command mode.

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

Table 49 describes the parameters and variables for the `no snmp-server host` for old-style table command.

**Table 49** `no snmp-server host` for old-style table command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<host-ip>* [*<community-string>*] | Enter the following variables:<br>• *host-ip*—IP address of a trap destination host.<br>• *community-string*— community string that works as a password and permits access to the SNMP protocol.<br>If both parameters are omitted, nothing is cleared.<br>If a host IP is included, the community-string is required or an error is reported. |

## no snmp-server host for new-style table command

The `no snmp-server` for new-style table command deletes trap receivers from the new-style table (SNMPv3 MIB). Any trap receiver matching the IP address and SNMP version is deleted. The syntax for the `no snmp-server host` for new-style table command is:

```
no snmp-server host <host-ip> {v1|v2c|v3}
```

The `no snmp-server host` for new-style table command is in the config command mode.

Table 50 describes the parameters and variables for the `no snmp-server host` for new-style table command.

**Table 50** `no snmp-server host for new-style` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<host-ip>* | Enter the IP address of a trap destination host. |
| v1\|v2c\|v3 | Specifies trap receivers in the SNMPv3 MIBs. |

## default snmp-server host command

The `default snmp-server host` command restores the old-style table to defaults (that is, it clears the table). The syntax for the `default snmp-server host` command is:

```
default snmp-server host
```

The `default snmp-server host` command is in the config command mode.

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

## 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 snmpCommunityTable, 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 <community-string>
{read-view <view-name>|write-view <view-name>|
notify-view <view-name>}
```

The `snmp-server community` command is in the config command mode.

Table 51 describes the parameters and variables for the `snmp-server community` command.

**Table 51** `snmp-server community` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<community-string>* | Enter a community string to be created with access to the specified views.<br>Note: This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new community string. |
| `read-view` *<view-name>* | Changes the read view used by the new community string for different types of SNMP operations.<br>• *view-name*—specifies the name of the view that 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.<br>• *view-name*—specifies the name of the view that 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.<br>• *view-name*—specifies the name of the view that is a set of MIB objects/instances that can be accessed; enter an alphanumeric string. |

## show snmp-server command

The `show snmp-server` command displays the SNMP v3 configuration. The syntax for the `show snmp-server` command is:

```
show snmp-server {community|host|user|view}
```

The `show snmp-server` command is in the privExec command mode.

Table 52 describes the parameters and variables for the `show snmp-server` command.

**Table 52** `show snmp-server` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `community\|host\|user\|view` | Displays SNMPv3 configuration information:<br>• community strings as configured in SNMPv3 MIBs (this parameter is not displayed when Password Security is enabled).<br>• trap receivers as configured in SNMPv3 MIBs<br>• SNMPv3 users, including views accessible to each user<br>• SNMPv3 views |

## 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. The command 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). It consists of a set of initial users, groups, and views. This `snmp-server bootstrap` command deletes ALL existing SNMP configurations, so it should be used with caution.

The syntax for the `snmp-server bootstrap` command is:

```
snmp-server bootstrap <minimum-secure> | <semi-secure>
|<very-secure>
```

The `snmp-server bootstrap` command is in the config command mode.

Table 53 describes the parameters and variables for the `snmp-server bootstrap` command.

**Table 53** `snmp-server bootstrap` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<minimum-secure>* | Specifies a minimum security configuration that allows read access to everything using noAuthNoPriv, and write access to everything using authNoPriv. |
| *<semi-secure>* | Specifies a partial security configuration that allows read access to a small subset of system information using noAuthNoPriv, and read and write access to everything using authNoPriv. |
| *<very-secure>* | Specifies a maximum security configuration that allows no access. |

## Configuring the RADIUS-based management password authentication

Using the RADIUS protocol and a server, you can configure the switch for authentication. With the CLI system, you can use the following commands:


- "show radius-server command"
- "radius-server command" on page 136
- "no radius-server command" on page 137
- "radius-server password fallback" on page 137


### show radius-server command

The `show radius-server` command displays the RADIUS server configuration. The syntax for the `show radius-server` command is:

```
show radius-server
```

The `show radius-server` command is in the privExec command mode.

The `show radius-server` command has no parameters or variables.

Figure 22 on page 136 displays sample output from the `show radius-server` command.

**Figure 22** `show radius-server` command output

```
470_24T#show radius-server
host: 0.0.0.0
Secondary-host: 0.0.0.0
port: 1645
key:
470_24T#
```

## radius-server command

The `radius-server` command changes the RADIUS server settings. The syntax for the `radius-server` command is:

`radius-server host <address> [secondary-host <address>] port <num> key <string> timeout <1-60>`

The `radius-server` command is in the config command mode.

Table 54 describes the parameters and variables for the `radius-server` command.

**Table 54** `radius-server` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `host <address>` | Specifies the primary RADIUS server. Enter the IP address of the RADIUS server. |
| `secondary-host <address>` | Specifies the secondary RADIUS server Enter the IP address of the secondary RADIUS server. |
| `port <num>` | Enter the port number of the RADIUS server. |

**Table 54** `radius-server` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `key <string>` | Specifies a secret text string that is shared between the switch and the RADIUS server. Enter the secret string, which is an alphanumeric string up to 16 characters.<br>Note: The *<string>* parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new secret text string. |
| `timeout <1-60>` | Specifies the time in seconds that the RADIUS client waits for a response from a RADIUS server before timeout. |

### no radius-server command

The `no radius-server` command clears the RADIUS server settings. The syntax for the `no radius-server` command is:

```
no radius-server
```

The `no radius-server` command is in the config command mode.

The `no radius-server` command has no parameters or values.

### radius-server password fallback

The `radius-server password fallback` command enables you to configure password fallback as an option when using RADIUS authentication for login and password. The syntax for the `radius-server password fallback` command is:

```
radius-server password fallback
```

The `radius-server password fallback` command is in the config command mode.

## Securing your network

You can secure your network using the following CLI commands.

## Configuring MAC address filter-based security

You configure the BaySecure* application using MAC addresses with the following commands:



### 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 `show mac-security` command is in the privExec command mode.

Table 55 describes the parameters and variables for the `show mac-security` command.

**Table 55** `show mac-security` command parameters and variables

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

Figure 23 displays sample output from the `show mac-security` command.

**Figure 23** `show mac-security` command output

```
470_24T#show mac-security config
MAC Address Security: Disabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
Generate SNMP Trap on Intrusion: Disabled
MAC Auto-Learning Age-Time:  60 minutes
Current Learning Mode: Disabled
Learn by Ports: NONE
```

## show mac-security mac-da-filter command

The `show mac-security mac-da-filter` command displays configuration information for filtering MAC destination addresses (DAs). You can filter packets 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 in the privExec command mode.

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

Figure 24 displays sample output from the `show mac-security mac-da-filter` command.

**Figure 24** `show mac-security mac-da-filter` command output

```
470_24T#show mac-security mac-da-filter
Index Mac Address
_____ _________________
 1    00-60-AF-00-12-30
```

## mac-security command

The `mac-security` command modifies the BaySecure configuration. The syntax for the `mac-security` command is:

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

The `mac-security` command is in the config command mode.

Table 56 describes the parameters and variables for the `mac-security` command.

**Table 56** `mac-security` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `disable\|enable` | Disables or enables MAC address-based security. |
| `filtering {enable\|disable}` | Enables or disables destination address (DA) filtering on intrusion detected. |

**Table 56** `mac-security` command parameters and variables (Continued)

| Parameters and variables | Description |
|---|---|
| `intrusion-detect {enable\|disable\|forever}` | Specifies partitioning of a port when an intrusion is detected:<br>• `enable`—port is partitioned for a period of time<br>• `disabled`—port is not partitioned on detection<br>• `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 you want. |
| `learning-ports <portlist>` | Specifies MAC address learning. Learned addresses are added to the table of allowed MAC addresses. Enter the ports you want to learn; it can be a single port, a range of ports, several ranges, all, or none. |
| `learning {enable\|disable}` | Specifies MAC address learning:<br>• `enable`—enables learning by ports<br>• `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. |

## mac-security mac-address-table address command

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

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

**Note:** In this command, *`portlist`* must specify only a single port

The `mac-security mac-address-table address` command is in the config command mode.

Table 57 describes the parameters and variables for the `mac-security mac-address-table address` command.

**Table 57** `mac-security mac-address-table address` command parameters and variables

| Parameters and variables | 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. |

## 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 `mac-security security-list` command is in the config command mode.

Table 58 describes the parameters and variables for the `mac-security security-list` command.

**Table 58** `mac-security security-list` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<1-32>* | Enter the number of the security list you want to use. |
| *<portlist>* | Enter a list or range of port numbers. |

## no mac-security command

The `no mac-security` command disables MAC source address-based security. The syntax for the `no mac-security` command is:

`no mac-security`

The `no mac-security` command is in the config command mode.

The `no mac-security` command has no parameters or values.

## no mac-security mac-address-table command

The `no mac-security mac-address-table` command clears entries from the MAC address security table. 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 `no mac-security mac-address-table` command is in the config command mode.

Table 59 describes the parameters and variables for the `no mac-security mac-address-table` command.

**Table 59** `no mac-security mac-address-table` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `address <H.H.H.>` | Enter the MAC address in the form of H.H.H. |
| `port <portlist>` | Enter a list or range of port numbers. |
| `security-list <1-32>` | Enter the security list number. |

## 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>
```

The `no mac-security security-list` command is in the config command mode.

Table 60 describes the parameters and variables for the `no mac-security security-list` command.

**Table 60** `no mac-security security-list` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *<1-32>* | Enter the number of the security list you want to clear. |

## 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 `mac-security` command for specific ports is in the config-if command mode

Table 61 describes the parameters and variables for the `mac-security` command for specific ports.

**Table 61** `mac-security` command for a single port parameters and variables

| Parameters and variables | Description |
|---|---|
| `port <portlist>` | Enter the port numbers. |
| `disable\|enable\|learning` | Directs the specific port:<br>• `disable`—disables BaySecure on the specified port<br>• `enable`—enables BaySecure on the specified port<br>• `learning`—adds selected ports to the list of ports for which MAC address learning is being performed |

## mac-security mac-da-filter command

The `mac-security mac-da-filter` command allows you to filter packets from up to 10 specified MAC DAs. You also use this command 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.>
```

The `mac-security mac-da-filter` command is in the config command mode.

Table 62 describes the parameters and variables for the `mac-security mac-da-filter` command.

**Table 62** `mac-security mac-da-filter` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `{add\|delete} <H.H.H>` | Add or delete the specified MAC address; enter the MAC address in the form of H.H.H. |

**Note:** Ensure that you do not enter the MAC address of the management unit.

## mac-security auto-learning command

The `mac-security auto-learning` command configures MAC security auto-learning on the switch.

The syntax for the command is:

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

The `mac-security auto-learning` command is in the config-if command mode.

Table 63 describes the parameters and variables for the `mac-security auto-learning` command.

**Table 63** `mac-security auto-learning` command parameters and variables

| Parameters and variables | Description |
|---|---|
| *`portlist`* | Specifies the ports to configure with auto-learning |
| *`[enable \| disable]`* | Enables and disables the auto-learning feature. |
| *`max-addrs <1-25>`* | Sets the maximum number of addresses stored in the MAC Security Table for each port. The default is 2. |

### 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>
```

where the aging time is specified in minutes. An aging time of 0 means that the auto-learned addresses never age out. The default is 60 minutes.

The `mac-security auto-learning aging time` command is in the config command mode.

## Configuring EAPOL-based security

You configure the security based on the Extensible Authentication Protocol over LAN (EAPOL) using the following CLI commands:


- "show eapol command"
- "eapol command" on page 148
- "eapol command for modifying parameters" on page 149
- "eapol user-based-policies command" on page 150

## show eapol command

The `show eapol` command displays the status of the EAPOL-based security. The syntax for the `show eapol` command is:

`show eapol [port <portlist>]`

The `show eapol` command is in the privExec command mode.

Table 64 describes the parameters and variables for the `show eapol` command.

**Table 64** `show eapol` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `port <portlist>` | Enter a list or range of port numbers. If left blank, EAPOL status of all ports will be displayed. |

The `show eapol` command displays the current status of the EAPOL parameters.

Figure 25 on page 148 displays the `show eapol` command output.

**Figure 25** `show eapol` command output

```
460_24T_PWR#show eapol
EAPOL Administrative State:  Disabled
EAPOL User-Based Policies :  Disabled
     Admin          Admin Oper ReAuth ReAuth Quiet  Xmit   Supplic Server  Max
Port Status   Auth Dir   Dir  Enable Period Period Period Timeout Timeout Req
---- -------- ---- ----- ---- ------ ------ ------ ------ ------- ------- ---
1    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
2    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
3    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
4    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
5    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
6    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
7    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
8    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
9    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
10   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
11   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
12   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
13   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
14   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
15   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
16   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
17   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
----More ----
```

## eapol command

The `eapol` command enables or disables EAPOL-based security. The syntax of the `eapol` command is:

`eapol {disable|enable}`

The `eapol` command is in the config command mode.

Table 65 describes the parameters and variables for the `eapol` command.

**Table 65** `eapol` command parameters and variables

| Parameters and variables | Description |
|---|---|
| `disable\|enable` | Disables or enables EAPOL-based security. |

## eapol command for modifying parameters

The `eapol` command for modifying parameters modifies EAPOL-based security parameters for a specific port. The syntax of 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-interval <num>]
[re-authentication-period <1-604800>] [re-authenticate]
[quiet-interval <num>] [transmit-interval <num>]
[supplicant-timeout <num>]
[server-timeout <num>][max-request <num>]
```

The `eapol` command for modifying parameters is in the config-if command mode.

Table 66 describes the parameters and variables for the `eapol` command for modifying parameters

**Table 66** `eapol` command for modifying parameters and variables

| Parameters and variables | Description |
|---|---|
| `port <portlist>` | Specifies the ports to configure for EAPOL; enter the port numbers you want.<br><br>Note: If you omit this parameter, the system uses the port number specified when you issued the `interface` command. |
| `init` | Re-initiates EAP authentication. |
| `status authorized\|unauthorized\|auto` | Specifies the EAP status of the port:<br>• `authorized`—port is always authorized<br>• `unauthorized`—port is always unauthorized<br>• `auto`—port authorization status depends on the result of the EAP authentication<br>Note: In the CLI (or JDM), if this parameter is set to auto for all ports, the switch can take up to 5 minutes to implement the configuration change, depending on the size of the stack. No configurations can be made on the switch until the change is completed. |

**Table 66** `eapol` command for modifying parameters and variables (Continued)

| Parameters and variables | Description |
|---|---|
| `traffic-control in-out\|in` | Sets the level of traffic control:<br>• `in-out`—if EAP authentication fails, both ingressing and egressing traffic are blocked<br>• `in`—if EAP authentication fails, only ingressing traffic is blocked |
| `re-authentication enable\|disable` | Enables or disables re-authentication. |
| `re-authentication-interval <num>` | Enter the number of seconds you want between re-authentication attempts; range is 1 to 604800.<br>Use either this variable or the re-authentication-period variable; do not use both variables because the two variables control the same setting. |
| `re-authentication-period <1-604800>` | Enter the number of seconds you want between re-authentication attempts.<br>Use either this variable or the re-authentication-interval variable; do not use both variables because the two variables control the same setting. |
| `re-authenticate` | Specifies an immediate re-authentication. |
| `quiet-interval <num>` | Enter the number of seconds you want between an authentication failure and the start of a new authentication attempt; range is 1 to 65535. |
| `transmit-interval <num>` | Specifies a waiting period for response from supplicant for EAP Request/Identity packets. Enter the number of seconds you want 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 you want to wait; range is 1-65535. |
| `server-timeout <num>` | Specifies a waiting period for response from the server. Enter the number of seconds you want to wait; range is 1-65535 |
| `max-request <num>` | Enter the number of times to retry sending packets to supplicant. |

## eapol user-based-policies command

The `eapol user-based-policies` command enables EAPOL user-based policies on the device.

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

```
eapol user-based-policies enable
```

The `eapol user-based-policies` command has no parameters or variables.

The `eapol user-based-policies` command is in the config command mode.

## eapol guest-vlan port command

`The eapol guest-vlan port` command specifies the ID of a Guest VLAN that the port is able to access while unauthorized.

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

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

where *<portlist>* specifies the ports, and *<1-4094>* specifies the Guest VLAN ID.

The `eapol guest-vlan port` command is in the config command mode.

## no eapol guest-vlan command

`The no eapol guest-vlan` command disables Guest VLAN on the port.

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

`no eapol guest-vlan <portlist>`

where *<portlist>* specifies the ports on which to disable Guest VLAN.

The `no eapol guest-vlan` command is in the config command mode.

## default eapol guest-vlan command

`The default eapol guest-vlan` command sets the Guest VLAN settings to defaults.

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

`default eapol guest-vlan`

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

The `default eapol guest-vlan` command is in the config command mode.

### show eapol guest-vlan command

The `show eapol guest-vlan` command displays the global Guest VLAN configuration on the switch.

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

```
show eapol guest-vlan
```

The `show eapol guest-vlan` command is in the privExec command mode.

Figure 26 displays sample output from the `show eapol guest-vlan` command.

**Figure 26** `show eapol guest-vlan` command output

```
470-24T#show eapol guest-vlan
EAPOL Guest Vlan   :  Disabled
EAPOL Guest Vlan ID:  1
```

### show eapol guest-vlan interface command

The `show eapol guest-vlan interface` command displays the Guest VLAN configuration for a port or list of ports.

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

```
show eapol guest-vlan interface <portlist>
```

where *<portlist>* specifies the ports for which to display the Guest VLAN configuration.

The `show eapol guest-vlan interface` command is in the privExec command mode.

Figure 27 shows a sample output from the `show eapol guest-vlan interface` command.

**Figure 27** `show eapol guest-vlan interface` command output

```
470-24T#show eapol guest-vlan interface 9-12
       Guest   Guest
Port   Vlan   Vlan ID
---- -------- -------
9    Enabled  1
10   Disabled Global
11   Enabled  1
12   Disabled Global
```

## eapol multihost enable command

The `eapol multihost enable` command enables EAPOL multihost (MHMA) on the device.

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

`eapol multihost enable [eap-mac-max <1-32>]`

where `eap-mac-max` sets the maximum of EAP-authenticated MAC addresses allowed on the ports. (The default value is 1.)

The `eapol multihost enable` command is in the config-if command mode.

## no eapol multihost enable command

The `no eapol multihost enable` command disables EAPOL multihost (MHMA) on the device.

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

`no eapol multihost enable`

The `no eapol multihost enable` command has no parameters or variables.

The `no eapol multihost enable` command is in the config-if command mode.

## eapol multihost port enable command

The `eapol multihost port enable` command enables EAPOL multihost (MHMA) on the port.

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

```
eapol multihost <port> enable [eap-mac-max <1-32>]
```

where `<port>` specifies the port to enable, and `eap-mac-max` sets the maximum of EAP-authenticated MAC addresses allowed on the port. (The default value is 1.)

The `eapol multihost port enable` command is in the config-if command mode.

## no eapol multihost port enable command

The `no eapol multihost port enable` command disables EAPOL multihost (MHMA) on the port.

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

```
no eapol multihost <port> enable
```

where `<port>` specifies the port to disable.

The `no eapol multihost port enable` command is in the config-if command mode.

## default eapol multihost enable command

The `default eapol multihost enable` command sets the EAPOL multihost feature to default values.

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

```
default eapol multihost enable
```

The `default eapol multihost enable` command has no parameters or variables.

The `default eapol multihost enable` command is in the config-if command mode.

## default eapol multihost eap-mac-max command

The `default eapol multihost eap-mac-max` command resets the maximum number of EAPOL clients to the default value.

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

```
default eapol multihost eap-mac-max
```

The `default eapol multihost eap-mac-max` command has no parameters or variables.

The `default eapol multihost eap-mac-max` command is in the config-if command mode.

## show eapol multihost status command

The `show eapol multihost status` command displays the multihost status on the switch.

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

```
show eapol multihost status
```

The `show eapol multihost status` command is in the privExec command mode.

Figure 28 on page 156 shows a sample output from the `show eapol multihost status` command.

**Figure 28** `show eapol multihost status` command output

```
470-24T#show eapol multihost status
Port Client MAC Address Pae State      Backend Auth State
---- ------------------ -------------- ------------------
4    00:0B:6A:6C:41:16  Authenticated  Idle
4    00:0B:6A:6C:31:20  Authenticated  Idle
```

## show eapol multihost interface command

The `show eapol multihost interface` command displays the multihost configuration on a port or set of ports.

The syntax for the `show eapol multihost interface` command is:

`show eapol multihost interface <portlist>`

where *<portlist>* specifies the ports for which to display the multihost configuration.

The `show eapol multihost interface` command is in the privExec command mode.

Figure 29 shows a sample output from the `show eapol multihost interface` command.

**Figure 29** `show eapol multihost interface` command output

```
470-24T#show eapol multihost interface 9-12
     MultiHost Maximum Eap Allow Non-EAP Maximum Non-EAP Use RADIUS To
Port  Status   Client MACs Client MACs   Client MACs     Auth Non-EAP MACs
---- --------- ----------- ------------- --------------- -----------------
9    Disabled  12
10   Enabled   15
11   Disabled  12
12   Enabled   22
```

# Chapter 3
# Configuring security using Device Manager

You can set the security features for a switch so that the actions are performed by the software when a violation occurs. The security actions you specify are applied to all ports of the switch.

This chapter describes the security information available in Device Manager, and contains the following topics:

# EAPOL tab

The EAPOL tab allows you to set and view EAPOL security information for the switch.

To view the EAPOL tab:

➨ From the Device Manager menu bar, select Edit > Security.

The Security dialog box opens with the EAPOL tab displayed (Figure 30).

**Figure 30** EAPOL tab

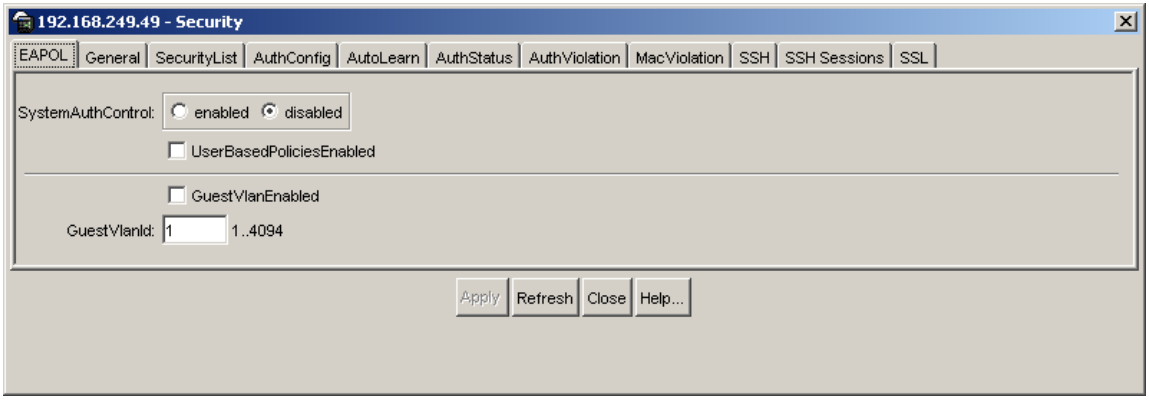


Table 67 describes the EAPOL tab items.

**Table 67** EAPOL tab items

| Items | Description |
|---|---|
| SystemAuthControl | SystemAuthControl field enables port access control in the system. |
| UserBasedPolicies | This object indicates whether EAPOL User-based policies are enabled or disabled. |
| GuestVlanEnabled | Enables or disables access to the global default Guest VLAN for the switch. |
| GuestVlanId | This object specifies the ID of the global default Guest VLAN. This VLAN is used for ports that do not have a configured Guest VLAN. Access to the global default Guest VLAN is allowed for MAC addresses before EAP authentication has been performed.<br>The GuestVlanEnabled field must be selected in order to provide ports with access to the global default Guest VLAN. |

# General tab

The General tab allows you to set and view general security information for the switch.

To view the General tab:

1. From the Device Manager menu bar, select Edit > Security.

   The Security dialog box opens with the EAPOL tab displayed (Figure 30 on page 158).

2. Click the General tab.

   The General tab opens (Figure 31 on page 160).

**Figure 31** General tab

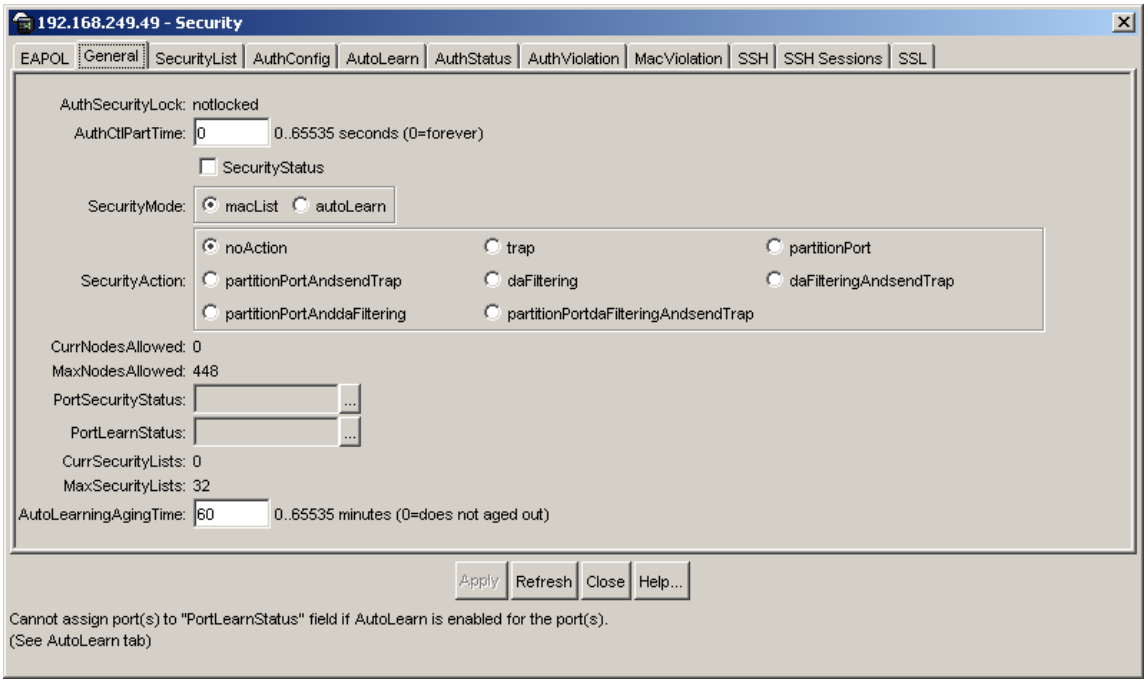



Table 68 describes the General tab items.

**Table 68** General tab items

| Items | Description |
|---|---|
| AuthSecurityLock | If this parameter is listed as “locked,” the agent refuses all requests to modify the security configuration. Entries also include:<br>• other<br>• notlocked |
| AuthCtlPartTime | This value indicates the duration of the time for port partitioning in seconds. Default: 0 (zero). When the value is zero, the port remains partitioned until it is manually re-enabled. |
| SecurityStatus | Indicates whether the switch security feature is enabled. |

**Table 68** General tab items (Continued)

| Items | Description |
|---|---|
| SecurityMode | Mode of switch security. Entries include:<br>• macList: Indicates that the switch is in the MAC-list mode. You can configure more than one MAC address per port.<br>• autoLearn: Indicates that the switch learns the first MAC address on each port as an allowed address of that port.<br>Note: If autoLearn is selected, and no ports are selected in the PortLearnStatus field, all ports are enabled for autoLearn. |
| 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.<br>A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include:<br>• noAction: Port does not have any security assigned to it, or the security feature is turned off.<br>• trap: Listed trap.<br>• partitionPort: Port is partitioned.<br>• partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receive station.<br>• daFiltering: Port filters out the frames where the destination address field is the MAC address of unauthorized Station.<br>• daFilteringAndsendTrap: Port filters out the frames where the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive station(s).<br>• partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station.<br>• partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive station(s).<br>Note: “da” means destination address. |
| CurrNodesAllowed | Current number of entries of the nodes allowed in the AuthConfig tab. |
| MaxNodesAllowed | Maximum number of entries of the nodes allowed in the AuthConfig tab. |
| PortSecurityStatus | Set of ports for which security is enabled. |
| PortLearnStatus | Set of ports where auto-learning is enabled. |
| CurrSecurityLists | Current number of entries of the Security listed in the SecurityList tab |

**Table 68** General tab items (Continued)

| Items | Description |
|---|---|
| MaxSecurityLists | Maximum entries of the Security listed in the SecurityList tab. |
| AutoLearningAging Time | When Autolearning is enabled, sets the lifetime, in minutes, for MAC addresses that are auto-learned. A value of 0 means addresses do not age out. |

# SecurityList tab

The SecurityList tab contains a list of Security port items.

To view the SecurityList tab:

1. From the Device Manager menu bar, select Edit > Security.

   The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

2. Click the SecurityList tab.

   The SecurityList tab opens (Figure 32).

**Figure 32** SecurityList tab

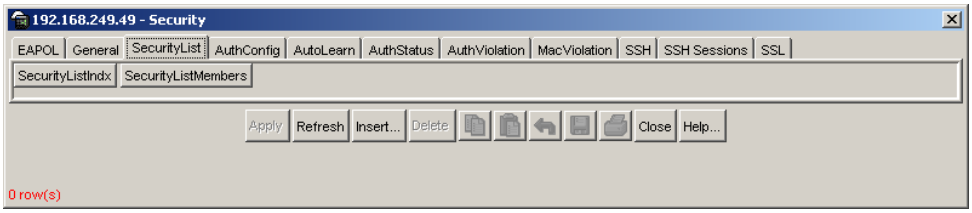



Table 69 describes the SecurityList tab fields.

**Table 69** SecurityList tab fields

| Field | Description |
|---|---|
| SecurityListIndx | An index of the security list. This corresponds to the Security port list that can be used as an index into AuthConfig tab. |
| SecurityListMembers | The set of ports that are currently members in the Port list. |

## Security, Insert SecurityList dialog box

The Security, Insert SecurityList dialog box has editable fields for the SecurityList tab. Each row in this dialog box has information that can be updated or changed.

To view the Security, Insert SecurityList dialog box:

1. From the Device Manager menu bar, select Edit > Security.

   The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

2. Click the SecurityList tab.

   The SecurityList tab opens (Figure 32 on page 162).

3. Click inside a row.

4. Click Insert.

   The Security, Insert SecurityList dialog box opens (Figure 33).

**Figure 33** Security, Insert SecurityList dialog box

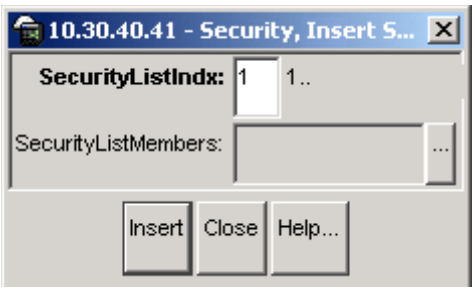



Table 70 describes the Security, Insert SecurityList dialog box items.

**Table 70** Security, Insert SecurityList dialog box fields

| Field | Description |
|---|---|
| SecurityListIndx | An index of the security list. This corresponds to the Security port list that can be used as an index into AuthConfig tab. |
| SecurityListMembers | The set of ports that are currently members in the Port list. |

# AuthConfig tab

The AuthConfig tab contains a list of boards, ports and MAC addresses that have the security configuration. An SNMP SET PDU for a row in the tab requires the entire sequence of the MIB objects in each entry to be stored in one PDU. Otherwise, GENERR return-value is returned.

To view the AuthConfig tab:

1. From the Device Manager menu bar, select Edit > Security.

   The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

2. Click the AuthConfig tab.

   The AuthConfig tab opens (Figure 34).

**Figure 34** AuthConfig tab

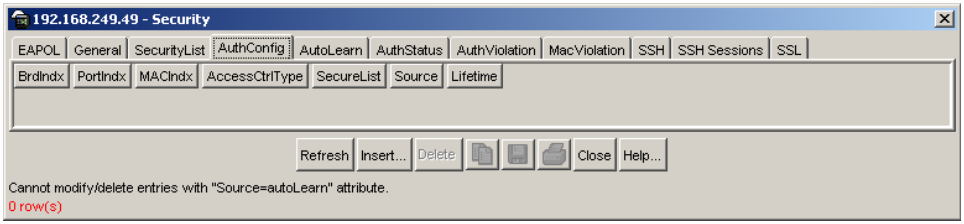



Table 71 describes the AuthConfig tab fields.

**Table 71** AuthConfig tab fields

| Field | Description |
|---|---|
| BrdIndx | Index of the slot containing the board where the port is located. This value is meaningful only if SecureList value is zero. For other SecureList values, this parameter should have the value of zero. |
| PortIndx | Index of the port on the board. This value is meaningful only if SecureList value is zero. For other SecureList values, this parameter should have the value of zero. |
| MACIndx | An index of MAC addresses that are either designated as `allowed` (station) or `not-allowed` (station). |
| AccessCtrlType | Displays whether the node entry is `node allowed` or `node blocked`. A MAC address may be allowed on multiple ports. |

**Table 71** AuthConfig tab fields (Continued)

| Field | Description |
|---|---|
| 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, it should also have the value of zero.<br>The corresponding MAC Address of this entry is allowed or blocked on all ports of that this port list. |
| Source | Indicates the source of an entry:<br>• static indicates that the entry was manually created by a user.<br>• autoLearn indicates that the entry was auto-learned.<br>**Note:** An auto-learned entry cannot be directly deleted. Also, disabling auto-learning for a port deletes all auto-learned MAC addresses for the port. |
| Lifetime | Indicates the lifetime of an auto-learned entry; that is, the time until the entry is automatically deleted.<br>This does not apply to user-created (static) entries (the value for static entries is 0). |

## Security, Insert AuthConfig dialog box

The Security, Insert AuthConfig dialog box has editable fields for the AuthConfig tab. Each row in this dialog box has information that can be updated or changed.

To view the Security, Insert AuthConfig dialog box:

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

The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

**2** Click the AuthConfig tab.

The AuthConfig tab opens (Figure 34 on page 164).

**3** Click inside a row.

**4** Click Insert.

The Security, Insert AuthConfig dialog box opens (Figure 35 on page 166).

**Figure 35** Security, Insert AuthConfig dialog box


Table 72 describes the Security, Insert AuthConfig dialog box fields.

**Table 72** Security, Insert AuthConfig dialog box fields

| Item | Description |
|---|---|
| BrdIndx | Index of the board. This corresponds to the index of the slot containing the board, but only if the index is greater than zero. A zero index is a wild card. |
| PortIndx | Index of the port on the board. This corresponds to the index of the last manageable port on the board, but only if the index is greater than zero. A zero index is a wild card. |
| MACIndx | An index of MAC addresses that are either designated as `allowed` (station) or `not-allowed` (station). |
| AccessCtrlType | Displays whether the node entry is `node allowed` or `node blocked`. A MAC address may 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, it should also have the value of zero.<br>The corresponding MAC Address of this entry is allowed or blocked on all ports of that this port list. |

# AutoLearn tab

The AutoLearn tab contains editable fields that allow the user to configure the Autolearning feature.

To configure the Autolearning feature:

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

The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

**2** Click the AutoLearn tab.

The AutoLearn tab opens (Figure 36).

**Figure 36** AutoLearn tab

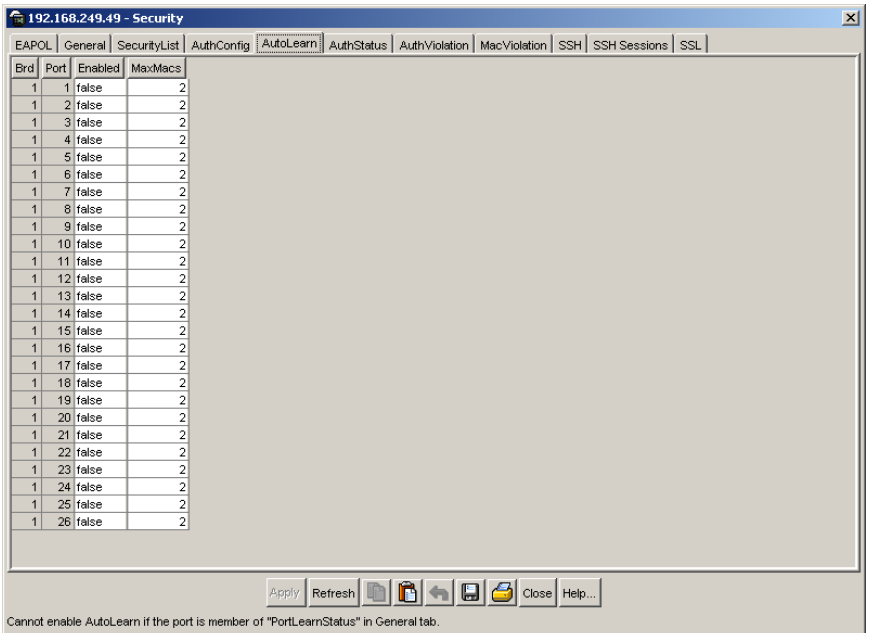



Table 73 describes the AutoLearn tab fields.

**Table 73** Security, Insert SecurityList dialog box fields

| Field | Description |
|---|---|
| BrdIndx | The unit number. |
| PortIndx | The port number. |

**Table 73** Security, Insert SecurityList dialog box fields (Continued)

| Field | Description |
|---|---|
| Enabled | Indicates if Autolearning is enabled on the port. Choose true to enable, and false to disable. |
| MaxMacs | The maximum number of MAC addresses that can be learned on the port. Range is 1-25. |

# AuthStatus tab

The AuthStatus tab displays information of the authorized boards and port status data collection. Information includes actions to be performed when an unauthorized station is detected and the current security status of a port. An entries in this tab may include:

- A single MAC address
- all MAC addresses on a single port
- a single port
- all the ports on a single board
- a particular port on all the boards
- all the ports on all the boards

To view the AuthStatus tab:

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

The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

**2** Click the AuthStatus tab.

The AuthStatus tab opens (Figure 37 on page 169).

**Figure 37** AuthStatus tab

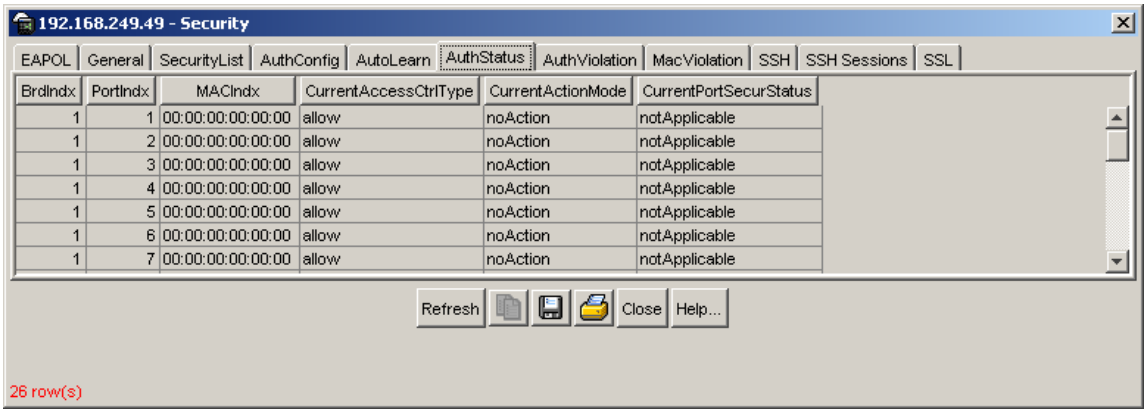



Table 74 describes the AuthStatus tab fields.

**Table 74** AuthStatus tab fields

| Item | Description |
|---|---|
| BrdIndx | The index of the board. This corresponds to the index of the slot containing the board if the index is greater than zero. |
| PortIndx | 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. |
| MACIndx | 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`. |

**Table 74** AuthStatus tab fields (Continued)

| Item | Description |
|---|---|
| CurrentActionMode | A value representing the type of information contained, including:<br>noAction: Port does not have any security assigned to it, or the security feature is turned off.<br>partitionPort: Port is partitioned.<br>partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receive station.<br>Filtering: Port filters out the frames, where the destination address field is the MAC address of unauthorized station.<br>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.<br>sendTrap: A trap is sent to trap receive station(s).<br>partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station.<br>partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive station(s). |
| CurrentPortSecurStatus | Displays the security status of the current port, including:<br>• If the port is disabled, notApplicable is returned.<br>• If the port is in a normal state, portSecure is returned.<br>• If the port is partitioned, portPartition is returned. |

# AuthViolation tab

The AuthViolation tab contains a list of boards and ports where network access violations have occurred, and also the identity of the offending MAC addresses.

To view the AuthViolation tab:

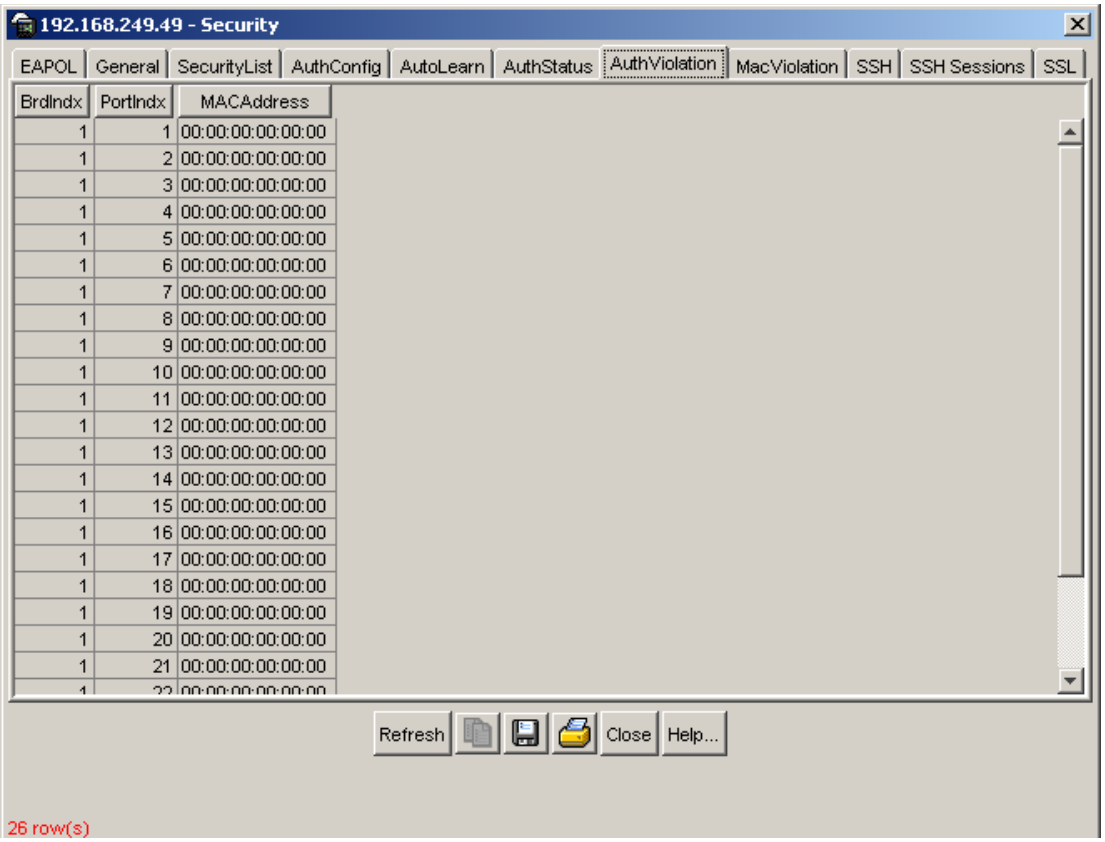
1. From the Device Manager menu bar, select Edit > Security.

   The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

2. Click the AuthViolation tab.

The AuthViolation tab opens (Figure 38 on page 171).

**Figure 38** AuthViolation tab




| BrdIndx | PortIndx | MACAddress |
|---|---|---|
| 1 | 1 | 00:00:00:00:00:00 |
| 1 | 2 | 00:00:00:00:00:00 |
| 1 | 3 | 00:00:00:00:00:00 |
| 1 | 4 | 00:00:00:00:00:00 |
| 1 | 5 | 00:00:00:00:00:00 |
| 1 | 6 | 00:00:00:00:00:00 |
| 1 | 7 | 00:00:00:00:00:00 |
| 1 | 8 | 00:00:00:00:00:00 |
| 1 | 9 | 00:00:00:00:00:00 |
| 1 | 10 | 00:00:00:00:00:00 |
| 1 | 11 | 00:00:00:00:00:00 |
| 1 | 12 | 00:00:00:00:00:00 |
| 1 | 13 | 00:00:00:00:00:00 |
| 1 | 14 | 00:00:00:00:00:00 |
| 1 | 15 | 00:00:00:00:00:00 |
| 1 | 16 | 00:00:00:00:00:00 |
| 1 | 17 | 00:00:00:00:00:00 |
| 1 | 18 | 00:00:00:00:00:00 |
| 1 | 19 | 00:00:00:00:00:00 |
| 1 | 20 | 00:00:00:00:00:00 |
| 1 | 21 | 00:00:00:00:00:00 |

Table 75 describes fields for the AuthViolation tab fields.

**Table 75** AuthViolation tab fields

| Field | Description |
|---|---|
| BrdIndx | The index of the board. This corresponds to the slot containing the board. The index is 1 where it is not applicable. |
| PortIndx | The index of the port on the board. This corresponds to the port on that a security violation was seen. |
| MACAddress | The MAC address of the device attempting unauthorized network access (MAC address-based security). |

# MacViolation tab

The MacViolation tab contains a list of boards and ports where MAC address violations have occurred, and the identity of the offending MAC addresses.

To view the MacViolation tab:

1. From the Device Manager menu bar, select Edit > Security.

   The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

2. Click the MacViolation tab.

   The MacViolation tab opens (Figure 39).

**Figure 39** MacViolation tab

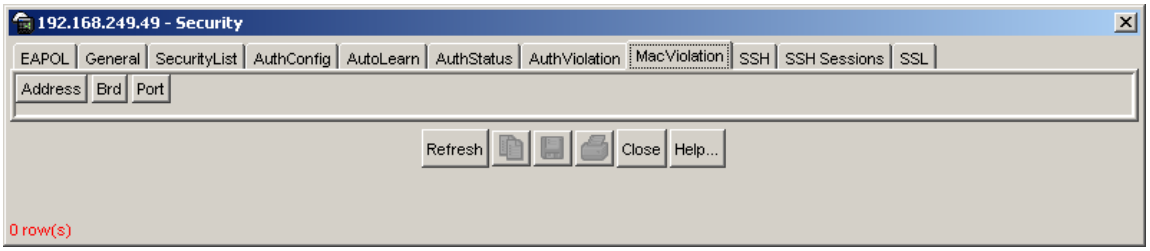



Table 76 describes fields for the MacViolation tab fields.

**Table 76** MacViolation tab fields

| Field | Description |
|---|---|
| Address | The MAC address of the device attempting unauthorized network access (MAC address-based security). |
| Brd | The last port number on which the MAC address caused an access violation. |
| Port | The last port number on which the MAC address caused an access violation. |

# SSH tab

The SSH tab displays the parameters available for SSH.

To view the SSH tab:

1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

2 Click the SSH tab.

The SSH tab opens (Figure 40).

**Figure 40** SSH tab

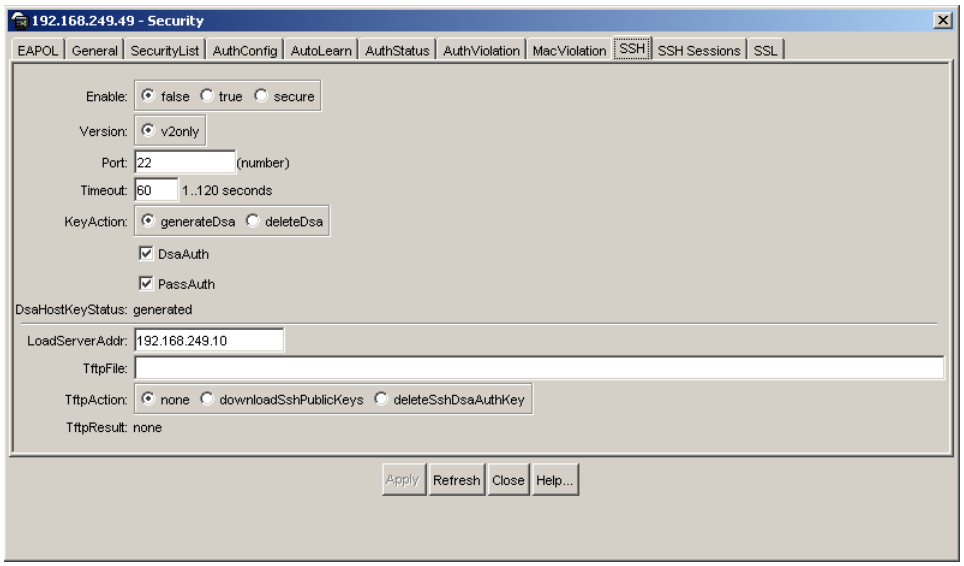



Table 77 describes the SSH tab fields.

**Table 77** SSH tab fields

| Field | Description |
|---|---|
| Enable | Enables, disables or securely enables SSH. Securely enable turns off other daemon flag, and it takes effect after reboot |
| Version | Indicates the SSH version |

**Table 77** SSH tab fields (Continued)

| Field | Description |
|---|---|
| Port | Indicates the SSH connection port. |
| Timeout | Indicates the SSH connection timeout in seconds. |
| KeyAction | Indicates the SSH key action |
| DsaAuth | Enables or disables the SSH DSA authentication |
| PassAuth | Enables or disables the SSH RSA authentication |
| DsaHostKeyStatus | Indicates the current status of the SSH DSA host key. Possible values are:<br>• notGenerated<br>• generated<br>• generating |
| LoadServerAddr | Indicates the current server IP address |
| TftpFile | Name of file for the TFTP transfer. |
| TftpAction | The action for the TFTP transfer |
| TftpResult | Contains result of the last Tftp action request |

# SSH Sessions tab

The SSH Sessions tab displays the currently active SSH sessions.

To view the SSH Sessions tab:

1. From the Device Manager menu bar, select Edit > Security.

   The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

2. Click the SSH Sessions tab.

   The SSH Sessions tab opens (Figure 41 on page 175).

**Figure 41** SSH Sessions tab

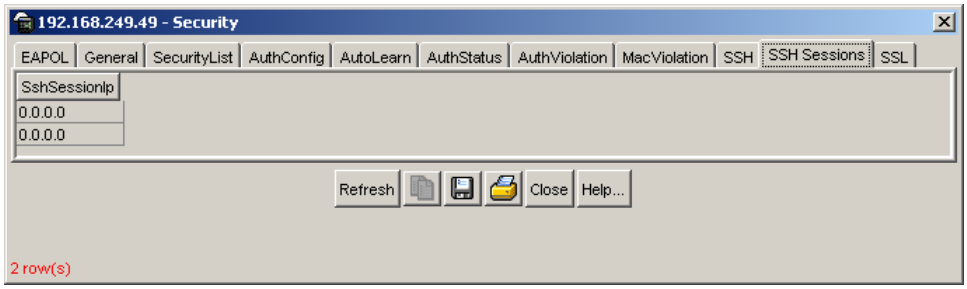



Table 78 describes the SSH Sessions tab fields.

**Table 78** SSH Sessions tab fields

| Field | Description |
|---|---|
| SSHSessions | Lists the currently active SSH sessions. |

# Opening an SSH connection to the switch

From Device Manager, you can initiate a Secure Shell (SSH) connection to the Console Interface for the switch or stack you are currently accessing.

To open an SSH connection to a switch:

**1** Do one of the following:

- From the Device Manager main menu, Choose Device > SSH Connection.
- On the toolbar, click the SSH button.

An SSH window to the switch opens.

**2** Enter a valid SSH user name and password.

# SSL tab

The SSL tab allows you to enable or disable Secure Socket Layer (SSL) to provide security for the Web-based management system.

1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the EAPOL tab displayed (Figure 30 on page 158).

2 Click the SSL tab.

The SSL tab opens (Figure 42).

**Figure 42** SSL tab

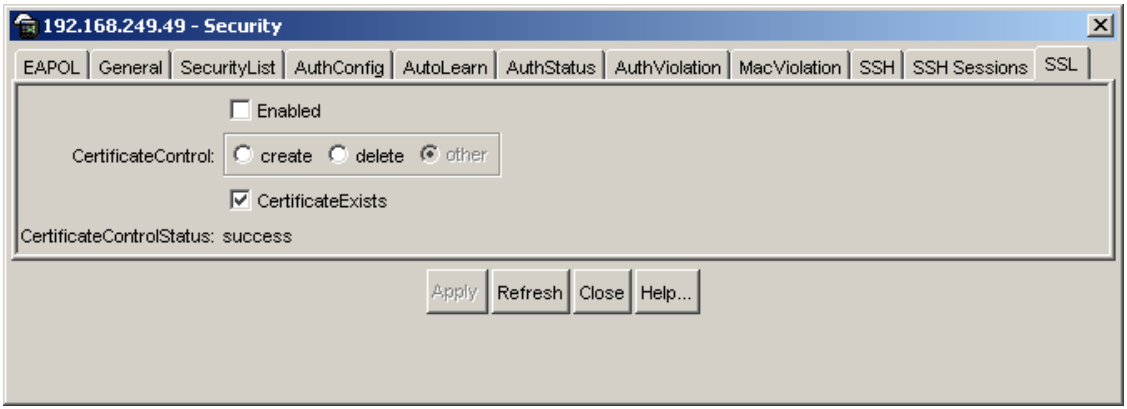



Table 79 describes the SSL tab fields.

**Table 79** SSL tab fields

| Field | Description |
|---|---|
| Enabled | Enables and disables SSL on the switch. When SSL is enabled, the Web server operates in secure mode. |
| CertificateControl | Allows the user to create or delete a certificate. On creation, this new certificate is used only on the next system reset or SSL server reset. The certificate generated is stored in NVRAM as file "SSLCERT.DAT", and replaces the existing file. |
| CertificateExists | Indicates whether a certificate currently exists. |
| CertificateControl Status | Read-only field that displays the status of the last certificate create or delete operation. |

# Configuring EAPOL on ports

This section contains the following topics:



## EAPOL tab for a single port

The EAPOL tab allows you to configure EAPOL-based security for a single port.

To view the EAPOL tab:

1. Select the port you want to edit.
2. Do one of the following:
   - Double-click the selected port
   - From the shortcut menu, choose Edit.
   - From the Device Manager main menu, choose Edit > Port.
   - On the toolbar, click Edit.

   The Port dialog box for a single port opens with the Interface tab displayed.
3. Click the EAPOL tab.

   The EAPOL tab opens (Figure 43 on page 178).

**Figure 43** Edit Port dialog box — EAPOL tab for a single port

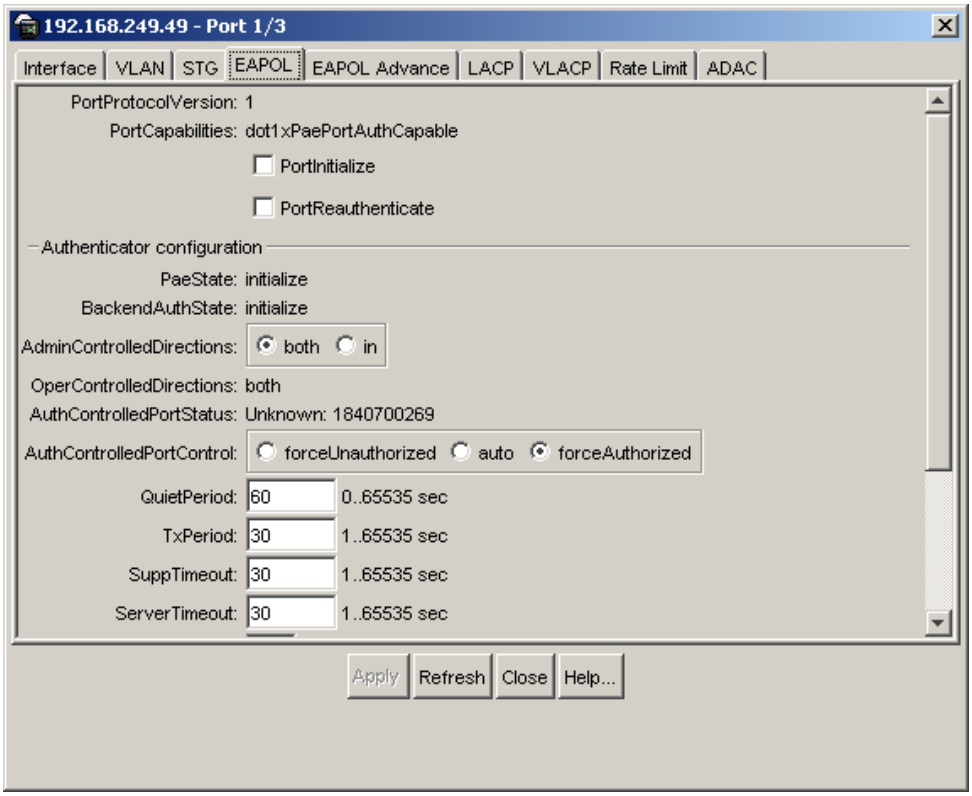



Table 80 describes the EAPOL tab items.

**Table 80** EAPOL tab items for a single port

| Item | Description |
|---|---|
| PortProtocolVersion | The EAP Protocol version that is running on this port. |
| PortCapabilities | The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0). |
| PortInitialize | Setting this attribute to True causes this port's EAPOL state to be initialized. |
| PortReauthenticate | Setting this attribute to True causes the reauthentication of the client. |
| PaeState | The current authenticator PAE state machine stat value. |

**Table 80** EAPOL tab items for a single port (Continued)

| Item | Description |
|---|---|
| BackendAuthState | The current state of the Backend Authentication state machine. |
| AdminControlledDirections | The current value of the administrative controlled directions parameter for the port. |
| OperControlledDirections | The current value of the operational controlled directions parameter for the port. |
| AuthControlledPortStatus | The current value of the controlled port status parameter for the port. |
| AuthControlledPortControl | The current value of the controlled port control parameter for the port.<br>Note: In the JDM (or CLI), if this field is set to auto for all ports, the switch can take up to 5 minutes to implement the configuration change, depending on the size of the stack. No configurations can be made on the switch until the change is completed. |
| QuietPeriod | The current value of the time interval between authentication failure and the start of a new authentication. |
| TxPeriod | Time to wait for response from supplicant for EAP requests/ Identity packets. |
| SuppTimeout | Time to wait for response from supplicant for all EAP packets except EAP Request/Identity. |
| ServerTimeout | Time to wait for a response from the RADIUS server |
| MaxReq | Number of times to retry sending packets to the supplicant. |
| ReAuthPeriod | Time interval between successive re-authentications. |
| ReAuthEnabled | Whether to re-authenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field. |
| KeyTxEnabled | The value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant. |
| LastEapolFrameVersion | The protocol version number carried in the most recently received EAPOL frame. |
| LastEapolFrameSource | The source MAC address carried in the most recently received EAPOL frame. |

## EAPOL tab for multiple ports

The EAPOL tab shows EAPOL statistics for the selected ports.

To view or edit the EAPOL tab for multiple ports:

1. Select the ports that you want to edit.

   Press [Ctrl] + left-click the ports that you want to edit. A yellow outline appears around the selected ports.

2. Do one of the following:

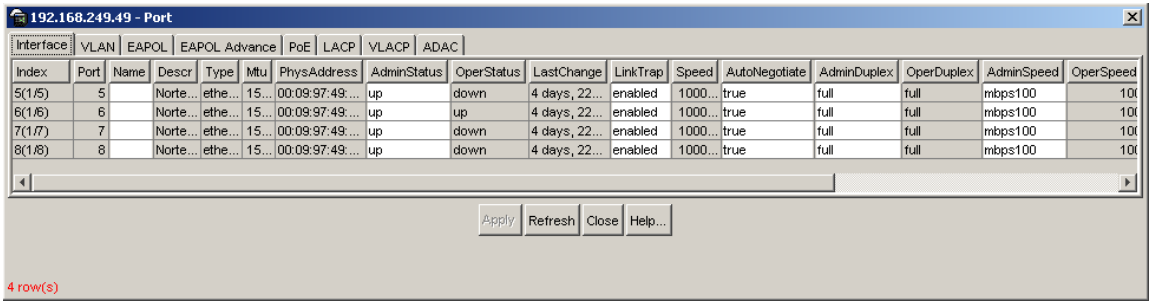
   - From the shortcut menu, choose Edit.
   - From the Device Manager main menu, choose Edit > Port.
   - On the toolbar, click Edit.

   The Port dialog box for multiple ports opens with the Interface tab displayed.

3. Click the EAPOL tab.

   The EAPOL tab opens (Figure 44).

**Figure 44** EAPOL tab for multiple ports




| Index | Port | Name | Descr | Type | Mtu | PhysAddress | AdminStatus | OperStatus | LastChange | LinkTrap | Speed | AutoNegotiate | AdminDuplex | OperDuplex | AdminSpeed | OperSpeed |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5(1/5) | 5 | | Norte... | ethe... | 15... | 00:09:97:49:... | up | down | 4 days, 22... | enabled | 1000... | true | full | full | mbps100 | 10( |
| 6(1/6) | 6 | | Norte... | ethe... | 15... | 00:09:97:49:... | up | up | 4 days, 22... | enabled | 1000... | true | full | full | mbps100 | 10( |
| 7(1/7) | 7 | | Norte... | ethe... | 15... | 00:09:97:49:... | up | down | 4 days, 22... | enabled | 1000... | true | full | full | mbps100 | 10( |
| 8(1/8) | 8 | | Norte... | ethe... | 15... | 00:09:97:49:... | up | down | 4 days, 22... | enabled | 1000... | true | full | full | mbps100 | 10( |

Table 81 describes the EAPOL tab fields for multiple ports.

**Table 81** EAPOL tab fields for multiple ports

| Field | Description |
|---|---|
| Index | Displays the unique value assigned to each interface. |
| PortProtocolVersion | The EAP Protocol version that is running on this port. |
| PortCapabilities | The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0). |
| PortInitialize | Setting this attribute to True causes this port's EAPOL state to be initialized. |
| PortReauthenticate | Setting this attribute to True causes the reauthentication of the client. |
| PaeState | The current authenticator PAE state machine stat value. |
| BackendAuthState | The current state of the Backend Authentication state machine. |
| AdminControlledDirections | Sets the value of the administrative controlled directions parameter for the port:<br>• both<br>• in |
| OperControlledDirections | The current value of the operational controlled directions parameter for the port. |
| AuthControlledPortStatus | The current value of the controlled port status parameter for the port. |
| AuthControlledPortControl | Sets the current value of the controlled port control parameter for the port:<br>• force Unauthorized<br>• auto<br>• forceAuthorized<br>Note: If this field is set to auto for all ports, the switch can take up to 5 minutes to implement the configuration change, depending on the size of the stack. No configurations can be made on the switch until the change is completed. |

**Table 81** EAPOL tab fields for multiple ports (Continued)

| Field | Description |
|---|---|
| QuietPeriod | Set the value of the time interval between authentication failure and the start of a new authentication. |
| TxPeriod | Set the time to wait for response from supplicant for EAP requests/Identity packets. |
| SuppTimeout | Set the time to wait for response from supplicant for all EAP packets except EAP Request/Identity. |
| ServerTimeout | Set the time to wait for a response from the RADIUS server |
| MaxReq | Set the number of times to retry sending packets to the supplicant. |
| ReAuthPeriod | Set the time interval between successive re-authentications. |
| ReAuthEnabled | Whether to re-authenticate or not. Setting this object to true causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field. |
| KeyTxEnabled | The value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant. |
| LastEapolFrameVersion | The protocol version number carried in the most recently received EAPOL frame. |
| LastEapolFrameSource | The source MAC address carried in the most recently received EAPOL frame. |

## EAPOL Advance tab for a single port

The EAPOL Advance tab allows you to configure additional EAPOL-based security parameters for a single port.

To view the EAPOL Advance tab:

1. Select the port you want to edit.
2. Do one of the following:
   - Double-click the selected port

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for a single port opens with the Interface tab displayed.

**3** Click the EAPOL Advance tab.

The EAPOL Advance tab opens (Figure 45).

**Figure 45** EAPOL Advance tab for a single port

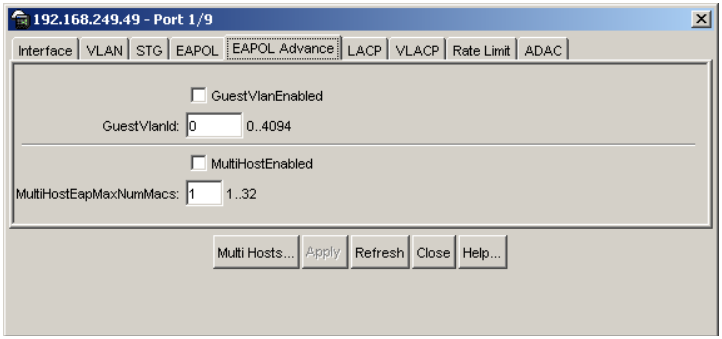



Table 82 describes the EAPOL Advance tab fields for a single port.

**Table 82** EAPOL Advance tab fields for a single port

| Field | Description |
|---|---|
| GuestVlanEnabled | Enables and disables Guest VLAN on the port. |
| GuestVlanId | Specifies the ID of a Guest VLAN that the port is able to access while unauthorized.<br>This value overrides the Guest VLAN ID value set for the switch in the EAPOL tab. |
| MultiHostEnabled | Enables and disables EAPOL MultHost on the port. |
| MustiHostEapMax NumMacs | Sets the maximum number of EAP-authenticated MAC addresses allowed on the port. (The default value is 1.) |

## EAPOL Advance tab for multiple ports

The EAPOL Advance tab allows you to configure additional EAPOL-based security parameters for multiple ports.

To view or edit the EAPOL Advance tab for multiple ports:

1. Select the ports that you want to edit.

   Press [Ctrl] + left-click the ports that you want to edit. A yellow outline appears around the selected ports.

2. Do one of the following:

   - From the shortcut menu, choose Edit.
   - From the Device Manager main menu, choose Edit > Port.
   - On the toolbar, click Edit.

   The Port dialog box for multiple ports opens with the Interface tab displayed.

3. Click the EAPOL Advance tab.

   The EAPOL Advance tab for multiple ports opens (Figure 46).

**Figure 46** EAPOL Advance tab for multiple ports

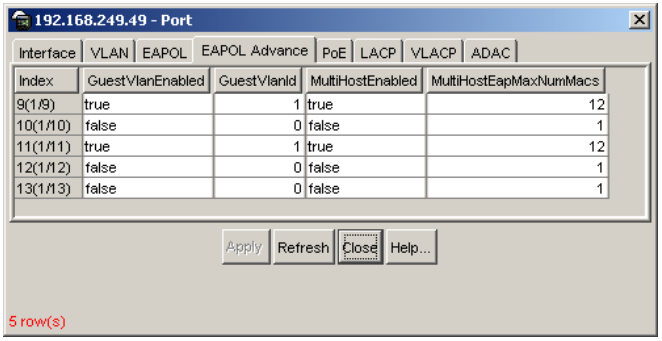


Table 82 describes the EAPOL Advance tab fields for multiple ports.

**Table 83** EAPOL Advance tab fields for multiple ports

| Field | Description |
|---|---|
| GuestVlanEnabled | Enables and disables Guest VLAN on the port. |
| GuestVlanId | Specifies the ID of a Guest VLAN that the port is able to access while unauthorized.<br>This value overrides the Guest VLAN ID value set for the switch in the EAPOL tab. |
| MultiHostEnabled | Enables and disables EAPOL MultHost on the port. |
| MustiHostEapMax NumMacs | Sets the maximum number of EAP-authenticated MAC addresses allowed on the port. (The default value is 1.) |

## Multi Host Status tab

The Multi Host Status tab provides information about the status of the Multi Host feature on the switch.

**Note:** The Multi Host button is not available from the EAPOL Advance tab for multiple ports. The Multi Host button is available only from the EAPOL Advance tab for a single port.

To view the Multi Host Status tab:

➨ From the EAPOL Advance tab for a single port (Figure 45 on page 183), click the Multi Host button.

The EAPOL Multi Host dialog box appears, with the Multi Host Status tab displayed (Figure 47).

**Figure 47** Multi Host Status tab

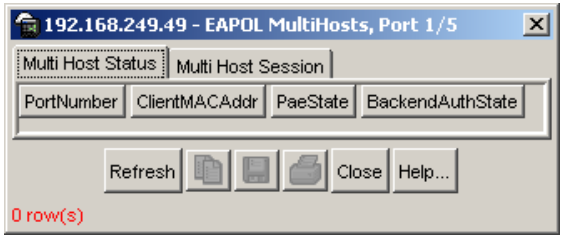


Table 84 describes the Multi Host Status tab fields.

**Table 84** Multi Host Status tab fields

| Field | Description |
|---|---|
| PortNumber | The Port number. |
| ClientMACAddr | The MAC address of the multihost client associated with the port. |
| PaeState | The PAE (Port Access Entity) State field displays the port status. The possible values are:<br>• initialize<br>• disconnected<br>• connecting<br>• authenticating<br>• authenticated<br>• aborting<br>• held<br>• forceAuth<br>• forceUnauth |
| BackendAuthState | The current state of the Backend Authentication state machine. The possible values are:<br>• request<br>• response<br>• success<br>• fail<br>• timeout<br>• idle<br>• initialize |

## Multi Host Session tab

The Multi Host Session tab displays the currently active Multi Host sessions.

**Note:** The Multi Host button is not available from the EAPOL Advance tab for multiple ports. The Multi Host button is available only from the EAPOL Advance tab for a single port.

To view the Multi Host Session tab:

**1** From the EAPOL Advance tab for a single port (Figure 45 on page 183), click the Multi Host button.

The EAPOL Multi Host dialogue box appears, with the Multi Host Status tab displayed (Figure 47 on page 185).

**2** Click the Multi Host Session tab.

The Multi Host Session tab opens (Figure 48).

**Figure 48** EAPOL Multi Host Session tab

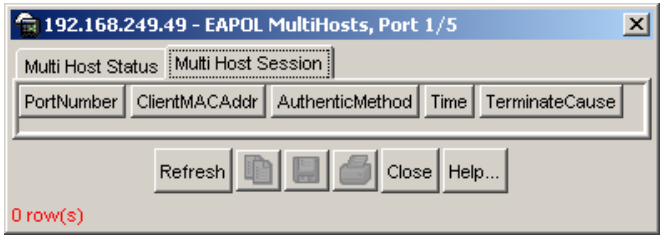



Table 84 describes the Multi Host Session tab fields.

**Table 85** Multi Host Session tab fields

| Field | Description |
|---|---|
| PortNumber | Port number. |
| ClientMACAddr | The MAC address of the multihost client. |
| AuthenticMethod | The authentication method used to establish the session:<br>• remoteAuthServer<br>• localAuthServer |
| Time | The duration of the session in seconds |
| TerminateCause | The reason for the session termination:<br>• supplicantLogoff<br>• portFailure<br>• supplicantRestart<br>• reauthFailed<br>• authControlForceUnauth<br>• portReInit<br>• portAdminDisabled<br>• notTerminatedYet |

## EAPOL Stats tab for graphing ports

The EAPOL Stats tab displays EAPOL statistics.

To open the EAPOL Stats tab for graphing:

1. Select the port or ports you want to graph.

   To select multiple ports, press [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2. Do one of the following:

   - From the Device Manager main menu, choose Graph > Port.
   - From the shortcut menu, choose Graph.
   - On the toolbar, click Graph.

   The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

3. Click the EAPOL Stats tab.

   The EAPOL Stats tab for graphing multiple ports opens (Figure 49).

**Figure 49** Graph Port dialog box — EAPOL Stats tab

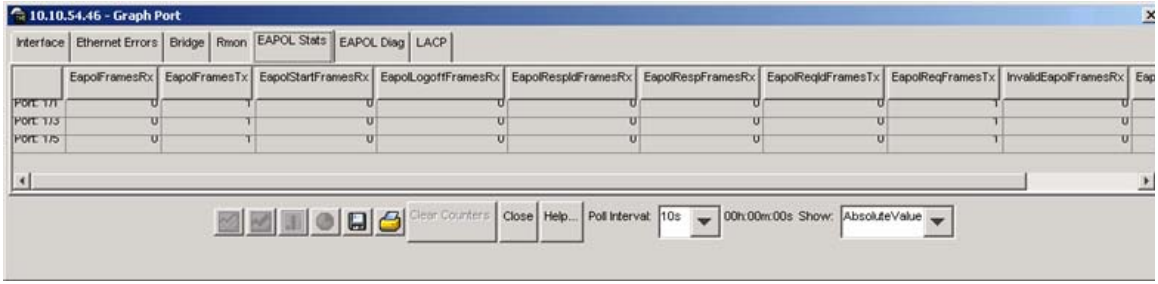


Table 86 describes the EAPOL tab fields.

**Table 86** EAPOL tab fields

| Field | Description |
|---|---|
| EapolFramesRx | The number of valid EAPOL frames of any type that this authenticator received. |
| EapolFramesTx | The number of EAPOL frame types of any type that this authenticator transmitted. |
| EapolStartFramesRx | The number of EAPOL start frames that this authenticator received. |
| EapolLogoffFramesRx | The number of EAPOL Logoff frames that this authenticator received. |
| EapolRespIdFramesRx | The number of EAPOL Resp/Id frames that this authenticator received. |
| EapolRespFramesRx | The number of valid EAP Response frames (other than Resp/Id frames) that this authenticator received. |
| EapolReqIdFramesTx | The number of EAPOL Req/Id frames that this authenticator transmitted. |
| EapolReqFramesTx | The number of EAP Req/Id frames (Other than Rq/Id frames) that this authenticator transmitted. |
| InvalidEapolFramesRx | The number of EAPOL frames that this authenticator received in which the frame type is not recognized. |
| EapLengthErrorFramesRx | The number of EAPOL frames that this authenticator received in which the packet body length field is not valid. |

## EAPOL Diag tab for graphing ports

The EAPOL Diag tab displays EAPOL diagnostics statistics.

To open the EAPOL Diag tab for graphing:

**1** Select the port or ports you want to graph.

To select multiple ports, press [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

**2** Do one of the following:

- From the Device Manager main menu, choose Graph > Port.

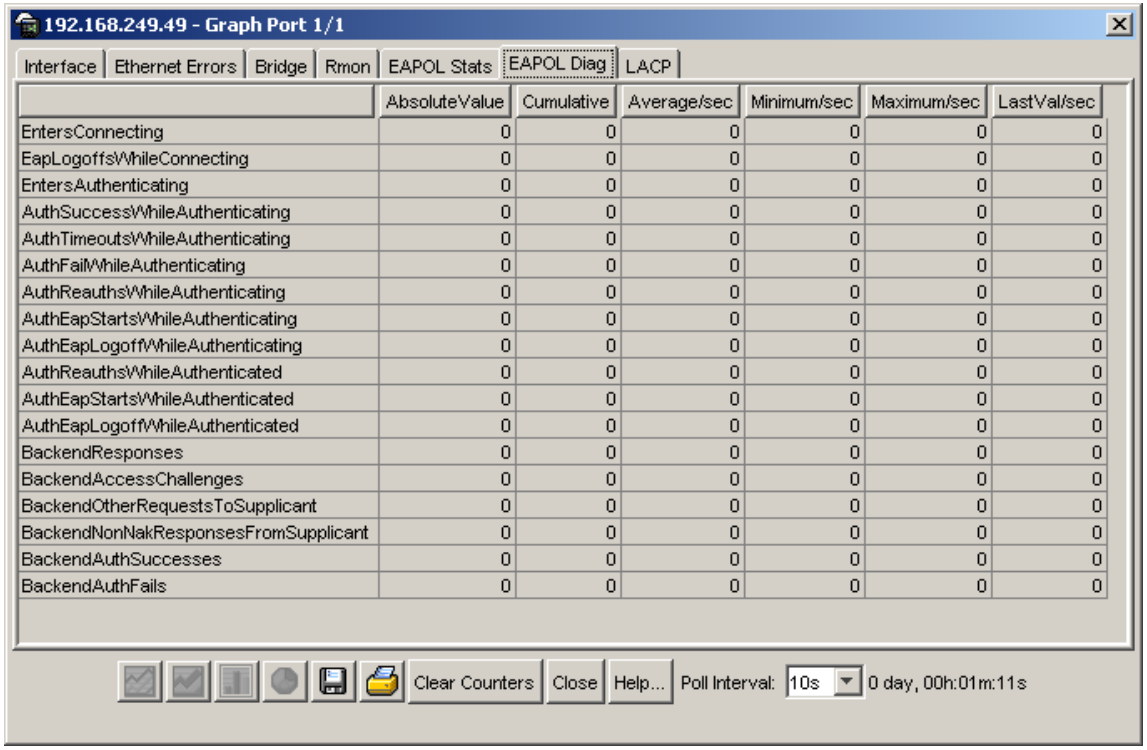
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

**3** Click the EAPOL Diag tab.

The EAPOL Diag tab for graphing ports opens (Figure 50).

**Figure 50** Graph Port dialog box — EAPOL Diag tab (single port)




| | AbsoluteValue | Cumulative | Average/sec | Minimum/sec | Maximum/sec | LastVal/sec |
|---|---|---|---|---|---|---|
| EntersConnecting | 0 | 0 | 0 | 0 | 0 | 0 |
| EapLogoffsWhileConnecting | 0 | 0 | 0 | 0 | 0 | 0 |
| EntersAuthenticating | 0 | 0 | 0 | 0 | 0 | 0 |
| AuthSuccessWhileAuthenticating | 0 | 0 | 0 | 0 | 0 | 0 |
| AuthTimeoutsWhileAuthenticating | 0 | 0 | 0 | 0 | 0 | 0 |
| AuthFailWhileAuthenticating | 0 | 0 | 0 | 0 | 0 | 0 |
| AuthReauthsWhileAuthenticating | 0 | 0 | 0 | 0 | 0 | 0 |
| AuthEapStartsWhileAuthenticating | 0 | 0 | 0 | 0 | 0 | 0 |
| AuthEapLogoffWhileAuthenticating | 0 | 0 | 0 | 0 | 0 | 0 |
| AuthReauthsWhileAuthenticated | 0 | 0 | 0 | 0 | 0 | 0 |
| AuthEapStartsWhileAuthenticated | 0 | 0 | 0 | 0 | 0 | 0 |
| AuthEapLogoffWhileAuthenticated | 0 | 0 | 0 | 0 | 0 | 0 |
| BackendResponses | 0 | 0 | 0 | 0 | 0 | 0 |
| BackendAccessChallenges | 0 | 0 | 0 | 0 | 0 | 0 |
| BackendOtherRequestsToSupplicant | 0 | 0 | 0 | 0 | 0 | 0 |
| BackendNonNakResponsesFromSupplicant | 0 | 0 | 0 | 0 | 0 | 0 |
| BackendAuthSuccesses | 0 | 0 | 0 | 0 | 0 | 0 |
| BackendAuthFails | 0 | 0 | 0 | 0 | 0 | 0 |

Table 87 describes the EAPOL Diag tab fields.

**Table 87** EAPOL Diag tab fields

| Field | Description |
|---|---|
| EntersConnecting | Counts the number of times that the Authenticator PAE state machine transitions to the Connecting state from any other state. |
| EapLogoffsWhileConnecting | Counts the number of times that the Authenticator PAE state machine transitions from Connected to Disconnected as a result of receiving an EAPOL-Logoff message. |
| EntersAuthenticating | Counts the number of times that the Authenticator PAE state machine transitions from Connecting to Authenticating as a result of receiving an EAP-Response/Identity message being received from the supplicant. |
| AuthSuccessWhileAuthenticating | Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Authenticated as a result of the Backend authentication state machine indicating successful authentication of the supplicant. |
| AuthTimeoutsWhile Authenticating | Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of the Backend authentication state machine indicating authentication timeout. |
| AuthFailWhileAuthenticating | Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Held as a result of the Backend authentication state machine indicating authentication failure. |
| AuthReauthsWhileAuthenticating | Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of a reauthentication request. |
| AuthEapStartsWhileAuthenticating | Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Start message being received from the supplicant. |
| AuthEapLogoffWhileAuthenticating | Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Logoff message being received from the supplicant. |
| AuthReauthsWhileAuthenticated | Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of a reauthentication request. |

**Table 87** EAPOL Diag tab fields (Continued)

| Field | Description |
|---|---|
| AuthEapStartsWhileAuthenticated | Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of an EAPOL-Start message being received from the supplicant. |
| AuthEapLogoffWhileAuthenticated | Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Disconnected as a result of an EAPOL-Logoff message being received from the supplicant. |
| BackendResponses | Counts the number of times that the Backend Authentication state machine sends an Initial-Access request packet to the Authentication server. |
| BackendAccessChallenges | Counts the number of times that the Backend Authentication state machine receives an Initial-Access challenge packet from the Authentication server. |
| BackendOtherRequestsToSupplicant | Counts the number of times that the Backend Authentication state machine sends an EAP request packet (other than an Identity, Notification, failure, or success message) to the supplicant. |
| BackendNonNakResponsesFromSupplicant | Counts the number of times that the Backend Authentication state machine receives a response from the supplicant to an initial EAP request and the response is something other than EAP-NAK. |
| BackendAuthSuccesses | Counts the number of times that the Backend Authentication state machine receives an EAP-success message from the Authentication server. |
| BackendAuthFails | Counts the number of times that the Backend Authentication state machine receives an EAP-failure message from the Authentication server. |

# Configuring SNMP

This section contains the following topics:

## SNMP tab

The SNMP tab provides read-only information about the addresses that the agent software uses to identify the switch.

To open the SNMP tab:

1. Select the chassis.
2. From the shortcut menu, choose Edit > Chassis.

   The Chassis dialog box opens with the System tab displayed.
3. Click the SNMP tab.

   The SNMP tab opens (Figure 51).

**Figure 51** Edit Chassis dialog box — SNMP tab

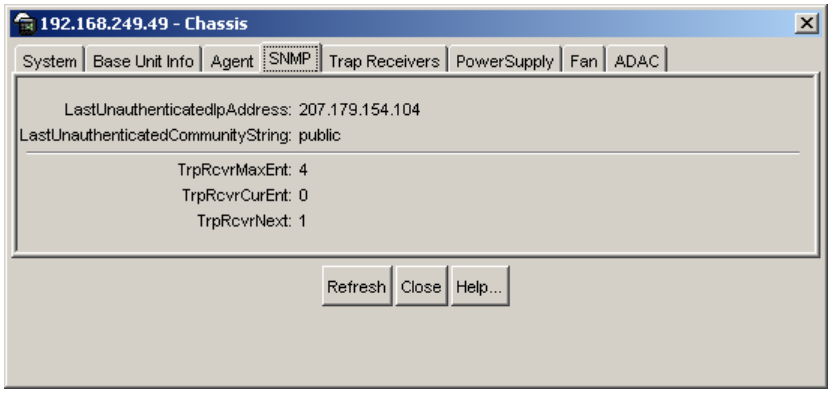



Table 88 describes the SNMP tab fields.

**Table 88** SNMP tab fields

| Field | Description |
|---|---|
| LastUnauthenticatedIpAddress | The last IP address that was not authenticated by the device. |
| LastUnauthenticatedCommunityString | The last community string that was not authenticated by the device. |
| TrpRcvrMaxEnt | The maximum number of trap receiver entries. |

**Table 88** SNMP tab fields (Continued)

| Field | Description |
|---|---|
| TrpRcvrCurEnt | The current number of trap receiver entries. |
| TrpRcvrNext | The next trap receiver entry to be created. |

## Trap Receivers tab

The Trap Receivers tab lists the devices that receive SNMP traps from the Ethernet Switch.

When Device Manager opens a device, it automatically adds the device to the Trap Receivers list.

To open the Trap Receivers tab:

1. Right-click the chassis and choose Edit > Chassis from the shortcut menu.

   The Chassis dialog box opens with the System tab displayed.

2. Click the Trap Receivers tab.

   The Trap Receivers tab opens (Figure 52).

**Figure 52** Edit Chassis dialog box—Trap Receivers tab

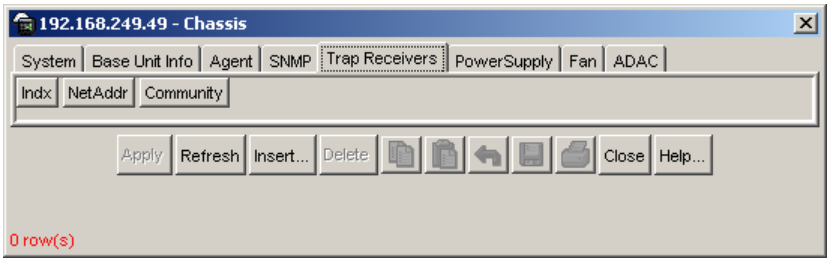


Table 89 describes the Trap Receivers tab items.

**Table 89** Edit Chassis dialog box — Trap Receivers tab items

| Item | Description |
|---|---|
| NetAddr | The address (or DNS hostname) for the trap receiver. |
| Community | Community string used for trap messages to this trap receiver. |

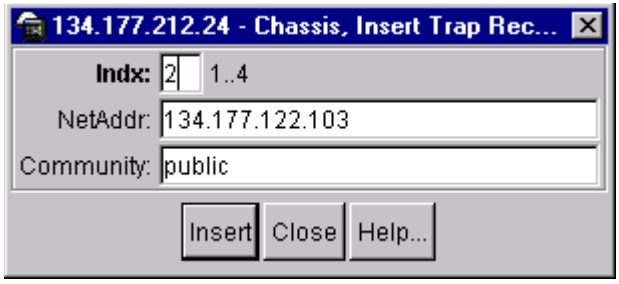
## Editing network trap receivers

To edit the network trap receivers table:

1 In the Trap Receivers tab (Figure 52 on page 194), click Insert.

The Chassis, Insert Trap Receivers dialog box opens (Figure 53).

**Figure 53** Chassis, Insert Trap Receivers dialog box




2 Type the Index, NetAddr, and the Community information.

**Note:** Refer to Table 89 for a description of the Chassis, Insert Trap Receivers dialog box items.

3 Click Insert.

## Graphing SNMP statistics

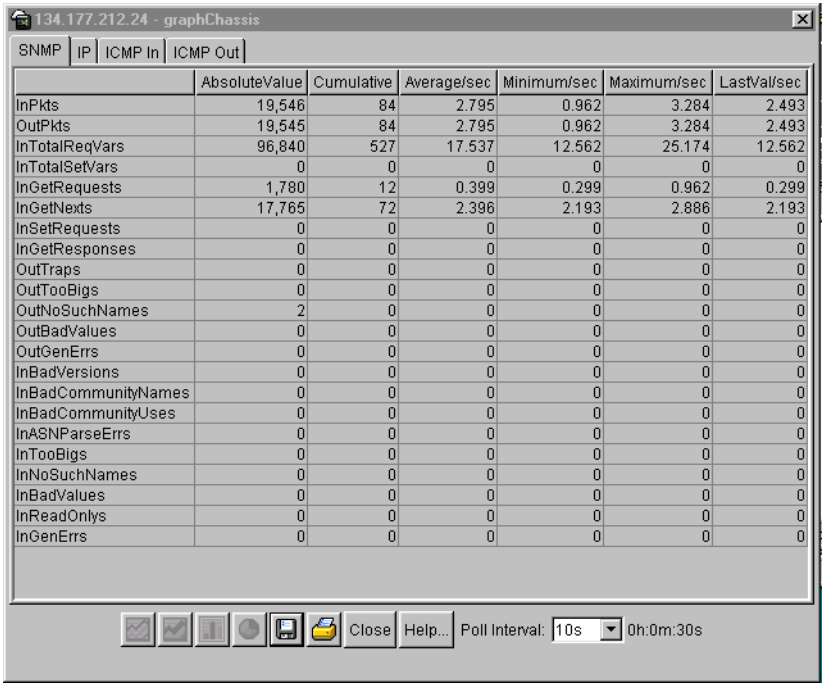
In the Graph Chassis dialog box, the SNMP tab provides read-only information about the addresses that the agent software uses to identify the switch.For descriptions of the type of statistics shown in each column, refer to Table 90 on page 197.

To open the SNMP tab:

1 From the Main Menu, choose Graph > Chassis.

The Graph Chassis dialog box opens with the SNMP tab displayed (Figure 54).

**Figure 54** Graph Chassis dialog box — SNMP tab




| | AbsoluteValue | Cumulative | Average/sec | Minimum/sec | Maximum/sec | LastVal/sec |
|---|---|---|---|---|---|---|
| InPkts | 19,546 | 84 | 2.795 | 0.962 | 3.284 | 2.493 |
| OutPkts | 19,545 | 84 | 2.795 | 0.962 | 3.284 | 2.493 |
| InTotalReqVars | 96,840 | 527 | 17.537 | 12.562 | 25.174 | 12.562 |
| InTotalSetVars | 0 | 0 | 0 | 0 | 0 | 0 |
| InGetRequests | 1,780 | 12 | 0.399 | 0.299 | 0.962 | 0.299 |
| InGetNexts | 17,765 | 72 | 2.396 | 2.193 | 2.886 | 2.193 |
| InSetRequests | 0 | 0 | 0 | 0 | 0 | 0 |
| InGetResponses | 0 | 0 | 0 | 0 | 0 | 0 |
| OutTraps | 0 | 0 | 0 | 0 | 0 | 0 |
| OutTooBigs | 0 | 0 | 0 | 0 | 0 | 0 |
| OutNoSuchNames | 2 | 0 | 0 | 0 | 0 | 0 |
| OutBadValues | 0 | 0 | 0 | 0 | 0 | 0 |
| OutGenErrs | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadVersions | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadCommunityNames | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadCommunityUses | 0 | 0 | 0 | 0 | 0 | 0 |
| InASNParseErrs | 0 | 0 | 0 | 0 | 0 | 0 |
| InTooBigs | 0 | 0 | 0 | 0 | 0 | 0 |
| InNoSuchNames | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadValues | 0 | 0 | 0 | 0 | 0 | 0 |
| InReadOnlys | 0 | 0 | 0 | 0 | 0 | 0 |
| InGenErrs | 0 | 0 | 0 | 0 | 0 | 0 |

Table 90 describes the SNMP tab fields.

**Table 90** SNMP tab fields

| Field | Description |
|---|---|
| InPkts | The total number of messages delivered to the SNMP from the transport service. |
| OutPkts | The total number of SNMP messages passed from the SNMP protocol to the transport service. |
| InTotalReqVars | The total number of MIB objects retrieved successfully by the SNMP protocol as the result of receiving valid SNMP Get-Request and Get-Next PDUs. |
| InTotalSetVars | The total number of MIB objects altered successfully by the SNMP protocol as the result of receiving valid SNMP Set-Request PDUs. |
| InGetRequests | The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol. |
| InGetNexts | The total number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol. |
| InSetRequests | The total number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol. |
| InGetResponses | The total number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol. |
| OutTraps | The total number of SNMP Trap PDUs generated by the SNMP protocol. |
| OutTooBigs | The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is tooBig. |
| OutNoSuchNames | The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is noSuchName. |
| OutBadValues | The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is badValue. |
| OutGenErrs | The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is genErr. |
| InBadVersions | The total number of SNMP messages delivered to the SNMP protocol for an unsupported SNMP version. |
| InBadCommunityNames | The total number of SNMP messages delivered to the SNMP protocol that used an unknown SNMP community name. |

**Table 90** SNMP tab fields (Continued)

| Field | Description |
|---|---|
| InBadCommunityUses | The total number of SNMP messages delivered to the SNMP protocol that represented an SNMP operation not allowed by the SNMP community named in the message. |
| InASNParseErrs | The total number of ASN.1 or BER errors encountered by the SNMP protocol when decoding received SNMP messages. |
| InTooBigs | The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is tooBig. |
| InNoSuchNames | The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is noSuchName. |
| InBadValues | The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is badValue. |
| InReadOnlys | The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is readOnly. It is a protocol error to generate an SNMP PDU containing the value “readOnly” in the error-status field. This object is provided to detect incorrect implementations of the SNMP. |
| InGenErrs | The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is genErr. |

# Working with SNMPv3

**Note:** SNMPv3 includes MD5 and SHA encryption along with the DES privacy encryption that is already available.

In previous Ethernet Switch software releases that supported SNMP, MD5 was the only encryption method supported. Release 3.5 software and later provide support for DES/SHA and MD5 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, including MD5 and SHA-based user authentication and message integrity verification, as well as 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. Release 3.5 software and later use the SNMP Research EMANATE-Lite agent.

## Configuring SNMPv3

This section describes how to use Device Manager to configure the following SNMPv3 options:



## Using CLI commands to create an SNMPv3 view and user

Use the following procedure as a guide to using CLI commands to create or change an SNMPv3 access view and user:

**1** In the CLI, create a view using the following syntax:

```
snmp-server view <view-name> <oid>
```

For example:

```
snmp-server view allView +1.3
```

Specifying +1.3 allows you to access everything on the switch in the OID tree. You can restrict access to a particular OID or to a section of the OID tree. For example: +1.3.6.1.6.3.1.1.5 limits the user to traps only.

**2** In the CLI, create a user and define the authentication and privacy method:

**a** Syntax for no authentication and no privacy:

```
snmp-server user <user-name> read-view <view-name>
write-view <view-name> notify-view <view-name>
```

For example:

```
snmp-server user fbarnes read-view allView write-view
allView notify-view allView
```

**b** Syntax for md5 authentication and no privacy:

```
snmp-server user <user-name> md5
<authentication-password> read-view <view-name>
write-view <view-name> notify-view <view-name>
```

For example:

```
snmp-server user fbarnes md5 myPass read-view allView
write-view allView notify-view allView
```

**c** Syntax for sha authentication with des encryption:

```
snmp-server user <user-name> sha
<authentication-password> des <privacy-password>
read-view <view-name> write-view <view-name> notify-view
<view-name>
```

For example: sha authentication with des encryption:

```
snmp-server user fbarnes sha myPass des myPass read-view
allView write-view allView notify-view allView
```

You cannot specify both md5 and sha authentication. You can use one or the other. If you wish to access your device using both authentication methods, then define a separate user for each.

**3** Set up a target address and parameter for user trap notification:

For an authenticated user:

```
snmp-server host <trap-server-ip-address> v3 auth
<user-name>
```

For a user with privacy:

```
snmp-server host <trap-server-ip-address> v3 auth-priv
<user-name>
```

## Using CLI commands to create a default SNMPv3 user

Use the following procedure as a guide to using CLI commands for creating a default SNMPv3 user.

In the CLI, use the `snmp-server bootstrap` command to specify the level of security for the SNMP configuration and to configure a set of initial users, groups, and views.

The `snmp-server bootstrap` command provides three levels of security: minimum-secure, semi-secure and very-secure. (For additional details on this command, refer to "snmp-server bootstrap command" on page 134.)

For example, to specify a minimum security configuration in the CLI:

**1** From the config command mode, enter the following command:

```
470-24T(config)#snmp bootstrap minimum-secure
```

The following warning and prompt are displayed:

```
WARNING: This command will destroy *all* existing SNMP
configuration
Do you want to continue (y/n) ?
```

**2** Enter `y`.

The following prompt is displayed:

```
Enter authentication password/phrase for user 'initial':
```

**3** Enter an authentication password or phrase for user initial. The following prompt is displayed:

```
Re-Enter authentication password/phrase for user
'initial':
```

4 Re-enter the authentication password or phrase. The following prompt is displayed:

```
Enter authentication password/phrase for user
'templateMD5':
```

5 Enter the authentication password or phrase for user templateMD5.

```
Re-Enter authentication password/phrase for user
'templateMD5':
```

6 Re-enter the authentication password or phrase user templateMD5.

**Note:** If you are running an SSH-enabled image, you must also enter and confirm a password for a third user, templateSHA.

**Note:** You cannot use the templateMD5 and templateSHA users to log in to the switch; once created, they serve only as templates to create additional users.

To successfully log in to the switch using SNMPv3 snmp after using the `snmp-server bootstrap` command, you must enter the user name `initial` with the appropriate password.

## Opening a device using SNMPv3 with Device Manager

To open a device using Device Manager with the SNMPv3 check box enabled, parameters are required to initially log in. Some of these required parameters are:

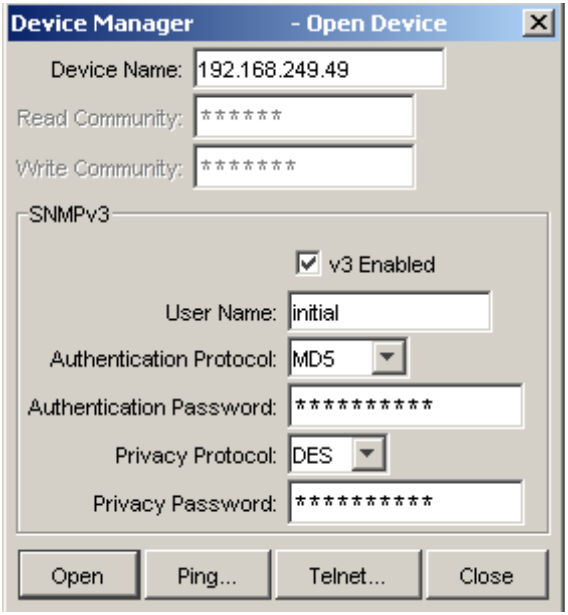
- User name
- Authentication Protocol
- Authentication Password
- Privacy Protocol
- Privacy Password

To open a device using SNMPv3 with Device Manager:

1 Click Device > Open.

2 The Open Device dialog box opens (Figure 55).

**Figure 55** Open Device dialog box




3 Check the SNMPv3 check box.

4 In the User Name field, enter a user name and the required passwords as configured in "Using CLI commands to create an SNMPv3 view and user" on page 199 or "Using CLI commands to create a default SNMPv3 user" on page 201. (The configured User Names are also listed in the User Security Model (USM) Table (Figure 56 on page 204)).

You can now use Device Manager to configure the SNMPv3 options.

## Creating a user security model

**Note:** You must configure a valid SNMPv3 user through the CLI (or the Web interface for a default user only) before you can access the switch in SNMPv3 mode or by using the Device Manager.

To create a user security model (USM):

1 From the Device Manager menu bar, click Edit > SnmpV3 > USM Table.

The USM dialog box opens (Figure 56 on page 204).

**Figure 56** USM dialog box

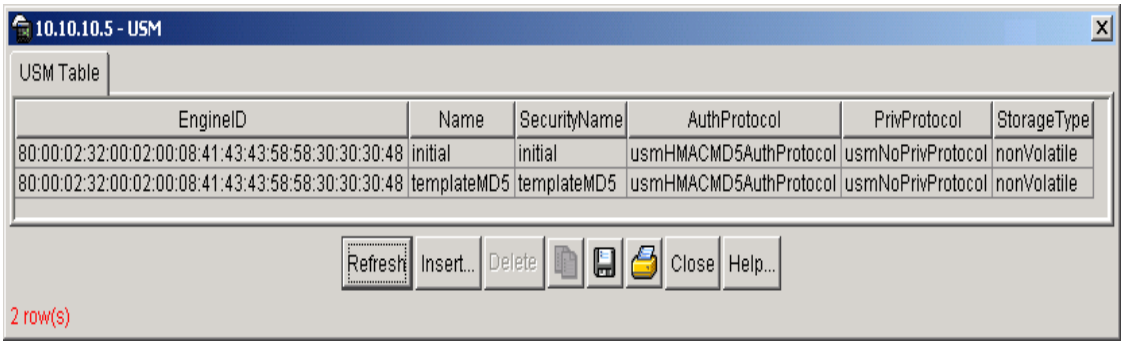



Table 91 describes the USM dialog box fields.

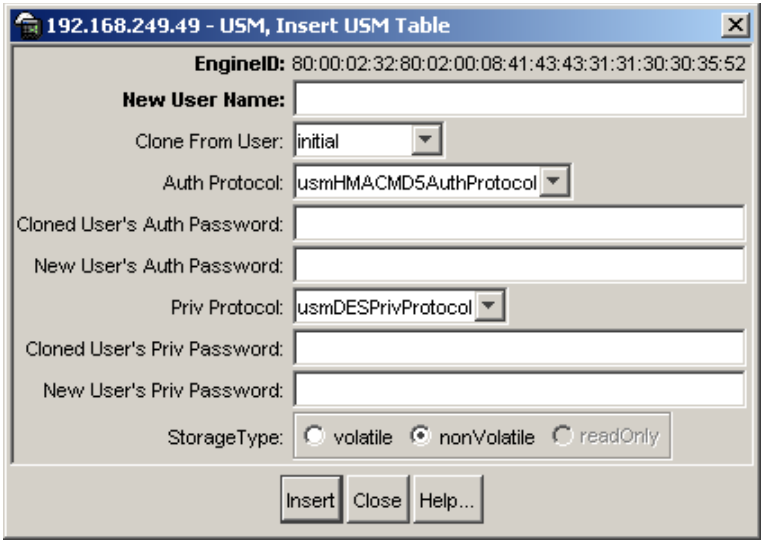
**Table 91** USM dialog box fields

| Field | Description |
|---|---|
| EngineID | Indicates the SNMP engine's administratively 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 | Specifies the storage type, volatile or non-volatile. |

2 Click Insert.

The USM, Insert USM Table dialog box opens (Figure 57 on page 205).

**Figure 57** USM, Insert USM Table dialog box




**3** Enter a new user name.

**4** In the Clone From User field, select a security name from which the new entry copies authentication data and private data.

**5** Select an authentication protocol.

**6** Enter the cloned user's authentication password.

**7** Enter a new authentication password for the new user.

**8** Select a privacy protocol.

**9** Enter the cloned user's privacy password.

**10** Enter a new privacy password for the new user.

**11** Specify the StorageType.

**12** Click Insert.

The USM dialog box opens. The new user model appears in the list.

---

**Caution:** To ensure security, change the GroupAccess table default views after you have set up new users in the USM table. This prevents unauthorized people from accessing the switch using the default user login. Also, change the Community table defaults because the community name is used as a community string in SNMPv1/v2.

---

Table 92 describes the USM, Insert USM Table dialog box fields.

**Table 92** USM, Insert USM Table dialog box fields

| Field | Description |
|---|---|
| New User Name | Creates the new entry with this security name. The name is used as an index to the table. The range is 1 to 32 characters. |
| Clone From User | Specifies the security name from which the new entry must copy privacy and authentication parameters. The range is 1 to 32 characters. |
| AuthProtocol (Optional) | Assigns an authentication protocol (or no authentication) from a drop-down menu. If you select an authentication protocol, you must enter the cloned user's authentication password and specify a new authentication password for the new user. |
| Cloned User's Auth Password | Enter the cloned user's authentication password. |
| New User's Auth Password | Enter a new authentication password for the new user. |
| Priv Protocol (Optional) | Assigns a privacy protocol (or no privacy) from a drop-down menu. If you select a privacy protocol, you must enter the cloned user's privacy Pass and specify a new privacy password for the new user. |
| Cloned User's Priv Password | Enter the cloned user's privacy password. |
| New User's Priv Password | Enter a new privacy password for the new user. |
| StorageType | Specifies the storage type, volatile or non-volatile. |

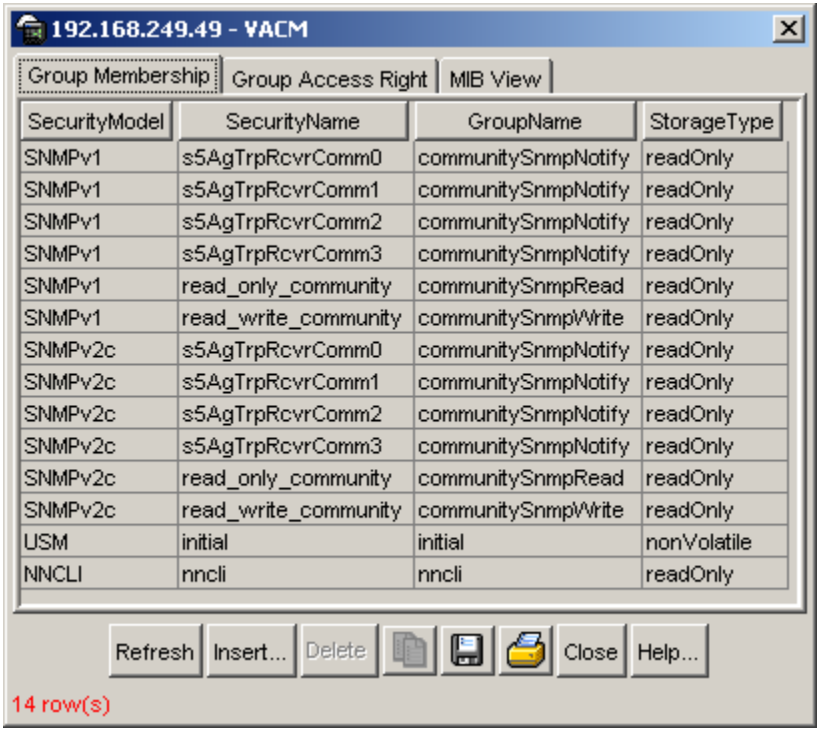
## Creating membership for a group

To add membership for a group in the view-based access control model (VACM):

1 From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

The VACM dialog box with the Group Membership tab options visible opens (Figure 58 on page 207).

**Figure 58** VACM dialog box




| SecurityModel | SecurityName | GroupName | StorageType |
|---|---|---|---|
| SNMPv1 | s5AgTrpRcvrComm0 | communitySnmpNotify | readOnly |
| SNMPv1 | s5AgTrpRcvrComm1 | communitySnmpNotify | readOnly |
| SNMPv1 | s5AgTrpRcvrComm2 | communitySnmpNotify | readOnly |
| SNMPv1 | s5AgTrpRcvrComm3 | communitySnmpNotify | readOnly |
| SNMPv1 | read_only_community | communitySnmpRead | readOnly |
| SNMPv1 | read_write_community | communitySnmpWrite | readOnly |
| SNMPv2c | s5AgTrpRcvrComm0 | communitySnmpNotify | readOnly |
| SNMPv2c | s5AgTrpRcvrComm1 | communitySnmpNotify | readOnly |
| SNMPv2c | s5AgTrpRcvrComm2 | communitySnmpNotify | readOnly |
| SNMPv2c | s5AgTrpRcvrComm3 | communitySnmpNotify | readOnly |
| SNMPv2c | read_only_community | communitySnmpRead | readOnly |
| SNMPv2c | read_write_community | communitySnmpWrite | readOnly |
| USM | initial | initial | nonVolatile |
| NNCLI | nncli | nncli | readOnly |

Table 93 describes the VACM dialog box fields

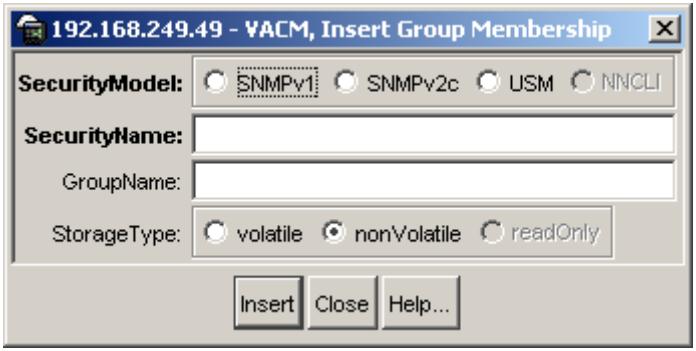
**Table 93** VACM dialog box fields

| Field | Description |
|---|---|
| SecurityModel | The security model currently in use |
| SecurityName | The name representing the user in usm user. The range is 1 to 32 characters. |
| GroupName | The name of the group to which this entry (combination of securityModel and securityName) belongs. |
| StorageType | Specifies the storage type, volatile, non-volatile, or read-only. |

**2** Click Insert.

The VACM, Insert Group Membership dialog box opens (Figure 59 on page 208).

**Figure 59** VACM, Insert Group Membership dialog box




3 Select a SecurityModel.

4 Enter a SecurityName.

5 Enter a GroupName.

6 Enter the StorageType.

7 Click Insert.

The VACM dialog box opens. The new group membership appears in the list.

Table 94 describes the Insert Group Membership tab fields.

**Table 94** VACM dialog box—Insert Group Membership tab fields

| Field | Description |
|---|---|
| SecurityModel | The authentication checking to communicate to the switch. |
| SecurityName | The security name assigned to this entry in the VACM table. The range is 1 to 32 characters. |
| GroupName | The name assigned to this group in the VACM table. The range is 1 to 32 characters. |
| StorageType | Specifies the storage type, volatile or non-volatile. |

## Creating access for a group

To create new access for a group:

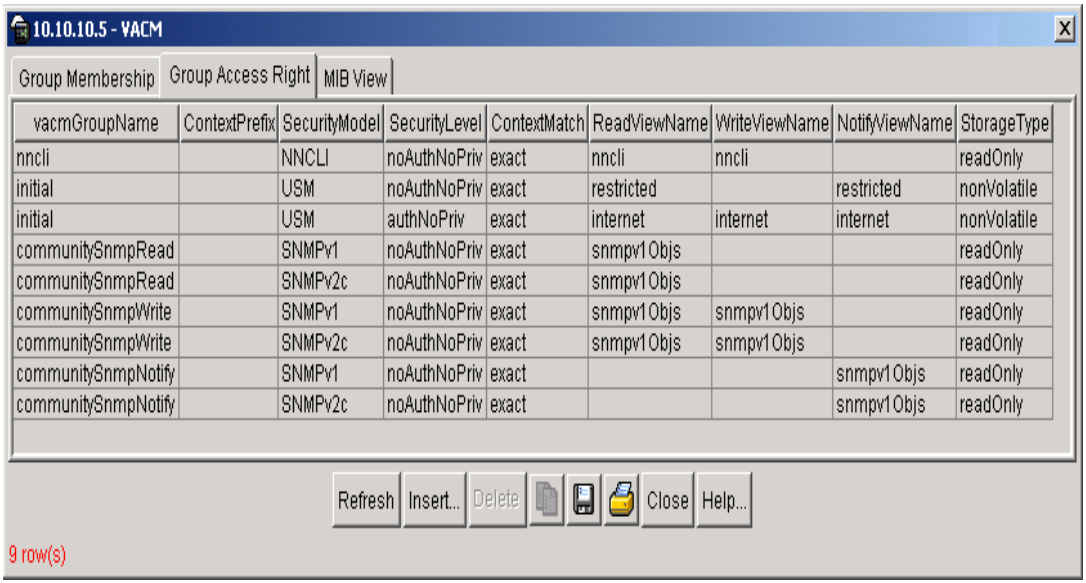
**1** From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

The VACM dialog box opens (Figure 58 on page 207).

**2** Click the Group Access Right tab.

The Group Access Right tab displays (Figure 60).

**Figure 60** Group Access Right tab

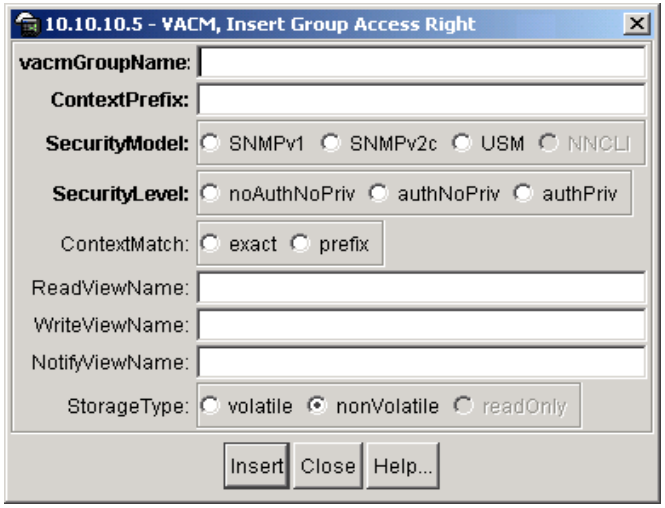



| vacmGroupName | ContextPrefix | SecurityModel | SecurityLevel | ContextMatch | ReadViewName | WriteViewName | NotifyViewName | StorageType |
|---|---|---|---|---|---|---|---|---|
| nncli | | NNCLI | noAuthNoPriv | exact | nncli | nncli | | readOnly |
| initial | | USM | noAuthNoPriv | exact | restricted | | restricted | nonVolatile |
| initial | | USM | authNoPriv | exact | internet | internet | internet | nonVolatile |
| communitySnmpRead | | SNMPv1 | noAuthNoPriv | exact | snmpv1Objs | | | readOnly |
| communitySnmpRead | | SNMPv2c | noAuthNoPriv | exact | snmpv1Objs | | | readOnly |
| communitySnmpWrite | | SNMPv1 | noAuthNoPriv | exact | snmpv1Objs | snmpv1Objs | | readOnly |
| communitySnmpWrite | | SNMPv2c | noAuthNoPriv | exact | snmpv1Objs | snmpv1Objs | | readOnly |
| communitySnmpNotify | | SNMPv1 | noAuthNoPriv | exact | | | snmpv1Objs | readOnly |
| communitySnmpNotify | | SNMPv2c | noAuthNoPriv | exact | | | snmpv1Objs | readOnly |

**3** Click Insert.

The VACM, Insert Group Access Right dialog box opens (Figure 61 on page 210).

**Figure 61** VACM, Insert Group Access Right dialog box




4 Enter a vacmGroupName.

5 Enter a ContextPrefix.

6 Select a SecurityModel.

7 Select a SecurityLevel.

8 If desired, select a ContextMatch.

9 In the ReadViewName field, enter the name of the MIB view authorized for read access.

10 In the WriteViewName field, enter the name of the MIB view authorized for write access.

11 In the NotifyViewName field, enter the name of the MIB view authorized for notification access.

12 Select a StorageType.

13 Click Insert.

The VACM dialog opens. The new group access appears in the list.

Table 95 describes the Group Access Right tab fields.

**Table 95** VACM dialog box—Group Access Right tab fields

| Field | Description |
|---|---|
| vacmGroupName | The name of the new group name in the VACM table. The name is a numeral. The range is 1 to 32 characters. |
| ContextPrefix | The contextName of an incoming SNMP packet must match exactly or partially the value of the instance of this object. The range is an SnmpAdminString, 1 to 32 characters. |
| SecurityModel | The security model of the entry, either SNMPv1, SNMPv2, or SNMPv3. |
| SecurityLevel | The minimum level of security required to gain access rights. The security levels are:<br>• noAuthNoPriv<br>• authNoPriv<br>• authpriv |
| ContextMatch (Optional) | Specifies 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. |
| Notify ViewName | Specifies the MIB view name to which notification access is authorized. |
| StorageType | Specifies the storage type, volatile or non-volatile. |

## Assigning MIB view access for an object

To assign MIB view access for an object:

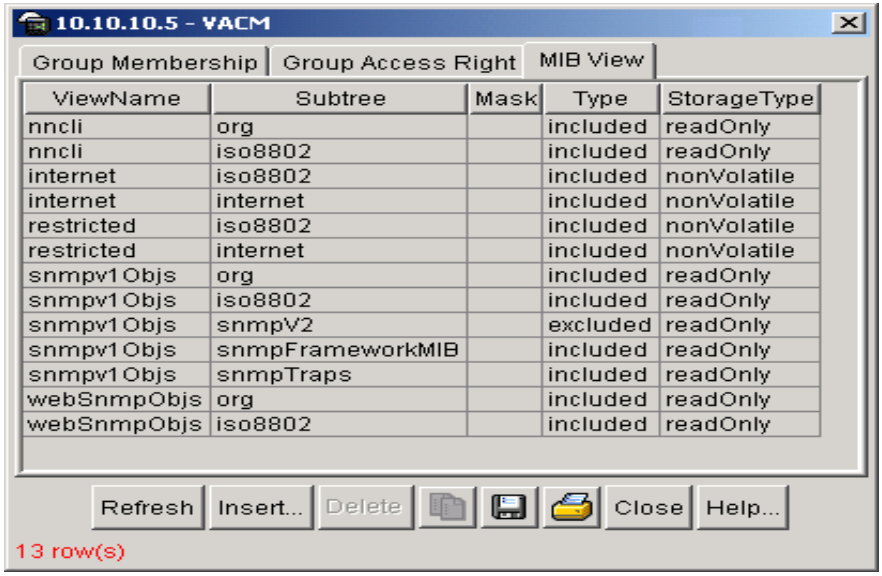
1. From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

   The VACM dialog box opens (Figure 58 on page 207).

2. Select the MIB View tab.

   The MIB View tab opens (Figure 62 on page 212).

**Figure 62** MIB View tab

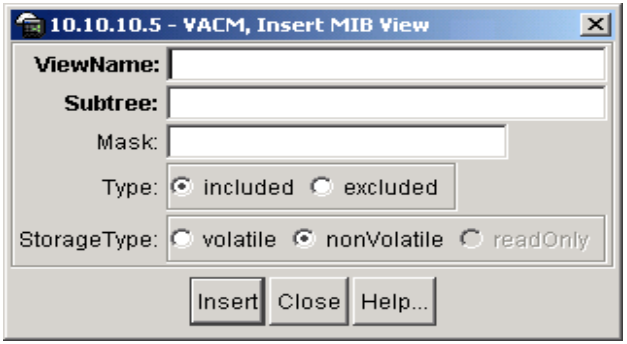



| ViewName | Subtree | Mask | Type | StorageType |
|---|---|---|---|---|
| nncli | org | | included | readOnly |
| nncli | iso8802 | | included | readOnly |
| internet | iso8802 | | included | nonVolatile |
| internet | internet | | included | nonVolatile |
| restricted | iso8802 | | included | nonVolatile |
| restricted | internet | | included | nonVolatile |
| snmpv1Objs | org | | included | readOnly |
| snmpv1Objs | iso8802 | | included | readOnly |
| snmpv1Objs | snmpV2 | | excluded | readOnly |
| snmpv1Objs | snmpFrameworkMIB | | included | readOnly |
| snmpv1Objs | snmpTraps | | included | readOnly |
| webSnmpObjs | org | | included | readOnly |
| webSnmpObjs | iso8802 | | included | readOnly |

**3** Click Insert.

The VACM, Insert MIB View dialog box opens (Figure 63).

**Figure 63** VACM, Insert MIB View dialog box




**4** Enter a ViewName.

**5** Enter a Subtree.

**6** Enter a Mask.

**7** Select a Type.

**8** Select a StorageType

**9** Click Insert.

The VACM dialog opens. The assigned MIB view appears in the list.

Table 96 describes the MIB View tab fields.

**Table 96** MIB View tab fields

| Field | Description |
|---|---|
| ViewName | Creates a new entry with this group name. The range is 1 to 32 characters. |
| Subtree | Any valid object identifier that defines the set of MIB objects or MIB node name accessible by this SNMP entity. For example 1.3.6.1.1.5 or Org, ISO 8802. |
| Mask<br>(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 | Specifies the storage type, volatile or non-volatile. |

## Creating a community

A community table contains objects for mapping between community strings and the security name created in VACM Group Member. To create a community:

**1** From the Device Manager menu bar, click Edit > SnmpV3 > Community Table.

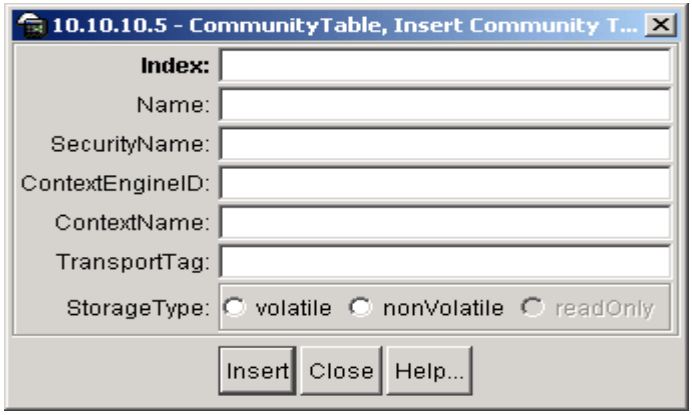
The Community Table dialog box opens (Figure 64 on page 214).

**Figure 64** Community Table dialog box


**2** Click Insert.

The Community Table, Insert Community Table dialog box opens (Figure 65).

**Figure 65** Community Table, Insert Community Table dialog box




**3** Enter an Index.

**4** Enter name that is a community string.

**5** Enter a SecurityName.

**6** Enter a TransportTag.

**7** Click Insert.

The Community Table dialog opens. The new community appears in the list.

Table 97 describes the Community Table dialog box fields.

**Table 97** Community Table dialog box fields

| Field | Description |
|---|---|
| Index | The unique index value of a row in this table. SnmpAdminString 1-32 characters. |
| Name | The community string for which a row in this table represents a configuration |
| SecurityName | The security name assigned to this entry in the Community table. The range is 1 to 32 characters. |
| ContextEngineID | The contextEngineID indicating the location of the context in which management information is accessed. |
| ContextName | The context in which management information is accessed. |
| TransportTag | The transport endpoints that are associated with the community string. The community string is only valid when found in an SNMPv1 (or SNMPv2c) message received from one of these transport endpoints, or when used in an SNMPv1 (or SNMPv2c) message to be sent to one of these transport endpoints.<br>The value of this object identifies a set of entries in the snmpTargetAddrTable.<br>If the value of this object has zero-length, transport endpoints are not checked when attempting to choose an entry in the snmpCommunityTable (that is, the community string is valid for use with any transport endpoint). |
| StorageType | Specifies the storage type, volatile or non-volatile. |

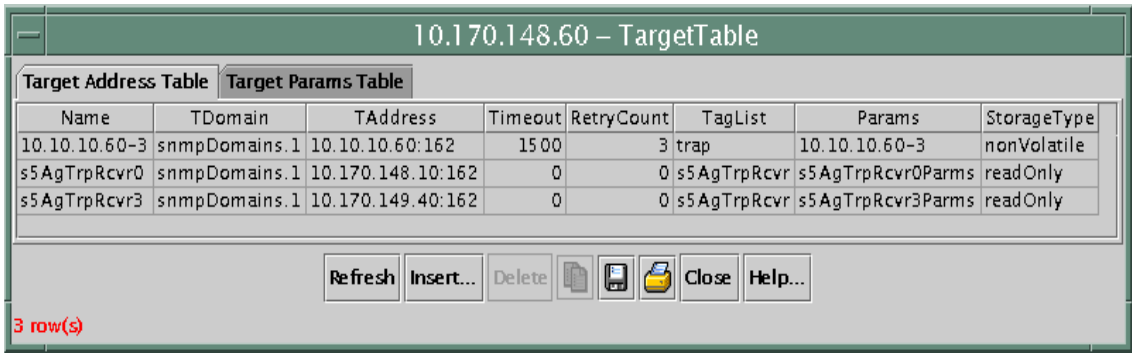
## Creating a target table

To create a target table:

1 From the Device Manager menu bar, click Edit > SnmpV3 > Target Table.

The Target Table dialog box opens (Figure 66 on page 216).

**Figure 66** Target Table dialog box

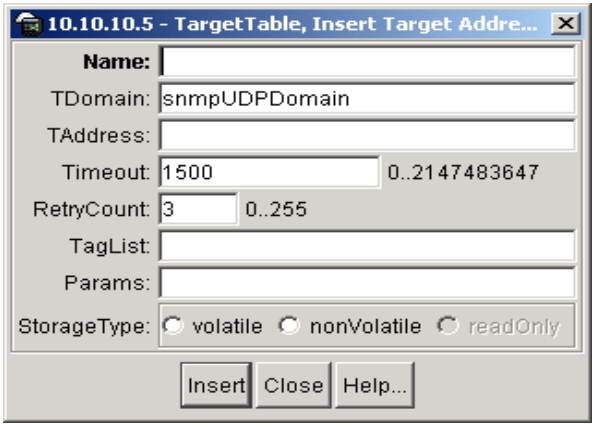



| Name | TDomain | TAddress | Timeout | RetryCount | TagList | Params | StorageType |
|---|---|---|---|---|---|---|---|
| 10.10.10.60-3 | snmpDomains.1 | 10.10.10.60:162 | 1500 | 3 | trap | 10.10.10.60-3 | nonVolatile |
| s5AgTrpRcvr0 | snmpDomains.1 | 10.170.148.10:162 | 0 | 0 | s5AgTrpRcvr | s5AgTrpRcvr0Parms | readOnly |
| s5AgTrpRcvr3 | snmpDomains.1 | 10.170.149.40:162 | 0 | 0 | s5AgTrpRcvr | s5AgTrpRcvr3Parms | readOnly |

**2** Click Insert.

The Target Table, Insert Target Address dialog box opens (Figure 67).

**Figure 67** Target Table, Insert Target Address dialog box




**3** Enter a Name.

**4** Enter a TDomain Name.

**5** Enter a TAddress Name.

**6** Enter a Timeout value. Value is in 1/100 seconds.

**7** Enter a RetryCount value. Value can be from 0 to 255.

**8** Enter a TagList.

**9** Enter a Params.

**10** Specify a StorageType.

**11** Click Insert.

The Target Table dialog box opens. The new Target address appears in the list.

Table 98 describes the Target Table dialog box fields.

**Table 98** Target Table dialog box fields

| Field | Description |
|---|---|
| Name | Specifies the name of the target table. |
| TDomain | Specifies the TDomain for the target table. |
| TAddress | Specifies the TAddress for the target table. |
| Timeout | Specifies the length of the timeout in 1/100 seconds. |
| RetryCount | Specifies the retry count. |
| Taglist | Specifies the taglist. |
| Params | Specifies the parameters. |
| StorageType | Specifies the storage type, volatile or non-volatile. |

## Creating target parameters

To create a target parameter:

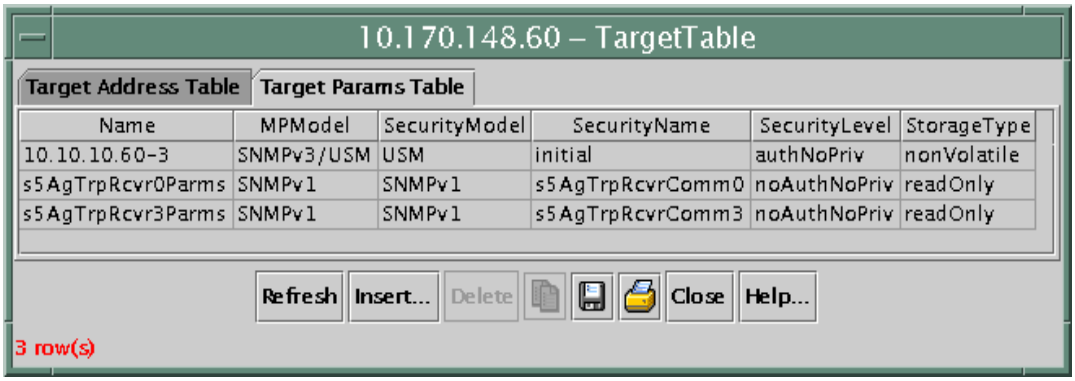
**1** From the Device Manager menu bar, click Edit > SnmpV3 > Target Table.

The Target Table dialog box opens (Figure 66 on page 216).

**2** Select the Target Params Table tab.

The Target Params Table tab opens (Figure 68 on page 218).

**Figure 68** Target Params Table dialog box

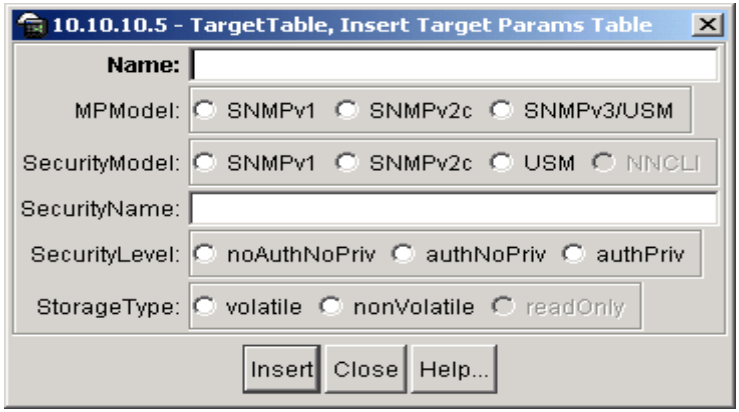



| Name | MPModel | SecurityModel | SecurityName | SecurityLevel | StorageType |
|---|---|---|---|---|---|
| 10.10.10.60-3 | SNMPv3/USM | USM | initial | authNoPriv | nonVolatile |
| s5AgTrpRcvr0Parms | SNMPv1 | SNMPv1 | s5AgTrpRcvrComm0 | noAuthNoPriv | readOnly |
| s5AgTrpRcvr3Parms | SNMPv1 | SNMPv1 | s5AgTrpRcvrComm3 | noAuthNoPriv | readOnly |

**3** Click Insert.

The Target Table, Insert Target Params Table dialog box opens (Figure 69).

**Figure 69** Target Table, Insert Target Params Table dialog box




**4** Enter a Name.

**5** Select the MPModel.

**6** Select the SecurityModel.

**7** Enter a SecurityName.

**8** Specify a SecurityLevel value

**9** Enter the storage type.

**10** Click Insert.

The Target Table dialog opens. The new target parameter appears in the list.

Table 99 describes the Target Params Table dialog box fields.

**Table 99** Target Params Table dialog box fields

| Field | Description |
|---|---|
| Name | Specifies the name of the target parameters table |
| MPModel | Specifies the Message Processing model, SNMPv1, SNMPv2c, or SNMPv3/USM. |
| SecurityModel | Specifies the security model, SNMPv1, SNMPv2c, or SNMPv3/USM. |
| SecurityName | Specifies the security name for generating SNMP messages. |
| SecurityLevel | Specifies the security level for SNMP messages: noAuthnoPriv, authnoPriv, or authPriv. |
| Storage Type | Specifies the storage type: volatile or non-volatile. |

## Creating a notify table

To create a notify table:

1 From the Device Manager menu bar, click Edit > SnmpV3 > Notify.

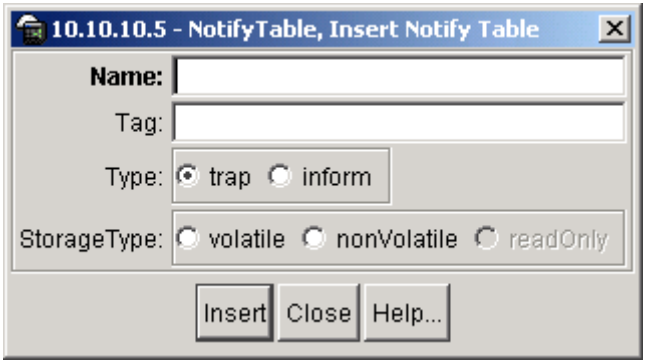
The Notify Table dialog box opens (Figure 70).

**Figure 70** NotifyTable dialog box


2 Click Insert.

The Notify Table, Insert Notify Table dialog box opens (Figure 71).

**Figure 71** Notify Table, Insert Notify Table dialog box




3 Enter a Name.

4 Enter a Tag name.

5 Specify the Type.

6 Specify the StorageType

7 Click Insert.

The Notify Table dialog box opens. The new notify entry appears in the list.

Table 100 describes the Notify Table dialog box fields.

**Table 100** Notify Table dialog box fields

| Field | Description |
|---|---|
| Name | Specifies the unique identifier associated for the notify table. |
| Tag | A single tag value used to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable that contains a tag value 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. |

**Table 100** Notify Table dialog box fields (Continued)

| Field | Description |
|---|---|
| Type | This object determines the type of notification generated for entries in the snmpTargetAddrTable that are selected by the corresponding instance of<br>snmpNotifyTag.<br>If the value of this object is trap, then any messages generated for selected rows contain SNMPv2-Trap PDUs.<br>If the value of this object is inform, then any messages generated for selected rows contain Inform PDUs.<br>Note: If an SNMP entity only supports generation of traps (and not informs), then this object may be read-only. |
| StorageType | Specifies the type of storage, volatile or non-volatile. |

# Chapter 4
# Configuring security using Web-based management

This chapter describes the security configurations available through Web-based management. For more information about these security features, as well as using the console interface (CI) menus, refer to Chapter 1, "Using security in your network," on page 31.

This chapter covers the following topics:



## Configuring system security

This section describes the steps you follow to manage system security using the Web-based management interface. It contains the following topics:



### Managing remote access by IP address

You can configure the remote access by IP address. You can specify up to 50 IP addresses to allow Web-based management access, SNMP access, or Telnet access to the switch.

To configure remote access using the Web-based management system:

1 From the main menu of the Ethernet Switch Web-based Manager, choose Configuration > Remote Access.

The Remote Access page opens (Figure 72 on page 224).

**Figure 72** Remote Access page

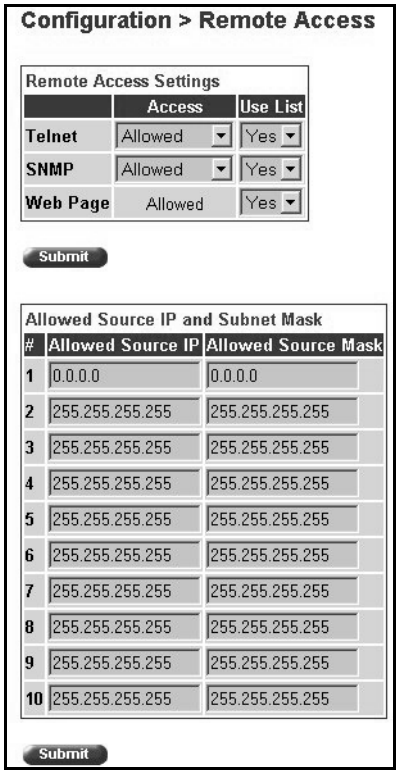



Table 101 describes the fields on the Remote Access page.

**Table 101** Remote Access page fields

| Section | Item | Range | Description |
|---|---|---|---|
| Remote Access Settings | Telnet/Access | (1)Allowed<br>(2) Disallowed | Allows Telnet access. |
| | Telnet/Use List | (1) Yes<br>(2) No | Restricts Telnet access to the specified 50 source IP addresses. |

**Table 101** Remote Access page fields (Continued)

| Section | Item | Range | Description |
|---|---|---|---|
| | SNMP/Access | (1)Allowed<br>(2) Disallowed | Allows SNMP access. |
| | SNMP/Use List | (1) Yes<br>(2) No | Restricts SNMP access to the specified 50 source IP addresses. |
| | Web Page/Access | | Displays allowed Web access. |
| | Web/Use List | (1) Yes<br>(2) No | Restricts Web access to the specified 50 source IP addresses. |
| Allowed Source IP and Subnet Mask | Allowed Source IP | XXX.XXX.XXX.XXX | Enter the source IP address you want to allow switch access. |
| | Allowed Source Mask | XXX.XXX.XXX.XXX | Enter the source IP mask you want to allow switch access. |

2 Complete fields as described in the table.

3 Click Submit.

## Setting console, Telnet, and Web passwords

To set console, Telnet, and Web passwords:

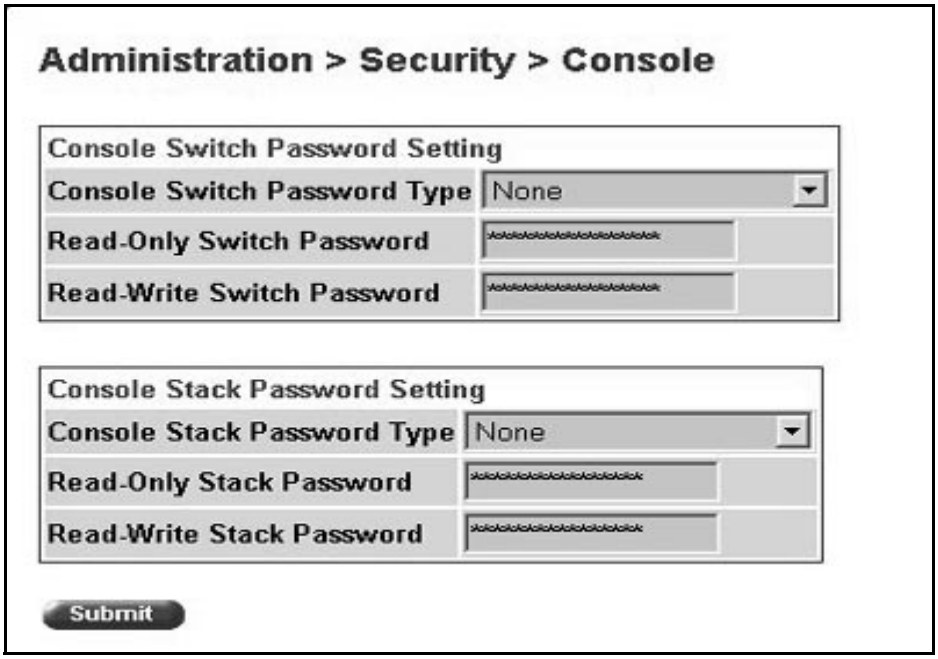
1 From the Web-based management main menu, choose Administration > Security.

2 From the Security menu, choose Console, Telnet, or Web.

The selected password page opens (Figure 73 on page 226).

**Note:** The title of the page corresponds to the menu selection you choose. In Figure 73 on page 226, the network administrator selected Administration > Security > Console.

**Figure 73** Console password setting page




**Note:** Console, Telnet, and Web settings share the same switch and stack password type and password.

**Note:** The switch logging mode cannot be changed while the system is in a stack configuration.

Table 102 describes the fields on the Console page.

**Table 102** Console page fields

| Section | Field | Setting | Description |
|---|---|---|---|
| Console Switch Password Setting | Console Switch Password Setting Type | (1) None<br>(2) Local Password<br>(3) RADIUS Authentication | Displays the switch password types.<br><br>Note: The default is None. |
| | Read-Only Switch Password. | 1..15 alphanumeric string. Default is User. | Type the read-only password setting for the read-only access user. |
| | Read-Write Switch Password | 1..15 alphanumeric string. Default is secure | Type the read-write password setting for the read-write access user. |
| Console Stack Password Setting | Console Stack Password Setting Type | (1) None<br>(2) Local Password<br>(3) RADIUS Authentication | Displays the stack password types.<br><br>Note: The default is None. |
| | Read-Only Stack Password | 1..15 alphanumeric string | Type the read-only password setting for the read-only access user. |
| | Read-Write Stack Password | 1..15 alphanumeric string | Type the read-write password setting for the read-write access user. |

3 Type the required information, or make a selection from the list.

4 Click Submit.

## Configuring RADIUS security

To configure RADIUS security parameters:

1 From the Web-based management main menu, choose Administration > Security > RADIUS.

The RADIUS page opens.

**Figure 74** RADIUS page

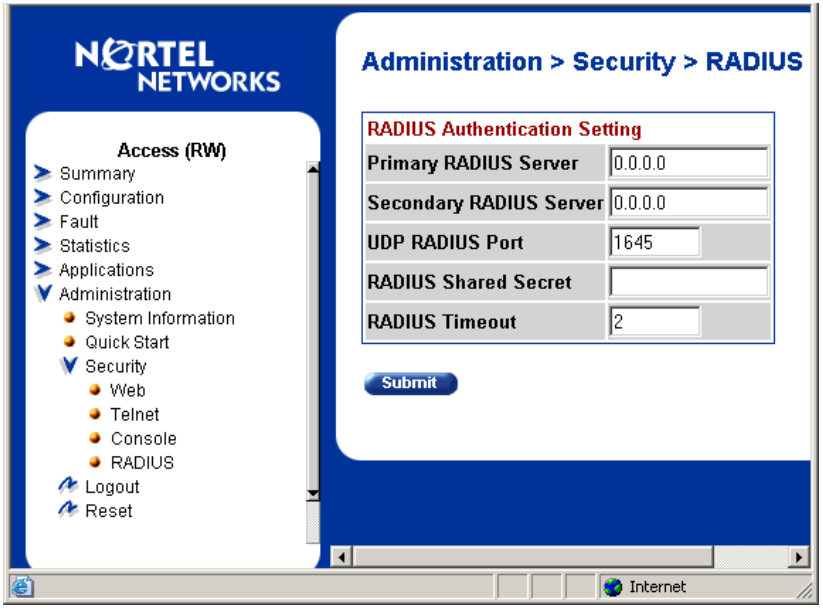



Table 103 describes the fields on the RADIUS page.

**Table 103** RADIUS page fields

| Field | Setting | Description |
|---|---|---|
| Primary RADIUS Server | XXX.XXX.XXX.XXX | Type a Primary RADIUS server IP address in the appropriate format. |
| Secondary RADIUS Server | XXX.XXX.XXX.XXX | Type a Secondary RADIUS server IP address in the appropriate format. |
| UDP RADIUS Port | Integer | Type the UDP RADIUS port number. |
| RADIUS Shared Secret | 1..16 | Type a unique character string to create a secret password. |
| RADIUS Timeout | 1-60 | Type the desired time in seconds for the RADIUS client to wait for a response from a RADIUS server before timeout. |

2 Type the required information.

3 Click Submit.

# Configuring EAPOL-based security

You can configure security based on the Extensible Authentication Protocol over LAN (EAPOL) protocol. For more information about EAPOL-based security, see Chapter 1, “Using security in your network,” on page 31.

To configure EAPOL:

1 From the Web-based management main menu, choose Application > EAPOL Security.

The EAPOL Security Configuration page opens (Figure 75 and Figure 76 on page 230). Use the scroll bar on the right to move down the page and the scroll bar on the bottom to move across the page.

**Figure 75** EAPOL Security Configuration page (1 of 2)

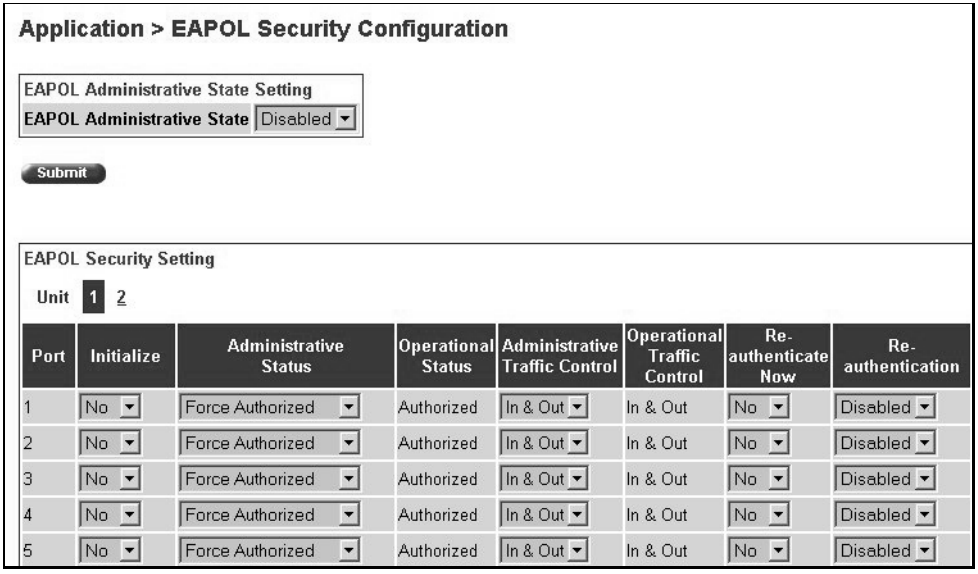
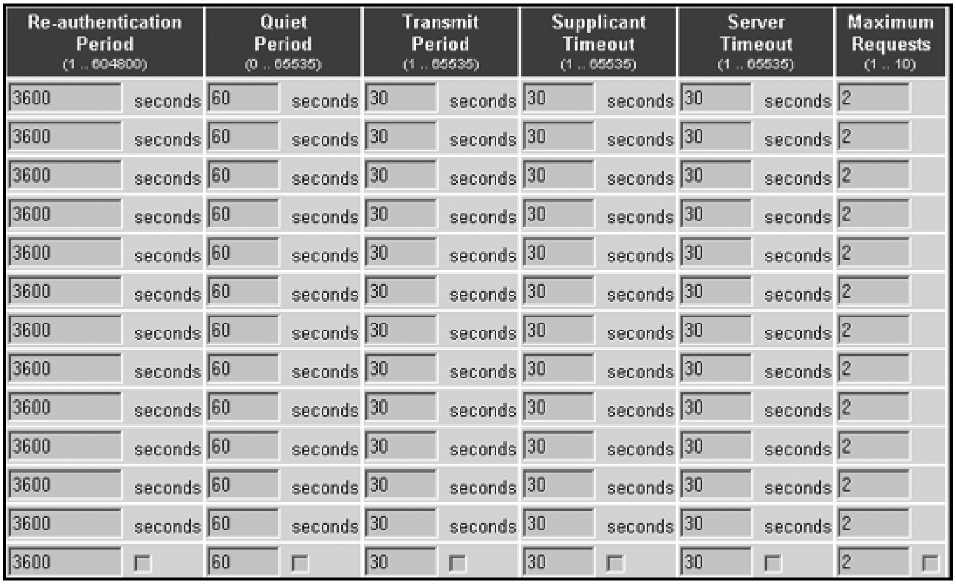


**Figure 76** EAPOL Security Configuration page (2 of 2)



| Re-authentication Period (1 .. 604800) | Quiet Period (0 .. 65535) | Transmit Period (1 .. 65535) | Supplicant Timeout (1 .. 65535) | Server Timeout (1 .. 65535) | Maximum Requests (1 .. 10) |
|---|---|---|---|---|---|
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 seconds | 60 seconds | 30 seconds | 30 seconds | 30 seconds | 2 |
| 3600 ☐ | 60 ☐ | 30 ☐ | 30 ☐ | 30 ☐ | 2 ☐ |

Table 104 describes the fields on the EAPOL Security Configuration page.

**Table 104** EAPOL Security Configuration page fields

| Section | Field | Range | Description |
|---|---|---|---|
| EAPOL Administrative State Setting | EAPOL Administrative State | (1) Enabled<br>(2) Disabled | Enables or disables EAPOL-based security. |
| EAPOL Security Setting | Unit | | Displays the unit you are viewing. |
| | Port | 1 to 26 for 470-24T and<br>1 to 48 for 470-48T | Displays the port number. |
| | Initialize | (1) Yes<br>(2) No | Activates EAPOL state on this port. |
| | Administrative Status | (1) Force Unauthorized<br>(2) Auto<br>(3) Force Authorized | Allows you to set the EAPOL authorization status:<br>• Force Unauthorized—Always unauthorized<br>• Auto—Status depends on EAP authentication results<br>• Force Authorized—Always authorized |

**Table 104** EAPOL Security Configuration page fields (Continued)

| Section | Field | Range | Description |
|---|---|---|---|
| EAPOL Security Setting, continued | Operational Status | (1) Authorized<br>(2) Unauthorized | Displays the current authorization status. |
| | Administrative Traffic Control | (1) In & Out<br>(2) In Only | Allows you to set EAPOL authentication either for incoming and outgoing traffic or for incoming traffic only. |
| | Operational Traffic Control | (1) In & Out<br>(2) In Only | Displays the current administrative traffic control setting. |
| | Re-authenticate Now | (1) Yes<br>(2) No | Allows you to activate EAPOL authentication immediately, without waiting for the re-authentication period to expire. |
| | Re-authentication | (1) Enabled<br>(2) Disabled | Allows you to repeat EAPOL authentication according to the time value specified in Re-authentication Period field. |
| | Re-authentication Period | 1..604800 | With Re-authentication enabled, allows you to specify the time period between successive EAPOL authentications. |
| | Quiet Period | 0..65535 | Allows you to specify the time interval between an authentication failure and the start of a new authentication attempt. |
| | Transmit Period | 1..65535 | Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets. |
| | Supplicant Timeout | 1..65535 | Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets. |
| | Server Timeout | 1..65535 | Allows you to specify how long the switch waits for the RADIUS server to respond to all EAP packets. |
| | Maximum Requests | 1..10 | Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant. |

**2** Complete the fields as described in Table 104.

**3** Click Submit.

# Configuring MAC address-based security

The MAC address-based security system allows you to use the Web-based management system to specify a range of system responses to unauthorized network access to your switch.

The system response can range from sending a trap to disabling the port. The network access control is based on the MAC source addresses (SA) of the authorized stations. You can specify a list of up to 448 MAC SAs that are authorized to access the switch, or use the auto-learning feature to allow the switch to identify the MAC SAs automatically. You can also specify the ports that each MAC SA is allowed to access. The options for allowed MAC SA port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, and so forth. You must also include the MAC SA of any router connected to any secure ports.

When the switch software detects an SA security violation, the response can be to send a trap, turn on DA filtering for all SAs, disable the specific port, or any combination of these three options.

You can configure the Ethernet Switches 460 and 470 to drop all packets having a specified MAC DA. You can create a list of up to 10 MAC DAs you want to filter. The packet with the specified MAC DA is dropped regardless of the ingress port, source address (SA) intrusion, or VLAN membership.

**Note:** Ensure that you do not enter the MAC address of the switch or stack you are working on.

**Note:** After configuring the switch for MAC address-based security, you must enable the ports you want, using the Port Configuration page.

# Configuring MAC address-based security using Web-based management

To configure MAC address-based security using the Web-based management system:

1 From the Web-based management main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 77).

**Figure 77** Security Configuration page

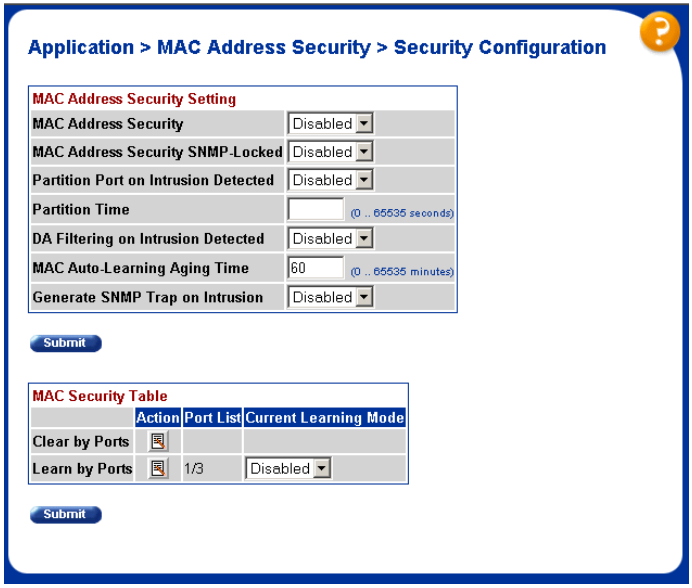


Table 105 describes the fields on the Security Configuration page.

**Table 105** Security Configuration page fields

| Section | Field | Range | Description |
|---|---|---|---|
| MAC Address Security Setting | MAC Address Security | (1) Enabled<br>(2) Disabled | Enables the MAC address security features. |
| | MAC Address Security SNMP-Locked | (1) Enabled<br>(2) Disabled | Enables locking SNMP, so that you cannot use SNMP to modify the MAC address security features. |
| | Partition Port on Intrusion Detected | (1) Forever<br>(2) Enabled<br>(3) Disabled | Configures how the switch reacts to an intrusion event:<br>• Forever—The port is disabled and remains disabled (partitioned) until reset. The port does not reset after the Partition Time elapses.<br>• Enabled—The port is disabled, then automatically reset to enabled after the time specified in the Partition Time field elapses.<br>• Disabled—The port remains enabled, even if an intrusion event is detected. |
| | Partition Time | 1 to 65535 | Sets the time to partition a port on intrusion.<br><br>Note: Use this field only if the Partition Port on Intrusion Detected field is set to Enabled. |
| | DA Filtering on Intrusion Detected | (1) Enabled<br>(2) Disabled | Enables you to isolate the intruding node (discard) the packets. |
| | MAC Auto-Learning Aging Time | 0-65535 | Sets the aging time, in minutes, for the auto-learned addresses in the MAC Security Table.<br>Note: An aging time of 0 means that the auto-learned addresses never age out. |
| | Generate SNMP Trap on Intrusion | (1) Enabled<br>(2) Disabled | Enables generation of an SNMP when an intrusion is detected. |
| MAC Security Table/Clear by Ports | Action | | Allows you to clear specific ports from participation in the MAC address security features. |
| | Port List | | Will be blank. |
| | Current Learning Mode | | Will be blank. |

**Table 105** Security Configuration page fields (Continued)

| Section | Field | Range | Description |
|---|---|---|---|
| MAC Security Table/Learn by Ports | Action | | Allows you to identify ports that will learn incoming MAC addresses. All source MAC addresses of any packets received on a specified port(s) are added to the MAC Security Table (maximum of 448 MAC addresses allowed). |
| | Port List | | Displays all the ports that will learn incoming MAC address to detect intrusions (unallowed MAC addresses). |
| | Current Learning Mode | (1) Enabled<br>(2) Disabled | Enables learning. |

2 On the Security Configuration page, type information in the text boxes, or select from a list.

3 Click Submit.

## Configuring ports

In this section, you create a list of ports, and you can add ports to or delete ports from each list.

To activate an entry or add or delete ports to a list:

1 From the Web-based management main menu, choose Application > MAC Address Security > Port Lists.

The Port Lists page opens (Figure 78 on page 236).

**Figure 78** Port Lists page

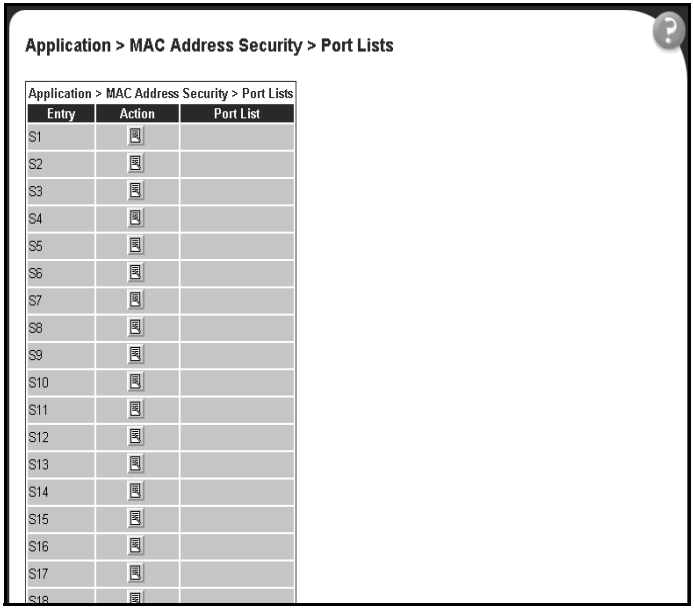



Table 106 describes the fields on the Ports Lists page.

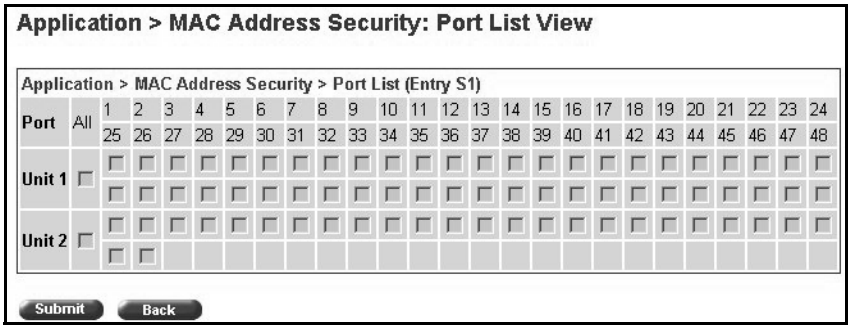
**Table 106** Ports Lists page fields

| Field | Range | Description |
|---|---|---|
| Entry | | These are the lists of ports. |
| Action | | Allows you to add or delete ports to the lists. |
| Port List | | Displays which ports are associated with each list. |

**2** To add or delete ports to a list, click the icon in the Action column in the list row you want.

The Port List View, Port List page opens (Figure 79 on page 237).

**Figure 79** Port List View, Port List page




**a** Click the ports you want to add to the selected list or click None.

**b** To delete a port from a list, clear the box by clicking it.

**c** Click Submit.

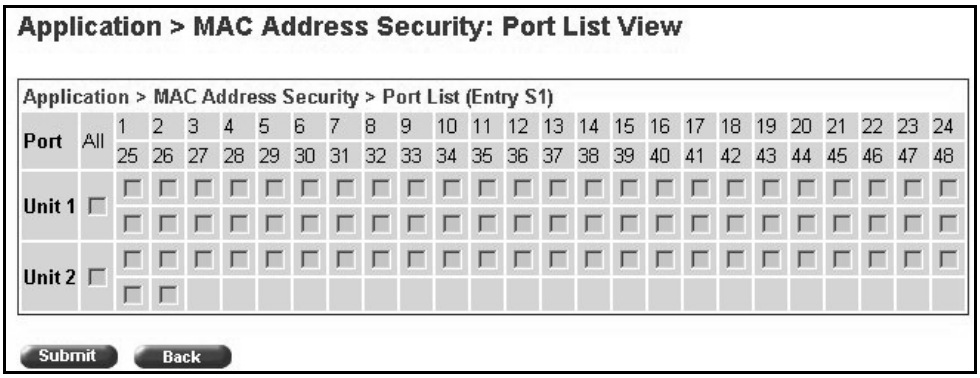
**3** From the Web-based management main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 77 on page 233).

**4** In the MAC Security Table section, click the icon in the Action column of the Learn By Ports row.

The Port List View, Learn by Ports page opens (Figure 80).

**Figure 80** Port List View, Learn by Ports page




**a** Click the ports through which you want the switch to learn MAC addresses, or click None.

**b** If you want that port to no longer learn MAC addresses, click the checked box to clear it.

**c** Click Submit.

**5** In the MAC Security Table section, choose Enabled in the Current Learning Mode column of the Learn By Ports row.

**6** Click Submit.

**Note:** You cannot include any of the port values you have chosen for the secure ports field.

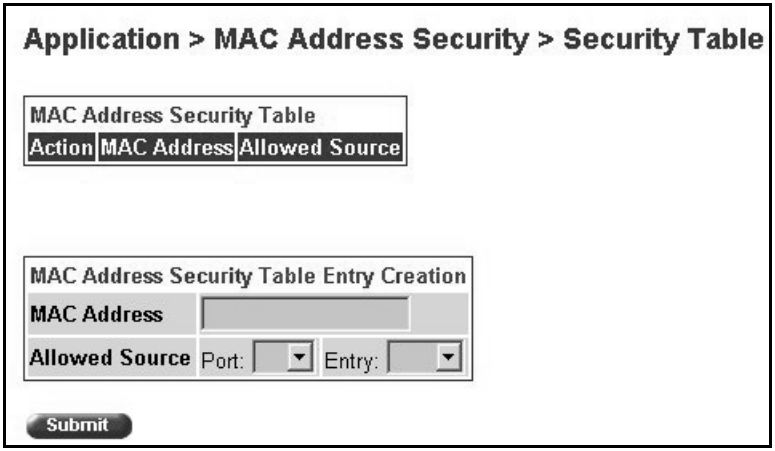
## Adding MAC addresses

To add MAC address to the MAC address-based security system:

**1** In the Web-based management main menu, choose Applications > MAC Address Security > Security Table.

It may take a few moments for the required addresses to be learned. Then, the Security Table page opens (Figure 81 on page 239).

**Figure 81** Security Table Page




**Note:** Using this page, you instruct the switch to allow the specified MAC address access *only* through the specified port or port list.

Table 107 describes the fields on the Security Table page.

**Table 107** Security Table page fields

| Section | Field | Range | Description |
|---|---|---|---|
| MAC Address Security Table | Action | | Allows you to delete a MAC address. |
| | MAC Address | | Displays the MAC address. |
| | Allowed Source | (1) Unit/Port<br>(2) Entry | Displays the entry through which the MAC address is allowed. |
| MAC Address Security Table Entry Creation | MAC Address | | Enter the MAC address you want to allow to access the switch. |
| | Allowed Source | | Select the unit and port through which the MAC address is allowed. |
| | Entry | | Select the port list through which the MAC address is allowed. |

2 Complete the fields as described in Table 107.

**Note:** If you choose an Entry as the Allowed Source, you must have configured that specific entry on the Port View List, Port List page.

3 On the Security Table page, type the required information in the fields, or select from a list.

4 Click Submit.

**Note:** Be certain to include the MAC address for the default LAN router as an allowed source MAC address.

## Clearing ports

You can clear all information from the specified port or ports that learn MAC addresses. If Learn by Ports is enabled, the specified ports begin again to learn the MAC addresses.

To clear information from selected ports:

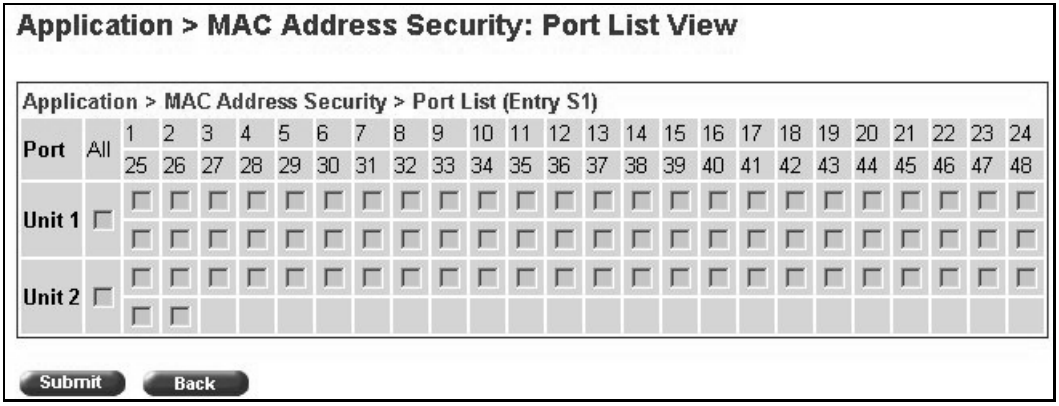
1 From the Web-based management main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 77 on page 233).

2 In the MAC Security Table section, click the icon in the Action column of the Clear By Ports row.

The Port List View, Clear by Ports page opens (Figure 82 on page 241).

**Figure 82** Port List View, Clear by Ports page




**3** Select the ports you want to clear, or click None.

**4** Click Submit.

---

**Note:** When you specify a port (or ports) to be cleared using this field, the specific port (or ports) are cleared for each of the entries listed in the MAC Address Security Table. If you totally clear the allowed Source Port field (leaving a blank field) for an entry, the associated MAC address for that entry is also cleared.

---

## Enabling security on ports

To enable or disable MAC address-based security on the port:

**1** From the Web-based management main menu, choose Application > MAC Address Security > Port Configuration.

The Port Configuration page opens (Figure 83 on page 242).

**Figure 83** Port Configuration page

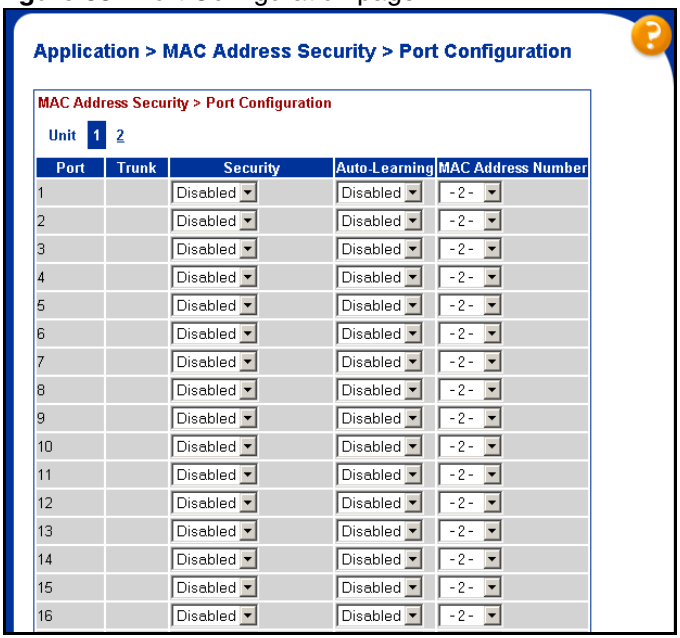



Table 108 describes the fields on the Port Configuration page.

**Table 108** Port Configuration page fields

| Field | Range | Description |
|---|---|---|
| Unit | 1 to 8 | Displays the unit number of the ports shown in the table. |
| Port | 1 to 26 for 470-24T<br>and<br>1 to 48 for 470-48T | Lists each port on the unit. |
| Trunk | Blank, 1 to 6 | Displays the MultiLink Trunk that the port belongs to. |
| Security | (1) Enabled<br>(2) Disabled | Enables MAC address-based security on that port.<br><br>Note: You must configure the port for MAC address-based security before enabling the security. |
| Auto Learning | (1) Enabled<br>(2) Disabled | Enables Auto-Learning for MAC address-based security on that port. |
| Mac Address Number | 1-25 | Sets the maximum number of addresses stored in the MAC Security Table for each port. |

## Deleting ports

You can delete ports from the security system in a variety of ways:

- In the Ports List View, Port List page (Figure 79 on page 237), click the check mark of a selected port to delete that port from the specified port list.
- In the Ports List View, Learn by Ports page (Figure 80 on page 237), click the check mark of a selected port to remove that port from those that learn MAC addresses.
- In the Port Configuration page (Figure 83 on page 242), click Disabled to remove that port from the MAC address-based security system; this action disables all MAC address-based security on that port.

## Filtering MAC destination addresses

To drop all packets from a specified MAC destination address (DA):

1. From the Web-based management main menu, choose Application > MAC Address Security > DA MAC Filtering.

   The DA MAC Filtering page opens (Figure 84).

**Figure 84** DA MAC Filtering page

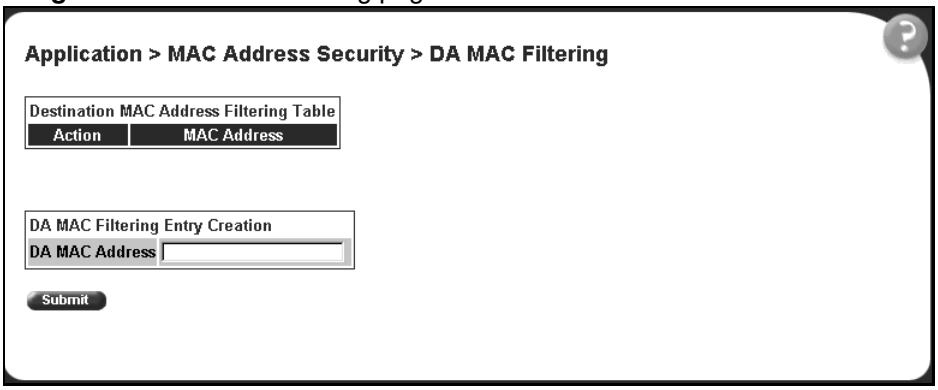


Table 109 describes the fields on the DA MAC Filtering page.

**Table 109** DA MAC Filtering page fields

| Section | Field | Range | Description |
|---|---|---|---|
| Destination MAC Address Filtering Table | Action | | Allows you to delete a MAC DA you are filtering. |
| | MAC Address | 1 -10 | Displays list of MAC DAs you want filtered. |
| DA MAC Filtering Entry Creation | DA MAC Address | XX:XX:XX:XX:XX:XX | Enter the MAC DA you want to filter. |

**Note:** Ensure that you do not enter the MAC address of the management station.

2 In the DA MAC Filtering Entry Creation area, enter the MAC DA you want to filter.

You can list up to 10 MAC DAs to filter.

3 Click Submit.

The system returns you to the DA MAC Filtering page (Figure 84 on page 243) with the new DA listed in the table.

## Deleting MAC DAs

To delete a MAC DA:

1 From the Web-based management main menu, choose Application > MAC Address Security > DA MAC Filtering.

The DA MAC Filtering page opens (Figure 84 on page 243).

2 In the Destination MAC Address Filtering Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the target parameter configuration.
- Click Cancel to return to the table without making changes.

# Configuring SNMP

Simple Network Management Protocol (SNMP) is the standard for network management that uses a common software agent to manage local and wide-area network equipment from different vendors; part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and defined in RFC1157. SNMPv1 is version one, or the original standard protocol. SNMPv3 is a combination of proposal updates to SNMP, most of which deal with security.

This section contains the following topics:



# Configuring SNMPv1

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

To configure the community string, trap mode, and Autotopology settings and features:

1 From the Web-based management main menu, choose Configuration > SNMPv1.

The SNMPv1 page opens (Figure 85 on page 246).

**Figure 85** SNMPv1 page

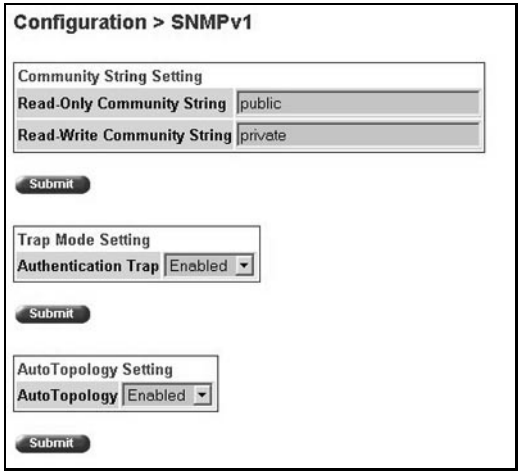



Table 110 describes the fields on the SNMPv1 page.

**Table 110** SNMPv1 page fields

| Section | Field | 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.<br><br>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.<br><br>The default value is private. |
| Trap Mode Setting | Authentication Trap | (1) Enable<br>(2) Disable | Choose to enable or disable the authentication trap. |
| AutoTopology Setting | AutoTopology | (1) Enable<br>(2) Disable | Choose to enable or disable the autotopology feature. |

**2** Type the required information in the text boxes, or select from a list.

**3** Click Submit in any section to save your changes.

# Configuring SNMPv3

This section describes the steps to build and manage SNMPv3 in the Web-based management user interface. It contains the following topics:



## Viewing SNMPv3 system information

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

To view SNMPv3 system information:

1. From the Web-based management main menu, choose Configuration > SNMPv3 > System Information.

   The System Information page opens (Figure 86 on page 248).

**Figure 86** System Information page

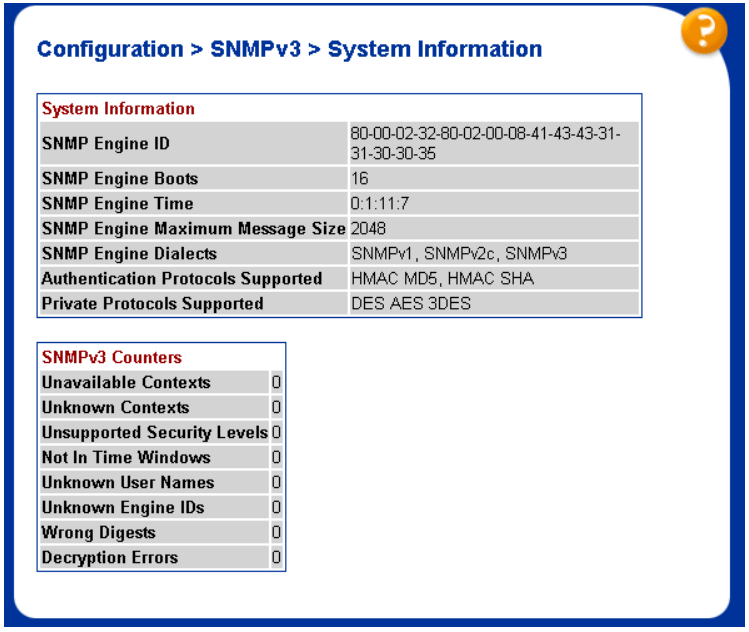



Table 111 describes the fields on the System Information section of the SNMPv3 System Information page.

**Table 111** SNMPv3 System Information section fields

| Field | Description |
|---|---|
| SNMP Engine ID | The SNMP engine identification number. |
| SNMP Engine Boots | The number of times that the SNMP engine has re-initialized itself since its initial configuration. |
| SNMP Engine Time | The number of seconds since the SNMP engine last incremented the snmpEngineBoots object. |
| SNMP Engine Maximum Message Size | The maximum length, in octets, of an SNMP message which this SNMP engine can send or receive and process determined as the minimum of the maximum message size values supported among all transports available to and supported by the engine. |
| SNMP Engine Dialects | The SNMP dialect the engine recognizes. The dialects are:SNMP1v1, SNMPv2C, and SNMPv3. |
| Authentication Protocols Supported | The registration point for standards-track authentication protocols used in SNMP Management Frameworks. The registration points are: None, HMAC MD5, HMAC SHA. |
| Private Protocols Supported | The registration point for standards-track privacy protocols used in SNMP Management Frameworks. The registration points are: None or CBC-DES. |

Table 112 describes the fields on the SNMPv3 Counters section of the SNMPv3 System Information page.

**Table 112** SNMPv3 Counters section fields

| Field | Description |
|---|---|
| Unavailable Contexts | The total number of packets dropped by the SNMP engine because the context contained in the message was unavailable. |
| Unknown Contexts | The total number of packets dropped by the SNMP engine because the context contained in the message was unknown. |
| Unsupported Security Levels | The total number of packets dropped by the SNMP engine because they requested a security level that was unknown to the SNMP engine or otherwise unavailable. |
| Not in Time Windows | The total number of packets dropped by the SNMP engine because they appeared outside of the authoritative SNMP engine's window. |
| Unknown User Names | The total number of packets dropped by the SNMP engine because they referenced an unknown user. |
| Unknown Engine IDs | The total number of packets dropped by the SNMP engine because they referenced an snmpEngineID that was not known to the SNMP engine. |
| Wrong Digests | The total number of packets dropped by the SNMP engine because they did not contain the expected digest value. |
| Decryption Errors | The total number of packets dropped by the SNMP engine because they could not be decrypted. |

## Configuring user access to SNMPv3

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

### Creating an SNMPv3 system user configuration

To create an SNMPv3 system user configuration:

1 From the Web-based management main menu, choose Configuration > SNMPv3 > User Specification.

The User Specification page opens (Figure 87 on page 250).

**Figure 87** User Specification page

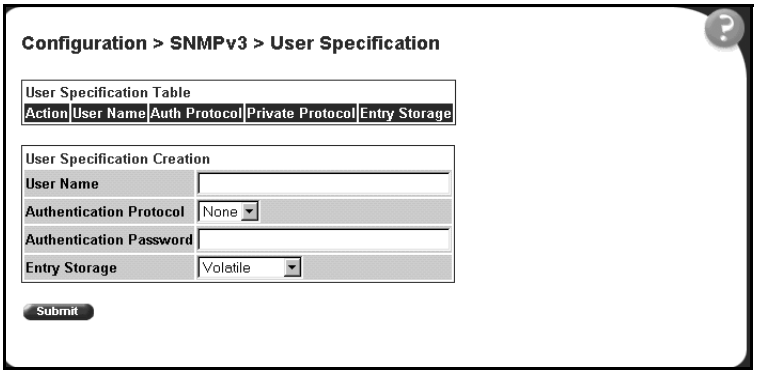



Table 113 describes the fields on the User Specification Table section of the User Specification page.

**Table 113** User Specification Table section fields

| Field and MIB association | Description |
|---|---|
| | Deletes the row. |
| User Name (usmUserSecurityName) | The name of an existing SNMPv3 user. |
| Authentication Protocol (usmUserAuthProtocol) | Indicates whether the message sent on behalf of this user to/from the SNMP engine identified by UserEngineID can be authenticated by the MD5 or SHA authentication protocol. |
| Private Protocol (usmUserPrivProtocol) | Displays whether 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 used. |
| Entry Storage | The current storage type for this row. If you select Volatile, information is dropped (lost) when you turn the power off. If you select Non-volatile, information is saved in NVRAM when you turn the power off |

Table 114 describes the fields on the User Specification Creation section of the User Specification page.

**Table 114** User Specification Creation section fields

| Field and MIB association | Range | Description |
|---|---|---|
| User Name (usmUserSecurityName) | 1..32 | Type a string of characters to create an identity for the user. |
| Authentication Protocol (usmUserAuthProtocol) | None<br>MD5<br>SHA | Choose whether the message sent on behalf of this user to or from the SNMP engine identified by UserEngineID can be authenticated with either the MD5 or SHA protocol. |
| Authentication Password (usmUserAuthPassword) | 1..32 | Type a string of character to create a password to use in conjunction with the authorization protocol. |
| Entry Storage (usmUserStorageType) | (1) Volatile<br>(2) Non-Volatile | Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off. |

**2** In the User Specification Creation section, type the required information in the fields, or select from a list.

**3** Click Submit.

The new configuration is displayed in the User Specification Table (Figure 87 on page 250).

## Deleting an SNMPv3 system user configuration

To delete an existing SNMPv3 user configuration:

**1** From the Web-based management main menu, choose Configuration > SNMPv3 > User Specification.

The User Specification page opens (Figure 87 on page 250).

**2** In the User Specification Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

**3** Do one of the following:

- Click Yes to delete the SNMPv3 user configuration.

- Click Cancel to return to the User Specification page without making changes.

## Configuring an SNMPv3 system user group membership

You can view a table of existing SNMPv3 group membership configurations and map or delete an SNMPv3 user to a group configuration.

### Mapping an SNMPv3 system user to a group

To map an SNMPv3 system user to a group:

1 From the Web-based management main menu, choose Configuration > SNMPv3 > Group Membership.

The Group Membership page opens (Figure 88).

**Figure 88** Group Membership page

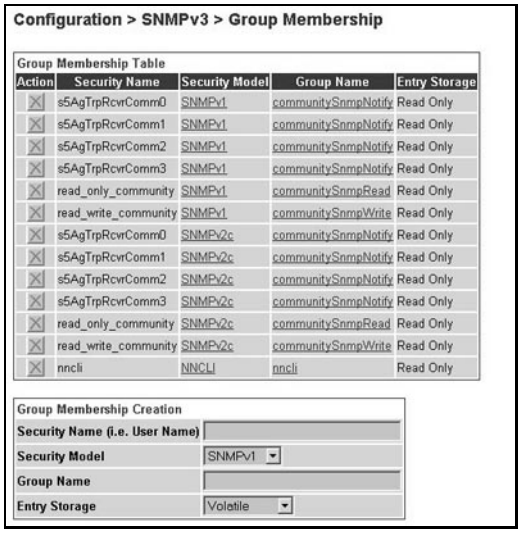


Table 115 describes the fields on the Group Membership page.

**Table 115** Group Membership page fields

| Field and MIB association | Range | Description |
|---|---|---|
| | | Deletes the row. |
| Security Name (vacmSecurityToGroupStatus) | 1..32 | Type a string of character to create a security name for the principal which is mapped by this entry to a group name. |
| Security Model (vacmSecurityToGroupStatus) | (1) SNMPv1<br>(2) SNMPv2c<br>(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<br>(2) Non-Volatile | Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off. |

2 In the Group Membership Creation section, type the required information in the fields, or select from a list.

3 Click Submit.

The new entry appears in the Group Membership Table.

## Deleting an SNMPv3 group membership configuration

To delete an SNMPv3 group membership configuration:

1 From the Web-based management main menu, choose Configuration > SNMPv3 > Group Membership.

The Group Membership page opens (Figure 88 on page 252).

2 In the Group Membership Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the group membership configuration.
- Click Cancel to return to the Group Membership page without making changes.

**Note:** This Group Membership Table section of the Group Membership page contains hyperlinks to the SNMPv3 User Specification and Group Access Rights pages. For more information about these pages, see "Configuring user access to SNMPv3" on page 249 and "Configuring SNMPv3 group access rights" on page 255.

# Configuring SNMPv3 group access rights

You can view a table of existing SNMPv3 group access rights configurations, and you can create or delete a group's SNMPv3 system-level access rights.

## Creating an SNMPv3 group access rights configuration

To create a group's SNMPv3 system-level access right configuration:

1 From the Web-based management main menu, choose Configuration > SNMPv3 > Group Access Rights.

The Group Access Rights page opens (Figure 89).

**Figure 89** Group Access Rights page

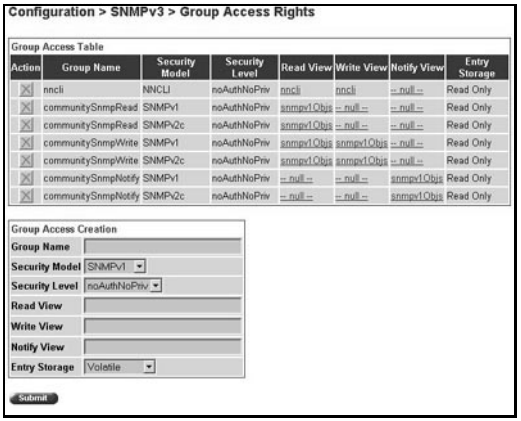



Table 116 describes the fields on the Group Access Rights page.

**Table 116** Group Access Rights page fields

| Field and MIB association | Range | Description |
|---|---|---|
| ✕ | | Deletes the row. |
| Group Name (vacmAccessToGroupStatus) | 1..32 | Type a character string to specify the group name to which access is granted. |
| Security Model (vacmAccessSecurityModel)l | (1) SNMPv1<br>(2) SNMPv2c<br>(3) USM | Choose the security model to which access is granted. |

**Table 116** Group Access Rights page fields (Continued)

| Field and MIB association | Range | Description |
|---|---|---|
| Security Level (vacmAccessSecurityLevel) | (1) noAuthNoPriv<br>(2) authNoPriv | Choose the minimum level of security required in order to gain the access rights allowed to the group. |
| 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<br>(2) Non-Volatile | Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off. |

2 In the Group Access Creation section, type the required information in the fields, or select from a list.

3 Click Submit.

The new entry appears in the Group Access Table.

## Deleting an SNMPv3 group access rights configuration

To delete an SNMPv3 group access configuration:

1 From the Web-based management main menu, choose Configuration > SNMPv3 > Group Access Rights.

The Group Access Rights page opens (Figure 89 on page 255).

2 In the Group Access Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the group access configuration.
- Click Cancel to return to the Group Access Rights page without making changes.

**Note:** This Group Access Table section of the Group Access Rights page contains hyperlinks to the Management Information View page. For more information, see "Configuring an SNMPv3 management information view" on page 257.

## Configuring an SNMPv3 management information view

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

**Note:** A view can consist of multiple entries in the table, each with the same view name, but a different view subtree.

### Creating an SNMPv3 management information view configuration

To create an SNMPv3 management information view configuration:

1 From the Web-based management main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information View page opens (Figure 90 on page 258).

**Figure 90** Management Information View page

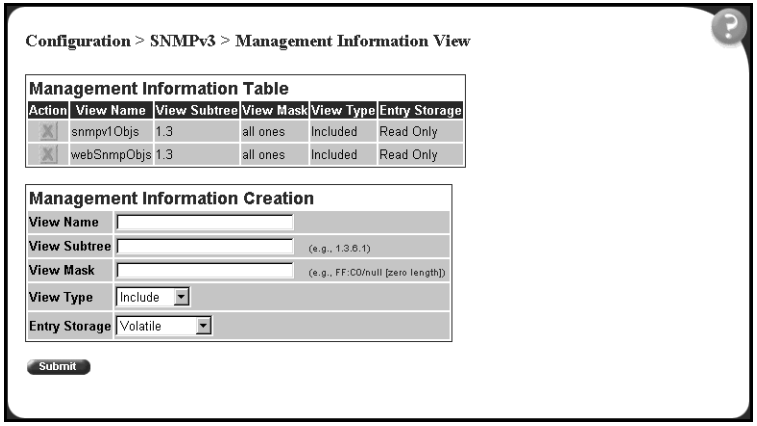



Table 117 describes the fields on the Management Information View page.

**Table 117** Management Information View page fields

| Field and MIB association | Range | Description |
|---|---|---|
| | | Deletes the row. |
| View Name (vacmViewTreeFamilyViewName) | 1..32 | Type a character string to create a name for a family of view subtrees. |
| View Subtree (vacmViewTreeFamilySubtree) | X.X.X.X.X... | Type an object identifier (OID) to specify the MIB subtree which, when combined with the corresponding instance of vacmViewTreeFamilyMask, defines a family of view subtrees.<br><br>Note: If no OID is entered and the field is blank, a default mask value consisting of “1s” is recognized. |
| View Mask (vacmViewTreeFamilyMask) | Octet String (0..16) | Type the bit mask which, in combination with the corresponding instance of vacmViewFamilySubtree, defines a family of view subtrees. |
| View Type (vacmViewTreeFamilyType) | (1) Included<br>(2) Excluded | Choose to include or exclude a family of view subtrees. |
| Entry Storage (vacmSecurityToGroupStorageType) | (1) Volatile<br>(2) Non-Volatile | Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off. |

2 In the Management Information Creation section, type the required information in the fields, or select from a list.

3 Click Submit.

The new entry appears in the Management Information Table (Figure 90 on page 258).

### Deleting an SNMPv3 management information view configuration

To delete an existing SNMPv3 management information view configuration:

1 From the Web-based management main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information View page opens (Figure 90 on page 258).

2 In the Management Information Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the management information view configuration.
- Click Cancel to return to the table without making changes.

## Configuring an SNMPv3 system notification entry

You can view a table of existing SNMPv3 system notification configurations, and you can configure specific SNMPv3 system notification types with particular message recipients and delete SNMPv3 notification configurations.

### Creating an SNMPv3 system notification configuration

To create an SNMPv3 system notification configuration:

1 From the Web-based management main menu, choose Configuration > SNMPv3 > Notification.

The Notification page opens (Figure 91 on page 260).

**Figure 91** Notification page

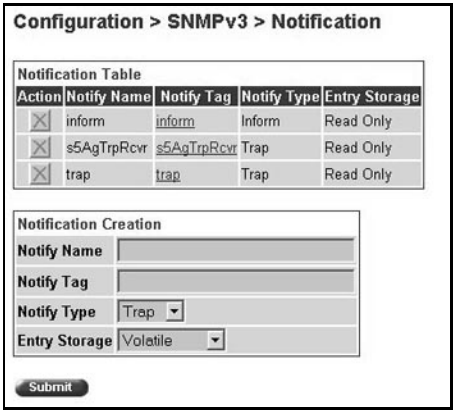



Table 118 describes the fields on the Notification page.

**Table 118** Notification page fields

| Field and MIB association | Range | Description |
|---|---|---|
| | | Deletes the row. |
| Notify Name (snmpNotifyRowStatus) | 1..32 | Type a character string to identify the entry. |
| Notify Tag (snmpNotifyTag) | 1..32 | Type a value which to use to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object carries a zero length, no entries are selected |
| Notify Type (snmpNotifyType) | (1) Trap<br>(2) Inform | Choose the type of notification to generate. |
| Entry Storage (snmpNotifyStorageTyp e) | (1) Volatile<br>(2) Non-Volatile | Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off. |

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

**3** Click Submit.

The new entry appears in the Notification Table (Figure 91 on page 260).

**Note:** This Notification Table section of the Notification page contains hyperlinks to the Target Parameter page. For more information, see "Configuring an SNMPv3 management target parameter" on page 264.

### Deleting an SNMPv3 system notification configuration

To delete an SNMPv3 notification configuration:

1. From the Web-based management main menu, choose Configuration > SNMPv3 > Notification.

   The Notification page opens (Figure 91 on page 260).

2. In the Notification Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the notification configuration.
   - Click Cancel to return to the table without making changes.

## Configuring an SNMPv3 management target address

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

### Creating an SNMPv3 target address configuration

To create an SNMPv3 target address configuration:

1. From the Web-based management main menu, choose Configuration > SNMPv3 > Target Address.

   The Target Address page opens (Figure 92 on page 262).

**Figure 92** Target Address page

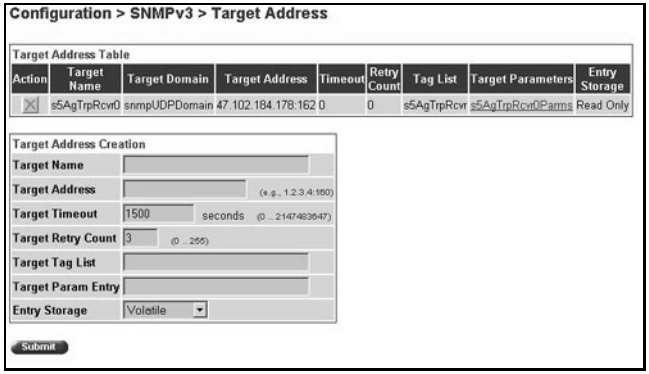



Table 119 describes the fields on the Target Address page.

**Table 119** Target Address page fields

| Field and MIB association | Range | Description |
|---|---|---|
|  | | Deletes the row. |
| Target Name (snmpTargetAddrName) | 1..32 | Type a character string to create a target name. |
| Target Domain (snmpTargetAddrTDomain) | 1..32 | The transport type of the address contained in the snmpTargetAddrTAddress object. |
| Target Address (snmpTargetAddrTAddress) | XXX.XXX.XXX.XXX:XXX | Type a transport address in the format of an IP address, colon, and UDP port number.<br><br>For example: 10.30.31.99:162 (see Figure 92 on page 262). |
| 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 re-sending the “Inform” notification. |
| Target Retry Count (snmpTargetAddrRetryCount) | 0..255 | Type the default number of retires to be attempted when a response is not received for a generated message. An application may 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. |

**Table 119** Target Address page fields

| Field and MIB association | Range | Description |
|---|---|---|
| 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 to be sent to this transport address |
| Entry Storage | (1) Volatile<br>(2) Non-Volatile | Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off. |

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

**3** Click Submit.

The new entry appears in the Target Address Table (Figure 92 on page 262).

**Note:** This Target Address Table section of the Target Address page contains hyperlinks to the Target Parameter page. For more information, see "Configuring an SNMPv3 management target parameter" on page 264.

## Deleting an SNMPv3 target address configuration

To delete an SNMPv3 target address configuration:

**1** From the Web-based management main menu, choose Configuration > SNMPv3 > Target Address.

The Target Address page opens (Figure 92 on page 262).

**2** In the Target Address Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

**3** Do one of the following:

- Click Yes to delete the target address configuration.

- Click Cancel to return to the table without making changes.

## Configuring an SNMPv3 management target parameter

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

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

To create an SNMPv3 target parameter configuration:

1 From the Web-based management main menu, choose Configuration > SNMPv3 > Target Parameter.

The Target Parameter page opens (Figure 93).

**Figure 93** Target Parameter page

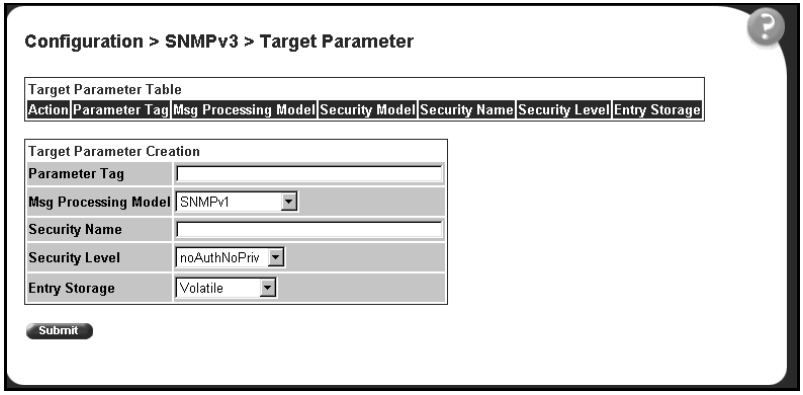


Table 120 describes the fields on the Target Parameter page.

**Table 120** Target Parameter page fields

| Field | Range | Description |
|---|---|---|
| | | Deletes the row. |
| Parameter Tag (snmpTargetParamsRowStatus) | 1..32 | Type a unique character string to identify the parameter tag. |
| Msg Processing Model (snmpTargetParamsMPModel) | (0) SNMPv1<br>(1) SNMPv2c<br>(2) SNMPv2*<br>(3) SNMPv3 / USM | Choose the message processing model to be used when generating SNMP messages using this entry. |
| Security Name (snmpTargetParamsSecuirtyName) | 1..32 | Type the principal on whose behalf SNMP messages are generated using this entry |
| Security Level (snmpTargetParamsSecuirtyLevel) | (1) noAuthNoPriv<br>(2) authNoPriv | Choose the level of security to be used when generating SNMP messages using this entry |
| Entry Storage (snmpTargetParamsStorageType) | (1) Volatile<br>(2) Non-Volatile | Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off. |

2 In the Target Parameter Creation section, type the required information in the fields, or select from a list.

3 Click Submit.

The new entry appears in the Target Parameter Table (Figure 93 on page 264).

## Deleting an SNMPv3 target parameter configuration

To delete an SNMPv3 target parameter configuration:

1 From the Web-based management main menu, choose Configuration > SNMPv3 > Target Address.

The Target Address page opens (Figure 92 on page 262).

2 In the Target Parameter Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

**3** Do one of the following:

- Click Yes to delete the target parameter configuration.
- Click Cancel to return to the table without making changes.

# Configuring SNMP traps

You can configure the IP address and community string for a new SNMP trap receiver, view a table of existing SNMP trap receiver configurations, or delete an existing SNMP trap receiver configuration(s).

**Note:** The SNMP Trap Receiver Table is an alternative to using the SNMPv3 Target Table and SNMPv3 Parameter Table. However, only SNMPv1 traps are configurable using this table.

## Creating an SNMP trap receiver configuration

To create an SNMP trap receiver configuration:

1 From the Web-based management main menu, choose Configuration > SNMP Trap.

The SNMP Trap Receiver page opens (Figure 94).

**Figure 94** SNMP Trap Receiver page

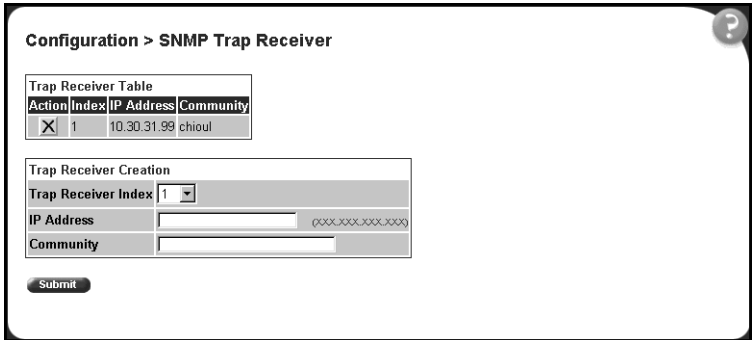


Table 121 describes the fields on the Trap Receiver Table and Trap Receiver Creation sections of the SNMP Trap Receiver page.

**Table 121** SNMP Trap Receiver page fields

| Fields | Range | Description |
|---|---|---|
| | | Deletes the row. |
| Trap Receiver Index | 1..4 | Choose the number of the trap receiver to create or modify. |
| IP Address | XXX.XXX.XXX.XXX | Type the network address for the SNMP manager that is to receive the specified trap. |
| Community | 0..32 | Type the community string for the specified trap receiver. |

2 In the Trap Receiver Creation section, specify the information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Trap Receiver Table (Figure 94 on page 267).

## Deleting an SNMP trap receiver configuration

To delete SNMP trap receiver configurations:

1 From the Web-based management main menu, choose Configuration > SNMP Trap.

The SNMP Trap Receiver page opens (Figure 94 on page 267).

2 In the Trap Receiver Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the SNMP trap receiver configuration.
- Click Cancel to return to the table without making changes.

# Appendix A
# SNMP Support

## SNMP MIB support for Ethernet Switches 460 and 470

The Ethernet Switches 460 and 470 support a Simple Network Management Protocol (SNMP) agent with industry-standard Management Information Bases (MIB), as well as private MIB extensions, which ensures compatibility with existing network management tools.

Table 122 lists supported SNMP MIBs for the Ethernet Switches 460 and 470.

**Table 122** SNMP MIB support for Ethernet Switches 460 and 470

| Application | Standard MIBs | Proprietary MIBs |
|---|---|---|
| SNMPv2-SMI | rfc2578.mib | |
| SNMPv2-TC | rfc2579.mib | |
| SNMP-FRAMEWORK MIB | rfc3411.mib | |
| IANAifType MIB | ianaIfType.mib | |
| IP MIB | rfc2011.mib | |
| TCP MIB | rfc2012.mib | |
| UDP MIB | rfc2013.mib | |
| SNMP-MPD MIB | rfc3412.mib | |
| SNMP-TARGET MIB | rfc3413-tgt.mib | |
| SNMP-NOTIFICATION MIB | rfc3413-notif.mib | |
| SNMP-USER-BASED-SM MIB | rfc3414.mib | |
| SNMP-VIEW-BASED-ACM MIB | rfc3415.mib | |
| SNMPv2 MIB | rfc3418.mib | |

**Table 122** SNMP MIB support for Ethernet Switches 460 and 470

| Application | Standard MIBs | Proprietary MIBs |
|---|---|---|
| IF MIB | rfc2863.mib | |
| EtherLike MIB | rfc2665.mib | |
| BRIDGE MIB (MIB for IEEE 802.1D devices) | draft-ietf-bridge-bridgemib-smiv2-05.txt | |
| Entity MIB | rfc2737.mib | |
| SNMP-Community MIB | rfc2576.mib | |
| INET-Address MIB | rfc3291.mib | |
| COPS-Client MIB | rfc2940.mib | |
| RMON MIB | rfc2819.mib | |
| Token-Ring-RMON MIB | rfc1513.mib | |
| RMON2 MIB | rfc2021.mib | |
| P-Bridge MIB | rfc2674-p.mib | |
| Q-Bridge MIB | rfc2674-q.mib | |
| Integrated-Services MIB | rfc2213.mib | |
| DiffServ-DSCP-TC | rfc3289tc.mib | |
| DiffServ MIB | rfc3289.mib | |
| MIB-II | rfc1213.mib | |
| SNMP-USM-AES MIB | rfc3826.mib | |
| IEEE8021-PAE MIB | eapol-d10.mib | |
| IEEE8023-LAG MIB | ieee8023-lag.mib | |
| Synoptics-ROOT MIB | | synro.mib |
| S5-ROOT MIB | | s5roo.mib |
| S5-TCS MIB | | s5tcs.mib |
| S5-Agent MIB | | s5age.mib |
| S5-Chassis MIB | | s5cha.mib |
| S5-ETH-MULTISEG-Topology MIB | | s5emt.mib |
| BN-IF-Extensions MIB | | s5ifx.mib |
| S5-REG MIB | | s5reg.mib |
| S5-Switch-BaySecure MIB | | s5sbs.mib |
| S5-Ethernet MIB | | s5eth.mib |
| S5-Ethernet-Common MIB | | s5ecm.mib |

**Table 122** SNMP MIB support for Ethernet Switches 460 and 470

| Application | Standard MIBs | Proprietary MIBs |
|---|---|---|
| S5-Ethernet-Redundant-Links MIB | | s5erl.mib |
| S5-Chassis-Trap MIB | | s5ctr.mib |
| S5-Ethernet-Trap MIB | | s5etr.mib |
| BN-Log-Message MIB | | bnlog.mib |
| Rapid-City | | rapidCity.mib |
| RC-Bridge MIB | | rcBridge.mib |
| RC-MLT MIB | | rcMlt.mib |
| RC-Port MIB | | rcPort.mib |
| RC-VLAN MIB | | rcVlan.mib |
| Policy-Framework-PIB | pibFramework.mib | |
| QoS-Policy-IP-PIB | pibIp.mib | |
| QoS-Policy-802-PIB | pib802.mib | |
| NTN-QoS-Policy-EXT-PIB | | pibNtn.mib |
| NTN-QoS-Policy-EVOL-PIB | | pibNtnEvol.mib |
| NTN-QoS-Policy-AUX MIB | | mibNtnQos.mib |
| Baystack-Notifications MIB | | bsn.mib |
| Baystack-EAPOL-Extension MIB | | bsee.mib |
| Baystack-LACP-Ext MIB | | bayStackLacpExt.mib |
| Baystack-ADAC MIB | | bayStackAdac.mib |
| Nortel-Networks-Rapid-Spanning-Tree MIB | | nnrst.mib |
| Nortel-Networks-Multiple-Spanning-Tree MIB | | nnmst.mib |
| **Additional MIBs supported by SSH-enabled image:** | | |
| Rapid-City-Baystack | | bayxlr.mib |
| **Additional MIBs supported by Ethernet Switch 460-24T PWR** | | |
| Baystack-PETH-Ext MIB | | bayStackPethExt.mib |
| Power-Ethernet MIB | rfc3621.mib | |

# SNMP trap support

Table 123 lists supported SNMP traps for the Ethernet Switch 460.

**Table 123** Supported SNMP traps for Ethernet Switch 460

| Trap name | Configurable | Sent when |
|---|---|---|
| **RFC 1215 (industry standard):** | | |
| linkUp | Per port | A port's link state changes to up. |
| linkDown | Per port | A port's link state changes to down. |
| authenticationFailure | System wide | There is an SNMP authentication failure. |
| coldStart | Always on | The system is powered on. |
| warmStart | Always on | The system restarts due to a management reset. |
| **pethMIB (industry standard):** | | |
| pethPsePortOnOffTrap | Per unit | Power to a port goes on or off. |
| pethPsePortCurrentStatusTrap | Per unit | A port's power status changes. |
| pethMainPowerUsageOnTrap | Per unit | Power use surpasses the configured power usage threshold. |
| pethMainPowerUsageOffTrap | Per unit | Power use returns below the configured power usage threshold. |
| **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 | An assigned base unit fails. |
| s5EtrSbsMacAccessViolation | Always on | A MAC address violation is detected. |
| bsnLoginFailure | Always on | A login attempt fails due to a user/password mismatch. |

Table 124 lists supported SNMP traps for the Ethernet Switch 470-24T.

**Table 124** Supported SNMP traps for Ethernet Switch 470-24T

| Trap name | Configurable | Sent when |
|---|---|---|
| **RFC 1215 (industry standard):** | | |
| linkUp | Per port | A port's link state changes to up. |
| linkDown | Per port | A port's link state changes to down. |
| authenticationFailure | System wide | There is an SNMP authentication failure. |
| coldStart | Always on | The system is powered on. |
| warmStart | Always on | The system restarts due to a management reset. |
| **s5CtrMIB (Nortel proprietary traps):** | | |
| s5CtrProblem | Always on | An assigned switch fails. (s5cir121.mib) |
| s5EtrSbsMacAccessViolation | Always on | A MAC address violation is detected. (s5etr113.mib) |
| bsnLoginFailure | Always on | A login attempt fails due to a user/password mismatch. |

Table 125 lists supported SNMP traps for the Ethernet Switch 470-48T.

**Table 125** Supported SNMP traps for Ethernet Switch 470-48T

| Trap name | Configurable | Sent when |
|---|---|---|
| **RFC 1215 (industry standard):** | | |
| linkUp | Per port | A port's link state changes to up. |
| linkDown | Per port | A port's link state changes to down. |
| authenticationFailure | System wide | There is an SNMP authentication failure. |
| coldStart | Always on | The system is powered on. |
| warmStart | Always on | The system restarts due to a management reset. |
| **s5CtrMIB (Nortel proprietary traps):** | | |
| s5CtrProblem | Always on | An assigned switch fails. (s5cir121.mib) |

**Table 125** Supported SNMP traps for Ethernet Switch 470-48T (Continued)

| Trap name | Configurable | Sent when |
|---|---|---|
| s5EtrSbsMacAccessViolation | Always on | A MAC address violation is detected. (s5etr113.mib) |
| bsnLoginFailure | Always on | A login attempt fails due to a user/password mismatch. |

# Index

## A



## B

## C



## D



## E

## F



## G



## H



## I



## K



## L

## M



## N

## O



## P

## Q



## R



## S

## T



## U



## V

## W