



NORTEL

Nortel Ethernet Routing Switch 2500 Series

Configuration — Security

Release: 4.3

Document Revision: 04.01

www.nortel.com

NN47215-505

Nortel Ethernet Routing Switch 2500 Series

Release: 4.3

Publication: NN47215-505

Document release date: 22 February 2010

Copyright © 2008-2010 Nortel Networks. All Rights Reserved.

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

THE SOFTWARE DESCRIBED IN THIS DOCUMENT IS FURNISHED UNDER A LICENSE AGREEMENT AND MAY BE USED ONLY IN ACCORDANCE WITH THE TERMS OF THAT LICENSE.

Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

Contents

Software license	13
New in this release	17
Features 17	
RADIUS Interim Accounting Updates support 17	
RADIUS Request use Management IP Address 18	
RADIUS password fallback configuration using EDM 18	
802.1X or NonEAP with VLAN names 18	
Extended IP Manager 18	
Other changes 18	
Enterprise Device Manager 18	
Introduction	21
NNCLI command modes 21	
Security fundamentals	23
Management password configuration 23	
Console/TELNET password Configuration 24	
User name and password 24	
Logging on 24	
MAC address-based security 25	
MAC address-based security autolearning 25	
RADIUS-based network security 26	
RADIUS password fallback 26	
RADIUS Interim Accounting Updates support 27	
RADIUS Request use Management IP Address 27	
Campus security example 28	
EAPOL-based security 30	
EAPOL Security Configuration 31	
EAPOL with Guest VLAN 31	
Advanced EAPOL features 32	
RADIUS-assigned VLAN use in MHMA mode 33	
Non-EAP IP Phone authentication 34	
Unicast EAP Requests in MHMA 34	
802.1X or non-EAP with VLAN names 34	

Non-EAP hosts on EAP-enabled ports	35
Non-EAPOL MAC RADIUS authentication	37
Multiple Host with Single Authentication	37
802.1X dynamic authorization extension (RFC 3576)	39
TACACS+	41
TACACS+ architecture	42
Feature operation	42
TACACS+ authentication	42
TACACS+ authorization	43
Changing privilege levels at run time	43
TACACS+ server configuration example	44
TACACS+ accounting	45
Feature limitations	45
TACACS+ configuration	46
IP Manager	46
Password security	47
Password length and valid characters	47
Password retry	47
Password history	47
Password display	47
Password verification	47
Password aging time	47
Read-Only and Read-Write passwords must be different	48
Applicable passwords	48
Enabling and disabling password security	48
Default passwords	48
HTTP port number change	49
Simple Network Management Protocol	49
SNMP Version 1 (SNMPv1)	49
Nortel Ethernet Routing Switch 2500 Series support for SNMP	50
SNMP MIB support	50
SNMP trap support	50
Secure Socket Layer protocol	51
Secure versus non-secure mode	52
DHCP snooping	52
DHCP binding table	53
Dynamic ARP inspection	54
IP Source Guard	54
Nortel Secure Network Access	56

Configuring and managing security using NNCLI	57
Setting the user name and password using NNCLI	58
username command	58
cli password command	59

Setting password security using NNCLI	60
password security command	60
no password security command	60
show password security command	61
password aging-time day command	61
show password aging-time day command	61
Configuring the number of password logon attempts	61
Changing the http port number using NNCLI	62
show http-port command	62
http-port command	62
default http-port	63
Setting Telnet access using NNCLI	63
show telnet-access command	64
telnet-access command	64
no telnet-access command	66
default telnet-access command	66
SSL configuration using NNCLI	67
Enabling SSL using NNCLI	67
Disabling SSL using NNCLI	67
Creating an SSL certificate using NNCLI	68
Deleting an SSL certificate using NNCLI	68
Viewing the SSL server configuration using NNCLI	69
Viewing the SSL certificate using NNCLI	70
Configuring Secure Shell using NNCLI	70
show ssh global command	71
show ssh session command	72
show ssh download-auth-key command	72
ssh dsa-host-key command	73
no ssh dsa-host-key command	73
ssh command	73
no ssh command	73
ssh secure command	74
ssh timeout command	74
ssh dsa-auth command	74
no ssh dsa-auth command	75
ssh pass-auth command	75
no ssh pass-auth command	75
ssh port command	75
ssh download-auth-key command	76
no ssh dsa-auth-key command	76
default ssh command	76
RADIUS Interim Accounting Updates support configuration using NNCLI	77
Configuring RADIUS Interim Accounting Updates support using NNCLI	77
Disabling RADIUS Interim Accounting Updates support using NNCLI	78

Configuring RADIUS Interim Accounting Updates support defaults using NNCLI	79
Viewing RADIUS Interim Accounting Updates support status using NNCLI	80
RADIUS Request use Management IP configuration using NNCLI	81
Enabling RADIUS Request use Management IP using NNCLI	81
Disabling RADIUS Request use Management IP using NNCLI	81
Viewing RADIUS Request use Management IP status using NNCLI	82
Configuring the RADIUS-based management password authentication using NNCLI	82
show radius-server command	83
radius-server command	83
no radius-server command	84
default radius-server command	84
radius-server password fallback command	84
802.1X dynamic authorization extension (RFC 3576) configuration using NNCLI	85
Configuring RADIUS dynamic authorization extension (802.1X RFC 3576) using NNCLI	85
Disabling RADIUS dynamic authorization extension (802.1X RFC 3576) using NNCLI	87
Viewing RADIUS dynamic authorization client configuration using NNCLI	87
Viewing RADIUS dynamic authorization client statistics using NNCLI	88
Enabling RADIUS dynamic authorization extension (802.1X RFC 3576) on a port using NNCLI	89
Disabling RADIUS dynamic authorization extension (802.1X RFC 3576) on a port using NNCLI	90
Viewing replay protection for RADIUS dynamic authorization extension using NNCLI	91
Disabling replay protection for RADIUS dynamic authorization extension using NNCLI	91
Enabling replay protection for RADIUS dynamic authorization extension using NNCLI	91
Setting SNMP parameters using NNCLI	92
Common SNMP and SNMPv3 NNCLI commands	92
snmp-server command	93
no snmp-server command	93
snmp-server notification-control authenticationFailure command	94
no snmp-server notification-control authenticationFailure command	94
default snmp-server notification-control authenticationFailure command	94
snmp-server community for read/write command	94
no snmp-server community command	95
default snmp-server community command	96
show snmp-server community command	97
snmp-server contact command	97
no snmp-server contact command	97

default snmp-server contact command 98
snmp-server location command 98
no snmp-server location command 98
default snmp-server location command 99
snmp-server name command 99
no snmp-server name command 99
default snmp-server name command 100
snmp trap link-status command 100
no snmp trap link-status command 101
default snmp trap link-status command 101
snmp-server notify-filter command 102
no snmp-server notify-filter command 103
show snmp-server notify-filter command 103
snmp-server notification-control command 104
no snmp-server notification-control command 104
NNCLI commands specific to SNMPv3 105
snmp-server user command 105
no snmp-server user command 107
snmp-server view command 108
no snmp-server view command 109
snmp-server host command 109
no snmp-server host command 111
default snmp-server host command 112
show snmp-server host command 112
snmp-server community command 113
show snmp-server command 114
snmp-server bootstrap command 115
Configuring MAC address filter-based security using NNCLI 116
show mac-security command 116
mac-security command 117
mac-security mac-address-table address command 119
mac-security security-list command 119
no mac-security command 120
no mac-security auto-learning aging-time command 120
no mac-security mac-address-table command 120
no mac-security security-list command 121
mac-security command for specific ports 121
mac-security mac-da-filter command 122
MAC address autolearning configuration using NNCLI 123
Configuring MAC address auto-learning aging time using NNCLI 123
Disabling MAC address auto-learning aging time using NNCLI 124
Configuring MAC address auto-learning aging time to default using
NNCLI 124
Configuring EAPOL-based security using NNCLI 124

-
- eapol command 125
 - eapol command for modifying parameters 125
 - eapol guest-vlan command 127
 - no eapol guest-vlan command 127
 - default eapol guest-vlan command 128
 - show eapol command 128
 - show eapol auth-diags interface command 130
 - show eapol auth-stats interface command 131
 - show eapol guest-vlan command 132
 - Configuring advanced EAPOL features using NNCLI 132
 - Configuring multihost support using NNCLI 132
 - Configuring support for non-EAPOL hosts on EAPOL-enabled ports using NNCLI 141
 - TACACS+ configuration using NNCLI 148
 - Configuring switch TACACS+ server settings using NNCLI 149
 - Disabling switch TACACS+ server settings using NNCLI 150
 - Enabling remote TACACS+ services using NNCLI 151
 - Enabling or disabling TACACS+ authorization using NNCLI 151
 - Configuring TACACS+ authorization privilege levels using NNCLI 152
 - Enabling or disabling TACACS+ accounting using NNCLI 153
 - Configuring the switch TACACS+ level using NNCLI 153
 - Viewing TACACS+ information using NNCLI 154
 - IP Manager configuration using NNCLI 154
 - Enabling IP Manager using NNCLI 154
 - Disabling IP Manager using NNCLI 155
 - Configuring the IP Manager list for IPv4 addresses using NNCLI 156
 - Configuring the IP Manager list for IPv6 addresses using NNCLI 157
 - Removing IP Manager list entries using NNCLI 157
 - Viewing the IP Manager configuration using NNCLI 158
 - DHCP snooping configuration using NNCLI 160
 - Enabling DHCP snooping globally using NNCLI 161
 - Disabling DHCP snooping globally using NNCLI 161
 - Enabling DHCP snooping on a VLAN using NNCLI 162
 - Disabling DHCP snooping on a VLAN using NNCLI 162
 - Configuring DHCP snooping port trust using NNCLI 163
 - Configuring DHCP snooping port trust to default using NNCLI 164
 - Viewing global DHCP snooping configuration information using NNCLI 164
 - Viewing VLAN DHCP snooping configuration information using NNCLI 165
 - Viewing DHCP snooping port trust information using NNCLI 165
 - Viewing the DHCP binding table using NNCLI 166
 - Dynamic ARP inspection configuration using NNCLI 166
 - Enabling dynamic ARP inspection on a VLAN using NNCLI 167
 - Disabling dynamic ARP inspection on a VLAN using NNCLI 167
 - Configuring dynamic ARP inspection port trust using NNCLI 168

Configuring dynamic ARP inspection port trust to default using NNCLI	169
Viewing VLAN dynamic ARP inspection configuration information using NNCLI	169
Viewing dynamic ARP inspection port trust information using NNCLI	170
IP Source Guard configuration using NNCLI	170
Enabling IP Source Guard using NNCLI	171
Viewing IP Source Guard port configuration information using NNCLI	172
Viewing IP Guard-allowed addresses using NNCLI	173
Disabling IP Source Guard using NNCLI	174

Configuring and managing security using Enterprise Device Manager **175**

EAPOL configuration using EDM	176
Configuring EAPOL globally using EDM	176
Configuring port-based EAPOL using EDM	178
Configuring advanced port-based EAPOL using EDM	180
Viewing Multihost status information using EDM	181
Viewing Multihost session information using EDM	182
Allowed non-EAP MAC address list configuration using EDM	183
Viewing port non-EAP host support status using EDM	184
Graphing port EAPOL statistics using EDM	185
Graphing port EAPOL diagnostics using EDM	187
TACACS+ configuration using EDM	189
Enabling TACACS+ accounting using EDM	189
Disabling TACACS+ accounting using EDM	190
Enabling TACACS+ authorization using EDM	190
Disabling TACACS+ authorization using EDM	191
Configuring the switch TACACS+ levels using EDM	191
Creating a TACACS+ server	192
Configuring general switch security using EDM	193
Security list configuration using EDM	195
Deleting specific ports from a security list using EDM	196
Deleting all ports from a security list using EDM	197
AuthConfig list configuration using EDM	198
Deleting entries from the AuthConfig list using EDM	199
Configuring MAC Address autolearn using EDM	199
Viewing AuthStatus information using EDM	201
Viewing AuthViolation information using EDM	202
Viewing MacViolation information using EDM	203
Web and Telnet password configuration using EDM	204
Configuring a Web and Telnet password for a switch using EDM	204
Configuring a Web and Telnet password for a stack using EDM	205
Console password configuration using EDM	205
Configuring a console password for a switch using EDM	206

Configuring a console password for a stack using EDM	206
Configuring the Secure Shell protocol using EDM	207
Viewing SSH Sessions information using EDM	209
Configuring SSL using EDM	209
RADIUS global configuration using EDM	211
Enabling RADIUS Request use Management IP using EDM	211
Disabling RADIUS Request use Management IP using EDM	211
Enabling RADIUS password fallback using EDM	212
Disabling RADIUS password fallback using EDM	212
RADIUS Server configuration using EDM	212
Configuring the RADIUS server using EDM	213
Viewing RADIUS Dynamic Authorization server information using EDM	214
802.1X dynamic authorization extension (RFC 3576) configuration using EDM	215
Viewing RADIUS Dynamic Server statistics using EDM	218
Configuring RADIUS Interim Accounting Updates support using EDM	219
DHCP snooping configuration using EDM	220
Configuring DHCP snooping globally using EDM	220
Configuring DHCP snooping on a VLAN using EDM	221
Configuring DHCP snooping port trust using EDM	222
Viewing the DHCP binding information using EDM	222
Dynamic ARP inspection configuration using EDM	223
Configuring dynamic ARP inspection on a VLAN using EDM	224
Configuring dynamic ARP inspection on a port using EDM	224
IP Source Guard configuration using EDM	225
Configuring IP Source Guard on a port using EDM	226
Filtering IP Source Guard addresses using EDM	227
SNMP configuration using EDM	228
Viewing SNMP information	229
Graphing SNMP statistics	230
Defining a MIB view	231
Configuring an SNMP user	232
Viewing SNMP user details	234
Configuring an SNMP community	234
Viewing SNMP community details	236
Configuring an SNMP host	236
Configuring SNMP host notification using EDM	237
Configuring SNMP notification control using EDM	238

Appendixes

241

TACACS+ server configuration examples	241
Configuration example: Cisco ACS (version 3.2) server	241
Configuration example: ClearBox server	246
Management Agent	254

SNMP trap support 255

Software license

This section contains the Nortel Networks software license.

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 MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

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

1. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer

software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

2. 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.
3. 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.
4. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
5. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
6. 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.

New in this release

The following sections detail what's new in *Nortel Ethernet Routing Switch 2500 Security—Configuration and Management* (NN47215-505) for Release 4.3.

- [“Features”](#) (page 17)
- [“Other changes”](#) (page 18)

Features

See the following sections for information about feature changes:

- [“RADIUS Interim Accounting Updates support”](#) (page 17)
- [“RADIUS Request use Management IP Address”](#) (page 18)
- [“RADIUS password fallback configuration using EDM”](#) (page 18)
- [“802.1X or NonEAP with VLAN names”](#) (page 18)
- [“Extended IP Manager”](#) (page 18)

RADIUS Interim Accounting Updates support

RADIUS Interim Accounting Updates support enhances network security by enabling the RADIUS server to make policy decisions based on real-time network attributes transmitted by the NAS. For more information, see:

- [“RADIUS Interim Accounting Updates support”](#) (page 27)
- [“RADIUS Interim Accounting Updates support configuration using NNCLI”](#) (page 77)
- [“Configuring RADIUS Interim Accounting Updates support using EDM”](#) (page 219)

RADIUS Request use Management IP Address

With RADIUS Request use Management IP Address, you can configure the switch to follow strict use of the Management IP address, when routing is enabled, to ensure that the switch uses the Management VLAN IP address as the source IP address for RADIUS. For more information, see:

- [“RADIUS Request use Management IP Address” \(page 27\)](#)
- [“RADIUS Request use Management IP configuration using NNCLI” \(page 81\)](#)
- [“Enabling RADIUS Request use Management IP using EDM” \(page 211\)](#)
- [“Disabling RADIUS Request use Management IP using EDM” \(page 211\)](#)

RADIUS password fallback configuration using EDM

The documenting of RADIUS password fallback in a previous release did not include procedures for configuring the feature using Device Manager. In this release, procedures for configuring RADIUS password fallback using EDM (EDM) have been documented. For more information, see:

- [“Enabling RADIUS password fallback using EDM” \(page 212\)](#)
- [“Disabling RADIUS password fallback using EDM” \(page 212\)](#)

802.1X or NonEAP with VLAN names

The Ethernet Routing Switch 2500 can match RADIUS assigned VLANs based on either the VLAN number or a VLAN name. For more information, see [“802.1X or non-EAP with VLAN names” \(page 34\)](#).

Extended IP Manager

With Release 4.3, the function of the existing IP Manager feature is extended to include IPv6 source IP addresses. For more information, see:

- [“IP Manager” \(page 46\)](#)
- [“IP Manager configuration using NNCLI” \(page 154\)](#)

Other changes

See the following sections for information about changes that are not feature-related:

Enterprise Device Manager

Enterprise Device Manager (EDM) replaces both the Java-based Device Manager and Web-based management user interfaces. EDM is an embedded element management and configuration application

for Ethernet Routing Switch 2500 Series switches. EDM provides a Web-based graphical user interface through a standard web browser for the convenience of full configuration and management on the switch, and retains the look and feel of Device Manager.

Multiple Port Configuration

Among the many functions available in EDM, you can configure port-specific features for a single port, a group of ports, or all ports. Multiple Port Configuration appears as a pane in the work area wherever this function is available. By default the pane appears and you can close and open it with a click of the task bar.

For more information about EDM, see *Ethernet Routing Switch 2500 Series Fundamentals* (NN47215-102).

Introduction

This guide provides information to configure and manage security features on the Nortel Ethernet Routing Switch 2500 Series.

NNCLI command modes

Nortel command line interface (NNCLI) provides the following configuration modes:

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

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

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

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

Table 1
NNCLI command modes

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC 2526T>	No entrance command, default mode.	exit or logout

Command mode and sample prompt	Entrance commands	Exit commands
Privileged EXEC 2526T#	<code>enable</code>	<code>exit</code> or <code>logout</code>
Global Configuration 2526T(config)#	From Privileged EXEC mode, type: <code>configure</code>	To return to Privileged EXEC mode, type: <code>end</code> or <code>exit</code> To exit NNCLI completely, type: <code>logout</code>
Interface Configuration 2526T(config-if)#	From Global Configuration mode: To configure a port, type: <code>interface fastethernet <port number></code> To configure a VLAN, type: <code>interface vlan <vlan number></code>	To return to Global Configuration mode, type: <code>exit</code> To return to Privileged EXEC mode, type: <code>end</code> To exit NNCLI completely, type: <code>logout</code>

For more information about the NNCLI configuration modes, see *Nortel Ethernet Routing Switch 2500 Series Fundamentals* (NN47215-102).

Navigation

- [“Security fundamentals” \(page 23\)](#)
- [“Configuring and managing security using NNCLI” \(page 57\)](#)
- [“Configuring and managing security using Enterprise Device Manager” \(page 175\)](#)
- [“Appendixes” \(page 241\)](#)

Security fundamentals

This chapter describes the security features available with the Ethernet Routing Switch 2500.

Navigation

- [“Management password configuration” \(page 23\)](#)
- [“MAC address-based security” \(page 25\)](#)
- [“RADIUS-based network security” \(page 26\)](#)
- [“Campus security example” \(page 28\)](#)
- [“EAPOL-based security” \(page 30\)](#)
- [“Advanced EAPOL features” \(page 32\)](#)
- [“802.1X dynamic authorization extension \(RFC 3576\)” \(page 39\)](#)
- [“TACACS+” \(page 41\)](#)
- [“IP Manager” \(page 46\)](#)
- [“Password security” \(page 47\)](#)
- [“HTTP port number change” \(page 49\)](#)
- [“Simple Network Management Protocol” \(page 49\)](#)
- [“Secure Socket Layer protocol” \(page 51\)](#)
- [“DHCP snooping” \(page 52\)](#)
- [“Dynamic ARP inspection” \(page 54\)](#)
- [“IP Source Guard” \(page 54\)](#)
- [“Nortel Secure Network Access” \(page 56\)](#)

Management password configuration

To provide security on your switch, you can configure a local or RADIUS password for management access, or you can configure SNMP community strings.

Console/TELNET password Configuration

A user at a remote console can use Telnet access to communicate with the Ethernet Routing Switch 2500 as if the console terminal were directly connected to the Switch. You can establish up to four active Telnet sessions at one time, in addition to one active Console connection, for a total of five possible concurrent users.

User name and password

You can set a local user name and password to restrict access to the switch. The user name and password can provide read/write access or read-only access to the switch.

ATTENTION

If you set a password, the next time you log on to the switch, you are prompted to enter a valid user name. Therefore, ensure you are aware of the valid user names (default RW and RO) before you change passwords. For information about modifying existing user names, see [“Setting the user name and password using NNCLI” \(page 58\)](#).

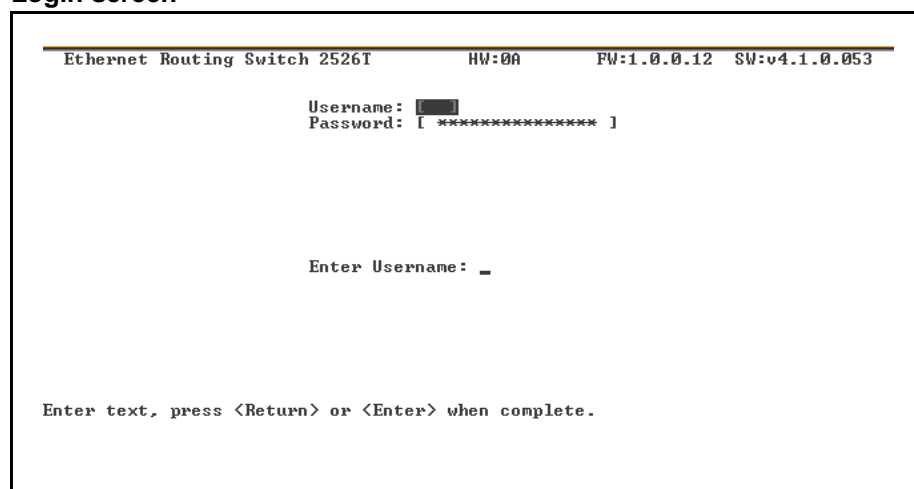
Logging on

If you set a password, the next time you access the switch, you are prompted for a user name and password as shown in the (default user names are RW and RO).

Enter a valid user name and password and press Enter. You are then directed to NNCLI.

For information about modifying the existing user names, see [“Setting the user name and password using NNCLI” \(page 58\)](#)

Figure 1
Login screen



MAC address-based security

Use the MAC address-based security to set up network access control based on source MAC addresses of authorized stations.

You can perform the following activities:

- Create a list of up to 448 MAC addresses and specify which addresses are authorized to connect to your switch. The 448 MAC addresses can be configured within a single standalone switch, or they can be distributed in any order among the units in a single stack configuration.
- Specify which switch port each MAC address can access.
The options for allowed port access include NONE, ALL, and single or multiple ports specified in a list.
- Specify optional switch actions if the software detects a security violation.
The response can be to send a trap, turn on destination address (DA) filtering, disable a specific port, or a combination of these three options.

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

MAC address-based security autolearning

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

MAC address-based security autolearning contains the following features:

- You can specify the number of addresses to learn on the ports to a maximum of 25 addresses for each port. The switch forwards traffic only for those MAC addresses statically associated with a port or learned with the autolearning process.
- You can configure an aging timer, in minutes, after which autolearned entries are refreshed in the MAC Security Address Table. If you set the aging time value to 0, the entries never age out. To force relearning of entries in the MAC Security Address Table you must reset learning for the port.
- If a port link goes down, the autolearned entries associated with that port in the MAC Security Address Table are removed.
- You cannot modify autolearned MAC addresses in the MAC Security Address Table.

- MAC Security port configuration including the aging timer and static MAC address entries are saved to the switch configuration file. MAC addresses learned with autolearning are not saved to the configuration file; the switch dynamically learns them.
- You can reset the MAC address table for a port by disabling the security on the port and then re-enabling it.
- If a MAC address is already learned on a port (port x) and the address migrates to another port (port y), the entry in the MAC Security Address Table changes to associate that MAC address with the new port (port y). The aging timer for the entry is reset.
- If you disable autolearning on a port, all autolearned MAC entries associated with that port in the MAC Security Address Table are removed.
- If a static MAC address is associated with a port (which may or may not be configured with the autolearning feature) and the same MAC address is learned on a different port, an autolearn entry associating that MAC address with the second port is not created in the MAC Security Address Table. In other words, user settings have priority over autolearning.

RADIUS-based network security

Use the RADIUS-based security feature to set up network access control by using the Remote Authentication Dial-In User Services (RADIUS) security protocol. The RADIUS-based security feature uses the RADIUS protocol to authenticate local console, Telnet, and SSH access logon sessions.

You need to set up specific user accounts (user names and passwords, and Service-Type attributes) on your RADIUS server before you can initiate the authentication process. These accounts provide you with appropriate levels of access to the switch.

Set the following user name attributes on your RADIUS server:

- Read-write access—set the Service-Type field value to Administrative.
- Read-only access—set the Service-Type field value to NAS-Prompt.

For instructions to set up your RADIUS server, see your RADIUS server documentation.

RADIUS password fallback

You can configure RADIUS password fallback as an option when you use RADIUS authentication for logon and password.

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

When RADIUS password fallback is disabled, you must specify the RADIUS user name and password from the NetLogin screen. Unless the RADIUS server is configured and reachable, you cannot log on to the switch to authenticate the logon and password.

The RADIUS password fallback feature is disabled by default.

RADIUS Interim Accounting Updates support

The Ethernet Routing Switch 2500 supports the RADIUS Interim Accounting Updates feature. With RADIUS Interim Accounting Updates support enabled, the RADIUS server can make policy decisions based on real-time network attributes transmitted by the NAS.

An example of how RADIUS Interim Accounting Updates support enhances network security is the Threat Protection System (TPS) alerting the Dynamic Authorization Client (RADIUS server) about abnormal traffic patterns from a specific IP address on the network. The RADIUS server can correlate IP address to MAC address information in the internal session database, locate the device access point on the network, and issue a Change-Of-Authorization or Disconnect message to NAS.

RADIUS Interim Accounting Updates support is not enabled by default.

RADIUS Request use Management IP Address

You can configure the Ethernet Routing Switch 2500 to apply strict use of the Management IP address to ensure that the switch uses the Management VLAN IP address as the source IP address for RADIUS, when routing is enabled.

The RADIUS Request use Management IP configuration has no impact when the switch operates in Layer 2 mode.

When the switch operates in Layer 3 mode, by default, a RADIUS request uses one of the routing IP addresses on the switch. RADIUS Request use Management VLAN IP configuration ensures that the switch or stack generates RADIUS requests using the source IP address of the management VLAN. In some customer networks, the source IP in the RADIUS request is used to track management access to the switch, or it can be used when non-EAP is enabled. Because non-EAP can use an IP in the password mask it is important to have a consistent IP address.

If the management VLAN is not operational, then the switch cannot send any RADIUS requests when:

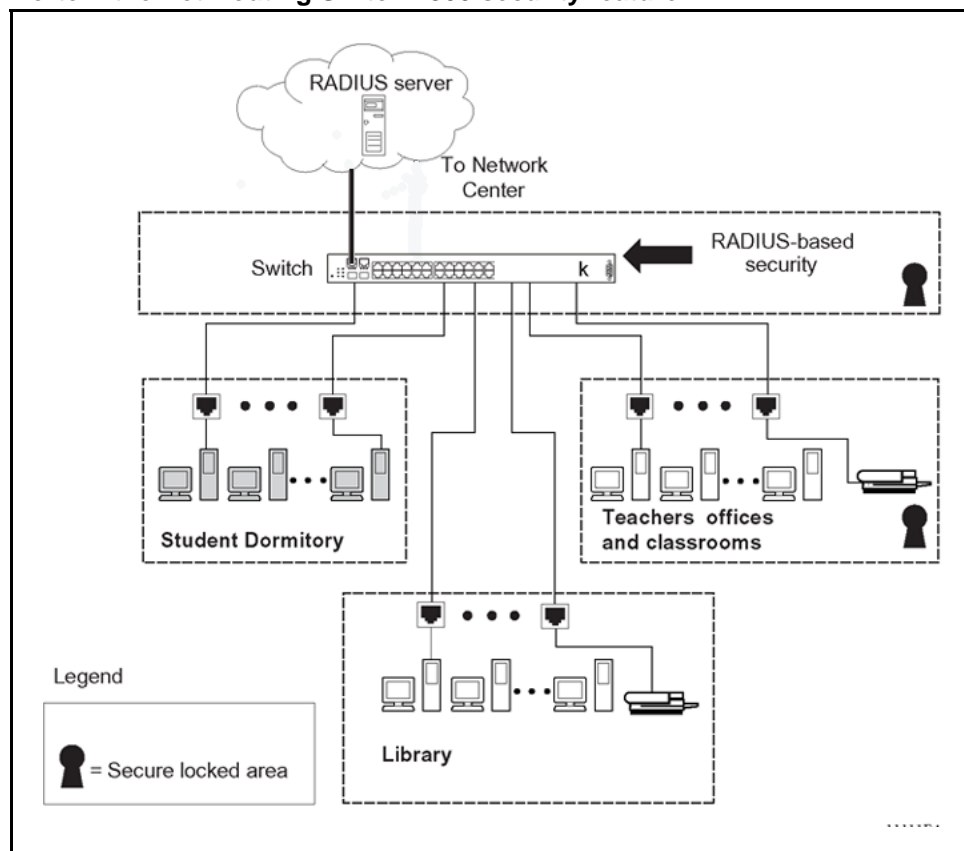
- the switch is operating in Layer 2 mode
- the switch is operating in Layer 3 mode (routing) and RADIUS Request Use Management VLAN IP is enabled

This is normal behavior in Layer 2 mode; if the Management VLAN is unavailable, there is no active Management IP instance. In Layer 3 mode, if RADIUS Request Use Management IP is enabled, the switch does not use any of the other routing instances to send RADIUS requests when the management VLAN is inactive or disabled.

Campus security example

The following figure shows a typical campus configuration using the RADIUS-based and MAC-address-based security features for the Nortel Ethernet Routing Switch 2500 Series.

Figure 2
Nortel Ethernet Routing Switch 2500 security feature



This example is based on the assumption that the switch, the teachers' offices, classrooms, and the library are physically secure. The student dormitory can also be physically secure.

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

- The switch
 - RADIUS-based security is used to limit administrative access to the switch through user authentication (see [“RADIUS-based network security” \(page 26\)](#)).
 - MAC address-based security is used to allow up to 448 authorized stations (MAC addresses) access to one or more switch ports (see [“MAC address-based security” \(page 25\)](#)).
 - The switch is in a locked closet, accessible only by authorized Technical Services personnel.
- Student dormitory

Dormitory rooms are typically occupied by two students and are pre-wired with two RJ-45 jacks. Only students who are authorized (as specified by the MAC address-based security feature) can access the switch on the secured ports.
- Teachers' offices and classrooms

The PCs that are in the teachers' offices and classrooms are assigned MAC address-based security that is specific for each classroom and office location. The security feature logically locks each wall jack to the specified station and prevents unauthorized access to the switch if someone attempts to connect a personal laptop PC into the wall jack. The printer is assigned as a single station and has full bandwidth on that switch port.

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

The wall jacks in the library are set up so that the PCs can connect to any wall jack in the room. With this arrangement, you can move the PCs anywhere in the room. The exception is the printer, which is assigned as a single station with full bandwidth to that port.

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

EAPOL-based security

The Ethernet Routing Switch 2500 provides security on the basis of Extensible Authentication Protocol over LAN (EAPOL), and it uses the EAP as is defined in the IEEE 802.1X so that you can set up a network access control over LANs. With EAP, you can authenticate user information through a connection between a client and the switch by using an authentication service such as RADIUS. This security feature works with the RADIUS-based server and to provide the advantages of remote authentication to internal LAN clients.

An example follows to show how an Ethernet Routing Switch 2500 reacts when it is configured with the EAPOL security feature and a new network connection:

- When the switch finds a new connection in one of its ports, the following activities occur:
 - a. The switch asks for a User ID of the new client.
 - b. The User ID is covered by EAPOL, and it passes to the RADIUS server.
 - c. The response from the RADIUS server is to ask for a password of the user.
- Within the EAPOL packet, the new client forwards a password to the switch:
 - The EAPOL packet is relayed to the RADIUS server.
 - If the RADIUS server validates the password, the new client is allowed to access the switch and the network.

The EAPOL-based security comprises of the following terms:

- Supplicant—the device applying for network access.
- Authenticator—software with the main purpose of authorizing the supplicant that is attached at the other end of the LAN segment.
- Authentication server—a RADIUS server that provides authorization services to an authenticator.
- Port Access Entity (PAE)—an entity that supports each port to the Authenticator or Supplicants. In the preceding example, the authenticator PAE is in the switch.

Controlled Port is a switch port with EAPOL-based security. The authenticator communicates with the Supplicant through EAP over LAN (EAPOL), which is an encapsulation mechanism.

The authenticator PAE encapsulates the EAP through the RADIUS server packet and sends it to the authentication server. The authenticator server sends the packet in an exchange that occurs

between the supplicant and authentication server. This exchange occurs when the EAP message is encapsulated to make it suitable for the destination of the packet.

The authenticator determines the operational state of the controlled port. The RADIUS server notifies the authenticator PAE of the success or failure of the authentication to change the operational state of the controlled port. PAE functions are then available for each port to forward; otherwise, the controlled port state depends upon the operational traffic control field in the EAPOL configuration screen. Operational traffic can be of two types:

- Incoming and Outgoing—For an unauthorized controlled port, the frames received and transmitted are discarded, and state of the port is blocked.
- Incoming—Although the frames received for an unauthorized port are discarded, the transmit frames are forwarded through the port.

EAPOL Security Configuration

EAPOL security lets you 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.

ATTENTION

Before you enable EAPOL, you must configure your Primary RADIUS Server and RADIUS Shared Secret. You must set up specific user accounts on your RADIUS server:

- User names
- Passwords
- VLAN IDs
- Port priority

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

ATTENTION

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

EAPOL with Guest VLAN

Basic EAP (802.1x) Authentication supports Port Based User Access. At any time, only one user (MAC) can be authenticated on a port, and the port can be assigned to only one Port-based VLAN. Only the MAC address

of the device or user that completed the EAP negotiations on the port has access to that port for traffic. Any tagging of ingress packets are to the PVID of that port. This remains the default configuration.

You can use EAP to configure Guest VLANs to access the port. Any active VLAN can be a Guest VLAN.

Advanced EAPOL features

The following sections describe advanced EAPOL-supported features.

Multiple Host with Multiple Authentication

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

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

RADIUS-assigned VLAN values can exist in the MHMA mode. For more information about RADIUS-assigned VLANs in the MHMA mode, see [“RADIUS-assigned VLAN use in MHMA mode” \(page 33\)](#).

MHMA support is on each port for an EAP-enabled port.

The following are some concepts associated with MHMA:

- Logical and physical ports
Each unique port and MAC address combination is treated as a logical port. MAX_MAC_PER_PORT defines the maximum number of MAC addresses that can perform EAP authentication on a port at any time. Each logical port is treated as if it is in the SHSA mode.
- Indexing for MIBs
Logical ports are indexed by a port and source MAC address (src-mac) combination. Enterprise-specific MIBs are defined for state machine-related MIB information for individual MACs.
- Transmitting EAPOL packets
Only unicast packets are sent to a specific port so that the packets reach the correct destination.
- Receiving EAPOL packets
The EAPOL packets are directed to the correct logical port for state machine action.
- Traffic on an authorized port
Only a set of authorized MAC addresses can access a port.

MHMA support for EAP clients includes the following features:

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

RADIUS-assigned VLAN use in MHMA mode

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

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

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

Non-EAP IP Phone authentication

Non-EAP IP Phone authentication can be used for IP Phones that cannot authenticate with EAP. For the Local and RADIUS Non-EAP authentications, EAP Guest VLAN must be disabled (Guest VLAN and Non-EAP are mutually exclusive features). On an EAP capable IP Phone, EAP must be disabled to use non-EAP IP Phone authentication. DHCP must be enabled on the phone, because the switch examines the phone signature in the DHCP Discover packet sent by the phone.

Unicast EAP Requests in MHMA

With unicast EAP requests in Multiple Host with Multiple Authentication (MHMA) enabled, the switch does not periodically query the connected MAC addresses to a port with EAP Request Identity packets. The clients must be able to initiate the EAP authentication sessions (send EAP Start packets to the switch) themselves. Not all EAP supplicants can support this operating mode.

Multicast mode is selected by default for all ports on the switch . You must set the EAP packet mode to unicast in both global and interface modes for switch ports to enable this feature. Any other combination (for example, multicast in global, unicast in interface mode) selects the multicast operating mode.

802.1X or non-EAP with VLAN names

When you use the 802.1X or non-EAP with VLAN names functionality, the switch can match RADIUS assigned VLANs based on either the VLAN number or the VLAN name. Because the 802.1X or non-EAP with VLAN names mode is always enabled, you do not have to configure this feature. Prior to Release 4.3, a match occurred based on the VLAN number of the Tunnel-Private-Group-Id attribute returned by the RADIUS server. Beginning with Release 4.3, you can use the VLAN number or name to configure VLAN membership of EAP or non-EAP clients.

The Tunnel-Private-Group-Id attribute is converted to either a VLAN ID or VLAN name, based on the first character of the returned attribute. The maximum length of a VLAN name can be 16 characters.

If the first character in the Tunnel-Private-Group-Id attribute is a number, the switch processes it as a VLAN number. If the first character in the attribute is not a number, the attribute is considered to be the VLAN name and the attribute is matched on the full string.

Non-EAP hosts on EAP-enabled ports

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

The following types of non-EAPOL users are allowed:

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

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

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

- EAPOL and authenticated non-EAPOL clients are allowed on the port at the same time. Authenticated non-EAPOL clients are hosts that satisfy one of the following criteria:
 - Host MAC address matches an entry in an allowed list preconfigured for the port.
 - Host MAC address is authenticated by RADIUS.
- Non-EAPOL hosts are allowed even if no authenticated EAPOL hosts exist on the port.
- When a new host is seen on the port, non-EAPOL authentication is performed as follows:

- If the MAC address matches an entry in the preconfigured allowed MAC list, the host is allowed.
- If the MAC address does not match an entry in the preconfigured allowed MAC list, the switch generates a <user name, password> pair, which it forwards to the network RADIUS server for authentication. For more information about the generated credentials, see [“Non-EAPOL MAC RADIUS authentication” \(page 37\)](#).
If the MAC address is authenticated by RADIUS, the host is allowed.
- If the MAC address does not match an entry in the preconfigured allowed MAC list and also fails RADIUS authentication, the host is counted as an intruder. Data packets from that MAC address are dropped.

EAPOL authentication is not affected.

- For RADIUS-authenticated non-EAPOL hosts, VLAN information from RADIUS is ignored. Upon successful authentication, untagged traffic is put in a VLAN preconfigured for the port.
- For RADIUS-authenticated non-EAPOL hosts, VLAN information from RADIUS is ignored. Upon successful authentication, untagged traffic follows the PVID of the port.
- Non-EAPOL hosts continue to be allowed on the port until the maximum number of non-EAPOL hosts is reached. The maximum number of non-EAPOL hosts allowed is configurable.
- After the maximum number of allowed non-EAPOL hosts is reached, any data packets received from additional non-EAPOL hosts are dropped. The additional non-EAPOL hosts are counted as intruders. New EAPOL hosts can continue to negotiate EAPOL authentication.
- When the intruder count reaches 32, a SNMP trap and system log message are generated. The port administrative status is set to force-unauthorized, and you must reset the port administrative status (from force-unauthorized to auto) to allow new EAPOL and non-EAPOL negotiations on the port.
- The feature uses enterprise-specific MIBs.
- Configuration settings are saved across resets.

ATTENTION

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

For information about configuring non-EAPOL host support, see [“Configuring support for non-EAPOL hosts on EAPOL-enabled ports using NNCLI” \(page 141\)](#).

Non-EAPOL MAC RADIUS authentication

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

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

ATTENTION

Use only lowercase letters for user names and passwords configured on the RADIUS server.

Follow these global configuration examples, to select a password format that combines one or more of these 3 elements:

password = 010010011253..0305 (when the switch IP address, unit and port are used).

password = 010010011253.. (when only the switch IP address is used).

Starting with Release 4.3, there is a new rule for Non-EAPOL MAC RADIUS Authentication—when you set the password format to use only the MAC address, the format omits the two dots at the end. Example: password = 010010011253

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

```
switch IP address = 10.10.11.253
non-EAP host MAC address = 00 C0 C1 C2 C3 C4
unit = 3
port = 25
```

- user name = 00c0c1c2c3c4
- password = 010010011253.00c0c1c2c3c4.0325

Multiple Host with Single Authentication

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

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

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

MHSA support is on each port for an EAPOL-enabled port.

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

- The port remains unauthorized when no authenticated hosts exist on it. Before the first successful authentication occurs, both EAPOL and non-EAPOL clients are allowed on the port to negotiate access, but at any time, only one host can negotiate EAPOL authentication.
- After the first EAPOL client successfully authenticates, EAPOL packets and data from that client are allowed on the port. No other clients are allowed to negotiate EAPOL authentication. The port is set to preconfigured VLAN assignments and priority values or to values obtained from RADIUS for the authenticated user.
- After the first successful authentication, any new hosts, up to a configured maximum number, are automatically allowed on the port, without authentication.
- After the maximum number of allowed non-EAPOL hosts is reached, any data packets received from additional non-EAPOL hosts are dropped. The additional non-EAPOL hosts are counted as intruders.
- When the intruder count reaches 32, a SNMP trap and system log message are generated. The port administrative status is set to force-unauthorized, and you must reset the port administrative status (from force-unauthorized to auto) to allow new EAPOL negotiations on the port.
- If the EAPOL-authenticated user logs off, the port returns to an unauthorized state and non-EAPOL hosts are not allowed.
- This feature uses enterprise-specific MIBs.

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

802.1X dynamic authorization extension (RFC 3576)

With 802.1X dynamic authorization extension (RFC 3576), you can enable a third party device to dynamically change VLANs on switches or close user sessions.

The 802.1X dynamic authorization extension process includes the following devices:

- Network Access Server (NAS)—the Ethernet Routing Switch 2500 that authenticates each 802.1X client at a RADIUS server.
- RADIUS server—sends disconnect and Change of Authorization (CoA) requests to the NAS. A CoA command modifies user session authorization attributes and a disconnect command ends a user session.

ATTENTION

The term RADIUS server, which designates the device that sends the requests, is replaced in RFC 5176 with the term Dynamic Authorization Client (DAC). The NAS is the Dynamic Authorization Server (DAS).

- 802.1X client—the device that requires authentication and uses the Ethernet Routing Switch 2500 services.

ATTENTION

Requests from the RADIUS server to the NAS must include at least one NAS identification attribute and one session identification attribute.

An Ethernet Routing Switch 2500 can receive disconnect or CoA commands in the following conditions:

- a user authenticated session exists on a port (one user session for single-host configuration or multiple user sessions for Multihost configuration)
- the port maintains the original VLAN membership (Guest VLAN and RADIUS VLAN configurations)
- the port is added to a RADIUS-assigned VLAN (PVID is the RADIUS-assigned VLAN ID)

802.1X dynamic authorization extension (RFC 3576) applies only to Extensible Authentication Protocol (EAP) clients and does not affect non-EAP clients.

802.1X dynamic authorization extension supports the following configured features:

- Guest VLAN
- RADIUS VLAN for EAP clients
- RADIUS VLAN for Non-EAP clients

802.1X dynamic authorization extension functions when any RADIUS VLAN assignment features are active on a port.

802.1X dynamic authorization extension functions with SHSA, MHMA, and MHSA port operating modes.

The following authorization considerations apply:

- Enable only used servers to prevent receiving and processing requests from servers not trusted.
- The requirements for the shared secret between the NAS and the RADIUS server are the same as those for a well-chosen password.
- If user identity is essential, do not use specific user identification attributes as the user identity. Use attributes that can identify the session without disclosing user identification attributes, such as port or calling-station-id session identification attributes.

To enable the 802.1X dynamic authorization extension feature on the Ethernet Routing Switch 2500, you must perform the following tasks:

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

ATTENTION

The switch ignores disconnect or CoA commands if the commands address a port on which 802.1X dynamic authorization extension is not enabled.

While listening for request traffic from the DAC, the NAS can copy and send a UDP packet, which can disconnect a user. Nortel recommends that you implement replay protection by including the Event Timestamp attribute in both the request and response. To correctly process the Event Timestamp attribute, the DAC and the NAS must be synchronized (an SNTP server must be used by both the DAC and the NAS).

The DAC must use the source IP address of the RADIUS UDP packet to determine which shared secret to accept for RADIUS requests to be forwarded by a proxy. When RADIUS requests are forwarded by a proxy, the NAS-IP-Address attribute will not match the source IP address

observed by the DAC. The DAC cannot resolve the NAS-Identifier attribute, whether a proxy is present. The authenticity check performed by the DAC cannot verify the NAS identification attributes, which makes it possible for an unauthorized NAS to forge identification attributes and impersonate an authorized NAS in your network.

To prevent these vulnerabilities, Nortel recommends that you configure proxies to confirm that NAS identification attributes match the source IP address of the RADIUS UDP packet.

802.1X dynamic authorization extension complies with the following standards and RFCs:

- IEEE 802.1X standard (EAP)
- RFC 2865—RADIUS
- RFC 3576—Dynamic Authorization Extensions to RADIUS

TACACS+

The Ethernet Routing Switch 2500 supports the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ is a security application implemented as a client/server-based protocol that provides centralized validation of users attempting to gain access to a router or network access server.

TACACS+ differs from RADIUS in two important ways:

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

ATTENTION

TACACS+ encrypts the entire body of the packet but uses a standard TACACS+ header.

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

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

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

The TACACS+ protocol is a draft standard available at <https://datatracker.ietf.org/drafts/draft-grant-tacacs/>

ATTENTION

TACACS+ is not compatible with previous versions of TACACS.

TACACS+ architecture

You can configure TACACS+ on the Ethernet Routing Switch 2500 by using the following methods:

- Connect the TACACS+ server through a local interface. Management PCs can reside on an out-of-band management port or serial port, or on the corporate network. The TACACS+ server is placed on the corporate network so that it can be routed to the Ethernet Routing Switch 2500.
- Connect the TACACS+ server through the management interface by using an out-of-band management network.

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

Feature operation

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

TACACS+ authentication

TACACS+ authentication offers complete control of authentication through logon and password dialog and response. The authentication session provides user name and password functionality.

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

ATTENTION

Prompts for logon and password occur prior to the authentication process. If TACACS+ fails because no valid servers are available, the user name and password are used for the local database. If TACACS+ or the local database return an access denied packet, the authentication process stops. No other authentication methods are attempted.

TACACS+ authorization

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

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

TACACS+ authorization is not mandatory for all privilege levels.

When authorization is requested by the NAS, the entire command is sent to the TACACS+ daemon for authorization. You preconfigure command authorization on the TACACS+ server by specifying a list of regular expressions that match command arguments and associating each command with an action to deny or permit. For an example of the configuration required on the TACACS+ server, see [“TACACS+ server configuration example”](#) (page 44).

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

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

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

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

Changing privilege levels at run time

Users can change their privilege levels at run time by using the following command on the switch:

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

[<level>] is the privilege level you want to access.

ATTENTION

You are prompted to provide the required password. If you do not specify a level in the command, the administration level (15) is selected by default.

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

```
tacacs switch back
```

To support run time switching of users to a particular privilege level, you must preconfigure a dummy user for that level on the daemon. The format of the user name for the dummy user is `$enab<n>$`.

`<n>` is the privilege level to which you want to allow access.

For an example of the configuration required on the TACACS+ server, see [“TACACS+ server configuration example” \(page 44\)](#).

TACACS+ server configuration example

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

Figure 3
Example: TACACS+ server configuration

```
#Setting the accounting file on the server and server key
accounting file = /var/log/tac_plus.act
key = n0rt3l
#Setting a user account used to log in
user= freddy {
  member=level6
  login=cleartext kruger
  expires="Dec 31 2006"
}
# Setting the runtime switching privilege level
user=$enab8$ {
  member=level8
  login=cleartext makemelevel8
}
#Setting the permissions for each privilege level
group=level6 {
  cmd=enable { permit .* }
  cmd=configure { permit terminal }
  cmd=vlan { permit .* }
  cmd=interface { permit .* }
  cmd=ip { permit .* }
  cmd=router { permit .* }
  cmd=network { permit .* }
  cmd=show { permit .* }
  cmd=exit { permit .* }
  cmd=logout { permit .* }
  service=exec {
    priv-lvl=6
  }
}
```

TACACS+ accounting

TACACS+ accounting enables you to track the following items:

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

When you enable accounting, the NAS reports user activity to the TACACS+ server in the form of accounting records. Each accounting record contains accounting attribute=value (AV) pairs. The accounting records are stored on the security server. You can analyze the accounting data for network management and auditing.

TACACS+ accounting provides information about user NNCLI terminal sessions within serial, Telnet, or SSH shells (from NNCLI management interface).

The accounting record includes the following information:

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

You cannot customize the set of events that TACACS+ accounting monitors and logs. TACACS+ accounting logs the following events:

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

Feature limitations

The following features are not supported in the current implementation of TACACS+ in the Ethernet Routing Switch 2500:

- S/KEY (One Time Password) authentication.
- PPP/PAP/CHAP/MSCHAP authentication methods.
- The FOLLOW response of a TACACS+ server, in which the authentication, authorization, and accounting (AAA) services are

redirected to another server. The response is interpreted as an authentication failure.

- User capability to change passwords at run time over the network. The system administrator must change user passwords locally on the server.

TACACS+ configuration

You can configure TACACS+ with NNCLI or EDM on the Ethernet Routing Switch 2500.

For information about configuring TACACS+ server information and TACACS+ authentication, authorization, and accounting see [“TACACS+ configuration using NNCLI” \(page 148\)](#) and [“TACACS+ configuration using EDM” \(page 189\)](#).

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

IP Manager

With IP Manager, you can limit access to the management features of the Ethernet Routing Switch 2500 by defining the IP addresses that are allowed access to the switch.

With the IP Manager, you can do the following:

- Define a maximum of 50 Ipv4 and 50 Ipv6 addresses, and masks that are allowed to access the switch. No other source IP addresses have management access to the switches.
- Enable or disable access to Telnet, SNMP, SSH, and Web-based management system.

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

ATTENTION

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

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

Password security

The Ethernet Routing Switch 2500 supports the password security feature that provides enhanced security for switch and stack passwords. With password security enabled, the following enhanced security features are applied.

Password length and valid characters

Valid passwords must be from 10 to 15 characters. The password must contain a minimum of the following:

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

The password is case sensitive.

Password retry

If the user fails to provide the correct password after a number of consecutive attempts, the switch resets the logon process. The number of failed logon attempts is configurable and the default is three.

Password history

The Nortel Ethernet Routing Switch 2500 keeps a history of the last three passwords. You cannot reuse a password stored in history. When you set the password for the fourth time, you can reuse the password that you used the first time.

Password display

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

Password verification

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

Password aging time

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

Read-Only and Read-Write passwords must be different

The RO and RW passwords cannot be the same.

Applicable passwords

The password security feature applies these enhanced features to the following passwords:

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

The password security feature applies only the display and verification restrictions to the following passwords:

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

Enabling and disabling password security

Password security can only be enabled or disabled from NNCLI. When password security is enabled, the following occurs:

- Current passwords remain unchanged if they meet the required specifications. If they do not meet the required specifications, the user is prompted to change them to valid passwords.
- An empty password history bank is established.
- Password verification is enabled.

When password security is disabled, the following occurs:

- Current passwords remain valid.
- Password history bank is removed.
- Password verification is disabled.

ATTENTION

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

Default passwords

For the standard software image, the default password for RO is "user" and "secure" for RW.

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

HTTP port number change

With this feature, you can define the UDP or TCP port number used for HTTP connections to the switch.

This feature provides enhanced security and network access. Port number 80 is the default port for communication between the Web client and the server. With this feature, you can modify the HTTP port while the switch is running. The HTTP port value is saved in NVRAM, and also is saved across reboots of the switch.

For more information about, see [“Changing the http port number using NNCLI” \(page 62\)](#).

Simple Network Management Protocol

The Nortel Ethernet Routing Switch 2500 Series supports Simple Network Management Protocol (SNMP).

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

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

SNMP Version 1 (SNMPv1)

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

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

SNMP Version 2 (SNMPv2)

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

SNMP Version 3 (SNMPv3)

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

Nortel Ethernet Routing Switch 2500 Series support for SNMP

The SNMP agent in the Nortel Ethernet Routing Switch 2500 Series supports SNMPv1, SNMPv2c, and SNMPv3. Support for SNMPv2c introduces a standards-based GetBulk retrieval capability using SNMPv1 communities.

SNMPv3 support in the Nortel Ethernet Routing Switch 2500 Series introduces industrial-grade user authentication and message security. This includes MD5- and SHA-based user authentication and message integrity verification, as well as AES, DES, and 3DES-based privacy encryption.

With the Nortel Ethernet Routing Switch 2500 Series you can configure SNMPv3 by using Enterprise Device Manager, or NNCLI.

SNMP MIB support

The Nortel Ethernet Routing Switch 2500 Series supports an SNMP agent with industry-standard Management Information Bases (MIB), as well as private MIB extensions, which ensures compatibility with existing network management tools.

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

SNMP trap support

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

The Nortel Ethernet Routing Switch 2500 Series supports both industry-standard SNMP traps, as well as private Nortel enterprise traps.

SNMP trap control

You can use SNMP to enable or disable individual SNMP traps. Only the traps corresponding to the applications running on the device are available for configuration. The software includes a defined set of supported SNMP traps, and you can enable or disable them by using filters. By default, all the SNMP traps are enabled.

The following conditions apply to SNMP traps:

- Ethernet Routing Switch 2500 series Release 4,3 maintains the SNMP traps states.
- The Power over Ethernet (PoE) related traps are available only on the PoE enabled switches or in a stack which has at least one PoE-enabled unit.
- The Rapid Spanning Tree Protocol (RSTP) -related traps are available only when the switch or switch stack is operating in the RSTP mode. When leaving the RSTP mode, the traps states are saved. They are restored when the switch or switch stack operates again in the RSTP mode.
- The state of an SNMP trap is not reflected by the application-specific commands when you enable or disable the trap.

Per host notification control

Per host notification control associates a trap receiver with SNMP traps so that you can enable or disable receiving these traps. You can add notification filters to trap receivers, and can include or exclude SNMP traps (the names or the OIDs) from a notification filter. SNMP traps that are included in a notification filter are allowed when sending traps to a receiver using that filter. SNMP traps that are excluded from a notification filter are disallowed when sending traps to a receiver using that filter.

Secure Socket Layer protocol

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

The SSL server supports the following features:

- SSLv3-compliant
- PKI key exchange
- Key size of 1024-bit encryption
- RC4 and 3DES cryptography
- MAC algorithms MD5 and SHA-1

An SSL certificate is generated when:

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

Each new certificate is stored in the NVRAM with the file name SSLCERT.DAT. The new certificate file replaces the existing file.

On deletion, the certificate in NVRAM is also deleted.

The current SSL server operation is not affected by the create or delete operation.

Secure versus non-secure mode

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

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

In the non-secure mode, the Web server listens on TCP port 80, by default, and responds only to HTTP client browser requests. All existing secure connections with the browser are closed down. The TCP port can be designated as any number from 1024 to 65535.

DHCP snooping

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

DHCP snooping classifies ports in the following two types:

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

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

- DHCP snooping allows only DHCP requests from untrusted ports. DHCP replies and all other types of DHCP messages from untrusted ports are dropped.
- DHCP snooping verifies the source of DHCP packets.
 - When the switch receives a DHCP request on an untrusted port, DHCP snooping compares the source MAC address and the

DHCP client hardware address. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

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

DHCP binding table

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

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

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

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

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

DHCP snooping configuration and management

DHCP snooping is configured on a VLAN-to-VLAN basis.

Configure and manage DHCP snooping by using the Nortel command line interface (NNCLI), Enterprise Device Manager (EDM), and SNMP. For information about configuring DHCP snooping, see [“DHCP snooping configuration using NNCLI” \(page 160\)](#) or [“DHCP snooping configuration using EDM” \(page 220\)](#).

DHCP snooping Global Configuration

This configuration enables or disables DHCP snooping for the entire unit or stack. If DHCP snooping is enabled globally, the agent determines whether the DHCP reply packets are forwarded based on the DHCP snooping mode (enable or disable) of the VLAN and the untrusted or trusted state of the port. You must globally enable DHCP snooping

before you use DHCP snooping on a VLAN. If you globally disable DHCP snooping, the switch or stack forwards DHCP reply packets to all required ports, whether the ports are configured as trusted or untrusted.

Dynamic ARP inspection

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

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

The address binding table is dynamically built from information gathered in the DHCP request and reply when DHCP snooping is enabled. The MAC address from the DHCP request is paired with the IP address from the DHCP reply to create an entry in the DHCP binding table. For information about the DHCP binding table, see [“DHCP binding table” \(page 53\)](#).

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

For dynamic ARP inspection to function, you must globally enable DHCP snooping.

Dynamic ARP inspection is configured on a VLAN-to-VLAN basis.

For information about configuring and managing dynamic ARP inspection, see [“Dynamic ARP inspection configuration using NNCLI” \(page 166\)](#) or [“Dynamic ARP inspection configuration using EDM” \(page 223\)](#).

IP Source Guard

IP Source Guard provides security to the network by filtering clients with invalid IP addresses. It is a Layer 2, feature for each port that works closely with information in the Dynamic Host Control Protocol (DHCP) snooping Binding Table. For information about DHCP snooping, see [“DHCP snooping” \(page 52\)](#). When IP Source Guard is enabled on an untrusted port with DHCP snooping enabled, an IP filter entry is created or deleted for that port automatically, based on IP information stored in the corresponding DHCP snooping Binding Table entry. When a connecting client receives a valid IP address from the DHCP server, a filter is installed

on the port to allow traffic only from the assigned IP address. A maximum of 10 IP addresses are allowed on each IP Source Guard-enabled port. When this number is reached, no additional filters are set up and traffic is dropped.

IP Source Guard is available to the Ethernet Routing Switch 2500 by using Broadcom 569x ASICs and is implemented with the facility provided by the Fast Filter Processor (FFP) for each port, in the ASIC.

ATTENTION

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

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

Table 2
IP source guard and DHCP snooping

IP Source Guard configuration state	DHCP snooping configuration state	DHCP snooping Binding Entry action (untrusted ports)	IP Source Guard action
disabled or enabled	enabled	creates a binding entry	creates a filter for the IP address using the IP address from the Binding Table entry
enabled	enabled	creates a binding entry	creates a filter for the IP address using the IP address from the Binding Table entry
enabled	enabled	deletes a binding entry	deletes the IP filter and installs a default filter to block all IP traffic on the port
enabled	enabled	deletes binding entries when one of the following conditions occurs: <ul style="list-style-type: none"> • DHCP is released • the port link is down, or the administrator is disabled • the lease time has expired 	deletes the corresponding IP Filter and installs a default filter to block all IP traffic
enabled or disabled	enabled	not applicable	deletes the installed IP filter for the port

IP Source Guard configuration state	DHCP snooping configuration state	DHCP snooping Binding Entry action (untrusted ports)	IP Source Guard action
disabled	enabled	creates a binding entry	not applicable
disabled	enabled	deletes a binding entry	not applicable

IP Source Guard does not support the following features:

- Manual assignment of IP addresses.
DHCP snooping does not support static binding entries.
- IP and MAC address filter.

You can configure IP Source Guard by using the Nortel command line interface (NNCLI), Enterprise Device Manager (EDM) and SNMP. For information about configuring IP Source Guard, see [“IP Source Guard configuration using NNCLI” \(page 170\)](#) or [“IP Source Guard configuration using EDM” \(page 225\)](#).

Nortel Secure Network Access

The Ethernet Routing Switch 2500 supports a lightweight version of Secure Network Access Switch (SNAS) Communication Protocol (SSCP-LT), an open network access control (NAC) enforcement mechanism that communicates with Ethernet switches to perform VLAN transitions using a combination of SNMP and Nortel command line interface (NNCLI) commands. SSCP-LT works in combination with the MAC registration database and the Nortel Health Agent on Windows, Linux, and Mac OS X platforms to control access to network resources. SSCP-LT ensures that only authenticated and compliant endpoints get access to corporate VLANs. Nonauthenticated or noncompliant endpoints can only access restricted VLANs.

Configuring and managing security using NNCLI

This chapter describes the methods and procedures necessary to configure security on the Nortel Ethernet Routing Switch 2500, using the Nortel command line interface (NNCLI).

Navigation

- [“Setting the user name and password using NNCLI” \(page 58\)](#)
- [“Setting password security using NNCLI” \(page 60\)](#)
- [“Changing the http port number using NNCLI” \(page 62\)](#)
- [“Setting Telnet access using NNCLI” \(page 63\)](#)
- [“SSL configuration using NNCLI” \(page 67\)](#)
- [“Configuring Secure Shell using NNCLI” \(page 70\)](#)
- [“Configuring the RADIUS-based management password authentication using NNCLI” \(page 82\)](#)
- [“RADIUS Request use Management IP configuration using NNCLI” \(page 81\)](#)
- [“802.1X dynamic authorization extension \(RFC 3576\) configuration using NNCLI” \(page 85\)](#)
- [“Setting SNMP parameters using NNCLI” \(page 92\)](#)
- [“Common SNMP and SNMPv3 NNCLI commands” \(page 92\)](#)
- [“NNCLI commands specific to SNMPv3” \(page 105\)](#)
- [“Configuring MAC address filter-based security using NNCLI” \(page 116\)](#)
- [“Configuring EAPOL-based security using NNCLI” \(page 124\)](#)
- [“Configuring advanced EAPOL features using NNCLI” \(page 132\)](#)
- [“TACACS+ configuration using NNCLI” \(page 148\)](#)

- [“IP Manager configuration using NNCLI” \(page 154\)](#)
- [“DHCP snooping configuration using NNCLI” \(page 160\)](#)
- [“Dynamic ARP inspection configuration using NNCLI” \(page 166\)](#)
- [“IP Source Guard configuration using NNCLI” \(page 170\)](#)

Setting the user name and password using NNCLI

This section contains information about the following topics:

- [“username command” \(page 58\)](#)
- [“cli password command” \(page 59\)](#)

username command

The `username` command sets the system user name and password for access through the serial console port and Telnet. This command supports only one read-only and one read-write user on the switch. The parameters are set for the standalone or stack environment depending on the current operational mode.

The syntax for the `username` command is:

```
username <username> <password> [ro|rw]
```

The `username` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `username` command.

Table 3
username command parameters and variables

Parameters and variables	Description
<code><username></code> <code><password></code>	Enter your user name for the first variable, and your password for the second variable. The default user name values are RO for read-only access and RW for read/write access.
<code>ro rw</code>	Specifies that you are modifying the read-only (ro) user name or the read-write (rw) user name. The ro/rw variable is optional. If it is omitted, the command applies to the read-only mode.

ATTENTION

After you configure the user name and password with the `username` command, if you then update the password using the `cli password` command, the new password is set, but the user name is unchanged.

cli password command

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

The NNCLI password is in two forms and performs the following functions for the switch:

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

The syntax for the `cli password` commands is:

```
cli password {read-only|read-write} <NAME> <PASSWORD>
cli password {serial|telnet}
{none|local|radius}
```

The `cli password` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `cli password` command.

Table 4
cli password command parameters and variables

Parameters and variables	Description
<code>read-only read-write</code>	Specifies that you are modifying the read-only (ro) password or the read-write (rw) password.
<code><NAME></code> <code><PASSWORD></code>	Enter your user name for the first variable, and your password for the second variable.

Table 4
cli password command parameters and variables (cont'd.)

Parameters and variables	Description
<code>serial telnet</code>	Specifies that you are modifying the password for serial console access or for Telnet access.
<code>none local radius</code>	Specifies the password that you are modifying: <ul style="list-style-type: none">• <code>none</code> —disables the password.• <code>local</code> —use the locally defined password for serial console or Telnet access• <code>radius</code>—use RADIUS authentication for serial console or Telnet access

Setting password security using NNCLI

The following commands can be used in the Global Configuration command mode to enable, disable and configure Password Security:

- [“password security command” \(page 60\)](#)
- [“no password security command” \(page 60\)](#)
- [“show password security command” \(page 61\)](#)
- [“password aging-time day command” \(page 61\)](#)
- [“show password aging-time day command” \(page 61\)](#)
- [“Configuring the number of password logon attempts” \(page 61\)](#)

password security command

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

The syntax for the command is:

```
password security
```

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

no password security command

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

The syntax for the command is:

```
no password security
```

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

show password security command

The `show password security` command displays the current status of password security on the switch.

The syntax for the command is:

```
show password security
```

The following shows a sample output for this command:

```
2550T (config)#show password security  
Password security is enabled
```

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

password aging-time day command

The `password aging-time day` command sets the password aging time. Password security must be enabled for the command to be available.

The syntax of the command is:

```
password aging-time <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 NNCLI, the password aging counters are not reset.

show password aging-time day command

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

The syntax of the command is:

```
show password aging-time
```

The following shows a sample output for this command:

```
2550T (config)#show password aging-time  
Aging time: 100 days
```

Configuring the number of password logon attempts

The `telnet-access retry` command configures the number of times a user can attempt a password:.

The syntax of the command is:

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

where <number> is an integer in the range 1-100 that specifies the allowed number of failed logon attempts. The default is 3.

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

Changing the http port number using NNCLI

This feature provides enhanced security and network access. The default HTTP port typically used to communicate between the Web client and the server is the well-known port 80. With this feature, you can change the HTTP port.

You can configure this feature by using the following commands:

- “show http-port command” (page 62)
- “http-port command” (page 62)
- “default http-port” (page 63)

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 executed in the Privileged EXEC command mode.

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

The following figure displays sample output from the `show http-port command` command.

Figure 4
show http-port command output

```
2500-26T(config)#show http-port
HTTP Port: 80
2500-26T(config)#
```

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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `http-port` command.

Table 5
http-port command parameters and variables

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

ATTENTION

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 executed in the Global Configuration command mode.

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

Setting Telnet access using NNCLI

You can access NNCLI through a Telnet session. To access NNCLI remotely, the management port must have an assigned IP address and remote access must be enabled. You can logon to the switch using Telnet from a terminal that has access to the Ethernet Routing Switch 2500.

ATTENTION

Multiple users can access NNCLI system simultaneously, through the serial port, Telnet, and modems. The maximum number of simultaneous users is four plus one at the serial port for a total of five users on the switch. 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” (page 64)
- “telnet-access command” (page 64)
- “no telnet-access command” (page 66)
- “default telnet-access command” (page 66)

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 executed in the Privileged EXEC command mode.

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

The following figure displays sample output from the `show telnet-access` command.

Figure 5
show telnet-access command output

```

2500-26T>enable
2500-26T#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
255.255.255.255     255.255.255.255
255.255.255.255     255.255.255.255
2500-26T#_

```

telnet-access command

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

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

The `telnet-access` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `telnet-access` command.

Table 6
telnet-access command parameters and variables

Parameters and variables	Description
<code>enable disable</code>	Enables or disables Telnet connections.
<code>logon-timeout <1-10></code>	Specifies the time in minutes that you want to wait between an initial Telnet connection and acceptance of a password before closing the Telnet connection; enter an integer between 1 and 10.
<code>retry <1-100></code>	Specifies the number of times that the user can enter an incorrect password before closing the connection; enter an integer between 1 and 100.
<code>inactive timeout <0-60></code>	Specifies in minutes how long to wait before closing an inactive session; enter an integer between 0 and 60.
<code>logging {none access failures all}</code>	<p>Specifies what types of events you want to save in the event log:</p> <ul style="list-style-type: none"> • all—Save all access events in the log: <ul style="list-style-type: none"> — Telnet connect—indicates the IP address and access mode of a Telnet session. — Telnet disconnect—indicates the IP address of the remote host and the access mode, due to either a log off or inactivity. — Failed Telnet connection attempts—indicates the IP address of the remote host that is not on the list of allowed addresses, or indicates the IP address of the remote host that did not supply the correct password. • none—No Telnet events are saved in the event log. • access—Connect and disconnect events are saved in the event log. • failure—Only failed Telnet connection attempts are saved in the event log.
<code>[source-ip <1-10> <XXX.XXX.XXX.XXX>[mask <XXX.XXX.XXX.XXX>]</code>	<p>Specifies up to 10 source IP addresses from which connections are allowed. Enter the IP address either as an integer or in dotted-decimal notation. Specifies the subnet mask from which connections are allowed; enter the IP mask in dotted-decimal notation.</p> <div style="border: 1px solid black; padding: 5px;"> <p>ATTENTION 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 for IPv4 addresses”</p> </div>

Table 6
telnet-access command parameters and variables (cont'd.)

Parameters and variables	Description
	using NNCLI" (page 156) and "Configuring the IP Manager list for IPv6 addresses using NNCLI" (page 157).

no telnet-access command

With the `no telnet-access` command, you can disable the Telnet connection. The syntax for the `no telnet-access` command is:

```
no telnet-access [source-ip [<1-10>]]
```

The `no telnet-access` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `no telnet-access` command.

Table 7
no telnet-access command parameters and variables

Parameters and variables	Description
<code>source-ip</code> [<1-10>]	<p>Disables the Telnet access.</p> <p>When you do not use the optional parameter, the source-ip list is cleared, meaning that the 1st index is set to 0.0.0.0./0.0.0.0. and the 2nd to 10th indexes are set to 255.255.255.255/255.255.255.255. When you do specify a source-ip value, the specified pair is set to 255.255.255.255/255.255.255.255.</p> <div style="border: 1px solid black; padding: 5px;"> <p>ATTENTION</p> <p>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 for IPv4 addresses using NNCLI" (page 156) and "Configuring the IP Manager list for IPv6 addresses using NNCLI" (page 157).</p> </div>

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 executed in the Global Configuration command mode.

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

SSL configuration using NNCLI

This section describes how you can configure SSL to provide a secure Web management interface using NNCLI.

SSL configuration using NNCLI navigation

- [“Enabling SSL using NNCLI” \(page 67\)](#)
- [“Disabling SSL using NNCLI” \(page 67\)](#)
- [“Creating an SSL certificate using NNCLI” \(page 68\)](#)
- [“Deleting an SSL certificate using NNCLI” \(page 68\)](#)
- [“Viewing the SSL server configuration using NNCLI” \(page 69\)](#)
- [“Viewing the SSL certificate using NNCLI” \(page 70\)](#)

Enabling SSL using NNCLI

Enable SSL for the Web server to function in a secure mode.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable SSL by using the following command: <pre>ssl</pre>
--End--	

Disabling SSL using NNCLI

Disable SSL for the Web server to function in a nonsecure mode.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Disable SSL by using the following command: <code>no ssl</code>
--End--	

Creating an SSL certificate using NNCLI

Create an SSL certificate to replace the existing SSL certificate in NVRAM.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Create an SSL certificate by using the following command: <code>ssl certificate</code>
--End--	

Deleting an SSL certificate using NNCLI

Delete an SSL certificate to remove the existing SSL certificate from NVRAM.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Delete an SSL certificate by using the following command: <code>no ssl certificate</code>
--End--	

Viewing the SSL server configuration using NNCLI

View the SSL server configuration to display the SSL server configuration and SSL server state.

Prerequisites

- Log on to the Privileged EXEC mode in NNCLI.

Procedure steps

Step	Action
1	View the SSL server configuration by using the following command: <code>show ssl</code>
--End--	

Job aid: Viewing the SSL certificate configuration using NNCLI

Use the data in the following table to understand field descriptions displayed with the `show ssl` command.

Field	Description
WEB Server SSL secured:	Shows if the Web server uses an SSL connection.
SSL server state	Displays one of the following states: <ul style="list-style-type: none"> • Uninitialized: The server is not running. • Certificate Initialization: The server is generating a certificate during the initialization phase. • Active: The server is initialized and running.

Field		Description
SSL Certificate:	Generation in progress	Shows whether SSL is generating a certificate. The SSL server generates a certificate during server startup initialization, or NNCLI user can regenerate a new certificate.
	Saved in NVRAM:	Shows whether an SSL certificate exists in the NVRAM. The SSL certificate is not present if the system is being initialized for the first time or NNCLI user deleted the certificate.
	Certificate file size:	Displays the certificate file size in bytes.
	RSA host key length:	Displays the RSA host key length in bits.

Viewing the SSL certificate using NNCLI

View the SSL certificate to display the SSL certificate stored in NVRAM.

Prerequisites

- Log on to the Privileged EXEC mode in NNCLI.

Procedure steps

Step	Action
1	View the SSL certificate by using the following command: <code>show ssl certificate</code>
--End--	

Configuring Secure Shell using NNCLI

This section provides the command line interface commands to configure and manage SSH on the Ethernet Routing Switch 2500. The SSH protocol provides secure access to NNCLI. By using NNCLI, you can run the following commands:

- [“show ssh global command” \(page 71\)](#)
- [“show ssh session command” \(page 72\)](#)
- [“show ssh download-auth-key command” \(page 72\)](#)

- “ssh dsa-host-key command” (page 73)
- “no ssh dsa-host-key command” (page 73)
- “ssh command” (page 73)
- “no ssh command” (page 73)
- “ssh secure command” (page 74)
- “ssh timeout command” (page 74)
- “ssh dsa-auth command” (page 74)
- “no ssh dsa-auth command” (page 75)
- “ssh pass-auth command” (page 75)
- “no ssh pass-auth command” (page 75)
- “ssh port command” (page 75)
- “ssh download-auth-key command” (page 76)
- “no ssh dsa-auth-key command” (page 76)
- “default ssh command” (page 76)

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 executed in the Privileged EXEC command mode.

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

The following figure displays sample output from the `show ssh global` command.

Figure 6
show ssh global command output

```
2500-26T#show ssh global
Active SSH Sessions      : 0
Version                  : Version 2 only
Port                     : 22
Authentication Timeout   : 60
DSA Authentication       : True
Password Authentication   : True
DSA Auth Key IFTP Server : 192.168.249.10
DSA Auth Key File Name   :
DSA Host Keys            : Exist
Enabled                  : False
2500-26T#_
```

show ssh session command

The **show ssh session** command displays the SSH 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 executed in the Privileged EXEC command mode.

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

The following figure displays sample output from the **show ssh session** command.

Figure 7
show ssh session command output

```
2500-26T#show ssh session
Session Host
-----
1       0.0.0.0
2       0.0.0.0
2500-26T#
```

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 executed in the Privileged EXEC command mode.

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

The following figure displays sample output from the **ssh download-auth-key** command.

Figure 8
show ssh download-auth-key command output

```
2500-26T#show ssh download-auth-key
DSA Auth Key TFTP Server: 192.168.249.10
DSA Auth Key File Name   :
Last Transfer Result     : None
2500-26T#_
```


ssh dsa-host-key command

The switch starts generating the DSA host keys immediately after the `ssh dsa-host-key` command is given. A reboot is not necessary.

ATTENTION

You cannot enable SSH while the host key is being generated.

This command can only be executed in SSH disable mode. The syntax of the `ssh dsa-host-key` command is:

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

The `ssh dsa-host-key` command is executed in the Global Configuration command mode.

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

no ssh dsa-host-key command

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

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

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

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

ssh command

The `ssh` command enables the SSH server on the Ethernet Routing Switch 2500 in nonsecure mode. In addition to accepting SSH connections, the Ethernet Routing Switch 2500 continues to accept SNMP, and Telnet connections while in this mode. The syntax of the `ssh` command is:

```
ssh
```

The `ssh` command is executed in the Global Configuration 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 Ethernet Routing Switch 2500. The syntax of the `no ssh` command is:

```
no ssh
```

The `no ssh` command executed in the Global Configuration 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 Ethernet Routing Switch 2500 in secure mode. In secure mode, the Ethernet Routing Switch 2500 does not accept SNMP, or Telnet connections. The syntax of the `ssh secure` command is:

```
ssh secure
```

The `ssh secure` command executed in the Global Configuration command mode.

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

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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `ssh timeout` command.

Table 8
ssh timeout command parameters and variables

Parameters and variables	Description
<1-120>	Specifies the timeout value for authentication. The 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 executed in the Global Configuration 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 for the `no ssh dsa-auth` command is:

```
no ssh dsa-auth
```

The `no ssh dsa-auth` command executed in the Global Configuration 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 executed in the Global Configuration 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 of the `no ssh pass-auth` command is:

```
no ssh pass-auth
```

The `no ssh pass-auth` command executed in the Global Configuration 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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `ssh port` command.

Table 9
ssh port command parameters and variables

Parameters and variables	Description
<1-65535>	Specifies the SSH connection port. The default is 22.

ssh download-auth-key command

The `ssh download-auth-key` command downloads the client public key from the TFTP server to the Ethernet Routing Switch 2500. The syntax for the `ssh download-auth-key` is:

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

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

The following table describes the parameters and variables for the `ssh download-auth-key` command.

Table 10
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.

no ssh dsa-auth-key command

The `no ssh dsa-auth-key` command deletes the SSH DSA authentication key. The syntax for the command is:

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

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

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

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|pass-auth|port|timeout]
```

The `default ssh` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `default ssh` command.

Table 11
default ssh command parameters and variables

Parameters and variables	Description
<code>dsa-auth</code>	Resets dsa-auth to the default value. Default is True.
<code>pass-auth</code>	Resets pass-auth to the default value. Default is True.
<code>port</code>	Resets the port number for SSH connections to the default. Default is 22.
<code>timeout</code>	Resets the timeout value for session authentication to the default. Default is 60.

RADIUS Interim Accounting Updates support configuration using NNCLI

Use the procedures in this section to configure RADIUS Interim Accounting Updates support on the Ethernet Routing Switch 2500.

RADIUS Interim Accounting Updates support configuration using NNCLI navigation

- [“Configuring RADIUS Interim Accounting Updates support using NNCLI” \(page 77\)](#)
- [“Disabling RADIUS Interim Accounting Updates support using NNCLI” \(page 78\)](#)
- [“Configuring RADIUS Interim Accounting Updates support defaults using NNCLI” \(page 79\)](#)
- [“Viewing RADIUS Interim Accounting Updates support status using NNCLI” \(page 80\)](#)

Configuring RADIUS Interim Accounting Updates support using NNCLI

Configure RADIUS Interim Accounting Updates support to permit the RADIUS server to make policy decisions based on real-time network attributes transmitted by the NAS.

Prerequisites

- Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure RADIUS Interim Accounting Updates support by using the following command: <pre>radius accounting interim-updates<enable> [interval <seconds>] <use-server-interval></pre>
	--End--

Variable definitions

The following table defines optional parameters that you enter with the `radius accounting interim-updates<enable> [interval <seconds>] <use-server-interval>` command.

Variable	Value
<code>enable</code>	Enables RADIUS Interim Accounting Updates support statically on the switch.
<code>interval <seconds></code>	Specifies the RADIUS Interim Accounting Updates support timeout interval in seconds. Values range from 60 to 3600 seconds. The default is 600 seconds.
<code>use-server-interval</code>	Selects the value transmitted by the RADIUS server as the RADIUS Interim Accounting Updates support timeout interval.

Disabling RADIUS Interim Accounting Updates support using NNCLI

Disable RADIUS Interim Accounting Updates support to prevent the RADIUS server from making policy decisions based on real-time network attributes transmitted by the NAS.

Prerequisites

- Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Disable RADIUS Interim Accounting Updates support by using the following command:

```
no radius accounting interim-updates <enable>
<use-server-interval>
```

--End--

Variable definitions

The following table defines optional parameters that you enter with the `no radius accounting interim-updates <enable> <use-server-interval>` command.

Variable	Value
<code>enable</code>	Disables RADIUS Interim Accounting Updates support statically on the switch.
<code>use-server-interval</code>	Sets the locally-configured server interval for use as the source RADIUS Interim Accounting Updates support timeout interval.

Configuring RADIUS Interim Accounting Updates support defaults using NNCLI

Configure RADIUS Interim Accounting Updates support defaults to define the default values the RADIUS server uses to make policy decisions based on real-time network attributes transmitted by the NAS.

Prerequisites

- Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure RADIUS Interim Accounting Updates support defaults by using the following command: <pre>default radius accounting interim-updates <enable> <interval> <use-server-interval></pre> <hr/> <p style="text-align: center;">--End--</p> <hr/>

Variable definitions

The following table defines optional parameters that you enter with the `default radius accounting interim-updates <enable> <interval> <use-server-interval>` command.

Variable	Value
<code>enable</code>	Configures the RADIUS Interim Accounting Updates support default status on the switch as disabled.
<code>interval</code>	Configures the default RADIUS Interim Accounting Updates support default interval on the switch as 600 seconds.
<code>use-server-interval</code>	Specifies the value transmitted by the RADIUS server as the default RADIUS Interim Accounting Updates support timeout interval source.

Viewing RADIUS Interim Accounting Updates support status using NNCLI

View RADIUS Interim Accounting Updates support status to review and confirm the configuration of parameters the RADIUS server uses to make policy decisions based on real-time network attributes transmitted by the NAS.

Prerequisites

- Log on to the User EXEC mode in NNCLI.

Procedure steps

Step	Action
1	Viewing RADIUS Interim Accounting Updates support by using the following command: <code>show radius accounting interim-updates</code>
	--End--

Job aid: show radius accounting interim-updates command output

The following figure shows sample output for the `show radius accounting interim-updates` command.

Figure 9

show radius accounting interim-updates command output

```
ERS-2500-50T-PWR>show radius accounting interim-updates
RADIUS accounting interim-updates: Disabled
RADIUS accounting interim-updates interval: 300
RADIUS accounting use-server-interval: Disabled
ERS-2500-50T-PWR>
```


RADIUS Request use Management IP configuration using NNCLI

You can enable or disable the use of Management VLAN IP by RADIUS requests using NNCLI.

RADIUS Request use Management IP configuration using NNCLI navigation

- [“Enabling RADIUS Request use Management IP using NNCLI” \(page 81\)](#)
- [“Disabling RADIUS Request use Management IP using NNCLI” \(page 81\)](#)
- [“Viewing RADIUS Request use Management IP status using NNCLI” \(page 82\)](#)

Enabling RADIUS Request use Management IP using NNCLI

Enable RADIUS Request use Management IP to enable the RADIUS requests to use the Management VLAN IP address.

Prerequisites

- Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable RADIUS Request use Management IP by using one of the following commands: <pre>radius use-management-ip default radius use-management-ip</pre> <hr/> <p style="text-align: center;">--End--</p> <hr/>

Disabling RADIUS Request use Management IP using NNCLI

Disable RADIUS Request use Management IP to prevent the RADIUS requests from using the Management VLAN IP address.

Prerequisites

- Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable RADIUS Request use Management IP by using the following command: <code>no radius use-management-ip</code> --End--

Viewing RADIUS Request use Management IP status using NNCLI

View RADIUS Request use Management IP status to see the feature is currently enabled or disabled.

Prerequisites

- Log on to the User EXEC mode in NNCLI.

Procedure steps

Step	Action
1	View RADIUS Request use Management IP status by using the following command: <code>show radius use-management-ip</code> --End--

Configuring the RADIUS-based management password authentication using NNCLI

By using the RADIUS protocol and server, you can configure the Ethernet Routing Switch 2500 for authentication. To configure this authentication by using NNCLI system, you can use the following commands:

- [“show radius-server command” \(page 83\)](#)
- [“radius-server command” \(page 83\)](#)
- [“no radius-server command” \(page 84\)](#)
- [“default radius-server command” \(page 84\)](#)
- [“radius-server password fallback command” \(page 84\)](#)

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 executed in the Privileged EXEC command mode.

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

The following figure shows sample output from the `show radius-server` command.

Figure 10
show radius-server command output

```
2500-26T#show radius-server
Password Fallback: Enabled
Primary Host: 0.0.0.0
Secondary Host: 0.0.0.0
Port: 1812
Key: *****
2500-26T#
```

radius-server command

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

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

ATTENTION

When password security is enabled, you must omit the `<string>` variable from the command line and end the command immediately after `key`. The switch then prompts you to enter and confirm the string.

The `radius-server` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `radius-server` command.

Table 12
radius-server command parameters and variables

Variable	Value
<code>host <address></code>	Specifies the primary RADIUS server. Enter the IP address of the RADIUS server.

Table 12
radius-server command parameters and variables (cont'd.)

Variable	Value
<code>key <string></code>	Specifies a secret text string that is shared between the switch and the RADIUS server for authentication. Enter the secret string, which is an alphanumeric string of up to 16 characters.
<code>password fallback</code>	Enables RADIUS password fallback.
<code>port <num></code>	Enter the port number of the RADIUS server.
<code>secondary-host <address></code>	Specifies the secondary RADIUS server. Enter the IP address of the secondary RADIUS server.
<code>timeout <num></code>	Specifies the RADIUS time-out period.

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 executed in the Global Configuration command mode.

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

default radius-server command

The `default radius-server` command sets the RADIUS server settings to the default values. The syntax for the `default radius-server` command is:

```
default radius-server
```

The `default radius-server` command is executed in the Global Configuration command mode.

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

radius-server password fallback command

With the `radius-server password fallback` command, you can configure password fallback as an option when you use RADIUS authentication for logon and password. When both RADIUS servers are unreachable the user can log in using the local passwords.

The syntax for the `radius-server password fallback` command is:

```
radius-server password fallback
```

The `radius-server password fallback` command is executed in the Global Configuration command mode.

802.1X dynamic authorization extension (RFC 3576) configuration using NNCLI

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

RADIUS dynamic authorization extension (802.1X RFC 3576) configuration using NNCLI navigation

- [“Configuring RADIUS dynamic authorization extension \(802.1X RFC 3576\) using NNCLI” \(page 85\)](#)
- [“Disabling RADIUS dynamic authorization extension \(802.1X RFC 3576\) using NNCLI” \(page 87\)](#)
- [“Viewing RADIUS dynamic authorization client configuration using NNCLI” \(page 87\)](#)
- [“Viewing RADIUS dynamic authorization client statistics using NNCLI” \(page 88\)](#)
- [“Enabling RADIUS dynamic authorization extension \(802.1X RFC 3576\) on a port using NNCLI” \(page 89\)](#)
- [“Disabling RADIUS dynamic authorization extension \(802.1X RFC 3576\) on a port using NNCLI” \(page 90\)](#)
- [“Viewing replay protection for RADIUS dynamic authorization extension using NNCLI” \(page 91\)](#)
- [“Disabling replay protection for RADIUS dynamic authorization extension using NNCLI” \(page 91\)](#)
- [“Enabling replay protection for RADIUS dynamic authorization extension using NNCLI” \(page 91\)](#)

Configuring RADIUS dynamic authorization extension (802.1X RFC 3576) using NNCLI

Configure RADIUS dynamic authorization extension (802.1X RFC 3576) to enable and configure RADIUS dynamic authorization extension parameters on the switch.

Prerequisites

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

ATTENTION

Disconnect or CoA commands are ignored if the commands address a port on which the feature is not enabled

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure RADIUS dynamic authorization extension by using the following command: <pre>radius dynamic-server client <A.B.C.D.></pre>
	--End--

Variable definitions

The following table defines parameters that you enter with the `radius dynamic-server client <A.B.C.D.>` command.

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

Disabling RADIUS dynamic authorization extension (802.1X RFC 3576) using NNCLI

Disable RADIUS dynamic authorization extension (802.1X RFC 3576) to prevent the RADIUS server from sending a change of authorization (CoA) or disconnect command to the Network Access Server (NAS).

Procedure steps

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

Variable definitions

The following table defines variable parameters that you enter with the `no radius dynamic-server client <A.B.C.D.>` command.

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

Viewing RADIUS dynamic authorization client configuration using NNCLI

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

Prerequisites

- Log on to the Privileged EXEC mode in NNCLI.

Procedure steps

Step	Action
1	Configure View RADIUS dynamic authorization client configuration by using the following command:

```
show radius dynamic-server client <A.B.C.D.>
```

--End--

Variable definitions

The following table defines parameters that you enter with the `show radius dynamic-server client <A.B.C.D.>` command.

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

Job aid: Viewing RADIUS dynamic authorization client configuration using NNCLI

The following figure displays sample output for the `show radius dynamic-server client <A.B.C.D.>` command.

Figure 11
Job aid: show radius dynamic-server client output

```
2526T#show radius dynamic-server client 1.1.1.2
Client      UDP      Client   Process   Process
Address     Port    Enabled  Disconnect Coa
-----
1.1.1.2     3799   No       Disabled  Disabled *****
2526T#
```

Viewing RADIUS dynamic authorization client statistics using NNCLI

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

Prerequisites

- Log on to the Privileged EXEC mode in NNCLI.

Procedure steps

Step	Action
1	Configure View RADIUS dynamic authorization client configuration by using the following command:


```
show radius dynamic-server statistics client
<A.B.C.D.>
```

--End--

Variable definitions

The following table defines parameters that you enter with the `show radius dynamic-server statistics client <A.B.C.D.>` command.

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

Job aid: Viewing RADIUS dynamic authorization client statistics using NNCLI

The following figure displays sample output for the `show radius dynamic-server statistics client <A.B.C.D.>` command.

Figure 12
show radius dynamic-server statistics client output

```
2526T#show radius dynamic-server statistics client 1.1.1.2
Disconnects From Invalid Client Addresses: 0
CoAs From Invalid Client Addresses: 0
-----
Client Address:1.1.1.2
                Disconnect      Change
                -----      -
Requests          0              0
AuthOnlyRequests  0              0
DupRequests       0              0
ACKs              0              0
NAKs              0              0
NAKAuthOnlyRequests 0              0
NAKSessNoContext  0              0
UserSessRemoved   0              0
MalformedRequests 0              0
BadAuthenticatorRequests 0          0
PacketsDropped    0              0
2526T#_
```

Enabling RADIUS dynamic authorization extension (802.1X RFC 3576) on a port using NNCLI

Enable RADIUS dynamic authorization extension (802.1X RFC 3576) on a port to use RADIUS dynamic authorization extension on the port.

Prerequisites

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

ATTENTION

Disconnect or CoA commands are ignored if the commands address a port on which the feature is not enabled

- Log on to the Interface Configuration mode in NNCLI.

Step	Action
1	Enable RADIUS dynamic authorization extension on a port by using the following command: <code>eaop1 radius-dynamic-server enable</code> <hr/> <p style="text-align: center;">--End--</p> <hr/>

Disabling RADIUS dynamic authorization extension (802.1X RFC 3576) on a port using NNCLI

Disable RADIUS dynamic authorization extension (802.1X RFC 3576) on a port to discontinue using RADIUS dynamic authorization extension on the port.

Prerequisites

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

ATTENTION

Disconnect or CoA commands are ignored if the commands address a port on which the feature is not enabled

- Log on to the Interface Configuration mode in NNCLI.

Step	Action
1	Enable RADIUS dynamic authorization extension on a port by using the following command: <code>no eaop1 radius-dynamic-server enable</code> <hr/> <p style="text-align: center;">--End--</p> <hr/>

Viewing replay protection for RADIUS dynamic authorization extension using NNCLI

Use this procedure to display replay protection for RADIUS dynamic authorization extension.

Step	Action
1	Display RADIUS dynamic server replay protection by using the following command: <code>show radius dynamic-server replay-protection</code>
--End--	

Disabling replay protection for RADIUS dynamic authorization extension using NNCLI

Use this procedure to disable replay protection for RADIUS dynamic authorization extension.

Step	Action
1	Disable RADIUS dynamic server replay protection by using the following command: <code>no radius dynamic-server replay-protection</code>
--End--	

Enabling replay protection for RADIUS dynamic authorization extension using NNCLI

Use this procedure to enable replay protection for RADIUS dynamic authorization extension.

Step	Action
1	Re-enable RADIUS dynamic server replay protection by using the following command: <code>default radius dynamic-server replay-protection</code>
--End--	

Setting SNMP parameters using NNCLI

For information about setting SNMP parameters and traps, see the following sections:

- [“Common SNMP and SNMPv3 NNCLI commands” \(page 92\)](#)
- [“NNCLI commands specific to SNMPv3” \(page 105\)](#)

Common SNMP and SNMPv3 NNCLI commands

This section describes the common NNCLI commands that you can use to configure SNMP and SNMPv3. For details about the SNMP NNCLI commands that are specific to SNMPv3, see [“NNCLI commands specific to SNMPv3” \(page 105\)](#).

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

- [“snmp-server command” \(page 93\)](#)
- [“no snmp-server command” \(page 93\)](#)
- [“snmp-server notification-control authenticationFailure command” \(page 94\)](#)
- [“no snmp-server notification-control authenticationFailure command” \(page 94\)](#)
- [“default snmp-server notification-control authenticationFailure command” \(page 94\)](#)
- [“snmp-server community for read/write command” \(page 94\)](#)
- [“no snmp-server community command” \(page 95\)](#)
- [“default snmp-server community command” \(page 96\)](#)
- [“show snmp-server community command” \(page 97\)](#)
- [“snmp-server contact command” \(page 97\)](#)
- [“no snmp-server contact command” \(page 97\)](#)
- [“default snmp-server contact command” \(page 98\)](#)
- [“snmp-server location command” \(page 98\)](#)
- [“no snmp-server location command” \(page 98\)](#)
- [“default snmp-server location command” \(page 99\)](#)
- [“snmp-server name command” \(page 99\)](#)
- [“no snmp-server name command” \(page 99\)](#)
- [“default snmp-server name command” \(page 100\)](#)
- [“snmp trap link-status command” \(page 100\)](#)

- “no snmp trap link-status command” (page 101)
- “default snmp trap link-status command” (page 101)
- “snmp-server notify-filter command” (page 102)
- “no snmp-server notify-filter command” (page 103)
- “snmp-server notification-control command ” (page 104)
- “no snmp-server notification-control command ” (page 104)

snmp-server command

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

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

The `snmp-server` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `snmp-server` command.

Table 13
snmp-server command parameters and variables

Parameters and variables	Description
enable disable	Enables or disables the SNMP server.

no snmp-server command

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

```
no snmp-server
```

The `no snmp-server` command is executed in the Global Configuration command mode.

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

ATTENTION

Disabling SNMP access also locks you out of Enterprise Device Manager management system.

snmp-server notification-control authenticationFailure command

The `snmp-server notification-control authenticationFailure` command enables the generation of SNMP authentication failure traps. The syntax for the `snmp-server notification-control authenticationFailure` command is:

```
snmp-server notification-control authenticationFailure
```

The `snmp-server notification-control authenticationFailure` command is executed in the Global Configuration command mode.

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

no snmp-server notification-control authenticationFailure command

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

```
no snmp-server notification-control authenticationFailure
```

The `no snmp-server notification-control authenticationFailure` command is executed in the Global Configuration command mode.

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

default snmp-server notification-control authenticationFailure command

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

```
default snmp-server notification-control authenticationFailure
```

The `default snmp-server notification-control authenticationFailure` command is executed in the Global Configuration command mode.

The `default snmp-server notification-control authenticationFailure` 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 SNMPv1 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` read/write command is executed in the Global Configuration command mode.

This command configures a single read-only or a single read/write community. A community configured using this command has no access to any of the SNMPv3 MIBs.

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

The following table describes the parameters and variables for the `snmp-server community` for read/write command.

Table 14
snmp-server community for read/write command parameters and variables

Parameters and variables	Description
<code><community-string></code>	<p>Changes community strings for SNMP v1 and SNMPv2c access. Enter a community string that functions as a password and permits access to the SNMP protocol. If you set the value to NONE, it is disabled.</p> <div style="border: 1px solid black; padding: 5px;"> <p>ATTENTION 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.</p> </div>
<code>ro rw</code>	<p>Specifies read-only or read/write access. Stations with <code>ro</code> access can retrieve only MIB objects, and stations with <code>rw</code> access can retrieve and modify MIB objects.</p> <div style="border: 1px solid black; padding: 5px;"> <p>ATTENTION If neither <code>ro</code> nor <code>rw</code> is specified, <code>ro</code> is assumed (default).</p> </div>

no snmp-server community command

The `no snmp-server community` command clears the `snmp-server community` configuration. The syntax for the `no snmp-server community` command is:

```
no snmp-server community {ro|rw|<community-string>}
```

The `no snmp-server community` command is executed in the Global Configuration command mode.

If you do not specify a read-only or read/write community parameter, all community strings are removed, including all communities controlled by the `snmp-server community` command and the `snmp-server community` command for read-write.

If you specify read-only or read/write, then only 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.

The following table describes the parameters and variables for the `no snmp-server community` command.

Table 15
no snmp-server community command parameters and variables

Parameters and variables	Description
ro rw	Sets the specified community string value to <code>NONE</code> , thereby disabling it.
<community-string>	Deletes the specified community string from the SNMPv3 MIBs (that is, from the new-style configuration).

default snmp-server community command

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

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

The `default snmp-server community` command is executed in the Global Configuration command mode.

If the read-only or read/write parameter is omitted from the command, 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.

The following table describes the parameters and variables for the `default snmp-server community` command.

Table 16
default snmp-server community command parameters and variables

Parameters and variables	Description
ro rw	Restores the read-only community to <code>public</code> , or the read/write community to <code>private</code> .

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 executed in the Privileged EXEC 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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `snmp-server contact` command.

Table 17
snmp-server contact command parameters and variables

Parameters and variables	Description
<text>	Specifies the SNMP <code>sysContact</code> 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 executed in the Global Configuration 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 executed in the Global Configuration 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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `snmp-server location` command.

Table 18
snmp-server location command parameters and variables

Parameters and variables	Description
<text>	Specifies the SNMP <code>sysLocation</code> 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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `no snmp-server location` command.

Table 19
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 executed in the Global Configuration 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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `snmp-server name` command.

Table 20
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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `no snmp-server name` command.

Table 21
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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `default snmp-server name` command.

Table 22
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 executed in the Interface Configuration command mode.

The following table describes the parameters and variables for the `snmp trap link-status` command.

Table 23
snmp trap link-status command parameters and variables

Parameters and variables	Description
port <portlist>	Specifies the port numbers on which to enable the linkUp/linkDown traps. Enter the port numbers or all. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>ATTENTION If you omit this parameter, the system uses the port number specified with the <code>interface</code> command.</p> </div>
disable enable	Disables or Enables generation of linkUp/Down traps.

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 executed in the Interface Configuration command mode.

The following table describes the parameters and variables for the `no snmp trap link-status` command.

Table 24
no snmp trap link-status command parameters and variables

Parameters and variables	Description
port <portlist >	Specifies the port numbers on which to disable the linkUp/linkDown traps. Enter the port numbers or all. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>ATTENTION If you omit this parameter, the system uses the port number specified with the <code>interface</code> command.</p> </div>

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 executed in the Interface Configuration command mode.

The following table describes the parameters and variables for the `no snmp trap link-status` command.

Table 25
default snmp trap link-status command parameters and variables

Parameters and variables	Description
<code>port <portlist></code>	<p>Specifies the port numbers on which to disable the linkUp/linkDown traps. Enter the port numbers or all.</p> <div style="border: 1px solid black; padding: 5px;"> <p>ATTENTION If you omit this parameter, the system uses the port number specified with the <code>interface</code> command.</p> </div>

snmp-server notify-filter command

You can use the `snmp-server notify-filter` command to add SNMP traps to a filter profile (filter name).

The syntax for the `snmp-server notify-filter` command is:

```
<filterName:WORD> <OID:WORD> [<OID:WORD> [<OID:WORD>
[<OID:WORD> [<OID:WORD> [<OID:WORD> <OID:WORD> [<OID:WORD>
[<OID:WORD> [<OID:WORD>]]]]]]]]
```

The `snmp-server notify-filter` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `snmp-server notify-filter` command

Table 26
snmp-server notify-filter command parameters and variables

Parameters and variables	Value
<code><filterName></code>	Specifies the filter profile name.
<code><WORD></code>	<p>Specifies the description of OID specification of the SNMP trap added to the filterName filter.</p> <p>By default, each OID specified is included in the filter. To indicate that an OID is included in the filter, insert a plus sign (+) at the beginning of</p>

Parameters and variables	Value
	the OID; example +OID. To indicate that an OID is excluded from the filter, insert a minus sign (–) at the beginning of the OID; example –OID.

no snmp-server notify-filter command

You can use the `snmp-server notify-filter` command to delete SNMP traps from a filter profile (filter name).

The syntax for the `snmp-server notify-filter` command is:

```
no <filterName:WORD> [<OID:WORD>]
```

The `no snmp-server notify-filter` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `no snmp-server notify-filter` command

Table 27
no snmp-server notify-filter command parameters and variables

Parameters and variables	Value
<filterName>	Specifies the filter profile name.
<WORD>	Specifies the description of OID specification of the SNMP trap added to the filterName filter. By default, each OID specified is included in the filter. To indicate that an OID is included in the filter, insert a plus sign (+) at the beginning of the OID; example +OID. To indicate that an OID is excluded from the filter, insert a minus sign (–) at the beginning of the OID; example –OID.

show snmp-server notify-filter command

The `show snmp-server notify-filter` command displays notify-filter details. The syntax for the this command is:

```
show snmp-server notify-filter
```

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

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

The following table describes the fields for the `show snmp-server notify-filter` command.

Table 28
show snmp-server notify-filter field descriptions

Field	Description
Profile Name	Specifies the filter profile name.
Subtree	Specifies the filter subtree address.
Mask	Specifies the filter mask.

snmp-server notification-control command

The `snmp-server notification-control` command enables the generation of SNMP traps. The syntax for the `snmp-server notification-control` command is:

```
snmp-server notification-control <notification>
```

The `snmp-server notification-control` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `snmp-server notification-control` command.

Table 29
snmp-server notification-control command parameters and variables

Parameters and variables	Value
<notification>	Specifies the name or the OID of the notification to be enabled

no snmp-server notification-control command

The `no snmp-server notification-control` command disables the generation of SNMP traps. The syntax for the `no snmp-server notification-control` command is:

```
no snmp-server notification-control <notification>
```

The `no snmp-server notification-control` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `no snmp-server notification-control` command.

Table 30
no snmp-server notification-control command parameters and variables

Parameters and variables	Value
<notification>	Specifies the name or the OID of the notification to be enabled

NNCLI commands specific to SNMPv3

This section describes the unique NNCLI commands for configuring SNMPv3. For details about NNCLI commands that are common to both SNMP and SNMPv3, see [“Common SNMP and SNMPv3 NNCLI commands” \(page 92\)](#).

The following SNMP commands are specific to SNMPv3:

- [“snmp-server user command” \(page 105\)](#)
- [“no snmp-server user command” \(page 107\)](#)
- [“snmp-server view command” \(page 108\)](#)
- [“no snmp-server view command” \(page 109\)](#)
- [“snmp-server host command” \(page 109\)](#) [“snmp-server host command” \(page 109\)](#)
- [“no snmp-server host command” \(page 111\)](#)
- [“default snmp-server host command” \(page 112\)](#)
- [“show snmp-server host command” \(page 112\)](#)
- [“snmp-server community command” \(page 113\)](#)
- [“snmp-server bootstrap command” \(page 115\)](#)

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 [engine-id <engineid>] <username>
[read-view <view-name>]
[write-view <view-name>] [notify-view <view-name>]
[{md5|sha} <password>] [read-view <view-name>]
[write-view <view-name>] [notify-view <view-name>]
[{3des|aes|des} <password>] [read-view <view-name>]
[write-view <view-name>] [notify-view <view-name>]
```

The `snmp-server user` command is executed in the Global Configuration command mode.

The `sha` and `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`, `aes`, or `3des` 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 that are used for authenticated access. These views are the unauthenticated views, if all the authenticated views are also omitted.

The following table describes the parameters and variables for the `snmp-server user` command.

Table 31
snmp-server user command parameters and variables

Parameters and variables	Description
<code>engine-id</code> <code><engineid></code>	Specifies the SNMP engine ID of the remote SNMP entity.
<code><username></code>	Specifies the user names; enter an alphanumeric string of up to 255 characters.
<code>md5/sha <password></code>	<p>Specifies the use of an md5/sha authentication pass phrase.</p> <ul style="list-style-type: none"> <code>password</code>—specifies the new user md5/sha authentication pass phrase; enter an alphanumeric string. <p>If this parameter is omitted, the user is created with only unauthenticated access rights.</p> <div style="border: 1px solid black; padding: 5px;"> <p>ATTENTION This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password.</p> </div>

Table 31
snmp-server user command parameters and variables (cont'd.)

Parameters and variables	Description
<code>read-view</code> <code><view-name></code>	Specifies the read view to which the new user has access: <ul style="list-style-type: none"> • <code>view-name</code>—specifies the view name; enter an alphanumeric string of up to 255 characters.
<code>write-view</code> <code><view-name></code>	Specifies the write view to which the new user has access: <ul style="list-style-type: none"> • <code>view-name</code>—specifies the view name; enter an alphanumeric string of up to 255 characters.
<code>notify-view</code> <code><view-name></code>	Specifies the notify view to which the new user has access: <ul style="list-style-type: none"> • <code>view-name</code>— specifies the view name; enter an alphanumeric string of up to 255 characters.
<code>des/aes/3des</code> <code><password></code>	Specifies the use of a des/aes/3des privacy pass phrase. <ul style="list-style-type: none"> • <code>password</code>—specifies the new user des/aes/3des privacy pass phrase; enter an alphanumeric string of minimum 8 characters. If this parameter is omitted, the user is created with only authenticated access rights. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>ATTENTION This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password.</p> </div>

no snmp-server user command

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

```
no snmp-server user [engine-id <engineid>] <username>
```

The `no snmp-server user` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `no snmp-server user` command.

Table 32
no snmp-server user command parameters and variables

Parameters and variables	Description
engine-id <engineid>	Specifies the SNMP engine ID of the remote SNMP entity.
<username>	Specifies the user to be removed.

snmp-server view command

The `snmp-server view` command creates an SNMPv3 view. The view is a set of MIB object instances 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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `snmp-server view` command.

Table 33
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 the Object identifier. <code>OID</code> can be entered as a MIB object English descriptor, a dotted form <code>OID</code> , or a mix of the two. Each <code>OID</code> can also be preceded by a plus (+) or minus (-) sign (if the minus sign is omitted, a plus sign is implied). For the dotted form, a subidentifier can be an asterisk (*), which indicates a wildcard. Some examples of valid <code>OID</code> parameters are as follows: <ul style="list-style-type: none"> • <code>sysName</code> • <code>+sysName</code> • <code>-sysName</code> • <code>+sysName.0</code> • <code>+ifIndex.1</code>

Parameters and variables	Description
	<ul style="list-style-type: none"> • <code>-ifEntry.*.1</code> (matches all objects in the if Table with an instance of 1, that is, the entry for interface #1) • <code>1.3.6.1.2.1.1.1.0</code> (dotted form of <code>sysDescr</code>) <p>The plus (+) or minus (-) sign indicates whether the specified <code>OID</code> is included in or excluded from, respectively, the set of MIB objects that are accessible by using this view. For example, if you create a view as follows:</p> <pre>snmp-server view myview +system -sysDescr</pre> <p>and you use that view for the read-view of a user, then the user can read only the system group, except for <code>sysDescr</code>.</p>

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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `no snmp-server view` command.

Table 34
no snmp-server view command parameters and variables

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

snmp-server host command

The `snmp-server host` command adds a trap receiver to the SNMPv3 tables. You can create several entries in this table, and each can generate v1, v2c, or v3 traps. You can use notification filters to trap receivers and include SNMP traps in notification filters. You must previously configure the community string or user that is specified with a `notify-view`. The syntax for the `snmp-server host` command is:

```
snmp-server host {A.B.C.D} [<ipv6addr>] [port <1-65535>]
{<community-string:WORD> | v1 <communityString:WORD> |
v2c <communityString:WORD> [inform [timeout <1-2147483647>]
[retries <0-255>]] |
v3 {auth|no-auth|auth-priv} <username:WORD> [inform [timeout
<1-2147483647>] [retries <0-255>]]} [filter <WORD>] [target-name
<WORD/1-32>]>
```

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

The following table describes the parameters and variables for the `snmp-server host` command.

Table 35
snmp-server host command parameters and variables

Parameters and variables	Description
<code>port <1-65535></code>	Sets the SNMP trap port.
<code>A.B.C.D</code>	Specifies the dotted-decimal IP address of a host to be the trap destination.
<code><community-string:WORD></code>	If you do not specify a trap type, this variable creates v1 trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels.
<code>filter <WORD></code>	Specifies the filter profile name. The <code>snmp-server host</code> command is improved with the filter parameter only for the hosts with a specified SNMP version (v1/v2c/v3). Add the filter parameter only for the normal syntax form of the <code>snmp-server host</code> command. When you delete a specific SNMP-server host with the <code>no</code> command or delete all configured SNMP-server hosts with the <code>default</code> command, the associated filters are also deleted.
<code>inform</code>	Generates acknowledge inform requests.
<code><ipv6addr></code>	Specifies the IPv6 address of the SNMP notification host.
<code>retries <0-255></code>	Specifies the number of retries for inform requests. The range is 0-2147483647.
<code>target-name <WORD/1-32></code>	Specifies the name of the target.

Table 35
snmp-server host command parameters and variables (cont'd.)

Parameters and variables	Description
<code>timeout <1-2147483647></code>	Specifies the timeout for inform requests. The range is 1-2147483647 centi-seconds..
<code><username:WORD></code>	Specifies the SNMPv3 user name for trap destination; enter an alphanumeric string.
<code>v1 <community-string:WORD></code>	Creates v1 trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels.
<code>v2c <community-string:WORD ></code>	Creates v2c trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels.
<code>v3 {auth no-auth auth-priv}</code>	Using v3 creates v3 trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels by entering the following variables: <ul style="list-style-type: none"> • <code>auth no-auth</code>—Specifies whether SNMPv3 traps can be authenticated. • <code>auth-priv</code>—This parameter is only available if the image has full SHA/DES support.

no snmp-server host command

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

```
no snmp-server host {A.B.C.D) | <ipv6addr>} {v1|v2c|v3}
```

The `no snmp-server host` command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `no snmp-server` command.

ATTENTION

When you delete a specific SNMP-server host with the `no` command or delete all configured SNMP-server hosts with the `default` command, the associated filters are also deleted.

Table 36
no snmp-server host command parameters and variables

Parameters and variables	Description
<ipv6addr>	Specifies the IPv6 address of the SNMP notification host.
<A.B.C.D>	Specifies the IP address of a trap destination host.
v1 v2c v3	Specifies the trap receivers in the SNMPv3 MIBs.

default snmp-server host command

The `default snmp-server host` command restores the 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 executed in the Global Configuration command mode.

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

ATTENTION

When you delete a specific SNMP-server host with the `no` command or delete all configured SNMP-server hosts with the `default` command, the associated filters are also deleted.

show snmp-server host command

The `show snmp-server host` command displays SNMP-server host-related information. The syntax for the `show snmp-server host` command is:

```
show snmp-server host
```

The `show snmp-server host` command is executed in the Privileged EXEC command mode.

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

The following figure shows partial output for the `show snmp-server host` command.

Figure 13
show snmp-server host command output (partial)

```

2526T(config)#show snmp-server host          10 Filter FILTER
-----
Notify Group: inform
Type          : Inform
Storage Type  : Read-Only
Status       : Active
-----
Destination   Port   Timeout  Rtr  SNMP Security  Community String
Address       Port   Timeout  Rtr  Uers  Level  or User Name
-----
1.1.1.1       162   10000    10  U3   Auth   WORD
-----
Notify Group: s50gTrpRcvr
Type          : Trap
Storage Type  : Read-Only
Status       : Active
-----
Destination   Port   Timeout  Rtr  SNMP Security  Community String
Address       Port   Timeout  Rtr  Uers  Level  or User Name
-----
1.1.1.1       162   1500     3   U2C  NoAuth *****
-----

```

snmp-server community command

With the **snmp-server community** command, you can create community strings with varying levels of read, write, and notification access based on SNMPv3 views. These community strings are separate from those created by using the **snmp-server community** command for read/write.

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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the **snmp-server community** command.

Table 37
snmp-server community command parameters and variables

Parameters and variables	Description
<code><community-string></code>	Enter a community string to be created with access to the specified views. <div style="border: 1px solid black; padding: 5px;"> <p>ATTENTION 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.</p> </div>
<code>read-view <view-name></code>	Changes the read view used by the new community string for different types of SNMP operations. <ul style="list-style-type: none"> • <code>view-name</code>—specifies the name of the view that is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.
<code>ro</code>	Read-only access with this community string.
<code>rw</code>	Read-write access with this community string.
<code>write-view <view-name></code>	Changes the write view used by the new community string for different types of SNMP operations. <ul style="list-style-type: none"> • <code>view-name</code>—specifies the name of the view that is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.
<code>notify-view <view-name></code>	Changes the notify view settings used by the new community string for different types of SNMP operations. <ul style="list-style-type: none"> • <code>view-name</code>—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 executed in the Privileged EXEC command mode.

The following table describes the parameters and variables for the `show snmp-server` command.

Table 38
show snmp-server command parameters and variables

Parameters and variables	Description
<code>community host user view</code>	<p>Displays SNMPv3 configuration information:</p> <ul style="list-style-type: none"> • community strings as configured in SNMPv3 MIBs (this parameter is not displayed when Password Security is enabled) • trap receivers as configured in SNMPv3 MIBs • SNMPv3 users, including views accessible to each user • SNMPv3 views

snmp-server bootstrap command

With the `snmp-server bootstrap` command, you can specify how you wish to secure SNMP communications, as described in the SNMPv3 standards. This 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). The data consists of a set of initial users, groups, and views. This `snmp-server bootstrap` command deletes all existing SNMP configurations, so use the command 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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `snmp-server bootstrap` command.

Table 39
snmp-server bootstrap command parameters and variables

Parameters and variables	Description
<code><minimum-secure></code>	Specifies a minimum security configuration that allows read access to everything using <code>noAuthNoPriv</code> , and write access to everything using <code>authNoPriv</code> .

Table 39
snmp-server bootstrap command parameters and variables (cont'd.)

Parameters and variables	Description
<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 MAC address filter-based security using NNCLI

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

- “show mac-security command” (page 116)
- “mac-security command” (page 117)
- “mac-security mac-address-table address command” (page 119)
- “mac-security security-list command” (page 119)
- “no mac-security command” (page 120)
- “no mac-security mac-address-table command” (page 120)
- “no mac-security security-list command” (page 121)
- “mac-security command for specific ports” (page 121)
- “mac-security mac-da-filter command” (page 122)

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|mac-da-filter}
```

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

The following table describes the parameters and variables for the `show mac-security` command.

Table 40
show mac-security command parameters and variables

Parameters and variables	Description
<code>config</code>	Displays the general BaySecure configuration.
<code>mac-address-table [address <macaddr>]</code>	Displays contents of the BaySecure table of allowed MAC addresses: <ul style="list-style-type: none"> <code>address</code> specifies a single MAC address to display; enter the MAC address.
<code>port</code>	Displays the BaySecure status of all ports.
<code>security-lists</code>	Displays the port membership of all security lists.
<code>mac-da-filter</code>	Displays MAC DA filtering addresses.

The following figure shows sample output from the `show mac-security <config>` command.

Figure 14
show mac-security config command output

```
2550T-PWR(config)#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
2550T-PWR(config)#
```

mac-security command

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

```
mac-security [auto-learning aging-time <0-65535>] [disable|enable] [filtering {enable|disable}] [intrusion-detect {enable|disable|forever}] [intrusion-timer <1-65535>] [learning-ports <portlist>] [learning {enable|disable}] | mac-address-table|mac-da-filter|security list [snmp-lock {enable|disable}] ]
```

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

The following table describes the parameters and variables for the `mac-security` command.

Table 41
mac-security command parameters and variables

Parameters and variables	Description
<code>auto-learning aging-time <0-65535></code>	Configures the maximum MAC address autolearn aging time. Values rang from 0 to 65535.
<code>disable enable</code>	Disables or enables MAC address-based security.
<code>filtering {enable disable}</code>	Enables or disables destination address (DA) filtering when an intrusion is detected.
<code>intrusion-detect {enable disable forever}</code>	Specifies the partitioning of a port when an intrusion is detected: <ul style="list-style-type: none"> • enable— port is partitioned for a period of time. • disabled— port is not partitioned on detection. • forever— port is partitioned until manually changed.
<code>intrusion-timer <1-65535></code>	Specifies, in seconds, length of time a port is partitioned when an intrusion is detected; enter the number of seconds to specify.
<code>learning {enable disable}</code>	Specifies MAC address learning: <ul style="list-style-type: none"> • enable— enables learning by ports • disable— disables learning by ports <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>ATTENTION The MAC address learning enable command must be executed to specify learning ports.</p> </div>
<code>learning-ports <portlist></code>	Specifies MAC address learning. Learned addresses are added to the table of allowed MAC addresses. Enter the ports you want to learn; this can be a single port, a range of ports, several ranges, all, or none.
<code>mac-address-table</code>	Adds addresses to the MAC security address table.
<code>mac-da-filter</code>	Adds or deletes MAC DA filtering addresses.
<code>security-list</code>	Modifies security list port membership.
<code>snmp-lock {enable disable}</code>	Enables or disables a lock on SNMP write-access to the BaySecure MIBs.

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>}
```

ATTENTION

In this command, `portlist` must specify only a single port.

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

The following table describes the parameters and variables for the `mac-security mac-address-table address` command.

Table 42
mac-security mac-address-table address 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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `mac-security security-list` command.

Table 43
mac-security security-list command parameters and variables

Parameters and variables	Description
<1-32>	Enter the number of the security list that 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 executed in the Global Configuration command mode.

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

no mac-security auto-learning aging-time command

The `no mac-security auto-learn aging-time` command disables maximum MAC address autolearn aging time. The syntax for the `no mac-security auto-learn aging-time` command is:

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

The `no mac-security auto-learn aging-time` 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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `no mac-security mac-address-table` command.

Table 44
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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `no mac-security security-list` command.

Table 45
no mac-security security-list command parameters and variables

Parameters and variables	Description
<1-32>	Enter the number of the security list that 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 executed in the Interface Configuration command mode

The following table describes the parameters and variables for the `mac-security` command for specific ports.

Table 46
mac-security command for a single port parameters and variables

Parameters and variables	Description
<code>port <portlist></code>	Enter the port numbers.
<code>disable enable learning</code>	Directs the specific port: <ul style="list-style-type: none"> • disable— disables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is performed • enable— enables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is performed • learning— disables BaySecure on the specified port and adds these port to the list of ports for which MAC address learning is performed

mac-security mac-da-filter command

With the `mac-security mac-da-filter` command, you can filter packets from up to 10 specified MAC DAs. You also can 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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `mac-security mac-da-filter` command.

Table 47
mac-security mac-da-filter command parameters and values

Parameters and variables	Description
<code>{add delete} <H.H.H></code>	Add or delete the specified MAC address; enter the MAC address in the form of H.H.H.

ATTENTION

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

MAC address autolearning configuration using NNCLI

Configure MAC address auto-learning to automatically add allowed MAC addresses to the MAC security address table.

MAC address auto-learning configuration using NNCLI navigation

- [“Configuring MAC address auto-learning aging time using NNCLI” \(page 123\)](#)
- [“Disabling MAC address auto-learning aging time using NNCLI” \(page 124\)](#)
- [“Configuring MAC address auto-learning aging time to default using NNCLI” \(page 124\)](#)

Configuring MAC address auto-learning aging time using NNCLI

Configure MAC address auto-learning aging time to configure the aging time for the MAC addresses automatically learned in the MAC security table.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure MAC address auto-learning aging time by using the following command: <pre>mac-security auto-learning aging-time <0-65535></pre> <hr/> <p style="text-align: center;">--End--</p>

Variable definitions

The following table defines variable parameters that you enter with the `mac-security auto-learning aging-time <0-65535>` command.

Variable	Value
<0—65535>	Specifies the aging time period in minutes. Values range from 0 to 65535. A value of 0 indicates an infinite aging time period. The default aging time is 60 minutes.

Disabling MAC address auto-learning aging time using NNCLI

Disable MAC address auto-learning aging time to configure the aging time for the MAC addresses automatically learned in the MAC security table to 0 and to disable the removal of automatically learned MAC addresses.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Disable MAC address auto-learning aging time by using the following command: <code>no mac-security auto-learning aging-time</code>
--End--	

Configuring MAC address auto-learning aging time to default using NNCLI

Configure MAC address auto-learning aging time to default to configure the aging time for the MAC addresses automatically learned in the MAC security table to the default value of 60 minutes.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure MAC address auto-learning aging time by using the following command: <code>default mac-security auto-learning aging-time</code>
--End--	

Configuring EAPOL-based security using NNCLI

You can configure security based on the Extensible Authentication Protocol over LAN (EAPOL) by using the following NNCLI commands:

ATTENTION

You must enable EAPOL prior to enabling features, such as UDP Forwarding and IP Source Guard, that use QoS policies.

- “eapol command” (page 125)
- “eapol command for modifying parameters” (page 125)
- “eapol guest-vlan command” (page 127)
- “no eapol guest-vlan command” (page 127)
- “default eapol guest-vlan command” (page 128)
- “show eapol command” (page 128)
- “show eapol auth-diags interface command” (page 130)
- “show eapol auth-stats interface command” (page 131)
- “show eapol guest-vlan command” (page 132)

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 executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `eapol` command.

Table 48
eapol command parameters and variables

Parameters and variables	Description
<code>disable enable</code>	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 [init] [max-request <num>] [port <portlist>]
[quiet-interval <num>] [radius-dynamic-server enable]
[re-authenticate] [re-authentication enable|disable]
[re-authentication-period <1-604800>] [server-timeout <num>]
[status authorized|unauthorized|auto] [supplicant-timeout
<num>] [traffic-control in-out|in] [transmit-interval <num>]
```

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

The following table describes the parameters and variables for the `eapol` command for modifying parameters.

Table 49
eapol command for modifying parameters and variables

Parameters and variables	Description
<code>init</code>	Reinitiates EAP authentication.
<code>max-request <num></code>	Enter the number of times to retry sending packets to supplicant.
<code>port <portl1ist></code>	Specifies the ports to configure for EAPOL; enter the port numbers you want to use. ATTENTION If you omit this parameter, the system uses the port number that you specified when you issued the <code>interface</code> command.
<code>quiet-interval <num></code>	Enter the number of seconds that you want between an authentication failure and the start of a new authentication attempt; the range is 1 to 65535.
<code>radius-dynamic-server enable</code>	Enables the switch to process requests from the RADIUS Dynamic Authorization server.
<code>re-authentication enable disable</code>	Enables or disables reauthentication.
<code>re-authentication-period <1-604800></code>	Enter the number of seconds that you want between re-authentication attempts. Use either this variable or the <code>reauthentication-interval</code> variable; do not use both variables because they control the same setting.
<code>re-authenticate</code>	Specifies an immediate reauthentication.
<code>server-timeout <num></code>	Specifies a waiting period for response from the server. Enter the number of seconds that you want to wait; the range is 1-65535.
<code>status authorized unauthorized auto</code>	Specifies the EAP status of the port: <ul style="list-style-type: none"> <code>authorized</code>— Port is always authorized. <code>unauthorized</code>— Port is always unauthorized. <code>auto</code>— Port authorization status depends on the result of the EAP authentication.

Table 49
eapol command for modifying parameters and variables (cont'd.)

Parameters and variables	Description
<code>supplicant-timeout</code> <code><num></code>	Specifies a waiting period for response from supplicant for all EAP packets, except EAP Request/Identity packets. Enter the number of seconds that you want to wait; the range is 1-65535.
<code>traffic-control</code> <code>in-out in</code>	Sets the level of traffic control: <ul style="list-style-type: none"> • <code>in-out</code>— If EAP authentication fails, both ingressing and egressing traffic are blocked. • <code>in</code>— If EAP authentication fails, only ingressing traffic is blocked.
<code>transmit-interval</code> <code><num></code>	Specifies a waiting period for response from supplicant for EAP Request/Identity packets. Enter the number of seconds that you want to wait; the range is 1-65535.

eapol guest-vlan command

The `eapol guest-vlan` command sets the guest VLAN globally.

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

```
eapol guest-vlan [vid <1-4094> | enable]
```

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

The following table describes the parameters and variables for the `eapol guest-vlan` command.

Table 50
eapol guest-vlan command parameters and variables

Parameters and variables	Description
<code><vid></code>	Guest VLAN ID.
<code>enable</code>	Enable Guest VLAN.

no eapol guest-vlan command

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

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

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

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

default eapol guest-vlan command

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

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

```
default eapol guest-vlan
```

The `default eapol guest-vlan` command is executed in the Global Configuration command mode and Interface Configuration command mode.

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

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 executed in the Privileged EXEC command mode.

The following figure displays sample output from the `show eapol` command.

Figure 15
show eapol command output

```

2500-26T#show eapol
EAPOL Administrative State: Disabled
  Port  Admin  Admin Oper  ReAuth ReAuth Quiet Xmit  Supplic Server Max
  Status Auth Dir  Dir  Enable Period Period Period Timeout Timeout Req
  1    F Auth Yes Both Both No    3600  60   30   30   30   30   2
  2    F Auth Yes Both Both No    3600  60   30   30   30   30   2
  3    F Auth Yes Both Both No    3600  60   30   30   30   30   2
  4    F Auth Yes Both Both No    3600  60   30   30   30   30   2
  5    F Auth Yes Both Both No    3600  60   30   30   30   30   2
  6    F Auth Yes Both Both No    3600  60   30   30   30   30   2
  7    F Auth Yes Both Both No    3600  60   30   30   30   30   2
  8    F Auth Yes Both Both No    3600  60   30   30   30   30   2
  9    F Auth Yes Both Both No    3600  60   30   30   30   30   2
 10   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 11   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 12   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 13   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 14   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 15   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 16   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 17   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 18   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 19   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 20   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 21   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 22   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 23   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 24   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 25   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 26   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 27   F Auth Yes Both Both No    3600  60   30   30   30   30   2
 28   F Auth Yes Both Both No    3600  60   30   30   30   30   2
2500-26T#_
    
```

Table 51 "show eapol command output parameters and variables" (page 129) describes the parameters and variables for the show eapol command output.

Table 51
show eapol command output parameters and variables

Parameters and variables	Description
Port	Specifies the port on which to change EAPOL settings
Administrative Status	Specifies the EAP status of the port: <ul style="list-style-type: none"> • Force Unauthorized - Port is always unauthorized • Auto - Port authorization status depends on the result of the EAP authentication • Force Authorized - Port is always authorized
Auth	Displays the current EAPOL authorization status for the port <ul style="list-style-type: none"> • Yes - Authorized • No - Unauthorized This field only specifies the authorization status of the port for EAPOL users and not for non-EAPOL users. Use the <code>show eapol multihost non-eap-mac status</code> command for Non-EAPOL users.

Table 51
show eapol command output parameters and variables (cont'd.)

Parameters and variables	Description
Admin Dir	Specifies whether EAPOL authentication is set for incoming and outgoing traffic (Both) or for incoming traffic only (In). For example, if you set the specified port field value to both, and EAPOL authentication fails, then both incoming and outgoing traffic on the specified port is blocked.
Oper Dir	Specifies the current operational value for the traffic control direction for the port.
Re-authentication	Enables or disables re-authentication
Re-authentication Period	Specifies the time interval between successive re-authentications; the range is <1-604800>
Quite Period	Specifies the time interval between authentication failure and start of new authentication; the range is <0-65535>
Transmit Period	Specifies a waiting period for response from supplicant for EAP Request or Identity packets; the range is <1-65535>
Supplicant Timeout	Specifies a waiting period for response from supplicant for all EAP packets; the range is <1-65535>
Server Timeout	Specifies the time to wait for response from RADIUS server; the range is <1-65535>
Max Request	Specifies the number of times to retry sending packets to supplicant; the range is <1-10>

show eapol auth-diags interface command

The `show eapol auth-diags interface` command displays EAPOL diags. The syntax for the `show eapol auth-diags interface` command is:

```
show eapol auth-diags interface
```

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

The following figure displays sample output from the `show eapol auth-diags interface` command.

Figure 16
show eapol auth-diags interface command output

```

2526T#show eapol auth-diags interface
Port: 1
  EntersConnecting:                0
  EapLogoffsWhileConnecting:      0
  EntersAuthenticating:           0
  AuthSuccessWhileAuthenticating: 0
  AuthTimeoutsWhileAuthenticating: 0
  AuthFailWhileAuthenticating:    0
  AuthReauthsWhileAuthenticating: 0
  AuthEapStartsWhileAuthenticating: 0
  AuthEapLogoffWhileAuthenticating: 0
  AuthReauthsWhileAuthenticated:  0
  AuthEapStartsWhileAuthenticated: 0
  AuthEapLogoffWhileAuthenticated: 0
  BackendResponses:                0
  BackendAccessChallenges:         0
  BackendOtherRequestsToSupplicant: 0
  BackendNonNakResponsesFromSupplicant: 0
  BackendAuthSuccesses:            0
  BackendAuthFails:                0
Port: 2
  EntersConnecting:                0
  EapLogoffsWhileConnecting:      0
----More (q=Quit, space/return=Continue)----

```

show eapol auth-stats interface command

The `show eapol auth-stats interface` command displays EAPOL diags. The syntax for the `show eapol auth-stats interface` command is:

```
show eapol auth-stats interface
```

The `show eapol auth-stats interface` command is executed in the Privileged EXEC command mode.

The following figure displays sample output from the `show eapol auth-stats interface` command.

Figure 17
show eapol auth-stats interface command output

```

2526T#show eapol auth-stats interface
Port: 1
  EapolFramesRx:                   0
  BackendAuthFails:                0
  EapolFramesTx:                   0
  EapolStartFramesRx:              0
  EapolLogoffFramesRx:             0
  EapolRespIdFramesRx:             0
  EapolRespFramesRx:               0
  EapolReqIdFramesTx:              0
  EapolReqFramesTx:                0
  InvalidEapolFramesRx:            0
  EapolLengthErrorFramesRx:        0
  LastEapolFrameVersion:           0
  LastEapolFrameSource:            0000:0000:0000
Port: 2
  EapolFramesRx:                   0
  BackendAuthFails:                0
  EapolFramesTx:                   0
  EapolStartFramesRx:              0
  EapolLogoffFramesRx:             0
  EapolRespIdFramesRx:             0
  EapolRespFramesRx:               0
----More (q=Quit, space/return=Continue)----

```

show eapol guest-vlan command

The `show eapol guest-vlan` command displays the current guest VLAN configuration.

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

```
show eapol guest-vlan
```

The `show eapol guest-vlan` command is executed in the Global Configuration command mode and Interface Configuration command mode.

The `show eapol guest-vlan` command has no parameters or variables.

The following figure displays sample output from the `eapol guest-vlan` command.

Figure 18
show eapol guest-vlan command output

```
2500-26T#show eapol guest-vlan
EAPOL Guest Ulan : Disabled
EAPOL Guest Ulan ID: 1
2500-26T#
```

Configuring advanced EAPOL features using NNCLI

Ethernet Routing Switch 2500, Software Release 4.3 supports advanced EAPOL features that allow multiple hosts and non-EAPOL clients on a port.

This section provides information about configuring the following features:

- Multiple Host with Multiple Authentication (MHMA) (see [“Configuring multihost support using NNCLI”](#) (page 132))
- Non-EAPOL hosts on EAPOL-enabled ports (see [“Configuring support for non-EAPOL hosts on EAPOL-enabled ports using NNCLI”](#) (page 141))
- Multiple Host with Single Authentication (MHSA) (see [“Configuring non-EAP MultiHost Single-Authentication \(MHSA\) using NNCLI”](#) (page 147))

Configuring multihost support using NNCLI

To configure multihost support, do the following:

1. Enable multihost support for the interface. The relevant command is executed in Interface Configuration mode. You can issue the command for the interface selected when you enter the Interface Configuration

mode (so that all ports have the same setting), or you can issue the command for specific ports on the interface.

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

eapol multihost command

The `eapol multihost` command controls the global multihost settings.

The syntax for the `eapol multihost` command is:

```
eapol multihost { [allow-non-eap-enable] [auto-non-eap-
mhsa-enable] [eap-packet-mode] [non-eap-phone-enable]
[non-eap-use-radius-assigned-vlan] [radius-non-eap-enable]
[use-radius-assigned-vlan] [non-eap-pwd-fmt { [ip-addr]
[mac-addr] [port-number] } ] }
```

This command is executed in the Global Configuration command mode.

The following table describes the parameters and variables for the `eapol multihost` command.

Table 52
eapol multihost command parameters and variables

Parameters and variables	Description
<code>allow-non-eap-enable</code>	Enables MAC addresses of non-EAP clients.
<code>auto-non-eap-mhsa-enable</code>	Enables auto-authentication of non-EAP clients in MHSa mode
<code>eap-packet-mode</code>	Selects the packet mode for EAP authentication. Values are multicast and unicast.
<code>non-eap-phone-enable</code>	Enables the use of non-EAP IP phone clients.
<code>non-eap-use-radius-assigned-vlan</code>	Enables the use of VLAN IDs assigned by the RADIUS for non-EAP clients.
<code>radius-non-eap-enable</code>	Enables RADIUS authentication of non-EAP clients
<code>use-radius-assigned-vlan</code>	Allows use of RADIUS-assigned VLAN value
<code>non-eap-pwd-fmt { [ip-addr] [mac-addr] [port-number] }</code>	Sets bits in RADIUS non-EAPOL password format

no eapol multihost command

The `no eapol multihost` command disables EAPOL multihost.

This command is executed in the Global Configuration command mode.

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

```
no eapol multihost { [allow-non-eap-enable] [auto-non-eap-mh
sa-enable] [non-eap-phone-enable] [non-eap-use-radius-assign
ed-vlan] [radius-non-eap-enable] [use-radius-assigned-vlan]
[non-eap-pwd-fmt { [ip-addr] [mac-addr] [port-number] }]} }
```

The following table describes the parameters and variables for the `no eapol multihost` command.

Table 53
no eapol multihost command parameters and variables

Parameters and variables	Description
<code>allow-non-eap-enable</code>	Disables control of non-EAP clients (MAC addresses).
<code>auto-non-eap-mhsa-enable</code>	Disables auto-authentication of non-EAP clients in MHSa mode.
<code>non-eap-phone-enable</code>	Disables the use of non-EAP phone clients.
<code>non-eap-use-radius-assigned-vlan</code>	Disables the use of VLAN IDs assigned by the RADIUS for non-EAP clients.
<code>radius-non-eap-enable</code>	Disables RADIUS authentication of non-EAP clients.
<code>use-radius-assigned-vlan</code>	Disables the use of RADIUS-assigned VLAN value.
<code>non-eap-pwd-fmt { [ip-addr] [mac-addr] [portnumber] }</code>	Clears bits from RADIUS non-EAPOL password format.

default eapol multihost command

The `default eapol multihost` command sets the EAPOL multihost feature to default.

This command is executed in the Global Configuration mode.

The syntax for the `default eapol multihost` command is:

```
default eapol multihost { [allow-non-eap-enable] [auto-non-
eap-mhsa-enable] [eap-packet-mode] [non-eap-phone-enable]
[non-eap-use-radius-assigned-vlan] [radius-non-eap-enable]
[use-radius-assigned-vlan] [non-eap-pwd-fmt { [ip-addr]
[mac-addr] [port-number] }] }
```

The following table describes the parameters and variables for the `default eapol multihost` command.

Table 54
default eapol multihost command parameters and variables

Parameters and variables	Description
<code>allow-non-eap-enable</code>	Resets control of non-EAP clients (MAC addresses)
<code>auto-non-eap-mhsa-enable</code>	Disables auto-authentication of non-EAP clients in MHSAs mode
<code>eap-packet-mode</code>	Specifies the type of packet used for initial EAP request for IDs.
<code>non-eap-phone-enable</code>	Disables the use of non-EAP IP phone clients.
<code>non-eap-use-radius-assigned-vlan</code>	Disables the use of VLAN IDs assigned by the RADIUS for non-EAP clients.
<code>radius-non-eap-enable</code>	Disables RADIUS authentication of non-EAP clients
<code>use-radius-assigned-vlan</code>	Disables the use of RADIUS-assigned VLAN value
<code>non-eap-pwd-fmt { [ip-addr] [mac-addr] [portnumber] }</code>	Restores default format for RADIUS non-EAPOL password attribute

eapol multihost command for a port

The `eapol multihost` command controls the multihost settings for a specific port or for all ports on an interface.

This command is executed in the Interface Configuration mode.

The syntax for the `eapol multihost` command is:

```
eapol multihost [allow-non-eap-enable] [auto-non-eap-
mhsa-enable] [eap-mac-max {<1-32>}] [eap-packet-mode
{<multicast|unicast>}] [enable] [non-eap-mac-max{<1-32>}] [no
n-eap-phone-enable] [non-eap-use-radius-assigned-vlan] [port
{<portlist>}] [radius-non-eap-enable] [use-radius-assigned-vlan
] [non-eap-mac {H.H.H | port}]
```

The following table describes the parameters and variables for the `eapol multihost` command.

Table 55
eapol multihost command parameters and variables

Parameters and variables	Description
<code>allow-non-eap-enable</code>	Enables MAC addresses of non-EAP clients.
<code>auto-non-eap-mhsa-enable</code>	Enables auto-authentication of non-EAP clients in MHSAs mode
<code>eap-mac-max {<1-32>}</code>	Specifies the maximum number of EAP-authenticated MAC addresses allowed
<code>[eap-packet-mode {<multicast unicast>}]</code>	Specifies the type of packet used for initial EAP request for IDs.
<code>enable</code>	Allows EAP clients (MAC addresses)
<code>non-eap-mac-max</code>	Specifies the maximum number of non-EAP authenticated MAC addresses allowed
<code>[non-eap-phone-enable]</code>	Allows the use of non-EAP IP phone clients.
<code>[non-eap-use-radius-assigned -vlan]</code>	Allows the use of RADIUS assigned VLAN IDs for non-EAP clients.
<code>port</code>	Displays port number on which to apply EAPOL multihost settings
<code>radius-non-eap-enable</code>	Enables RADIUS authentication of non-EAP clients
<code>use-radius-assigned-vlan</code>	Allows use of RADIUS-assigned VLAN value
<code>non-eap-mac {H.H.H port}</code>	Allows non-EAPOL MAC address

no eapol multihost command for a port

The `no eapol multihost` command disables the EAPOL multihost settings for a specific port or for all ports on an interface.

This command is executed in the Interface configuration mode.

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

```
no eapol multihost [allow-non-eap-enable] [auto-non-eap-mhsa-en
able] [enable] [port] [radius-non-eap-enable] [use-radius-assigne
d-vlan] [non-eap-mac {H.H.H | port}]
```


The following table describes the parameters and variables for the `no eapol multihost` command.

Table 56
no eapol multihost command parameters and variables

Parameter and Variables	Description
<code>allow-non-eap-enable</code>	Disables MAC addresses of non-EAP clients.
<code>auto-non-eap-mhsa-enable</code>	Disables auto-authentication of non-EAP clients in MHSAs mode
<code>enable</code>	Disallows EAP clients (MAC addresses)
<code>[non-eap-phone-enable]</code>	Disables the use of non-EAP IP phone clients.
<code>[non-eap-use-radius-assigned-vlan]</code>	Disables the use of RADIUS assigned VLAN IDs for non-EAP clients.
<code>port</code>	Displays port number on which to apply EAPOL multihost settings
<code>radius-non-eap-enable</code>	Disables RADIUS authentication of non-EAP clients
<code>use-radius-assigned-vlan</code>	Disallows use of RADIUS-assigned VLAN value
<code>non-eap-mac {H.H.H port}</code>	Disallows non-EAPOL MAC address

default eapol multihost command for a port

The `default eapol multihost` command sets the multihost settings for a specific port or for all the ports on an interface to default.

This command is executed in the Interface configuration mode.

The syntax for the `default eapol multihost` command is:

```
default eapol multihost [allow-non-eap-enable] [auto-
non-eap-mhsa-enable] [eap-mac-max {<1-32>}] [enable]
[non-eap-map-max{<1-32>}] [non-eap-phone-enable]
[non-eap-use-radius-assigned-vlan] [port {<portlist>}] [radius-
non-eap-enable] [use-radius-assigned-vlan] [non-eap-mac {H.H.H
| port}]
```

The following table describes the parameters and variables for the `default eapol multihost` command.

Table 57
default eapol multihost command parameters and variables

Parameter and Variables	Description
<code>allow-non-eap-enable</code>	Resets control of non-EAP clients (MAC addresses) to default
<code>auto-non-eap-mhsa-enable</code>	Disables auto-authentication of non-EAP clients
<code>eap-mac-max <1-32></code>	Resets maximum number of EAP-authenticated MAC addresses allowed to default
<code>enable</code>	Resets control of whether EAP Clients (MAC addresses) are allowed to default
<code>non-eap-mac-max <1-32></code>	Resets maximum number of non-EAP authenticated MAC addresses allowed to default
<code>[non-eap-phone-enable]</code>	Disables the use of non-EAP IP phone clients.
<code>[non-eap-use-radius-assigned-vlan]</code>	Disables the use of RADIUS assigned VLAN IDs for non-EAP clients.
<code>port<portlist></code>	Displays port number on which to default the EAPOL multihost configuration.
<code>radius-non-eap-enable</code>	Resets RADIUS authentication of non-EAP clients to default.
<code>use-radius-assigned-vlan</code>	Disallows use of RADIUS-assigned VLAN values.
<code>non-eap-mac {H.H.H port}</code>	Resets the non-EAP MAC addresses to default

eapol multihost non-eap-mac command

The `eapol multihost non-eap-mac` command configures the MAC addresses of non-EAPOL hosts on a specific port or on all ports on an interface.

This command is executed in the Interface configuration mode.

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

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

The following table describes the parameters and variables for the `eapol multihost non-eap-mac` command.

Table 58
eapol multihost non-eap-mac command parameters and variables

Parameter and Variables	Description
port	Port on which to apply EAPOL settings
H.H.H	MAC address of the allowed non-EAPOL host

show eapol multihost command

The `show eapol multihost` command displays global settings for non-EAPOL hosts on EAPOL-enabled ports.

This command is executed in the Privileged Exec, Global, and Interface configuration mode.

The syntax for the `show eapol multihost` command is:

```
show eapol multihost
```

The following table describes the parameters and variables for the `show eapol multihost` command.

Table 59
show eapol multihost command parameters and variables

Parameters and variables	Description
interface	Displays EAPOL multihost port configuration
non-eap-mac	Displays allowed non-EAPOL MACaddress
status	Displays EAPOL multihost port status

The following figure displays sample output from the `show eapol multihost` command:

Figure 19
show eapol multihost command output

```
2526T#show eapol multihost
Allow Non-EAPOL Clients: Disabled
Use RADIUS To Authenticate Non-EAPOL Clients: Enabled
Allow Non-EAPOL Clients After Single Auth (MHSA): Disabled
Allow Use of RADIUS Assigned VLANs: Enabled
Non-EAPOL RADIUS Password Attribute Format: ..
```

show eapol multihost interface command

The `show eapol multihost interface` command displays non-EAPOL support settings for each port.

This command is executed in the Privileged EXEC, Global, and Interface configuration mode.

The syntax for the `show eapol multihost interface` command is:

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

The following table describes the parameters and variables for the `show eapol multihost interface` command.

Table 60
show eapol multihost interface command parameters and variables

Parameter and Variables	Description
portList	List of ports

The following figure displays sample output from the `show eapol multihost interface` command:

Figure 20
show eapol multihost interface command output

```
2526T(config-if)#show eapol multihost interface 1,3
Port: 1
  MultiHost Status: Disabled
  Max Eap Clients: 1
  Allow Non-EAP Clients: Disabled
  Max Non-EAP Client MACs: 1
  Use RADIUS To Auth Non-EAP MACs: Disabled
  Allow Auto Non-EAP MSHA: Disabled
  Allow Non-EAP Phones: Disabled
  RADIUS Req Pkt Send Mode: Multicast
  Allow RADIUS ULANs: Disabled
  Allow Non-EAP RADIUS ULANs: Disabled

Port: 3
  MultiHost Status: Disabled
  Max Eap Clients: 1
  Allow Non-EAP Clients: Disabled
  Max Non-EAP Client MACs: 1
  Use RADIUS To Auth Non-EAP MACs: Disabled
  Allow Auto Non-EAP MSHA: Disabled
  Allow Non-EAP Phones: Disabled
  RADIUS Req Pkt Send Mode: Multicast
  Allow RADIUS ULANs: Disabled
  Allow Non-EAP RADIUS ULANs: Disabled

2526T(config-if)#_
```

show eapol multihost non-eap-mac status command

The `show eapol multihost non-eap-mac status` command displays information about non-EAPOL hosts currently active on the switch.

This command is executed in the Privileged EXEC, Global, and Interface Configuration mode.

The syntax for the `show eapol multihost non-eap-mac status` command is:

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

The following table describes the parameters and variables for the `show eapol multihost non-eap-mac status` command.

Table 61
show eapol multihost non-eap-mac status command parameters and variables

Parameter and Variables	Description
portList	List of ports

The following figure displays sample output from the `show eapol multihost non-eap-mac status` command:

Figure 21
show eapol multihost non-eap-mac status command output

```
2526T#show eapol multihost non-eap-mac status
Port Client MAC Address State
-----
1/11 00:00:00:00:31:02   Authenticated By RADIUS
1/12 00:00:00:00:11:08   Authenticated Locally
2/20 00:19:69:84:D6:00   Authenticated For IP Telephony
3/13 00:33:01:00:00:01   Auto-Learned For MHSA
2526T#
```

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

This section describes how to configure non-EAPOL authentication.

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

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

- a. local authentication (see “Enabling local authentication of non-EAPOL hosts on EAPOL-enabled ports using NNCLI” (page 142))
 - b. RADIUS authentication (see “Enabling RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports using NNCLI” (page 143))
2. Enable EAPOL multihost on ports
 3. Specify the maximum number of non-EAPOL MAC addresses allowed on a port (see “Specifying the maximum number of non-EAPOL hosts allowed using NNCLI” (page 144)).
 4. For local authentication only, identify the MAC addresses of non-EAPOL hosts allowed on the ports (see “Creating the allowed non-EAPOL MAC address list using NNCLI” (page 145)).

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

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

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

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

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

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

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

where

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

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

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

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

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

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

The following table describes the parameters and variables for the `eapol multihost radius-non-eap-enable` command.

Table 62
eapol multihost radius-non-eap-enable command parameters and variables

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

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

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

The following table describes the parameters and variables for the `eapol multihost radius-non-eap-enable` command: **Interface mode** command.

Table 63
eapol multihost radius-non-eap-enable command: Interface mode parameters and variables

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

The default for this feature is 'disabled'.

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

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

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

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

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

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

The following table describes the parameters and variables for the `eapol multihost non-eap-pwd-fmt` command.

Table 64
eapol multihost non-eap-pwd-fmt command parameters and variables

Parameter	Description
ip-addr	Configures the switch IP address to be part of the RADIUS password.
mac-addr	Configures the non-EAP client MAC address to be part of the RADIUS password.
port-number	Configures the port-number of the non-EAP client to be part of the RADIUS password.

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

Specifying the maximum number of non-EAPOL hosts allowed using NNCLI

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

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

where

`<portlist>` is the list of ports to which you want the setting to apply. You can enter a single port, a range of ports, several ranges, or all. If

you do not specify a port parameter, the command sets the value for all ports on the interface. **<value>** is an integer in the range 1-32 that specifies the maximum number of non-EAPOL clients allowed on the port at any one time. The default is 1.

ATTENTION

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

Creating the allowed non-EAPOL MAC address list using NNCLI

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

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

where

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

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

Viewing non-EAPOL host settings and activity using NNCLI

Various show commands allow you to view:

- global settings (see [“Viewing global settings for non-EAPOL hosts”](#) (page 146))
- port settings (see [“Viewing port settings for non-EAPOL hosts”](#) (page 146) [“Viewing port settings for non-EAPOL hosts”](#) (page 146))
- allowed MAC addresses, for local authentication (see [“Viewing allowed MAC addresses”](#) (page 146))
- current non-EAPOL hosts active on the switch (see [“Viewing current non-EAPOL host activity”](#) (page 146))
- status in the Privilege Exec mode (see [“show eapol multihost status command”](#) (page 147))

Viewing global settings for non-EAPOL hosts

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

```
show eapol multihost
```

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

Viewing port settings for non-EAPOL hosts

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

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

where

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

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

Viewing allowed MAC addresses

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

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

where

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

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

Viewing current non-EAPOL host activity

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

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

where

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

show eapol multihost status command

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

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

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

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

Configuring non-EAP MultiHost Single-Authentication (MHSA) using NNCLI

To configure non-EAP MHSA support, do the following:

1. Enable MHSA globally on the switch (see [“Globally enabling support for MHSA using NNCLI”](#) (page 147)).
2. Configure MHSA settings for the interface or for specific ports on the interface (see [“Configuring interface and port settings for MHSA using NNCLI”](#) (page 148)):
 - a. Enable MHSA support.
 - b. Specify the maximum number of non-EAPOL MAC addresses allowed.

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

Globally enabling support for MHSA using NNCLI

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

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

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

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

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

Configuring interface and port settings for MHSAs using NNCLI

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

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

where

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

This command includes the following parameters for configuring MHSAs:

eapol multihost [port <portlist>	
followed by:	
auto-non-eap-mhsa-enable	Enables MHSAs on the port. The default is disabled. To disable MHSAs, use the no or default keywords at the start of the command.
non-eap-mac-max <value>	Sets the maximum number of non-EAPOL clients allowed on the port at any one time. <ul style="list-style-type: none"> • <value> is an integer in the range 1 to 32. The default is 1. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>ATTENTION</p> <p>The configurable maximum number of non-EAPOL clients for each port is 32, but Nortel expects that the usual maximum allowed for each port will be lower. Nortel expects that the combined maximum will be approximately 200 for each box and 800 for a stack.</p> </div>

Viewing MHSAs settings and activity using NNCLI

For information about the commands to view MHSAs settings and non-EAPOL host activity, see [“Viewing non-EAPOL host settings and activity using NNCLI”](#) (page 145).

TACACS+ configuration using NNCLI

This section describes how to configure TACACS+ to perform AAA services for system users.

TACACS+ configuration using NNCLI navigation

- “Configuring switch TACACS+ server settings using NNCLI” (page 149)
- “Disabling switch TACACS+ server settings using NNCLI” (page 150)
- “Enabling remote TACACS+ services using NNCLI” (page 151)
- “Enabling or disabling TACACS+ authorization using NNCLI” (page 151)
- “Configuring TACACS+ authorization privilege levels using NNCLI” (page 152)
- “Enabling or disabling TACACS+ accounting using NNCLI” (page 153)
- “Configuring the switch TACACS+ level using NNCLI” (page 153)
- “Viewing TACACS+ information using NNCLI” (page 154)

Configuring switch TACACS+ server settings using NNCLI

Configure switch TACACS+ server settings to add a TACACS+ server to your system.

Prerequisites

- Configure the TACACS+ server to add to your system.
- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure switch TACACS+ server settings by using the following command: <pre>tacacs server</pre>
--End--	

Variable definitions

The following table describes variables that you use with the `tacacs server` command.

Variable	Value
<code>host <IPaddr></code>	Specifies the IP address of the primary server to add or configure.

Variable	Value
<code>key <key></code>	<p>Specifies the secret authentication and encryption key used for all communications between the NAS and the TACACS+ server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to confirm the key when you enter it.</p> <div style="border: 1px solid black; padding: 5px;"> <p>ATTENTION The key parameter is a required parameter when you create a new server entry. The parameter is optional when you modify an existing entry.</p> </div>
<code>[port <port>]</code>	Specifies the TCP port for TACACS+. <code><port></code> is an integer in the range of 1 to 65535. The default port number is 49.
<code>[secondary host <IPaddr>]</code>	Specifies the IP address of the secondary server. The secondary server is used only if the primary server does not respond.

Disabling switch TACACS+ server settings using NNCLI

Disable switch TACACS+ server settings to discontinue using TACACS+ services in your system.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	<p>Disable switch TACACS+ server settings by using one of the following command:</p> <pre>no tacacs OR default tacacs</pre>

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

--End--

Enabling remote TACACS+ services using NNCLI

Enable remote TACACS+ services to provide services to remote users over serial or Telnet connections.

Prerequisites

- Log on to Global Configuration mode in NNCLI.
- Configure a TACACS+ server on the switch before you can enable remote TACACS+ services. See [“Configuring switch TACACS+ server settings using NNCLI”](#) (page 149).

Procedure steps

Step	Action
1	Enable remote TACACS+ services for serial connections by using the following command: <code>cli password serial tacacs</code>
2	Enable remote TACACS+ services for Telnet connections by using the following command: <code>cli password telnet tacacs</code>

--End--

Enabling or disabling TACACS+ authorization using NNCLI

You can enable or disable TACACS+ authorization globally on the switch by following this procedure.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable TACACS+ authorization by using the following command: <code>tacacs authorization enable</code>

- 2 Disable TACACS+ authorization by using the following command:

```
tacacs authorization disable
```

--End--

TACACS+ authorization is disabled by default.

Configuring TACACS+ authorization privilege levels using NNCLI

Configure TACACS+ authorization privilege levels to specify the privilege levels to which TACACS+ authorization applies.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure TACACS+ authorization privilege levels by using the following command: <pre>tacacs authorization level</pre>
--End--	

Variable definitions

The following table defines the parameters that you can enter for the `tacacs authorization level` command.

Variable	Value
ALL	Enables authorization for all privilege levels.
LINE	Enables authorization for a specific privilege level. LINE is a numerical value in the range of 0 to 15.
NONE	Authorization is not enabled for any privilege level. All users can execute any command available on the switch. The default authorization level is NONE.

Enabling or disabling TACACS+ accounting using NNCLI

Enable or disable TACACS+ accounting globally on the switch by following this procedure.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable TACACS+ accounting by using the following command: <code>tacacs accounting enable</code>
2	Disable TACACS+ accounting by using the following command: <code>tacacs accounting disable</code>

--End--

Configuring the switch TACACS+ level using NNCLI

Configure the switch TACACS+ level to select a new level for a switch or use the last configured level.

Prerequisites

- Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure a new TACACS+ level for a switch by using the following command: <code>tacacs switch level</code>
2	Use the last configured TACACS+ level for a switch by using the following command: <code>tacacs switch back</code>

--End--

Variable definitions

The following table defines optional parameters that you enter after the `tacacs switch level` command.

Variable	Value
<cr>	Selects the default switch TACACS+ level (15).
<1-15>	Defines the new TACACS+ level for the switch. Values range from 1 to 15.

Viewing TACACS+ information using NNCLI

View TACACS+ information to display TACACS+ configuration status by following this procedure.

Prerequisites

- Log on to the Privileged EXEC mode in NNCLI.

Procedure steps

Step	Action
1	View TACACS+ information by using the following command: <code>show tacacs</code>
--End--	

IP Manager configuration using NNCLI

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

IP Manager configuration using NNCLI navigation

- [“Enabling IP Manager using NNCLI” \(page 154\)](#)
- [“Disabling IP Manager using NNCLI” \(page 155\)](#)
- [“Configuring the IP Manager list for IPv4 addresses using NNCLI” \(page 156\)](#)
- [“Configuring the IP Manager list for IPv6 addresses using NNCLI” \(page 157\)](#)
- [“Removing IP Manager list entries using NNCLI” \(page 157\)](#)
- [“Viewing the IP Manager configuration using NNCLI” \(page 158\)](#)

Enabling IP Manager using NNCLI

Enable IP Manager to control Telnet, SNMP, SSH, or HTTP access.

Prerequisites

- Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable IP Manager by using the following command: <code>ipmgr{telnet snmp web ssh}</code>
	--End--

Variable definitions

The following table defines parameters that you can enter with the `ipmgr{telnet | snmp | web | ssh}` command.

Variable	Value
<code>snmp</code>	Enables the IP Manager list check for SNMP, including Enterprise Device Manager.
<code>ssh</code>	Enables the IP Manager list check for SSH access.
<code>telnet</code>	Enables the IP Manager list check for Telnet access.
<code>web</code>	Enables the IP Manager list check for Web-based management system.

Disabling IP Manager using NNCLI

Disable IP Manager to discontinue controlling Telnet, SNMP, SSH, or HTTP access.

Prerequisites

- Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable IP Manager by using the following command: <code>no ipmgr{telnet snmp web ssh}</code>
	--End--

Variable definitions

The following table defines parameters that you can enter with the `no ipmgr{telnet | snmp | web | ssh}` command.

Variable	Value
<code>snmp</code>	Disables the IP Manager list check for SNMP, including Enterprise Device Manager.
<code>ssh</code>	Disables the IP Manager list check for SSH access.
<code>telnet</code>	Disables the IP Manager list check for Telnet access.
<code>web</code>	Disables the IP Manager list check for Web-based management system.

Configuring the IP Manager list for IPv4 addresses using NNCLI

Configure the IP manager list to specify the source IP addresses or address ranges, with list IDs between 1 and 50, that have access the switch or the stack when IP Manager is enabled.

Prerequisites

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

Procedure steps

Step	Action
1	Configure the IP manager list by using the following command: <pre>ipmgr source-ip <list ID> <Ipv4addr> [mask <mask>]</pre>
	--End--

Variable definitions

The following table defines parameters that you can enter with the `ipmgr source-ip <list ID> <Ipv4addr> [mask <mask>]` command.

Variable	Value
<code><Ipv4addr></code>	Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation.

Variable	Value
<list ID>	Specifies an integer in the range 1-50 for Ipv4 entries and 51-100 for Ipv6 entries that uniquely identifies the entry in the IP Manager list.
[mask <mask>]	Specifies the subnet mask from which access is allowed. Enter the IP mask in dotted-decimal notation.

Configuring the IP Manager list for IPv6 addresses using NNCLI

Configure the IP manager list for IPv6 to specify the source IP addresses or address ranges, with list IDs between 51 and 100, that have access to the switch or the stack when IP Manager is enabled.

Prerequisites

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

Procedure steps

Step	Action
1	Configure the IP manager list by using the following command: <pre>ipmgr source-ip <list ID> <Ipv6addr/prefix></pre>
	--End--

Variable definitions

The following table defines parameters that you can enter with the `ipmgr source-ip <list ID> <Ipv6addr/prefix>` command.

Variable	Value
<Ipv6addr/prefix>	Specifies the source IPv6 address and prefix from which access is allowed.
<list ID>	Specifies an integer in the range of 51 to 100 for Ipv6 entries that uniquely identifies the entry in the IP Manager list.

Removing IP Manager list entries using NNCLI

Remove IP Manager list entries to deny access to the switch or stack for specified source IP addresses or address ranges.

Prerequisites

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

Procedure steps

Step	Action
1	<p>Remove IP Manager list entries by using the following command:</p> <pre>no ipmgr source-ip [<list ID>]</pre> <p>The command sets both the IP address and mask for the specified entry to 255.255.255.255 for Ipv4 entries, and to ffff:fff:fff:fff:fff:fff:fff:fff/128 for Ipv6 entries. If you do not specify a <list ID> value, the command resets the whole list to factory defaults.</p>
--End--	

Variable definitions

The following table defines parameters that you can enter with the `no ipmgr source-ip [<list ID>]` command.

Variable	Value
<list ID>	Specifies an integer in the range 1-50 for Ipv4 addresses and range 51-100 for Ipv6 addresses, that uniquely identifies the entry in the IP Manager list.

Viewing the IP Manager configuration using NNCLI

View the IP Manager configuration to review current IP manager configuration information.

Prerequisites

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

Procedure steps

Step	Action
1	<p>View IP Manager settings by using the following command:</p> <pre>show ipmgr</pre>
--End--	

Job aid: show ipmgr command output

The following diagrams display sample output for the `show ipmgr` command.

Figure 22
IP Manager control status

```
ERS-2500-26T#show ipmgr
TELNET Access: Enabled
SNMP Access:   Enabled
WEB Access:    Enabled
SSH Access:    Disabled
TELNET IP List Access Control: Enabled
SNMP IP List Access Control:   Enabled
WEB IP List Access Control:    Enabled
SSH IP List Access Control:    Enabled
```

Figure 23
Allowed IPv4 addresses

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
11 255.255.255.255	255.255.255.255
12 255.255.255.255	255.255.255.255
13 255.255.255.255	255.255.255.255
14 255.255.255.255	255.255.255.255
15 255.255.255.255	255.255.255.255
16 255.255.255.255	255.255.255.255
17 255.255.255.255	255.255.255.255
18 255.255.255.255	255.255.255.255
19 255.255.255.255	255.255.255.255
20 255.255.255.255	255.255.255.255
21 255.255.255.255	255.255.255.255
22 255.255.255.255	255.255.255.255
23 255.255.255.255	255.255.255.255
24 255.255.255.255	255.255.255.255
25 255.255.255.255	255.255.255.255
26 255.255.255.255	255.255.255.255
27 255.255.255.255	255.255.255.255
28 255.255.255.255	255.255.255.255
29 255.255.255.255	255.255.255.255
30 255.255.255.255	255.255.255.255
31 255.255.255.255	255.255.255.255
32 255.255.255.255	255.255.255.255
33 255.255.255.255	255.255.255.255
34 255.255.255.255	255.255.255.255
35 255.255.255.255	255.255.255.255
36 255.255.255.255	255.255.255.255
37 255.255.255.255	255.255.255.255
38 255.255.255.255	255.255.255.255
39 255.255.255.255	255.255.255.255
40 255.255.255.255	255.255.255.255
41 255.255.255.255	255.255.255.255
42 255.255.255.255	255.255.255.255
43 255.255.255.255	255.255.255.255
44 255.255.255.255	255.255.255.255
45 255.255.255.255	255.255.255.255
46 255.255.255.255	255.255.255.255
47 255.255.255.255	255.255.255.255
48 255.255.255.255	255.255.255.255
49 255.255.255.255	255.255.255.255
50 255.255.255.255	255.255.255.255

Figure 24
Allowed IPv6 addresses

```
Allowed Source IPv6 Address
-----
51 ::/0
52 ::/0
53 ::/0
54 ::/0
55 ::/0
56 ::/0
57 ::/0
58 ::/0
59 ::/0
60 ::/0
61 ::/0
62 ::/0
63 ::/0
64 ::/0
65 ::/0
66 ::/0
67 ::/0
68 ::/0
69 ::/0
70 ::/0
71 ::/0
72 ::/0
73 ::/0
74 ::/0
75 ::/0
76 ::/0
77 ::/0
78 ::/0
79 ::/0
80 ::/0
81 ::/0
82 ::/0
83 ::/0
84 ::/0
85 ::/0
86 ::/0
87 ::/0
88 ::/0
89 ::/0
90 ::/0
91 ::/0
92 ::/0
93 ::/0
94 ::/0
95 ::/0
96 ::/0
97 ::/0
98 ::/0
99 ::/0
100 ::/0
ERS-2500-50T-PWR#
```

DHCP snooping configuration using NNCLI

Configure DHCP snooping to provide security to your network by preventing DHCP spoofing.

DHCP snooping configuration using NNCLI navigation

- [“Enabling DHCP snooping globally using NNCLI” \(page 161\)](#)
- [“Disabling DHCP snooping globally using NNCLI” \(page 161\)](#)
- [“Enabling DHCP snooping on a VLAN using NNCLI” \(page 162\)](#)
- [“Disabling DHCP snooping on a VLAN using NNCLI” \(page 162\)](#)
- [“Configuring DHCP snooping port trust using NNCLI” \(page 163\)](#)

- “Configuring DHCP snooping port trust to default using NNCLI” (page 164)
- “Viewing global DHCP snooping configuration information using NNCLI” (page 164)
- “Viewing VLAN DHCP snooping configuration information using NNCLI” (page 165)
- “Viewing DHCP snooping port trust information using NNCLI” (page 165)
- “Viewing the DHCP binding table using NNCLI” (page 166)

Enabling DHCP snooping globally using NNCLI

Enable DHCP snooping globally for DHCP snooping to be functional at the VLAN and port level on the switch. By default DHCP snooping is disabled globally.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable DHCP snooping globally by using the following command: <code>ip dhcp-snooping enable</code>
--End--	

Disabling DHCP snooping globally using NNCLI

Disable DHCP snooping globally to discontinue DHCP snooping functionality at the VLAN and port level on the switch.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable DHCP snooping globally by using one of the following commands:

```
no ip dhcp-snooping
OR
default ip dhcp-snooping
```

--End--

Enabling DHCP snooping on a VLAN using NNCLI

Enable DHCP snooping on a VLAN for DHCP snooping to be functional on the VLAN. You must enable DHCP snooping separately for each VLAN as required.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable DHCP snooping on a VLAN by using the following command: <code>ip dhcp-snooping vlan <vlanID></code>

--End--

Variable definitions

The following table defines variable parameters that you enter with the `ip dhcp-snooping vlan <vlanID>` command.

Variable	Value
<vlanID>	A number that identifies the VLAN in your network. Values range from 1 to 4094.

Disabling DHCP snooping on a VLAN using NNCLI

Disable DHCP snooping on a VLAN to discontinue DHCP snooping functionality on the VLAN.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Disable DHCP snooping on a VLAN by using the following command: <pre>no ip dhcp-snooping vlan <vlanID></pre>
--End--	

Variable definitions

The following table defines variable parameters that you enter with the `no ip dhcp-snooping vlan <vlanID>` command.

Variable	Value
<vlanID>	A number that identifies the VLAN in your network. Values range from 1 to 4094. <div style="border: 1px solid black; padding: 5px;"> <p>ATTENTION If you do not specify a VLAN ID, DHCP snooping is disabled on all VLANs.</p> </div>

Configuring DHCP snooping port trust using NNCLI

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

Prerequisites

- Log on to the Interface Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure DHCP snooping port trust by using the following command: <pre>ip dhcp-snooping [port <portlist>] <trusted untrusted></pre>
--End--	

Variable definitions

The following table defines variable parameters that you enter with the `ip dhcp-snooping [port <portlist>] <trusted|untrusted>` command.

Variable	Value
<portlist>	Specifies a port or list of ports. Use the format {slot/port[-slot/port][, ...]}.

Configuring DHCP snooping port trust to default using NNCLI

Configure DHCP snooping port trust to default to specify that a particular port or range of ports is untrusted.

Prerequisites

- Log on to the Interface Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure DHCP snooping port trust to default by using the following command: <code>default ip dhcp-snooping <portlist></code>
--End--	

Variable definitions

The following table defines variable parameters that you enter with the `default ip dhcp-snooping <portlist>` command.

Variable	Value
<portlist>	Specifies a port or list of ports. Use the format {slot/port[-slot/port][, ...]}.

Viewing global DHCP snooping configuration information using NNCLI

View global DHCP snooping configuration information to review and confirm the DHCP snooping configuration for the switch.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	View global DHCP snooping configuration information by using the following command:

```
show ip dhcp-snooping
```

```
--End--
```

Viewing VLAN DHCP snooping configuration information using NNCLI

View VLAN DHCP snooping configuration information to review and confirm the DHCP snooping configuration for VLANs on the switch.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	View global DHCP snooping configuration information by using the following command: <pre>show ip dhcp-snooping vlan</pre>

```
--End--
```

Viewing DHCP snooping port trust information using NNCLI

View DHCP snooping port trust information to review and confirm the port trust configuration for a port or list of ports.

Prerequisites

- Log on to the Interface Configuration mode in NNCLI.

Procedure steps

Step	Action
1	View DHCP snooping port trust information by using the following command: <pre>show ip dhcp-snooping interface [<interface type>] [<port>]</pre>

```
--End--
```

Variable definitions

The following table defines optional parameters that you enter for the `show ip dhcp-snooping interface [<interface type>] [<port>]` command.

Variable	Value
<interface type>	Specifies the type of interface (Ethernet or FastEthernet)
<port>	Specifies a port or list of ports. Use the format {slot/port[-slot/port][, ...]}.

Viewing the DHCP binding table using NNCLI

View the DHCP binding table to review current DHCP lease information.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	View the DHCP binding table by using the following command: <code>show ip dhcp-snooping binding</code>
--End--	

Dynamic ARP inspection configuration using NNCLI

Configure dynamic ARP inspection to validate ARP packets on your network.

Dynamic ARP inspection configuration using NNCLI navigation

- [“Enabling dynamic ARP inspection on a VLAN using NNCLI” \(page 167\)](#)
- [“Disabling dynamic ARP inspection on a VLAN using NNCLI” \(page 167\)](#)
- [“Configuring dynamic ARP inspection port trust using NNCLI” \(page 168\)](#)
- [“Configuring dynamic ARP inspection port trust to default using NNCLI” \(page 169\)](#)

- [“Viewing VLAN dynamic ARP inspection configuration information using NNCLI” \(page 169\)](#)
- [“Viewing dynamic ARP inspection port trust information using NNCLI” \(page 170\)](#)

Enabling dynamic ARP inspection on a VLAN using NNCLI

Enable dynamic ARP inspection on a VLAN to validate ARP packets transmitted on that VLAN. You must enable dynamic ARP inspection separately for each VLAN as required. Dynamic ARP inspection is disabled by default.

Prerequisites

- Log on to Global Configuration mode in NNCLI.
- Enable DHCP snooping globally on the switch. See [“Enabling DHCP snooping globally using NNCLI” \(page 161\)](#).

Procedure steps

Step	Action
1	Enable dynamic ARP inspection on a VLAN by using the following command: <pre>ip arp-inspection vlan <vlanID></pre>
	--End--

Variable definitions

The following table defines variable parameters that you enter with the `ip arp-inspection vlan <vlanID>` command.

Variable	Value
<vlanID>	A number that identifies the VLAN in your network. Values range from 1 to 4094.

Disabling dynamic ARP inspection on a VLAN using NNCLI

Disable dynamic ARP inspection on a VLAN to discontinue validating ARP packets transmitted on that VLAN.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable dynamic ARP inspection on a VLAN by using the following command: <code>no ip arp-inspection vlan <vlanID></code>
--End--	

Variable definitions

The following table defines variable parameters that you enter with the `ip arp-inspection vlan <vlanID>` command.

Variable	Value
<vlanID>	A number that identifies the VLAN in your network. Values range from 1 to 4094.

Configuring dynamic ARP inspection port trust using NNCLI

Configure dynamic ARP inspection port trust to specify whether a particular port or range of ports is trusted or untrusted. Ports are untrusted by default.

Prerequisites

- Log on to the Interface Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure dynamic ARP inspection port trust by using the following command: <code>ip arp-inspection [port <LINE>] <trusted untrusted></code>
--End--	

Variable definitions

The following table defines variable parameters that you enter with the `ip arp-inspection [port <LINE>] <trusted|untrusted>` command.

Variable	Value
<LINE>	Specifies a port or list of ports. Use the format {slot/port[-slot/port][, ...]}.

Configuring dynamic ARP inspection port trust to default using NNCLI

Configure dynamic ARP inspection port trust to default to specify that a particular port, a range of ports or all ports on the switch are untrusted.

Prerequisites

- Log on to the Interface Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure dynamic ARP inspection port trust to default on a single port or list of ports by using the following command: <code>default ip arp-inspection port <LINE></code>
2	Configure dynamic ARP inspection port trust to default on all ports on the switch by using the following command: <code>default ip arp-inspection port all</code>
--End--	

Variable definitions

The following table defines variable parameters that you enter with the `default ip arp-inspection port <LINE>` command.

Variable	Value
<LINE>	Specifies a port or list of ports. Use the format {slot/port[-slot/port][, ...]}.

Viewing VLAN dynamic ARP inspection configuration information using NNCLI

View VLAN dynamic ARP inspection configuration information to review VLANs on which dynamic ARP inspection is enabled.

Prerequisites

- Log on to Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	View VLAN dynamic ARP inspection configuration information by using the following command: <code>show ip arp-inspection vlan</code>
--End--	

Viewing dynamic ARP inspection port trust information using NNCLI

View dynamic ARP inspection port trust information to review and confirm the port trust configuration for a port or list of ports.

Prerequisites

- Log on to the Interface Configuration mode in NNCLI.

Procedure steps

Step	Action
1	View dynamic ARP inspection port trust information by using the following command: <code>show ip arp-inspection interface [<interface type>] [<port>]</code>
--End--	

Variable definitions

The following table defines optional parameters that you enter for the `show ip arp-inspection interface [<interface type>] [<port>]` command.

Variable	Value
<interface type>	Specifies the type of interface (Ethernet or FastEthernet)
<port>	Specifies a port or list of ports. Use the format {slot/port[-slot/port][, ...]}.

IP Source Guard configuration using NNCLI

This section describes how to configure IP Source Guard by using NNCLI.

Prerequisites

Before you can configure IP Source Guard, you must ensure the following:

- Dynamic Host Control Protocol (DHCP) snooping is globally enabled.
For information see [“Enabling DHCP snooping globally using NNCLI” \(page 161\)](#).
- The port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- The port is an untrusted DHCP snooping and dynamic ARP Inspection port.
- The bsSourceGuardConfigMode MIB object exists.
This MIB object is used to control the IP Source Guard mode on an interface.
- the following applications are not enabled:
 - Baysecure
 - EAPOL

ATTENTION

Due to an existing Ethernet Routing Switch 2500 Series hardware limitation, you can only enable a maximum of four ports simultaneously in the Ethernet Routing Switch 2500, no matter which operating mode (stand-alone or stacking) you use.

ATTENTION

Hardware resources can run out if IP Source Guard is enabled on trunk ports with a large number of VLANs that have DHCP snooping enabled. If this happens, traffic sending can be interrupted for some clients. Nortel recommends that you do not enable IP Source Guard on trunk ports.

IP Source Guard configuration using NNCLI navigation

- [“Enabling IP Source Guard using NNCLI” \(page 171\)](#)
- [“Viewing IP Source Guard port configuration information using NNCLI” \(page 172\)](#)
- [“Viewing IP Guard-allowed addresses using NNCLI” \(page 173\)](#)
- [“Disabling IP Source Guard using NNCLI” \(page 174\)](#)

Enabling IP Source Guard using NNCLI

Enable IP Source Guard to increase the security level to a port or ports by preventing IP spoofing.

ATTENTION

The IP addresses are obtained from DHCP snooping Binding Table entries defined automatically for the port. A maximum of 10 IP addresses from the Binding Table are allowed. The remainder are dropped.

Prerequisites

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

Procedure steps

Step	Action
1	Enable IP Source Guard by using the following command: <pre>ip verify source interface {<interface type>} [<interface id>]}</pre>
--End--	

Variable definitions

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

Variable	Value
<interface id>	Identifies the ID of the interface on which you want IP Source Guard enabled.
<interface type>	Identifies the interface on which you want IP Source Guard enabled.

Viewing IP Source Guard port configuration information using NNCLI

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

Prerequisites

- Log on to the Privileged Exec mode in NNCLI.

Procedure steps

Step	Action
1	View IP Source Guard port configuration information by using the following command: <pre>show ip verify source [interface {<interface type>} [<interface id>]</pre>
--End--	

Variable definitions

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

Variable	Value
<interface id>	Identifies the ID of the interface on which you want IP Source Guard enabled.
<interface type>	Identifies the interface on which you want IP Source Guard enabled.

Viewing IP Guard-allowed addresses using NNCLI

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

Prerequisites

- Log on to the Privileged Exec mode in NNCLI.

Procedure steps

Step	Action
1	View IP Source Guard-allowed addresses by using the following command: <pre>show ip source binding [<A.B.C.D.>] [interface {[<interface type>] [<interface id>]}]</pre>
--End--	

Variable definitions

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

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

Disabling IP Source Guard using NNCLI

Disable IP Source Guard to transmit all IP traffic unfiltered.

Prerequisites

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

Procedure steps

Step	Action
1	Disable IP Source Guard by using the following command: <pre>no ip verify source interface {<interface type>] [<interface id>]}</pre>
	--End--

Variable definitions

The following table defines optional parameters that you enter for the `Insert commandInsert variable` command.

Variable	Value
<interface id>	Identifies the ID of the interface on which you want IP Source Guard disabled.
<interface type>	Identifies the interface on which you want IP Source Guard disabled.

Configuring and managing security using Enterprise Device Manager

You can set the security features for a switch so that when a violation occurs the right actions are performed by the software. The security actions that you specify are applied to all ports of the switch. This chapter describes the procedures you can use to configure switch security using Enterprise Device Manager (EDM).

Navigation

- [“EAPOL configuration using EDM” \(page 176\)](#)
- [“TACACS+ configuration using EDM” \(page 189\)](#)
- [“Configuring general switch security using EDM” \(page 193\)](#)
- [“Security list configuration using EDM” \(page 195\)](#)
- [“AuthConfig list configuration using EDM” \(page 198\)](#)
- [“Configuring MAC Address autolearn using EDM” \(page 199\)](#)
- [“Viewing AuthStatus information using EDM” \(page 201\)](#)
- [“Viewing AuthViolation information using EDM” \(page 202\)](#)
- [“Viewing MacViolation information using EDM” \(page 203\)](#)
- [“Web and Telnet password configuration using EDM” \(page 204\)](#)
- [“Console password configuration using EDM” \(page 205\)](#)
- [“Configuring the Secure Shell protocol using EDM” \(page 207\)](#)
- [“Viewing SSH Sessions information using EDM” \(page 209\)](#)
- [“Configuring SSL using EDM” \(page 209\)](#)
- [“RADIUS Server configuration using EDM” \(page 212\)](#)
- [“DHCP snooping configuration using EDM” \(page 220\)](#)
- [“Dynamic ARP inspection configuration using EDM” \(page 223\)](#)

- [“IP Source Guard configuration using EDM” \(page 225\)](#)
- [“SNMP configuration using EDM” \(page 228\)](#)

EAPOL configuration using EDM

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

ATTENTION

You must enable EAPOL before you enable features, such as UDP Forwarding and IP Source Guard, that use QoS policies.

EAPOL configuration using EDM navigation

- [“Configuring EAPOL globally using EDM” \(page 176\)](#)
- [“Configuring port-based EAPOL using EDM” \(page 178\)](#)
- [“Configuring advanced port-based EAPOL using EDM” \(page 180\)](#)
- [“Viewing Multihost status information using EDM” \(page 181\)](#)
- [“Viewing Multihost session information using EDM” \(page 182\)](#)
- [“Allowed non-EAP MAC address list configuration using EDM” \(page 183\)](#)
- [“Viewing port non-EAP host support status using EDM” \(page 184\)](#)
- [“Graphing port EAPOL statistics using EDM” \(page 185\)](#)
- [“Graphing port EAPOL diagnostics using EDM” \(page 187\)](#)

Configuring EAPOL globally using EDM

Perform this procedure to configure EAPOL globally and to set and view EAPOL security information for the switch.

ATTENTION

You must enable EAPOL prior to enabling features, such as UDP Forwarding and IP Source Guard, that use QoS policies.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click 802.1X/EAP .
3	In the work area, click the EAPOL tab.

- 4 Configure EAPOL parameters as required.
- 5 On the toolbar, click **Apply**.

--End--

Variable definitions

The following table describes fields on the EAPOL tab.

Variable	Value
SystemAuthControl	Enables or disables EAPOL for your switch. When this field is set to disabled (the default state), the Controlled Port Status for all of the switch ports is set to Authorized (no security restriction).
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 is performed. The GuestVlanEnabled field must be selected to provide ports with access to the global default Guest VLAN.
MultiHostAllowNonEapClient (MAC addresses)	This object controls whether non-EAP clients (MAC addresses) are allowed on the port.
MultiHostSingleAuthEnabled	Enables or disables Multiple Host Single Authentication (MHSA). When selected, non-EAPOL hosts are allowed on a port if there is one authenticated EAPOL client on the port.
MultiHostRadiusAuthNonEapClient	This object controls whether non-EAP clients (MAC addresses) can be authenticated using RADIUS on the port.
MultiHostAllowNonEapPhones	Enables or disables Nortel IP Phone clients as another non-EAP type.
MultiHostAllowRadiusAssignedVlan	Enables or disables the use of RADIUS-assigned VLAN values in the Multihost mode.
MultiHostAllowNonEapRadiusAssignedVlan	Enables or disables the use of RADIUS-assigned VLANs in multihost-eap mode for non-EAP clients

Variable	Value
MultiHostEapPacketMode	Specifies the packet mode, either unicast or multicast, in the Multihost mode.
NonEAPRadiusPasswordAttributeFormat	Specifies the format of the RADIUS Server password attribute for non-EAP clients; either IP address, MAC address, or port number.

Configuring port-based EAPOL using EDM

Perform this procedure to configure EAPOL security parameters for a port.

Procedure steps

Step	Action
1	From the Device Physical View, right-click a port.
2	From the menu, click Edit .
3	In the work area, click the EAPOL tab.
4	Configure EAPOL parameters as required for the port.
5	On the toolbar, click Apply .
--End--	

Variable definitions

The following table describes fields on the EAPOL tab.

Variable	Value
EAP security	
PortProtocolVersion	The EAP Protocol version that is running on this port.
PortCapabilities	The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable.
PortInitialize	Enables and disables EAPOL authentication for the specified port.
PortReauthenticateNow	Activates EAPOL authentication for the specified port immediately, without waiting for the Re-Authentication Period to expire.
Authenticator configuration	

Variable	Value
PaeState	<p>Displays the EAPOL authorization status for the switch:</p> <ul style="list-style-type: none"> • Force Authorized: The authorization status is always authorized. • Force Unauthorized: The authorization status is always unauthorized. • Auto: The authorization status depends on the EAP authentication results.
BackendAuthState	The current state of the Backend Authentication state for the switch.
AdminControlledDirections	Specifies whether EAPOL authentication is set for incoming and outgoing traffic (both) or for incoming traffic only (in). For example, if you set the specified port field value to both, and EAPOL authentication fails, then both incoming and outgoing traffic on the specified port is blocked.
OperControlledDirections	A read-only field that indicates the current operational value for the traffic control direction for the port (see the preceding field description).
AuthControlledPort Status	<p>Displays the current EAPOL authorization status for the port:</p> <ul style="list-style-type: none"> • authorized • unauthorized
AuthControlledPortControl	<p>Specifies the EAPOL authorization status for the port:</p> <ul style="list-style-type: none"> • Force Authorized: The authorization status is always authorized. • Force Unauthorized: The authorization status is always unauthorized. • Auto: The authorization status depends on the EAP authentication results.
QuietPeriod	The current value of the time interval between any single EAPOL authentication failure and the start of a new EAPOL authentication attempt.
TransmitPeriod	Time to wait for response from supplicant for EAP requests/Identity packets.
SupplicantTimeout	Time to wait for response from supplicant for all EAP packets, except EAP Request/Identity.

Variable	Value
ServerTimeout	Time to wait for a response from the RADIUS server for all EAP packets.
MaximumRequests	The number of times the switch attempts to resend EAP packets to a supplicant.
ReAuthentication Period	Time interval between successive reauthentications. When the ReAuthenticationEnabled field (see the following field) is enabled, you can specify the time period between successive EAPOL authentications for the specified port.
ReAuthentication Enabled	When enabled, the switch performs a reauthentication of the existing supplicants at the time interval specified in the ReAuthenticationPeriod field (see preceding field description).
KeyTxEnabled	The value of the KeyTransmissionEnabled constant currently in use by the Authenticator PAE state of the switch. This always returns false as key transmission is irrelevant.
LastEapolFrame Version	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrame Source	The source MAC address carried in the most recently received EAPOL frame.

Configuring advanced port-based EAPOL using EDM

Perform this procedure to configure advanced port-based EAPOL for an individual port or multiple ports.

Procedure steps

Step	Action
1	From the Device Physical View, right-click a port.
2	From the menu, click Edit .
3	In the work area, click the EAPOL Advance tab.
4	Configure advanced EAPOL parameters for specific ports as required. .
5	On the toolbar, click Apply .

--End--

Variable definitions

The following table describes fields on the EAPOL Advance tab.

Variable	Value
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. This value overrides the Guest VLAN ID value set for the switch in the EAPOL tab. Specifies zero when switch global guest VLAN ID is used for this port.
MultiHostEnabled	Enables or disables EAPOL multihost on the port.
MultiHostEapMaxNumMacs	Specifies the maximum number of allowed EAP clients on the port.
MultiHostAllowNonEapClient (MAC addresses)	Enables or disables support for non EAPOL clients using local authentication.
MultiHostNonEapMaxNumMacs	Specifies the maximum number of non EAPOL clients allowed on this port. The default is 1. The maximum number can be between 1 and 32.
MultiHostSingleAuthEnabled	Enables or disables Multiple Host with Single Authentication (MHSA) support for non EAPOL clients.
MultiHostRadiusAuthNonEapClient	Enables or disables support for non EAPOL clients using RADIUS authentication.
MultiHostAllowNonEapPhones	Enables or disables support for Nortel IP Phone clients as another non-EAP type.
MultiHostAllowRadiusAssignedVlan	Enables or disables support for VLAN values assigned by the RADIUS server.
MultiHostAllowNonEapRadiusAssignedVlan	Enables or disables support for RADIUS-assigned VLANs in multihost-EAP mode for non-EAP clients.
MultiHostEapPacketMode	Specifies the mode of EAPOL packet transmission (multicast or unicast).
ProcessRadiusRequests (RADIUS Dynamic Authorization Server)	Enables or disables the processing of RADIUS requests-server packets that are received on this port.

Viewing Multihost status information using EDM

Perform this procedure to view Multihost status information to display multiple host status for a port.

Procedure steps

Step	Action
1	From the Device Physical View, right-click a port.

- 2 From the menu, click **Edit**.
- 3 In the work area, click the **EAPOL Advance** tab.
- 4 On the tool bar, click **Multi Hosts**.

--End--

Variable definitions

The following table describes fields on the EAPOL Advance, Multihost, Multihost Status tab.

Variable	Value
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.
PaeState	The current state of the authenticator PAE state machine.
BackendAuthState	The current state of the Backend Authentication state machine.
Reauthenticate	The current reauthentication state of the machine. When the reauthenticate attribute is set to True, the client reauthenticates.

Viewing Multihost session information using EDM

Perform this procedure to view Multihost session information for a port.

Procedure steps

Step	Action
1	From the Device Physical View , right-click a port.
2	From the menu, click Edit .
3	In the work area, click the EAPOL Advance tab.
4	On the tool bar, click the Multi Hosts button.
5	Click the Multi Host Session tab.

--End--

Variable definitions

The following table describes fields on the EAPOL Advance, Multihost, Multihost Session tab.

Variable	Value
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.
Id	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.
AuthenticMethod	The authentication method used to establish the session.
Time	The elapsed time of the session.
TerminateCause	The cause of the session termination.
UserName	The user name representing the identity of the supplicant PAE.

Allowed non-EAP MAC address list configuration using EDM

Use the procedures in this section to view and configure the list of MAC addresses for non-EAPOL clients that are authorized to access the port.

Allowed non-EAP MAC address list configuration using EDM navigation

- [“Adding a MAC address to the allowed non-EAP MAC address list using EDM” \(page 183\)](#)
- [“Deleting a MAC address from the allowed non-EAP MAC address list using EDM” \(page 184\)](#)

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

Perform this procedure to add a MAC address to the allowed non-EAP MAC address list. The new entry authorizes designated non-EAPOL clients to access the port.

Procedure steps

Step	Action
1	From the Device Physical View, right-click a port.
2	From the menu, click Edit .
3	In the work area, click the EAPOL Advance tab.
4	On the tool bar, click the Non-EAP MAC button.
5	On the tool bar, click Insert to open the Insert Allowed non-EAP MAC dialog.
6	Enter a MAC address in the ClientMACAddr box.

- 7 Click **Insert** to return to the Allowed non-EAP MAC tab.
- 8 On the Allowed non-EAP MAC toolbar, click **Apply**.

--End--

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

Perform this procedure to delete a MAC address from the allowed non-EAP MAC address list. When you delete the selected MAC address you remove authorized access to the port for designated non-EAPOL clients.

Procedure steps

Step	Action
1	From the Device Physical View , right-click a port.
2	From the menu, click Edit .
3	In the work area, click the EAPOL Advance tab.
4	On the tool bar, click the Non-EAP MAC button to open the Allowed non-EAP MAC tab.
5	In the table, click a row to delete.
6	On the toolbar, click Delete .
7	Click Yes to delete the entry and return to the Allowed non-EAP MAC tab.

--End--

Variable definitions

The following table describes fields on the EAPOL Advance, Non-EAP MAC, Allowed non-EAP MAC tab.

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

Viewing port non-EAP host support status using EDM

Perform this procedure to view non-EAP host support status for a port.

Procedure steps

Step	Action
1	From the Device Physical View , right-click a port.
2	From the menu, click Edit .
3	In the work area, click the EAPOL Advance tab.
4	On the tool bar, click the Non-EAP MAC button.
5	Click the Non-EAP Status tab.
--End--	

Variable definitions

The following table describes fields on the EAPOL Advance, Non-EAP MAC, Non-EAP Status tab. .

Variable	Value
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.
State	The authentication status. Possible values are: <ul style="list-style-type: none"> rejected: the MAC address cannot be authenticated on this port. locallyAuthenticated: the MAC address was authenticated using the local table of allowed clients radiusPending: the MAC address is awaiting authentication by a RADIUS server radiusAuthenticated: the MAC address was authenticated by a RADIUS server adacAuthenticated: the MAC address was authenticated using ADAC configuration tables mhsaAuthenticated: the MAC address was auto-authenticated on a port following a successful authentication of an EAP client
Reauthenticate	The value used to reauthenticate the MAC address of the client on the port

Graphing port EAPOL statistics using EDM

Perform this procedure to create a graph of port EAPOL statistics.

Procedure steps

Step	Action
1	From the navigation pane, double-click Graph to open the Graph tree.
2	From the Graph tree, double-click Port .
3	In the work area, click the EAPOL Stats tab.
4	Click a row to graph.
5	From the toolbar, select a graph type to create a graph.
--End--	

Variable definitions

The following table describes fields on the EAPOL Stats tab.

Variable	Value
EapolFramesRx	The number of valid EAPOL frames of any type that are received by this authenticator.
EapolFramesTx	The number of EAPOL frame types of any type that are transmitted by this authenticator.
EapolStartFramesRx	The number of EAPOL start frames that are received by this authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that are received by this authenticator.
EapolRespIdFramesRx	The number of EAPOL Resp/Id frames that are received by this authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (Other than Resp/Id frames) that are received by this authenticator.
EapolReqIdFramesTx	The number of EAPOL Req/Id frames that are transmitted by this authenticator.
EapolReqFramesTx	The number of EAP Req/Id frames (Other than Req/Id frames) that are transmitted by this authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that are received by this authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that are received by this authenticator in which the packet body length field is not valid.

Graphing port EAPOL diagnostics using EDM

Perform this procedure to create a graph of port EAPOL diagnostic statistics.

Procedure steps

Step	Action
1	From the navigation tree, double-click Graph to open the Graph tree.
2	From the Graph tree, double-click Port .
3	In the work area, click the EAPOL Diag tab.
4	Click a row to graph.
5	From the toolbar, click a graph type to create the graph.
--End--	

Variable definitions

The following table describes fields on the EAPOL Diag tab.

Variable	Value
EntersConnecting	Counts the number of times that the state machine transitions to the connecting state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the state machine transitions from connecting to disconnecting because of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the state machine transitions from connecting to authenticating, because of an EAP-Response or Identity message being received from the Supplicant.
AuthSuccessWhile Authenticating	Counts the number of times that the state machine transitions from authenticating to authenticated, because of the Backend Authentication state machine indicating a successful authentication of the Supplicant.
AuthTimeoutsWhile Authenticating	Counts the number of times that the state machine transitions from authenticating to aborting, because of the Backend Authentication state machine indicating an authentication timeout.

Variable	Value
AuthFailWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to held, because of the Backend Authentication state machine indicating an authentication failure.
AuthReauthsWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to aborting, because of a reauthentication request.
AuthEapStartsWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to aborting, because of an EAPOL-Start message being received from the Supplicant.
AuthEapLogoffWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to aborting, because of an EAPOL-Logoff message being received from the Supplicant.
AuthReauthsWhileAuthenticated	Counts the number of times that the state machine transitions from authenticated to connecting, because of a reauthentication request.
AuthEapStartsWhileAuthenticated	Counts the number of times that the state machine transitions from authenticated to connecting, because of an EAPOL-Start message being received from the Supplicant.
AuthEapLogoffWhileAuthenticated	Counts the number of times that the state machine transitions from authenticated to disconnected, because of an EAPOL-Logoff message being received from the Supplicant.
BackendResponses	Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
BackendAccessChallenges	Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.
BackendOtherRequestsToSupplicant	Counts the number of times that the state machine sends an EAP-Request packet, other than an Identity, Notification, Failure or Success message, to the Supplicant. Indicates that the Authenticator chooses an EAP-method.

Variable	Value
BackendNonNakResponses FromSupplicant	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the EAP-method that the Authenticator chooses.
BackendAuthSuccesses	Counts the number of times that the state machine receives an EAP-Success message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.
BackendAuthFails	Counts the number of times that the state machine receives an EAP-Failure message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.

TACACS+ configuration using EDM

This section describes how to configure TACACS+ to perform AAA services for system users.

Navigation

- [“Enabling TACACS+ accounting using EDM” \(page 189\)](#)
- [“Disabling TACACS+ accounting using EDM” \(page 190\)](#)
- [“Enabling TACACS+ authorization using EDM” \(page 190\)](#)
- [“Disabling TACACS+ authorization using EDM” \(page 191\)](#)
- [“Configuring the switch TACACS+ levels using EDM” \(page 191\)](#)
- [“Creating a TACACS+ server” \(page 192\)](#)

Enabling TACACS+ accounting using EDM

Perform this procedure to enable TACACS+ accounting using EDM.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security .
2	Double-click TACACS+ .
3	In the work area, click the Globals tab.

- 4 On the Globals tab, select the **Accounting** check box to enable accounting.
- 5 On the toolbar, click **Apply**.

--End--

Disabling TACACS+ accounting using EDM

Perform this procedure to disable TACACS+ accounting using EDM.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security .
2	Double-click TACACS+ .
3	In the work area, click the Globals tab.
4	On the Globals tab, deselect the Accounting check box to disable accounting.
5	On the toolbar, click Apply .

--End--

Variable definitions

Variable	Value
Accounting	Determines which application will be accounted by tacacs+.

Enabling TACACS+ authorization using EDM

Perform this procedure to enable TACACS+ authorization using EDM.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security .
2	Double-click TACACS+ .
3	In the work area, click the Globals tab.
4	On the Globals tab, select the AuthorizationEnabled check box to enable authorization.

- 5 On the toolbar, click **Apply**.

--End--

Disabling TACACS+ authorization using EDM

Perform this procedure to disable TACACS+ authorization using EDM.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security .
2	Double-click TACACS+ .
3	In the work area, click the Globals tab.
4	On the Globals tab, deselect the AuthorizationEnabled check box to disable authorization.
5	On the toolbar, click Apply .

--End--

Variable definitions

Variable	Value
AuthorizationEnabled	Enable/disable this feature.

Configuring the switch TACACS+ levels using EDM

Perform this procedure to configure the switch TACACS+ levels using EDM.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security .
2	Double-click TACACS+ .
3	In the work area, click the Globals tab.
4	In the AuthorizationLevels field, click the level of authorization <0-15>.
5	On the toolbar, click Apply .

--End--

Variable definitions

Variable	Value
AuthorizationLevels <0-15>	This object controls which NNCLI command privilege levels will be authorized by TACACS+.

Creating a TACACS+ server

Perform this procedure to create a TACACS+ server.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security .
2	Double-click TACACS+ .
3	In the work area, click the TACACS+ Server tab.
4	On the toolbar, click Insert to open the Insert TACACS+ Server dialog.
5	In the AddressType field, click ipv4.
6	In the Address field, enter the IP address of the TACACS+ server.
7	In the PortNumber field, enter the TCP port on which the client establishes a connection to the server.
8	In the Key field, enter the secret key shared with this TACACS+ server.
9	In the Confirm Key field, reenter the secret key shared with this TACACS+ server.
10	In the Priority field, click Primary or Secondary to determine the order in which the TACACS+ server is used.
11	Click Insert to accept the change and return to the work area.
12	On the toolbar, click Apply to apply the change to the configuration.
--End--	

Variable definitions

Variable	Value
AddressType	Specifies the type of IP address used on the TACACS+ server.
Address	The IP address of the TACACS+ server referred to in this table entry.

Variable	Value
PortNumber	The TCP port on which the client establishes a connection to the server. A value of 0 indicates that the system specified default value is used.
ConnectionStatus	Specifies the status of the TCP connection between a device and the TACACS+ server.
Key	Secret key to be shared with this TACACS+ server. If the key length is zero that indicates no encryption is being used.
Priority	Determines the order in which the TACACS+ servers will be used. If more than one server shares the same priority, they will be used in lexicographic order (the order of entries in this table).

Configuring general switch security using EDM

You can use the Mac Security tab to configure and view general security information .

Perform this procedure to configure general switch security.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click MAC Security .
3	In the work area, click the Mac Security tab.
4	Configure switch security parameters as required.
5	On the tool bar, click Apply .
--End--	

Variable definitions

The following table describes fields on the Mac Security tab.

Variable	Value
AuthSecurityLock	<p>If this parameter is listed as <i>locked</i>, the agent refuses all requests to modify the security configuration. Entries also include:</p> <ul style="list-style-type: none"> • other • notlocked
AuthCtlPartTime	<p>This value indicates the duration of the time for port partitioning in seconds. The default is zero. When the value is zero, the port remains partitioned until it is manually enabled.</p>
SecurityStatus	<p>Indicates whether or not the switch security feature is enabled.</p>
SecurityMode	<p>Mode of switch security. Entries include:</p> <ul style="list-style-type: none"> • macList: Indicates that the switch is in the MAC-list mode. You can configure more than one MAC address for each port. • autoLearn: Indicates that the switch learns the first MAC address on each port as an allowed address of that port.
SecurityAction	<p>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.</p> <p>A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include:</p> <ul style="list-style-type: none"> • noAction: Port does not have any security assigned to it, or the security feature is turned off. • trap: Listed trap. • partitionPort: Port is partitioned. • partitionPortAndsendTrap: Port is partitioned, and traps are sent to the trap receiver. • daFiltering: Port filters out the frames where the destination address field is the MAC address of the unauthorized station. • daFilteringAndsendTrap: Port filters out the frames where the destination address field is the MAC address of an unauthorized station. Traps are sent to trap receivers.

Variable	Value
	<ul style="list-style-type: none"> partitionPortAnddaFiltering: Port is partitioned and filters out the frames with the destination address field is the MAC address of unauthorized station. partitionPortdaFilteringAndsendTrap: Port is partitioned and filters out the frames where the destination address field is the MAC address of the unauthorized station. Traps are sent to trap receivers.
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 autolearning is enabled.
CurrSecurityLists	Current number of entries of the Security listed in the SecurityList tab.
MaxSecurityLists	Maximum entries of the Security listed in the SecurityList tab.
AutoLearningAgingTime	Specifies the lifetime (in minutes) for MAC addresses that are learned automatically. Values range from 0 to 65535. The default value is 0. A value of 0 specifies that MAC addresses do not age out.
<p>ATTENTION You cannot assign a port or ports to the PortLearnStatus field if you have enabled AutoLearn for the port or ports.</p>	

Security list configuration using EDM

Use the procedures in this section to configure the security list to manage the port members in a security list.

Security list configuration using EDM navigation

- [“Adding ports to a security list using EDM” \(page 195\)](#)
- [“Deleting specific ports from a security list using EDM” \(page 196\)](#)
- [“Deleting all ports from a security list using EDM” \(page 197\)](#)

Adding ports to a security list using EDM

Perform this procedure to add ports to the security list to insert new port members into a security list.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click MAC Security .
3	In the work area, click the SecurityList tab.
4	On the toolbar, click Insert .
5	Do one of the following: <ul style="list-style-type: none">• In the SecurityListIdx box, accept the default sequential security list number provided by the switch.• Enter a number for the security list.
6	Click the ellipsis (...) for SecurityListMembers and do one of the following: <ul style="list-style-type: none">• In the SecurityListMembers select ports to add to the security list.• Click All to select all ports.
7	Click Ok .
8	Click Insert to return to the SecurityList tab.
9	On the toolbar, click Apply .

--End--

Variable definitions

The following table describes fields on the SecurityList tab.

Variable	Value
SecurityListIdx	An index of the security list. This corresponds to the SecurityList field into AuthConfig tab.
SecurityListMembers	The set of ports that are currently members in the Port list.

Deleting specific ports from a security list using EDM

Perform this procedure to delete specific ports from a security list.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click MAC Security .
3	In the work area, click the SecurityList tab.
4	Click rows in the table to delete.
5	On the tool bar, click Delete .
6	Click Yes to delete the selections or click No to return to the SecurityList tab without deleting any entries.
7	On the tool bar, click Apply .

--End--

Variable definitions

The following table describes fields on the SecurityList tab.

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

Deleting all ports from a security list using EDM

Perform this procedure to remove all existing port members from a security list.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click MAC Security .
3	In the work area, click the SecurityList tab.
4	Select all rows to delete all entries.
5	On the tool bar, click Delete .
6	Click Yes .

--End--

Variable definitions

The following table describes fields on the SecurityList tab.

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

AuthConfig list configuration using EDM

The AuthConfig list 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, the switch returns a GENERR return-value.

AuthConfig list configuration using EDM navigation

- [“Adding entries to the AuthConfig list using EDM” \(page 198\)](#)
- [“Deleting entries from the AuthConfig list using EDM” \(page 199\)](#)

Adding entries to the AuthConfig list using EDM

Perform this procedure to add entries to the AuthConfig list.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click MAC Security .
3	In the work area, click the AuthConfig tab.
4	On the tool bar, click Insert to open the Insert AuthConfig dialog.
5	In the Insert AuthConfig dialog , enter new information.
6	Click Insert to return to the AuthConfig tab.
7	On the toolbar, click Apply .

--End--

Variable definitions

The following table describes fields on the AuthConfig tab.

Variable	Value
BrdIdx	Index of the slot that contains the board on which the port is located. If you specify SecureList, this field must be zero.
PortIdx	Index of the port on the board. If you specify SecureList, this field must be zero.
MACIdx	An index of MAC addresses that are designated as allowed (station).
AccessCtrlType	Displays the node entry as node allowed. A MAC address can be allowed on multiple ports.
SecureList	The index of the security list. This value is meaningful only if BrdIdx and PortIdx values are zero. For other board and port index values, this index must also have a value of zero. The corresponding MAC Address of this entry is allowed or blocked on all ports of this port list.
Source	Indicates the source MAC address.
Lifetime	Indicates the time period that the system stores information before it deletes the information.

Deleting entries from the AuthConfig list using EDM

Perform this procedure to remove entries from the AuthConfig list for boards, ports and MAC addresses that have the security configuration.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click MAC Security .
3	In the work area, click the AuthConfig tab.
4	Click a list entry.
5	On the tool bar, click Delete .
6	Click Yes .

--End--

Configuring MAC Address autolearn using EDM

Perform this procedure to configure automatic learning of MAC Addresses.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click MAC Security .
3	In the work area, click the AutoLearn tab.
4	In the Enabled column, double-click the cell for a port.
5	From the list, select true or false .
6	In the MaxMacs column, double-click the cell for the port.
7	Enter a value from 1..25.
8	On the tool bar, click Apply .
--End--	

Variable definitions

The following table describes fields on the AutoLearn tab.

Variable	Value
Brd	The index of the board. This corresponds to the slot containing the board. The index is 1 when it is not applicable. This column is titled Unit if the switch is in a stack.
Port	Identifies the switch port number.
Enabled	Enables or disables the automatic learning of MAC addresses on the port. Values are true (enabled) and false (disabled).
MaxMacs	Defines the maximum number of MAC addresses the port can learn. Values range from 1 to 25.
<p>ATTENTION You cannot enable AutoLearn if the port is a member of PortLearnStatus on the Mac Security tab. If you disable AutoLearn, the switch removes all automatically learned MAC addresses for the port or ports.</p>	

Viewing AuthStatus information using EDM

Perform this procedure to view AuthStatus information about the current security status of a port. The information includes actions to be performed when an unauthorized station is detected.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click MAC Security .
3	In the work area, click the AuthStatus tab.
--End--	

Variable definitions

The following table describes fields on the AuthStatus tab.

Variable	Value
AuthStatusBrdIndx	The index of the board. This corresponds to the index of the slot that contains the board if the index is greater than zero.
AuthStatusPortIndx	The index of the port on the board. This corresponds to the index of the last manageable port on the board if the index is greater than zero.
AuthStatusMACIndx	The index of MAC address on the port. This corresponds to the index of the MAC address on the port if the index is greater than zero.
CurrentAccessCtrlType	Displays whether the node entry is the <code>node allowed</code> or <code>node blocked</code> type.
CurrentActionMode	A value representing the type of information contained, including: <ul style="list-style-type: none"> • <code>noAction</code>: Port does not have any security assigned to it, or the security feature is turned off. • <code>partitionPort</code>: Port is partitioned. • <code>partitionPortAndsendTrap</code>: Port is partitioned and traps are sent to the trap receiver. • <code>Filtering</code>: Port filters out the frames where the destination address field is the MAC address of the unauthorized station. • <code>FilteringAndsendTrap</code>: Port filters out the frames where the destination address field is the MAC

Variable	Value
	<p>address of the unauthorized station. Traps are sent to the trap receiver.</p> <ul style="list-style-type: none"> • sendTrap: A trap is sent to the trap receiver(s). • partitionPortAnddaFiltering: Port is partitioned and filters out the frames where the destination address field is the MAC address of the unauthorized station. • partitionPortdaFilteringAndsendTrap: Port is partitioned and filters out the frames where the destination address field is the MAC address of the unauthorized station. Traps are sent to trap receiver(s).
CurrentPortSecur Status	<p>Displays the security status of the current port, including:</p> <ul style="list-style-type: none"> • If the port is disabled, notApplicable is returned. • If the port is in a normal state, portSecure is returned. • If the port is partitioned, portPartition is returned.

Viewing AuthViolation information using EDM

Perform this procedure to view authorization violation information that includes a list of boards and ports where network access violations have occurred, and the MAC addresses of violators.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click MAC Security .
3	In the work area, click the AuthViolation tab.
--End--	

Variable definitions

The following table describes fields on the AuthViolation tab.

Variable	Value
BrdIdx	The index of the board. This corresponds to the unit containing the board. The index will be 1 where it is not applicable.
PortIdx	The index of the port on the board. This corresponds to the port on that a security violation was seen.
MACAddress	The MAC address of the device attempting unauthorized network access (MAC address-based security).

Viewing MacViolation information using EDM

Perform this procedure to view MAC Violation information.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click MAC Security .
3	In the work area, click the MacViolation tab.
4	On the tool bar, click Refresh to update the MacViolation tab table.

--End--

Variable definitions

The following table describes fields on the MAC violation tab.

Variable	Value
Address	The MAC address of the device attempting unauthorized network access (MAC address-based security).
Brd	The index of the board. This corresponds to the slot containing the board. The index is 1 when it is not applicable.
Port	The index of the port on the board. This corresponds to the port on which a security violation was seen.

Web and Telnet password configuration using EDM

Use the information in this section to configure a Web and Telnet password for a switch or a stack.

Configuring a Web and Telnet password for a switch using EDM

Use this procedure to configure a Web and Telnet password for an individual switch.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security .
2	In the Security tree, double-click Web/Telnet/Console .
3	In the work area, click the Web/Telnet Password tab.
4	In the Web/Telnet Switch Password Setting, select a value from the Web/Telnet Switch Password Type list.
5	In the Read-Only Switch Password dialog box, type a character string.
6	In the Re-enter to verify dialog box for the Read-Only Switch Password, retype the character string.
7	In the Read-Write Switch Password dialog box, type a character string.
8	In the Re-enter to verify dialog box for the Read-Write Switch Password, retype the character string.
9	Click Apply .

--End--

Variable definitions

Use the data in this table to configure a Web and Telnet password for a switch.

Variable	Value
Web/Telnet Switch Password Type	<p>Specifies the password type. Values include:</p> <ul style="list-style-type: none"> • None (default) • Local Password • RADIUS Authentication

Configuring a Web and Telnet password for a stack using EDM

Use this procedure to configure a Web and Telnet password for an stack.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security .
2	In the Security tree, double-click Web/Telnet/Console .
3	In the work area, click the Web/Telnet Password tab.
4	In the Web/Telnet Stack Password Setting, select a value from the Web/Telnet Stack Password Type list.
5	In the Read-Only Stack Password dialog box, type a character string.
6	In the Re-enter to verify dialog box for the Read-Only Stack Password, retype the character string.
7	In the Read-Write Stack Password dialog box, type a character string.
8	In the Re-enter to verify dialog box for the Read-Write Stack Password, retype the character string.
9	Click Apply .

--End--

Variable definitions

Use the data in this table to configure a Web and Telnet password for a stack.

Variable	Value
Web/Telnet Stack Password Type	<p>Specifies the password type. Values include:</p> <ul style="list-style-type: none"> • None (default) • Local Password • RADIUS Authentication

Console password configuration using EDM

Use the information in this section to configure a Web and Telnet password for a switch or a stack.

Configuring a console password for a switch using EDM

Use this procedure to configure a Console password for an individual switch.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security .
2	In the Security tree, double-click Web/Telnet/Console .
3	In the work area, click the Console Password tab.
4	In the Console Switch Password Setting, select a value from the Console Switch Password Type list.
5	In the Read-Only Switch Password dialog box, type a character string.
6	In the Re-enter to verify dialog box for the Read-Only Switch Password, retype the character string.
7	In the Read-Write Switch Password dialog box, type a character string.
8	In the Re-enter to verify dialog box for the Read-Write Switch Password, retype the character string.
9	Click Apply .

--End--

Variable definitions

Use the data in this table to configure a Web and Telnet password for a switch.

Variable	Value
Console Switch Password Type	<p>Specifies the password type. Values include:</p> <ul style="list-style-type: none"> • None (default) • Local Password • RADIUS Authentication

Configuring a console password for a stack using EDM

Use this procedure to configure a Console password for a stack.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security .
2	In the Security tree, double-click Web/Telnet/Console .
3	In the work area, click the Web/Telnet Password tab.
4	In the Console Stack Password Setting, select a value from the Console Stack Password Type list.
5	In the Read-Only Stack Password dialog box, type a character string.
6	In the Re-enter to verify dialog box for the Read-Only Stack Password, retype the character string.
7	In the Read-Write Stack Password dialog box, type a character string.
8	In the Re-enter to verify dialog box for the Read-Write Stack Password, retype the character string.
9	Click Apply .

--End--

Variable definitions

Use the data in this table to configure a Web and Telnet password for a stack.

Variable	Value
Console Stack Password Type	Specifies the password type. Values include: <ul style="list-style-type: none"> • None (default) • Local Password • RADIUS Authentication

Configuring the Secure Shell protocol using EDM

Perform this procedure to configure the Secure Shell (SSH) protocol to provide secure access to the switch.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click SSH .
3	In the work area, click the SSH tab.
4	Configure SSH parameters as required.
5	On the tool bar, click Apply .
--End--	

Variable definitions

The following table describes fields on the SSH tab.

Variable	Value
Enable	Enables, disables, or securely enables SSH. Securely enable turns off all remote access, and it takes effect after a reboot.
Version	Indicates the SSH version.
Port	Indicates the SSH connection port.
Timeout	Indicates the SSH connection timeout in seconds.
KeyAction	Indicates the SSH key action; either generate DSA or delete DSA..
DsaAuth	Enables or disables SSH with DSA public key authentication.
PassAuth	Enables or disables SSH with password authentication.
DsaHostKeyStatus	Indicates the current status of the SSH DSA host key: <ul style="list-style-type: none"> • notGenerated: DSA host key has not yet been generated. • generated: DSA host key is generated. • generating: DSA host key is currently being generated.
TftpServerInetAddressType	Indicates the type of address stored in the TFTP server.
TftpServerInetAddress	Specifies the IP address stored in the TFTP server for all TFTP operations.
TftpFile	Indicates the name of the file for the TFTP transfer.

Variable	Value
TftpAction	Indicates the SSH public keys that are set to initiate a TFTP download; either none, download SSH public keys, or delete SSH DSA authorization key.
TftpResult	Indicates the retrieved value of the TFTP transfer.

Viewing SSH Sessions information using EDM

Perform this procedure to display currently active SSH sessions.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click SSH .
3	In the work area, click the SSH Sessions tab.
--End--	

Variable definitions

The following table describes the fields on the SSH Sessions tab.

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

Configuring SSL using EDM

Perform this procedure to configure Secure Socket Layer (SSL) to provide your network with a secure Web management interface.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click SSH .
3	In the work area, click the SSL tab.
4	Configure SSL parameters as required.

5 Click **Apply**.

--End--

Variable definitions

The following table describes fields on the SSL tab.

Variable	Value
Enabled	Enables or disables SSL.
CertificateControl	Enables the creation and deletion of SSL certificates. <ul style="list-style-type: none"> • create—creates an SSL certificate • delete—deletes an SSL certificate • other—results in a wrongValue error
CertificateExists	Indicates if a valid SSL certificate is created. <ul style="list-style-type: none"> • true—a valid SSL certificate is created • false—a valid SSL certificate is not created or the certificate has been deleted
CertificateControlStatus	Indicates the status of the most recent attempt to create or delete a certificate. <ul style="list-style-type: none"> • inProgress—the operation is not yet completed • success—the operation is complete • failure—the operation failed • other—the s5AgSslCertificateControl object was never set
ServerControl	Resets the SSL server. Values are reset and other. The default is other.
ATTENTION You cannot reset the SSL server while creating the SSL certificate.	

RADIUS global configuration using EDM

You can use the procedures in this section to configure RADIUS Request use Management IP and RADIUS password fallback.

RADIUS global configuration using EDM navigation

- “Enabling RADIUS Request use Management IP using EDM” (page 211)
- “Disabling RADIUS Request use Management IP using EDM” (page 211)
- “Enabling RADIUS password fallback using EDM” (page 212)
- “Disabling RADIUS password fallback using EDM” (page 212)

Enabling RADIUS Request use Management IP using EDM

Perform this procedure to enable RADIUS Request use Management IP.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the Globals tab.
4	Select the RadiusUseMgmtIp check box.
5	On the tool bar, click Apply .
--End--	

Disabling RADIUS Request use Management IP using EDM

Perform this procedure to disable RADIUS Request use Management IP.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the Globals tab.
4	Clear the RadiusUseMgmtIp check box.

- 5 On the tool bar, click **Apply**.

--End--

Enabling RADIUS password fallback using EDM

Perform this procedure to enable RADIUS password fallback.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the Globals tab.
4	Select the RadiusPasswordFallbackEnabled check box.
5	On the tool bar, click Apply .

--End--

Disabling RADIUS password fallback using EDM

Perform this procedure to disable RADIUS password fallback.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the Globals tab.
4	Clear the RadiusPasswordFallbackEnabled check box.
5	On the tool bar, click Apply .

--End--

RADIUS Server configuration using EDM

You can use the procedures in this section to configure RADIUS Server security to configure and manage RADIUS-based network security and 802.1X dynamic authorization extension (RFC 3576).

RADIUS Server configuration using EDM navigation

- “Configuring the RADIUS server using EDM” (page 213)
- “Viewing RADIUS Dynamic Authorization server information using EDM” (page 214)
- “802.1X dynamic authorization extension (RFC 3576) configuration using EDM” (page 215)
- “Viewing RADIUS Dynamic Server statistics using EDM” (page 218)
- “Graphing RADIUS Dynamic Server statistics using EDM” (page 219)

Configuring the RADIUS server using EDM

Perform this procedure to configure the RADIUS server to store client or user credentials, password, and access privileges.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the RADIUS Server tab.
4	Configure RADIUS server parameters as required.
5	On the tool bar, click Apply .

--End--

Variable definitions

The following table describes fields on the RADIUS server tab.

Variable	Value
AddressType	Specifies the type of IP address used by the RADIUS server.
PrimaryRadiusServer	Specifies the IP address of the primary RADIUS server (default: 0.0.0.0). <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <p>ATTENTION If there is no primary RADIUS server, set the value of this field to 0.0.0.0 .</p> </div>

Variable	Value
SecondaryRadiusServer	Specifies the IP address of the secondary RADIUS server (default: 0.0.0.0). The secondary RADIUS server is used only if the primary server is unavailable or unreachable.
RadiusServerUdpPort	Specifies the UDP port number (default: 1812). The port number can range between 1 and 65535.
RadiusServerTimeout	Specifies the timeout interval between each retry, for service requests to the RADIUS server. The default is 2 Seconds. The timeout period can range between 1 and 60 seconds.
SharedSecret(key)	Specifies the value of the shared secret key. <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <p>ATTENTION The shared secret key has a maximum of 16 characters.</p> </div>
ConfirmedSharedSecret(key)	Confirms the value of the shared secret key specified in the SharedSecret(Key) field. This field usually does not display anything (just a blank field). It is used when user is changing the SharedSecret(key) field. User usually need to enter twice to confirm the string already being entered in SharedSecret(Key).

Viewing RADIUS Dynamic Authorization server information using EDM

Perform this procedure to display RADIUS Dynamic Authorization server information for the switch.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the RADIUS Dynamic Auth. Server tab.
--End--	

Variable definitions

The following table describes the fields on the RADIUS Dynamic Author. Server tab.

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

802.1X dynamic authorization extension (RFC 3576) configuration using EDM

You can use the procedures in this section to configure 802.1X dynamic authorization extension (RFC 3576) to enable the RADIUS server to send a change of authorization (CoA) or to send a disconnect command to the Network Access Server (NAS)

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

- [“Configuring 802.1X dynamic authorization extension \(RFC 3576\) client using EDM” \(page 215\)](#)
- [“Editing the 802.1X dynamic authorization extension \(RFC 3576\) client information using EDM” \(page 216\)](#)
- [“Editing the 802.1X dynamic authorization extension \(RFC 3576\) client secret word using EDM” \(page 218\)](#)

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

Perform this procedure to configure the RADIUS Dynamic Authorization client parameters for the switch.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the RADIUS Dynamic Auth. Client tab.
4	On the tool bar, click Insert to open the Insert RADIUS Dynamic Auth. Client dialog.

- 5 Configure RADIUS Dynamic Authorization client parameters as required.
- 6 Click **Insert** to return to the RADIUS Dynamic Auth. Client tab.
- 7 On the toolbar, click **Apply**.

--End--

Variable definitions

The following table describes fields on the RADIUS Dynamic Auth. client tab.

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

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

Perform this procedure to configure the RADIUS Dynamic Authorization client parameters for the switch.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.

- 2 In the Security tree, double-click **RADIUS**.
- 3 In the work area, click the **RADIUS Dynamic Auth. Client** tab.
- 4 In the table, double-click a configurable RADIUS Dynamic Auth. Client cell.
- 5 Edit RADIUS Dynamic Authorization client parameters as required.
- 6 On the tool bar, click **Apply**.

--End--

Variable definitions

The following table describes the fields on the the RADIUS Dynamic Auth. Client tab.

Variable	Value
AddressType	Defines the IP address type of the RADIUS Dynamic Authorization Client. This is a read only value.
Address	Defines the IP address of the RADIUS Dynamic Authorization Client. This is a read only value.
Enabled	Enables or disables packet receiving from the RADIUS Dynamic Authorization Client. <ul style="list-style-type: none"> • enable—true • disable—false
UdpPort	Configures the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1025 to 65535.
ProcessCoARequests	Enables change-of-authorization (CoA) request processing.
ProcessDisconnectRequests	Enables disconnect request processing.
Secret	The RADIUS Dynamic Authorization Client secret word. This box remains empty.

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

Perform this procedure to change the existing RADIUS Dynamic Authorization client secret word.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the RADIUS Dynamic Auth. Client tab.
4	On the tool bar, click Change Secret .
5	In the Secret dialog box, enter a new secret word.
6	In the Confirmed Secret dialog box, reenter the new secret word.
7	Click Apply .

--End--

Viewing RADIUS Dynamic Server statistics using EDM

Perform this procedure to display RADIUS Dynamic Server statistical information.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the RADIUS Dynamic Server Stats tab.

--End--

Variable definitions

The following table describes the fields on the RADIUS Dynamic Server Stats tab.

Variable	Value
ClientIndex	Indicates the RADIUS Dynamic Server client index.

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

Graphing RADIUS Dynamic Server statistics using EDM

Perform this procedure to display a graphical representation of statistics for a RADIUS Dynamic Server client.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the RADIUS Dynamic Server Stats tab.
4	Click any cell for a displayed RADIUS Dynamic Server client.
5	On the tool bar, click Graph .

--End--

Configuring RADIUS Interim Accounting Updates support using EDM

Perform this procedure to configure RADIUS Interim Accounting Updates support to permit the RADIUS server to make policy decisions based on real-time network attributes transmitted by the NAS.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click RADIUS .
3	In the work area, click the Radius Accounting tab.
4	To enable RADIUS Accounting Interim Updates support, select the RadiusAccountingInterimUpdates box.
5	To configure an interim update interval, enter a value in the RadiusAccountingInterimUpdatesInterval box.

- 6 To configure an interim update interval source, select a radio button in **RadiusAccountingInterimUpdatesIntervalSource**.
- 7 On the tool bar, click **Apply**.

--End--

Variable definitions

The following table describes fields on the RADIUS Accounting tab.

Variable	Value
RadiusAccountingInterimUpdates	Enables or disables RADIUS Interim Accounting Updates support statically on the switch.
RadiusAccountingInterimUpdatesInterval	Specifies the RADIUS Interim Accounting Updates support timeout interval in seconds. Values range from 60 to 3600 seconds. The default is 600 seconds.
RadiusAccountingInterimUpdatesIntervalSource	Selects the source for the RADIUS Interim Accounting Updates support timeout interval. <ul style="list-style-type: none"> • configuredValue—uses the interval value configured in the RadiusAccountingInterimUpdatesInterval box. • radiusServer—uses the RADIUS Interim Accounting Updates support timeout interval transmitted by the RADIUS server

DHCP snooping configuration using EDM

Use the procedures in this section to configure DHCP snooping to provide security to your network by preventing DHCP spoofing.

DHCP snooping configuration using EDM navigation

- [“Configuring DHCP snooping globally using EDM” \(page 220\)](#)
- [“Configuring DHCP snooping on a VLAN using EDM” \(page 221\)](#)
- [“Configuring DHCP snooping port trust using EDM” \(page 222\)](#)

Configuring DHCP snooping globally using EDM

Perform this procedure to globally enable or disable DHCP snooping on the switch.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click DHCP Snooping .
3	In the work area, click the DHCP snooping tab.
4	Do one of the following: <ul style="list-style-type: none"> • Select the DhcpSnoopingEnabled check box to enable DHCP snooping. • Clear the DhcpSnoopingEnabled check box to disable DHCP snooping.
5	On the tool bar, click Apply .

--End--

Configuring DHCP snooping on a VLAN using EDM

Perform this procedure to enable or disable DHCP snooping on the VLAN.

ATTENTION

You must enable DHCP snooping separately for each VLAN ID.

ATTENTION

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

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click DHCP Snooping .
3	In the work area, click the DHCP snooping-VLAN tab.
4	In the DhcpSnoopingEnabled column, double-click the cell for the VLAN you are configuring.
5	From the list, select true to enable DHCP snooping on the VLAN or select false to disable DHCP snooping on the VLAN..
6	On the tool bar, click Apply .

--End--

Variable definitions

The following table describes fields on the DHCP Snooping-VLAN tab.

Variable	Value
VlanId	Identifies the VLANs configured on the switch.
DhcpSnoopingEnabled	Enables or disables DHCP snooping on a VLAN.

Configuring DHCP snooping port trust using EDM

Perform this procedure to configure DHCP snooping on ports. DHCP Snooping on ports is set to untrusted, by default.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click DHCP Snooping .
3	In the work area, click the DHCP snooping-port tab.
4	In the DhcpSnoopInIfTrusted column, double-click the cell for the port you want to configure.
5	From the list, select trusted to enable DHCP snooping on the port or untrusted to disable DHCP snooping on the port.
6	Repeat steps 4 and 5 to configure additional ports as required.
7	On the tool bar, click Apply .
--End--	

Variable definitions

The following table describes fields on the DHCP snooping-port tab.

Variable	Value
Port	Identifies the ports on the switch.
DhcpSnoopingIfTrusted	Specifies if the port is trusted or untrusted. Default is false.

Viewing the DHCP binding information using EDM

Perform this procedure to view the current DHCP snooping binding table.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click DHCP Snooping .
3	In the work area, click the DHCP Bindings tab.
--End--	

Variable definitions

The following table describes fields on the DHCP Bindings tab.

Variable	Value
VlanId	Identifies the VLAN on the switch.
MacAddress	Indicates the MAC address of the DHCP client.
AddressType	Indicates the MAC address type of the DHCP client.
Address	Indicates IP address of the DHCP client.
Interface	Indicates the interface to which the DHCP client is connected.
LeaseTime(sec)	Indicates the lease time (in seconds) of the DHCP client binding.
TimeToExpiry(sec)	Indicates the time (in seconds) before a DHCP client binding expires.

Dynamic ARP inspection configuration using EDM

Use the procedures in this section to configure Address Resolution Protocol inspection (ARP inspection) to validate ARP packets on your network.

ARP inspection configuration using EDM navigation

- [“Configuring dynamic ARP inspection on a VLAN using EDM” \(page 224\)](#)
- [“Configuring dynamic ARP inspection on a port using EDM” \(page 224\)](#)

Configuring dynamic ARP inspection on a VLAN using EDM

Perform this procedure to enable or disable dynamic ARP inspection on the VLAN.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click Dynamic ARP Inspection (DAI) .
3	In the work area, click the ARP Inspection-VLAN tab.
4	In the ArpInspectionEnabled column, double-click the cell for the VLAN you want to configure.
5	From the list, select true to enable ARP inspection on the VLAN or select false to disable ARP inspection on the VLAN..
6	On the tool bar, click Apply .
--End--	

Variable definitions

The following table describes the fields on the ARP inspection-VLAN tab.

Variable	Value
VlanId	Identifies VLANs configured on the switch.
ArpInspectionEnabled	Enables or disables ARP inspection on a VLAN.

Configuring dynamic ARP inspection on a port using EDM

Perform this procedure to enable or disable dynamic ARP inspection on a port.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click Dynamic ARP Inspection .
3	In the work area, click the ARP Inspection-Port tab.

- 4 In the **ArpInspectionIfTrusted** column, double-click the cell for the port you want to configure.
- 5 From the list, select **trusted** to enable ARP inspection on the port or select **untrusted** to disable ARP inspection on the port.
- 6 On the tool bar, click **Apply**.

--End--

Variable definitions

The following table describes the fields on the ARP Inspection-port tab.

Variable	Value
Port	Identifies ports on the switch, using the unit/port format.
ArpInspectionIfTrusted	Configures a port as trusted or untrusted for ARP inspection.

IP Source Guard configuration using EDM

Use the procedures in this section to configure IP Source Guard to add a higher level of security to a port or ports by preventing IP spoofing.

Prerequisites

- Globally enable Dynamic Host Control Protocol (DHCP) snooping.
For information see [“Configuring DHCP snooping globally using EDM” \(page 220\)](#).
- Ensure that the port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- Ensure that the port is an untrusted DHCP snooping and dynamic ARP Inspection port.
- Confirm that the bsSourceGuardConfigMode MIB object exists.
Use the MIB object to control the IP Source Guard mode on an interface.
- Ensure that the following applications are disabled:
 - IP Fix
 - Baysecure
 - Extensible Authentication Protocol over LAN (EAPOL)

ATTENTION

Due to an existing Ethernet Routing Switch 2500 Series hardware limitation, you can only enable a maximum of six ports simultaneously out of each group of eight, no matter which operating mode (stand-alone or stacking) you use.

ATTENTION

Nortel recommends that you do not enable IP Source Guard on trunk ports. You can consume all hardware resources if IP Source Guard is enabled on trunk ports with a large number of VLANs that have DHCP snooping enabled and traffic sending can be interrupted for some clients.

IP Source Guard configuration using EDM navigation

Use the procedures in this section to configure IP Source Guard on the switch.

- [“Configuring IP Source Guard on a port using EDM” \(page 226\)](#)
- [“Filtering IP Source Guard addresses using EDM” \(page 227\)](#)

Configuring IP Source Guard on a port using EDM

Perform this procedure to enable or disable a higher level of security on a port or ports.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click IP Source Guard (IPSG) .
3	In the work area, click the IP Source Guard-port tab.
4	In the Mode column, double click the cell of the port you want to configure.
5	From the list, select ip to enable IP Source Guard or select disabled to disable IP Source Guard on the port.
6	On the tool bar, click Apply .
--End--	

You can click **Refresh** to update the IP Source Guard-port table.

Variable definitions

The following table describes the fields on the IP Source Guard-port tab.

Variable	Value
Port	Identifies the port number.
Mode	Identifies the Source Guard mode for the port. The mode can be disabled or ip. The default mode is disabled.

Filtering IP Source Guard addresses using EDM

Perform this procedure to display IP Source Guard information for specific IP addresses.

Procedure steps

Step	Action
1	From the navigation tree, double-click Security to open the Security tree.
2	In the Security tree, double-click IP Source Guard (IPSG) .
3	In the work area, click the IP Source Guard-addresses tab.
4	On the tool bar, click Filter .
5	In the IP Source Guard-addresses - Filter dialog , select the required parameters to display specific port IP Source Guard information.
6	Click Filter .
--End--	

Variable definitions

The following table describes fields on the IP Source Guard-addresses Filter dialog.

Variable	Value
Condition	<p>Defines the search condition.</p> <ul style="list-style-type: none"> • AND: Includes keywords specified in both the Port and Address fields while filtering results. • OR: Includes either one of the keywords specified in the Port and Address fields while filtering results.
Ignore Case	Ignores the letter case while searching.

Variable	Value
Column	Specifies the content of the column search. <ul style="list-style-type: none">• Contains• Does not contain• Equals to
All records	Displays all entries in the table.
Port	Searches for the specified port.
Address	Searches for the specified IP address.

SNMP configuration using EDM

Simple Network Management Protocol (SNMP) provides a mechanism to remotely configure and manage a network device. An SNMP agent is a software process that listens on UDP port 161 for SNMP messages, and sends trap messages using the destination UDP port 162.

SNMPv3 is based on the architecture of SNMPv1 and SNMPv2c. It supports better authentication and data encryption than SNMPv1 and SNMPv2c.

SNMPv3 provides protection against the following security threats:

- modification of SNMP messages by a third party
- impersonation of an authorized SNMP user by an unauthorized person
- disclosure of network management information to unauthorized parties
- delayed SNMP message replays or message redirection attacks

The configuration parameters introduced in SNMPv3 make it more secure and flexible than the other versions of SNMP.

For more information about the SNMPv3 architecture, see RFC 3411.

SNMP configuration navigation

- [“Viewing SNMP information” \(page 229\)](#)
- [“Graphing SNMP statistics” \(page 230\)](#)
- [“Defining a MIB view” \(page 231\)](#)
- [“Configuring an SNMP user” \(page 232\)](#)
- [“Viewing SNMP user details” \(page 234\)](#)
- [“Configuring an SNMP community” \(page 234\)](#)

- “Viewing SNMP community details” (page 236)
- “Configuring an SNMP host” (page 236)
- “Configuring SNMP host notification using EDM” (page 237)
- “Configuring SNMP notification control using EDM” (page 238)

Viewing SNMP information

The SNMP tab provides read-only information about the addresses that the agent software uses to identify the switch.

Perform this procedure to view SNMP information.

Procedure steps

Step	Action
1	From the navigation tree, double-click Edit to open the Edit tree.
2	In the Edit tree, double-click Chassis .
3	In the Chassis tree, double-click Chassis .
4	In the work area, click the SNMP tab.

--End--

Variable definitions

The following table describes the SNMP tab fields.

Variable	Value
LastUnauthenticatedInetAddressType	The type of IP address that was not authenticated by the device last.
LastUnauthenticatedInetAddress	The last IP address that is not authenticated by the device.
LastUnauthenticatedCommunityString	The last community string that is not authenticated by the device.
RemoteLoginInetAddressType	Specifies either IPv4 or IPv6.
RemoteLoginInetAddress	Specifies the remote login IP address.
TrpRcvrMaxEnt	The maximum number of trap receiver entries.
TrpRcvrCurEnt	The current number of trap receiver entries.
TrpRcvrNext	The next trap receiver entry to be created.

Graphing SNMP statistics

Perform this procedure to graph SNMP statistics.

Procedure steps

Step	Action
1	From the navigation pane, double click Graph to open the navigation tree.
2	In the Graph tree, double-click Chassis .
3	In the work area, click the SNMP tab.
4	Click a cell in a row of data that you want to graph.
5	On the tool bar, click a graph type.
--End--	

Variable definitions

The following table describes the SNMP tab fields.

Variable	Value
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 are accepted and processed by the SNMP protocol.
InGetNexts	The total number of SNMP Get-Next PDUs that are accepted and processed by the SNMP protocol.
InSetRequests	The total number of SNMP Set-Request PDUs that are accepted and processed by the SNMP protocol.
InGetResponses	The total number of SNMP Get-Response PDUs that are accepted and processed by the SNMP protocol.
OutTraps	The total number of SNMP Trap PDUs generated by the SNMP protocol.
OutTooBig	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is tooBig.

Variable	Value
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.
InBadCommunity Names	The total number of SNMP messages delivered to the SNMP protocol that used an unknown SNMP community name.
InBadCommunity Uses	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.
InTooBig	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.
InReadOnly	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is <i>readOnly</i> . It is a protocol error to generate an SNMP PDU containing the value <i>readOnly</i> 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.

Defining a MIB view

Perform this procedure to assign MIB view access for an object.

Procedure steps

Step	Action
1	From the navigation tree, double-click Edit to open the Edit tree.
2	In the Edit tree, double-click Snmp Server .
3	In the Snmp Server tree, double-click MIB View .
4	On the toolbar, click Insert .
5	On the Insert MIB View dialog, enter and select criteria to describe the MIB View.
6	Click Insert .
7	On the tool bar, click Apply .
--End--	

The following table describes the MIB View tab fields.

Variable	Value
ViewName	Specifies a name for the new entry in a range from 1 to 32 characters.
Subtree	Specifies any valid object identifies that defines a set of MIB objects accessible by this SNMP entry. For example; ort, iso8802, or 1.3.5.1.1.5 OID string.
Type	To determine whether access to a MIB object is granted or denied, select one of the following: <ul style="list-style-type: none"> • included—granted • excluded—denied
Storage Type	Select one of the following: <ul style="list-style-type: none"> • volatile—entry does not persist if switch loses power • nonVolatile—entry persists if switch loses power

Configuring an SNMP user

Perform this procedure to create an SNMP user.

Procedure steps

Step	Action
1	From the navigation tree, double-click Edit to open the Edit tree.

- 2 In the Edit tree, double-click **Snm Server**.
- 3 In the Snmp Server tree, double-click **User**.
- 4 On the User tab tool bar, click **Details**.
- 5 On the Details page, click **Insert**.
- 6 Enter the parameters to describe the user.
- 7 Click **Insert**.
- 8 On the toolbar, click **Apply**.

--End--

The following table describes the User tab fields.

Variable	Value
Engine ID	Indicates the administratively-unique identifier of the SNMP engine.
Name	Indicates the name of the user in usmUser.
Auth Protocol	Select an authentication protocol from the following list: <ul style="list-style-type: none"> • None • MD5 • SHA
AuthPassword	Specifies the current authorization password.
ConfirmPassword	Reenter the password to confirm.
Priv Protocol	To assign a privacy protocol, select one of the following from the list: <ul style="list-style-type: none"> • None • DES • 3DES • AES
PrivacyPassword	Specifies the current privacy password.
ConfirmPassword	Reenter the password to confirm.
ReadViewName	Specifies the name of the MIB View to which the user is assigned read access.
WriteViewName	Specifies the name of the MIB View to which the user is assigned write access.

Variable	Value
NotifyViewName	Specifies the name of the MIB View from which the user receives notifications.
Storage Type	Specifies whether this table entry is stored in one of the following memory types: <ul style="list-style-type: none"> volatile—entry does not persist if switch loses power nonVolatile—entry persists if switch loses power

Viewing SNMP user details

Perform this procedure to view SNMP user details.

Procedure steps

Step	Action
1	From the navigation tree, double-click Edit to open the Edit tree.
2	In the Edit tree, double-click Sntp Server .
3	In the Sntp Server tree, double-click User .
4	In the work area, on the User tab, select a user.
5	On the toolbar, click the Details button.
--End--	

Configuring an SNMP community

A community string is a passphrase used by the switch in snmpv1 and snmpv2 operations. Perform this procedure to configure an SNMP community string.

Procedure steps

Step	Action
1	From the navigation tree, double-click Edit to open the Edit tree.
2	In the Edit tree, double-click Sntp Server .
3	In the Sntp Server tree, double-click Community .
4	On the Community tab tool bar, click Details .
5	On the toolbar, click Insert .
6	Enter the parameters to describe the community.

- 7 Click **Insert**.
- 8 On the toolbar, click **Apply**.

--End--

The following table describes the Community tab fields.

Variable	Value
Index	Specifies the unique index value of a row in the community table.
Name	Specifies the community string: a row in the Community table represents a configuration.
ContextEngineId	Specifies the contextEngineId that indicates the location of the context in which management information is accessed when using the community string specified by the corresponding instance of CommunityName. The default value is the EngineId of the entity in which this object is represented.
CommunityString	Specifies a community string to be created with access to specific views. You can create community strings with varying levels of read, write, and notification access based on SNMPv3 views.
ConfirmCommunity	Re-enter and confirm the community string.
ReadView Name	Specifies the name of the MIB View to which the user is assigned read access.
WriteViewName	Specifies the name of the MIB View to which the user is assigned write access.
NotifyViewName	Specifies the name of the MIB View from which the user receives notifications.
Storage Type	Select one of the following: <ul style="list-style-type: none"> • volatile—entry does not persist if switch loses power • nonVolatile—entry persists if switch loses power

Viewing SNMP community details

Perform this procedure to view SNMP community details.

Procedure steps

Step	Action
1	From the navigation tree, double-click Edit to open the Edit tree.
2	In the Edit tree, double-click Snmp Server .
3	In the Snmp Server tree, double-click Community .
4	In the work area, on the Community tab, select a community.
5	On the toolbar, click Details .
--End--	

Configuring an SNMP host

Perform this procedure to create an SNMP host.

Procedure steps

Step	Action
1	From the navigation tree, double-click Edit to open the navigation tree.
2	In the Edit tree, double-click Snmp Server .
3	In the Snmp Server tree, double-click Host .
4	On the Host tab tool bar, click Insert .
5	On the Insert Host dialog, enter and select criteria to describe the host.
6	Click Insert .
7	On the Host tab tool bar, click Apply .
--End--	

The following table describes the Insert Host tab fields.

Variable	Value
Domain	Select one of the following: <ul style="list-style-type: none"> • IPv4 • IPv6 The default value is IPv4.

Variable	Value
Destination Address	Specifies the destination address, expressed in IPv4 Address : port format.
Timeout	Specifies the timeout interval, expressed in 1/100 of a second. The default value is 1500.
RetryCount	Specifies the number of retries the system attempts; expressed as an integer from 0 to 255. The default value is 3.
Type	Specifies the type as one of the following: <ul style="list-style-type: none"> • trap • inform
Version	Specifies the SNMP version as one of the following: <ul style="list-style-type: none"> • SNMPv1 • SNMPv2c • SNMPv3/USM
SecurityName	Specifies security name used for generating SNMP messages.
SecurityLevel	Specifies the security level for SNMP messages as one of the following: <ul style="list-style-type: none"> • noAuthNoPriv • authNoPriv • authPriv
Storage Type	Select one of the following: <ul style="list-style-type: none"> • volatile—entry does not persist if switch loses power • nonVolatile—entry persists if switch loses power

Configuring SNMP host notification using EDM

Perform this procedure to configure SNMP trap notification.

Procedure steps

Step	Action
1	From the navigation tree, double-click Edit to open the Edit tree.
2	In the Edit tree, double-click Sntp Server .

- 3 In the Snmp Server tree, double-click **Host**.
- 4 On the Host tab tool bar, click **Notification**.
- 5 On the Insert Host dialog, enter and select criteria to describe the trap notification.
- 6 Click **Insert** to return to the Host tab.
- 7 On the Host tab tool bar, click **Apply**.

--End--

Field	Value
Domain	Indicates the address transport type; either IPv4 or IPv6.
DestinationAddr : Port	Indicates the transport address (in IPv4 Address : port format).
Timeout	Indicates the time interval that an application waits for a response in 1/100 second intervals from 0 to 2147483647.
RetryCount	Indicates the number of retries to be attempted when a response is not received for a generated message from 0 to 255.
Type	Indicates the type of the message; either trap or information.
Version	Indicates the SNMP version; either SNMPv1, SNMPv2c or SNMPv3/USM.
SecurityName	Enter the community string.
SecurityLevel	Indicates the security level; either no authorization and no privileges, authorization and no privileges, or authorization and privileges.
StorageType	Indicates the storage type; either volatile or nonvolatile..

Configuring SNMP notification control using EDM

Perform this procedure to enable or disable SNMP traps in the list. Notification Control is the Trap Web Page.

Procedure steps

Step	Action
1	From the navigation tree, double-click Edit to open the Edit tree.

- 2 In the Edit tree, double-click **Snmp Server**.
- 3 In the Snmp Server tree, double-click **Notification Control**.
- 4 In the NotifyControlEnabled column, double-click the cell in the NotifyControlType (SNMP trap) row that you wish to modify.
- 5 Select a value from the list: **true** to enable notification control, or **false** to disable notification control.
- 6 On the Notification Controls tool bar, click **Apply**.

--End--

Field	Value
NotifyControlType	Lists the SNMP trap names.
Notify Control Type (oid)	Lists the object identifiers for the SNMP traps.
NotifyControlEnabled	Specifies whether traps are enabled or disabled.

Appendix

Appendixes

This section contains information about the following topics:

- [“TACACS+ server configuration examples” \(page 241\)](#)
- [“SNMP MIB support” \(page 253\)](#)

TACACS+ server configuration examples

This section describes basic configuration examples of the TACACS+ server:

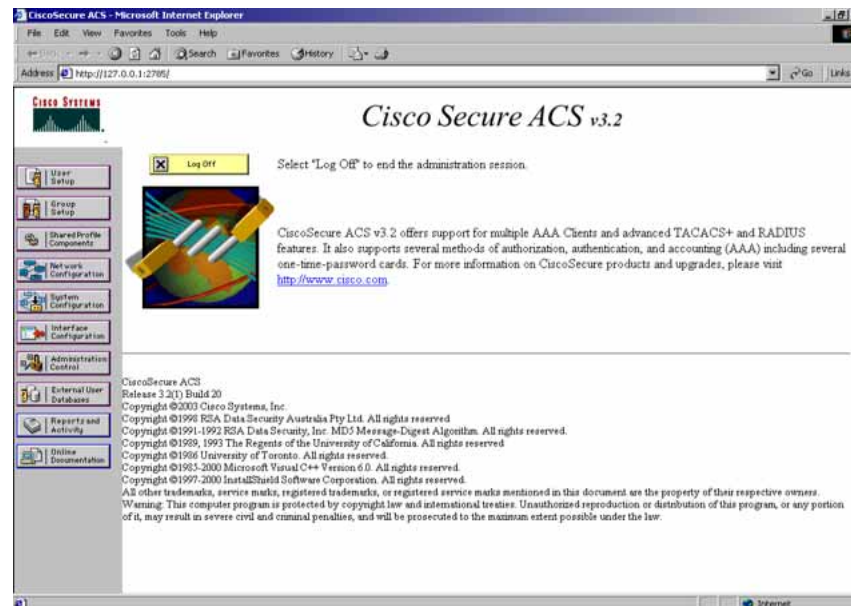
TACACS+ server configuration examples navigation

- [“Configuration example: Cisco ACS \(version 3.2\) server” \(page 241\)](#)
- [“Configuration example: ClearBox server” \(page 246\)](#)

Configuration example: Cisco ACS (version 3.2) server

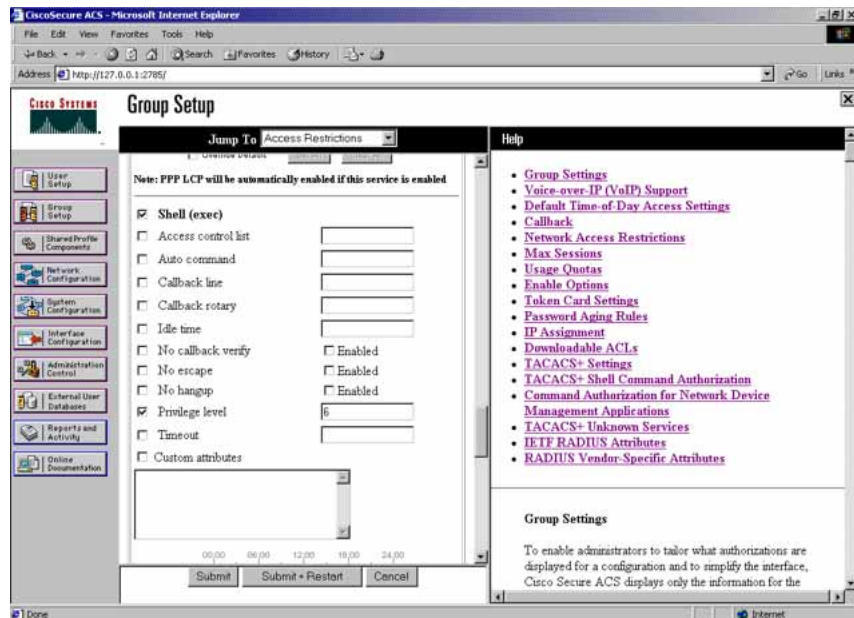
The following figure shows the main administration window.

Figure 25
Cisco ACS (version 3.2) main administration window



Step	Action
1	<p>Define the users and the corresponding authorization levels.</p> <p>If you map users to default group settings, it is easier to remember which user belongs to each group. For example, the rwa user belongs to group 15 to match Privilege level 15. All rwa user settings are picked up from group 15 by default.</p> <p>The following figure shows a sample Group Setup window.</p>

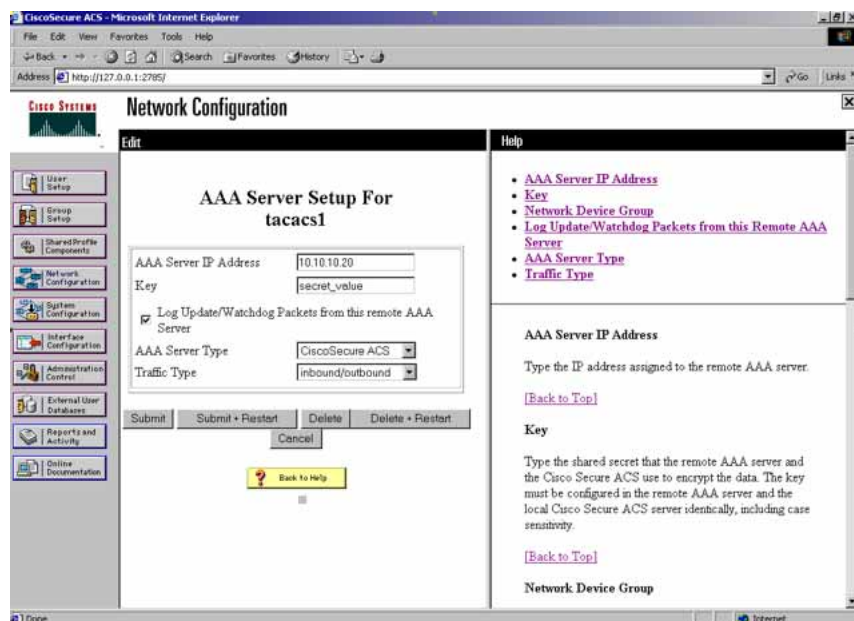
Figure 26
Group Setup window - Cisco ACS server configuration



2 Configure the server settings.

The following figure shows a sample Network Configuration window to configure the authentication, authorization, and accounting (AAA) server for TACACS+.

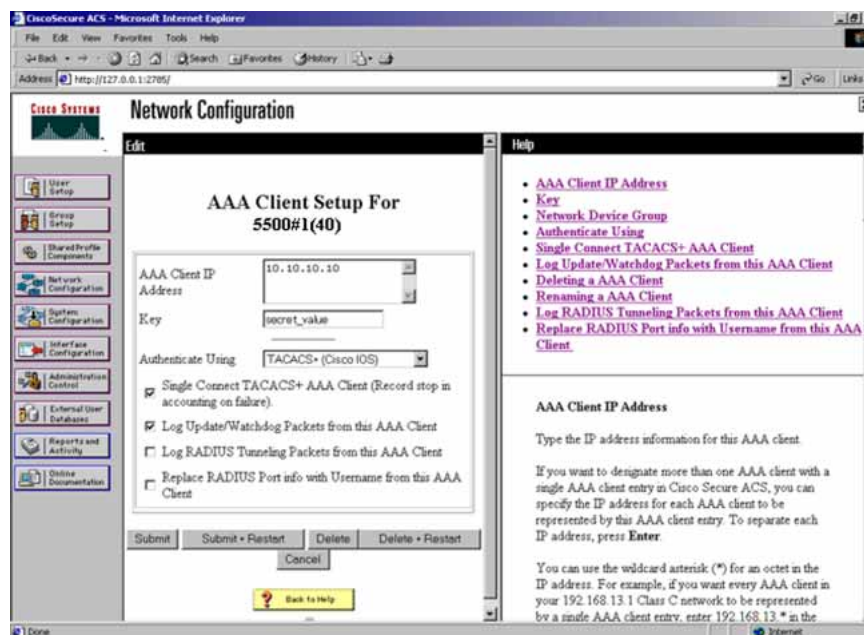
Figure 27
Network Configuration window - server setup



3 Define the client.

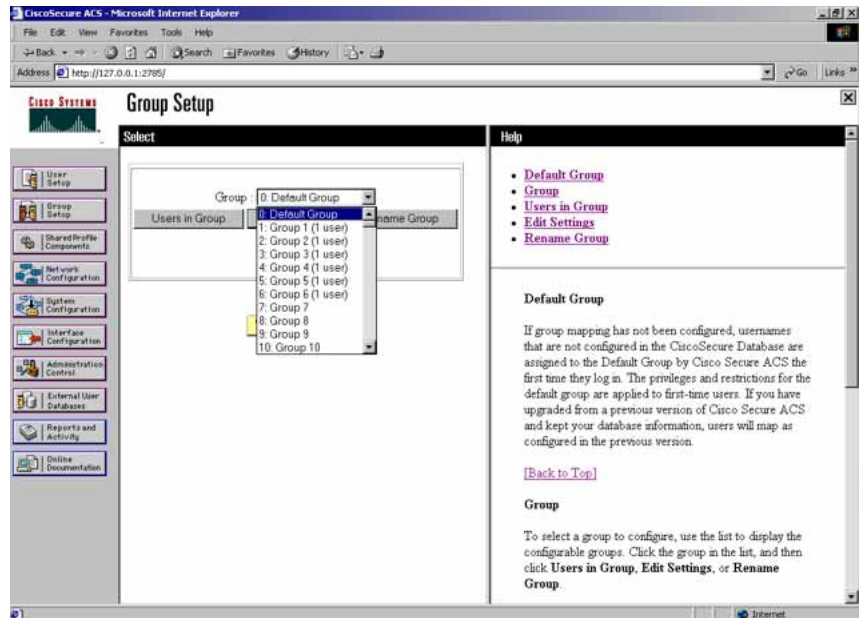
The following figure shows a sample Network Configuration window to configure the client. Authenticate using TACACS+. Single-connection can be used, but this must match the configuration on the Nortel Ethernet Routing Switch 2500 .

Figure 28
Network Configuration window - client setup

**4** Verify the groups you have configured.

In this example, the user is associated with a user group. The rwa account belongs to group 15, and its privilege level corresponds to the settings for group 15. The ro accounts belong to group 0, L1 accounts belong to group 2, and so on.

Figure 29
Group Setup window - viewing the group setup

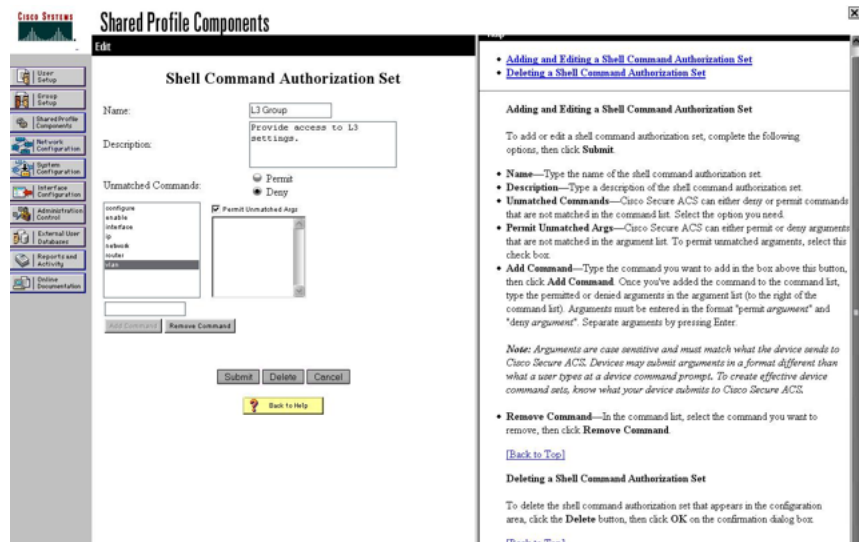


- 5 Go to **Shared Profile Components , Shell Command Authorization Set.**

The Shell Command Authorization Set screen appears.

Figure 30

Shared Profile Components window - defining the command set



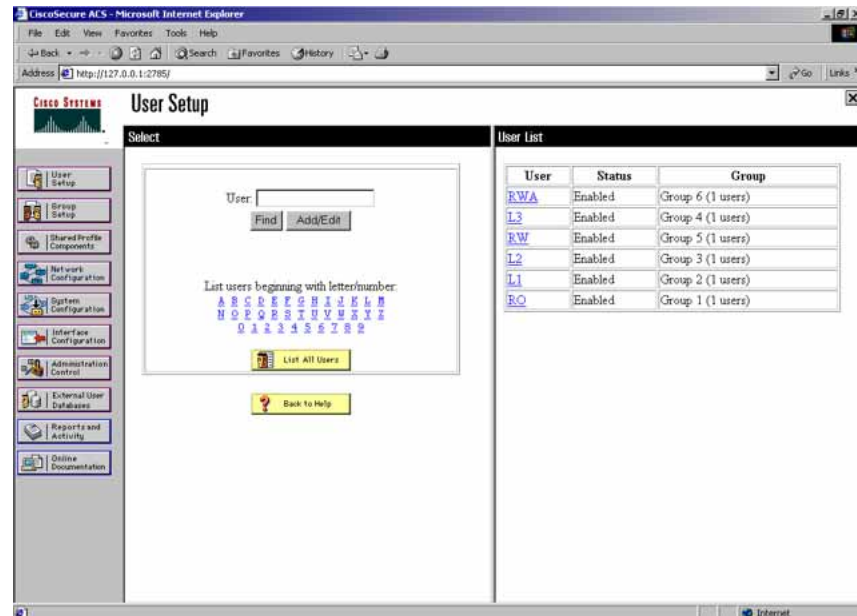
- 6 Select the commands to be added to the command set, and specify whether the action is permit or deny.

- 7 View users, their status, and the corresponding group to which each belongs.

The following figure shows a sample User Setup window. You can use this window to find, add, edit, and view users settings.

Figure 31

User Setup window - Cisco ACS server configuration

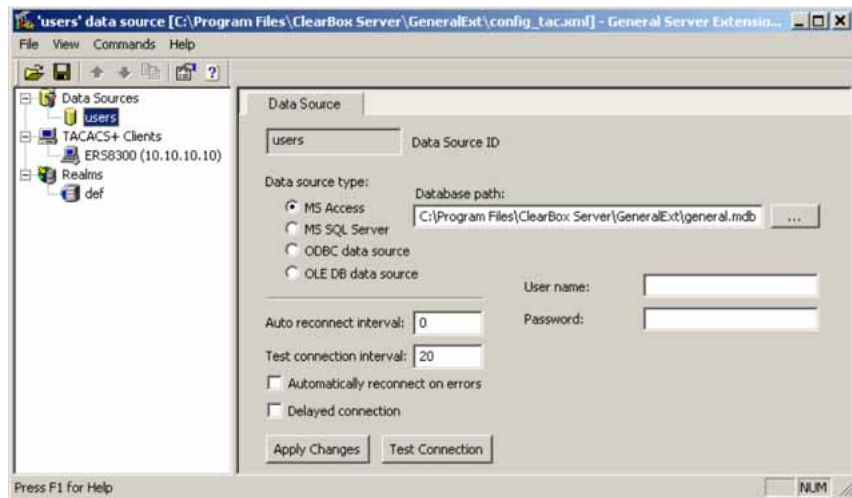


--End--

Configuration example: ClearBox server

Step	Action
1	<p>Run the General Extension Configurator and configure the user data source.</p> <p>In this example, Microsoft Access was used to create a database of user names and authorization levels; the general.mdb file needs to include these users.</p>

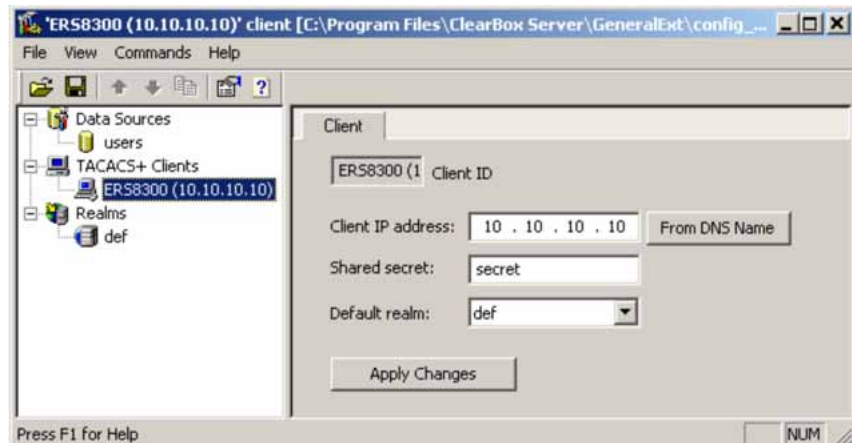
Figure 32
General Extension Configurator



- 2 Create a Client entry for the switch management IP address by right-clicking the **TACACS+ Clients** item.

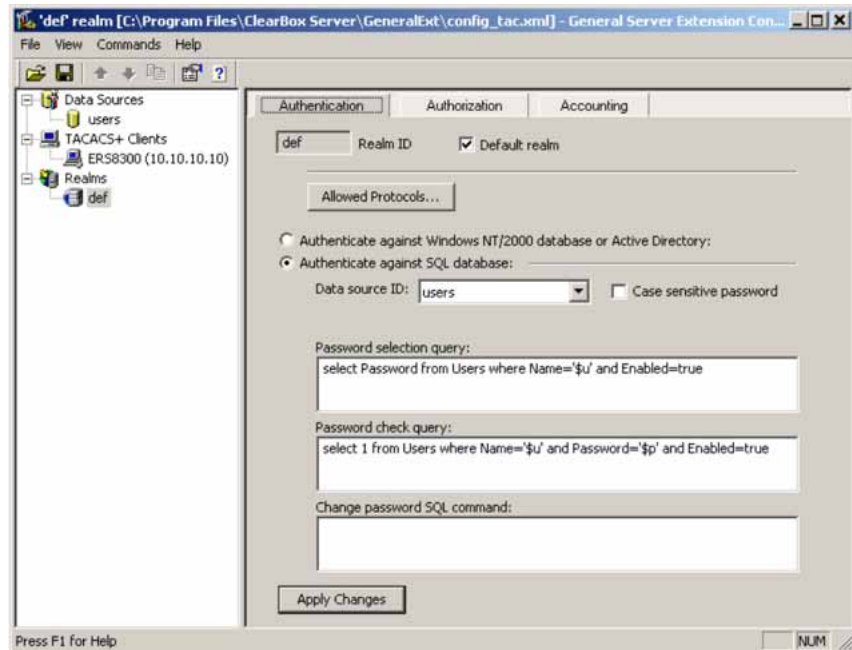
In this case, the TACACS+ Client is the Nortel Ethernet Routing Switch 2500 . Enter the appropriate information. The shared secret must match the value configured on the Nortel Ethernet Routing Switch 2500 .

Figure 33
Creating a client entry



The default realm Authentication tab looks like the following figure.

Figure 34
Default realm - Authentication tab

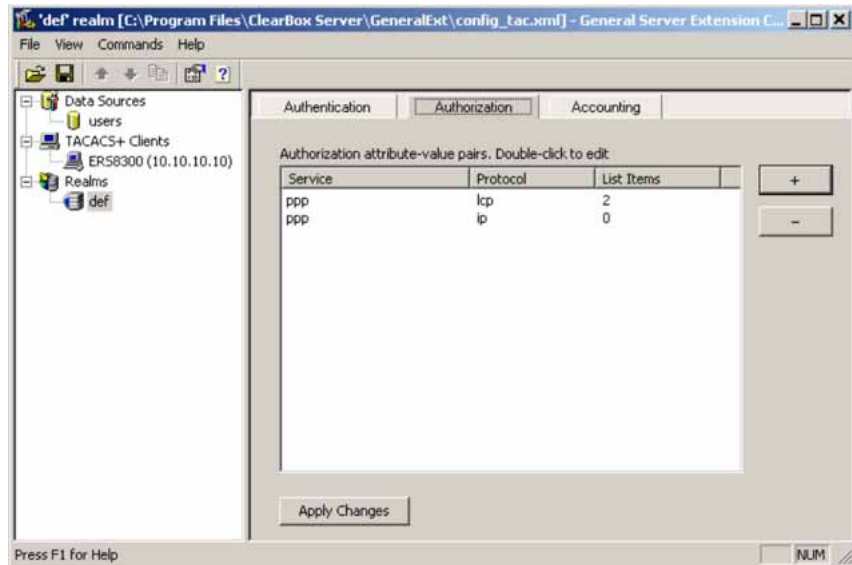


3 Select **Realms** , **def** , **Authorization** tab.

A new service is required that allows the server to assign certain levels of access.

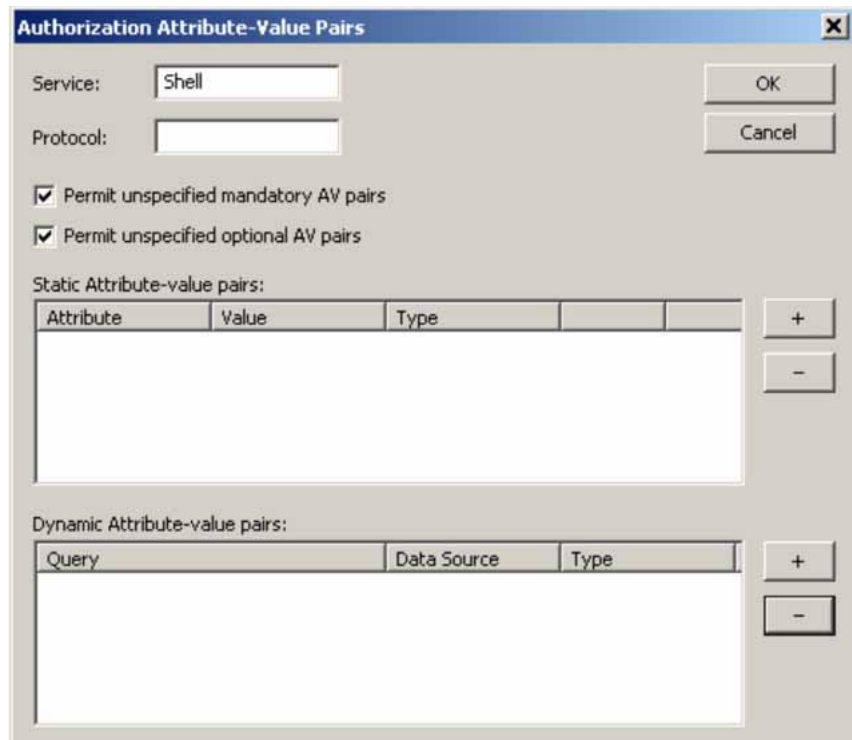
4 Click the **+** button to add an attribute-value pair for privilege levels .

Figure 35
Default realm - Authorization tab



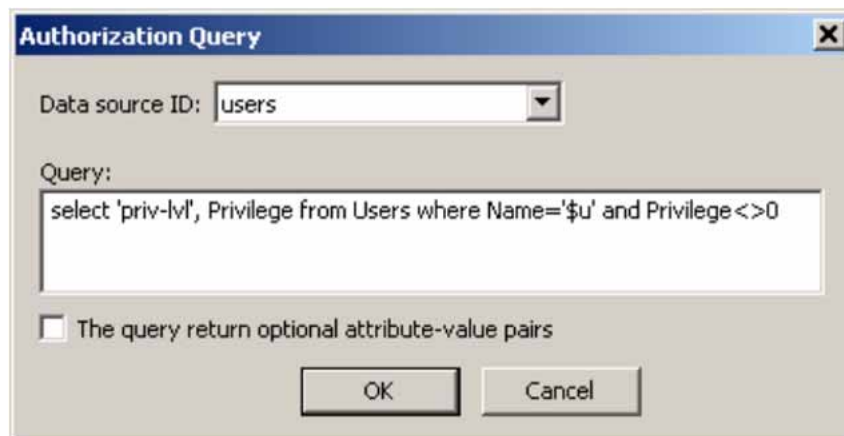
- 5 Enter information in the window as shown in the following figure to specify the query parameters.

Figure 36
Adding parameters for the query



- 6 Click the + button to add the parameters to the query.
- 7 Use the string shown in the following figure for the authorization query.

Figure 37
Authorization Query window



Authorization Query

Data source ID: users

Query:

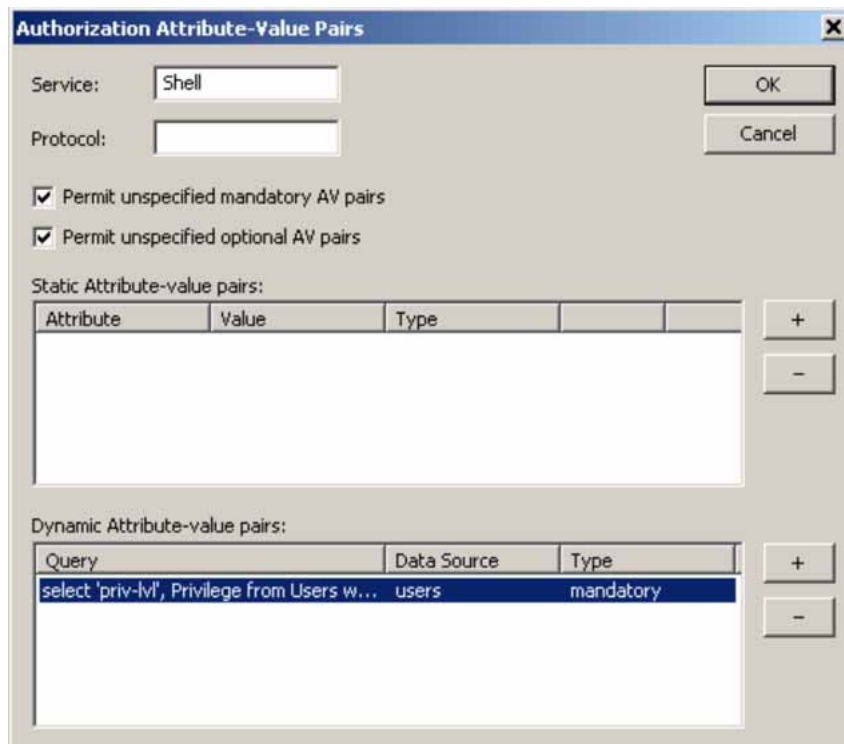
```
select 'priv-lvl', Privilege from Users where Name='$u' and Privilege <> 0
```

The query return optional attribute-value pairs

OK Cancel

The following figure shows the final window.

Figure 38
Query parameters added to Authorization Attribute-Value Pairs window



Authorization Attribute-Value Pairs

Service: Shell

Protocol:

Permit unspecified mandatory AV pairs

Permit unspecified optional AV pairs

Static Attribute-value pairs:

Attribute	Value	Type
-----------	-------	------

Dynamic Attribute-value pairs:

Query	Data Source	Type
select 'priv-lvl', Privilege from Users w...	users	mandatory

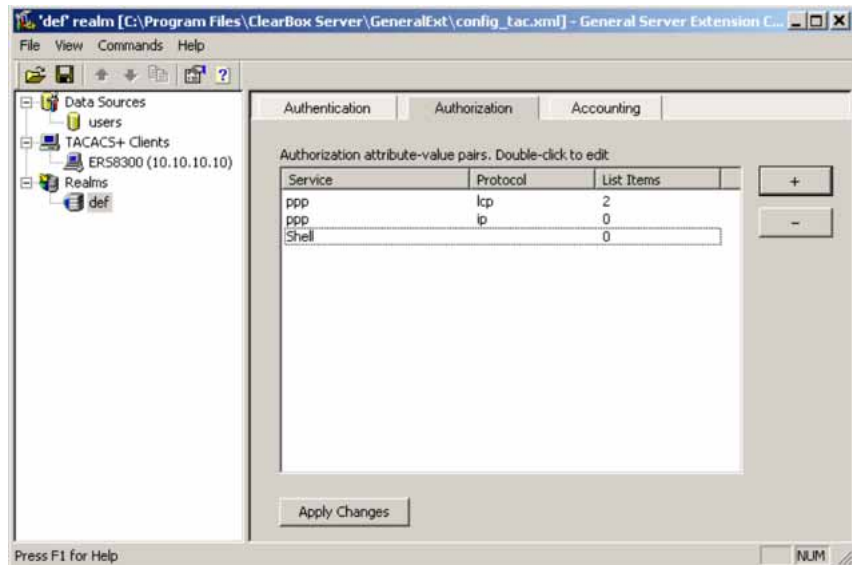
OK Cancel

- 8 Click **OK**.

The information appears on the **Authorization** tab.

Figure 39

Authorization attribute-value pairs added to Authorization tab



- 9 Navigate to the general.mdb file as specified earlier.

The user table should look like the one shown in the following figure. If the **Privilege** column does not exist, create one and populate it according to the desired access level.

Microsoft Access or third-party software is required to read this file.

If you use the 30-day demo for ClearBox, the user names cannot be more than four characters in length.

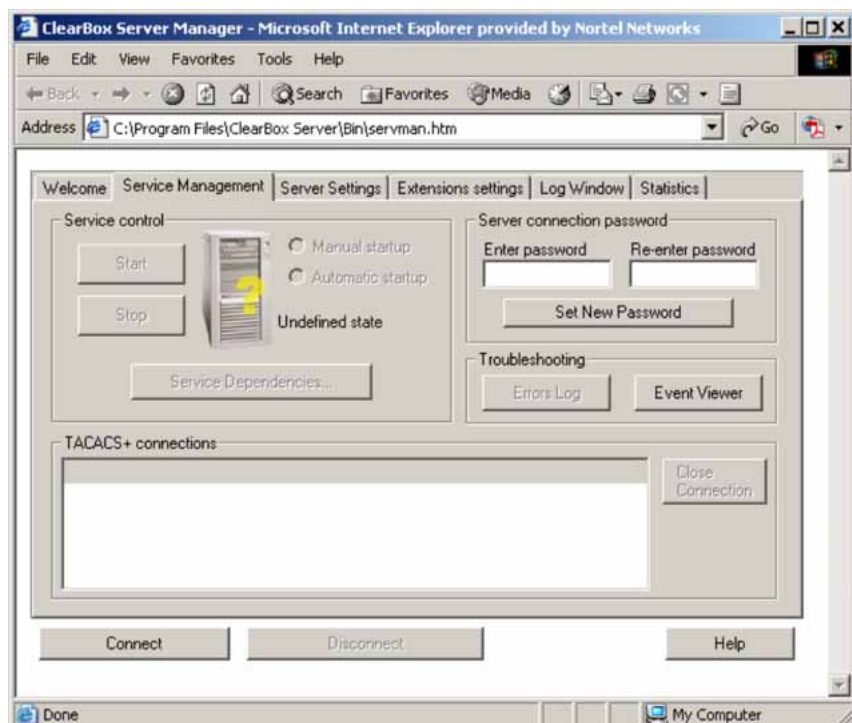
Figure 40

Users table - Microsoft Access

ID	Name	Password	Enabled	Privilege
1	admin	admin	<input checked="" type="checkbox"/>	6
2	user	user	<input checked="" type="checkbox"/>	5
3	guest	guest	<input checked="" type="checkbox"/>	1
(AutoNumber)			<input checked="" type="checkbox"/>	

- 10 Run the Server Manager.

Figure 41
ClearBox Server Manager



- 11 Click the **Connect** button.
The **Connect to...** dialog box appears.
Figure 42
Connect to... dialog box

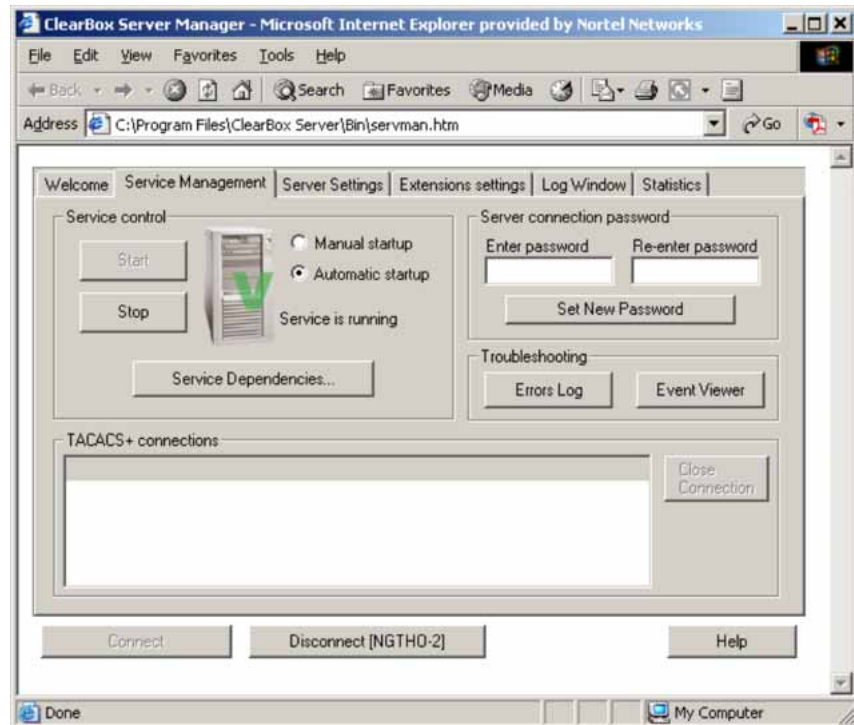


- 12 Click **OK** (do not fill in fields).
13 Click **OK** at the warning message.

14 Click **Start**.

The Server Manager should now look like the following figure. Changes to the General Server Extension Configurator require that the server be restarted.

Figure 43
TACACS+ server connected



--End--

SNMP MIB support

The Ethernet Routing Switch 2500 supports an SNMP agent with industry standard MIBs, as well as private MIB extensions, which ensures compatibility with existing network management tools. The switch supports the MIB-II (RFC 1213), Bridge MIB (RFC 1493), and the RMON MIB (RFC 1757), which provide access to detailed management statistics. With SNMP management, you can configure SNMP traps (on individual ports) to generate automatically for conditions such as an unauthorized access attempt or changes in the operating status of a port. [Table 65 "SNMP MIB support" \(page 254\)](#) lists the supported SNMP MIBs.

Table 65
SNMP MIB support

Application	Standard MIBs	Proprietary MIBs
S5 Chassis MIB		s5cha127.mib
S5 Agent MIB		s5age140.mib
RMON	rfc1757.mib	
MLT		rcMLT
SNMPv3 MIBs	RFCs 2571, 2572, 2573, 2574, 2575, 2576	
MIB2	rfc1213.mib	
IF-MIB	rfc2233.mib	
Etherlike MIB	rfc1643.mib	
Interface Extension MIB		s5ifx100.mib
Switch Bay Secure		s5sbs102.mib
System Log MIB		bnlog.mib
S5 Autotopology MIB		s5emt104.mib
VLAN		rcVlan
Entity MIB	RFC 2037	
Spanning Tree	RFC1493 Bridge MIB	
LLDP-MIB	IEEE 802.1ab	

Management Agent

The SNMP agent is trilingual and supports exchanges by using SNMPv1, SNMPv2c, and SNMPv3. SNMPv1 communities provide support for SNMPv2c by introducing standards-based GetBulk retrieval capability. SNMPv3 support provides MD5 and SHA-based user authentication and message security as well as DES-based message encryption.

Modules that support MIB are:

Standard MIBs

- MIB II (RFC 1213)
- Bridge MIB (RFC 1493) and proposed VLAN extensions
- 802.1Q Bridge MIB
- 802.1p
- Ethernet MIB (RFC 1643)
- RMON MIB (RFC 1757)

- SMON MIB
- High Capacity RMON
- Interface MIB (RFC2233)
- Entity MIB (RFC2037)
- SNMPv3 MIBs (RFC 2271 –RFC 2275)

Proprietary MIBs

- s5Chassis MIB
- s5Agent MIB
- Interface Extension MIB
- s5 Multi-segment topology MIB
- s5 Switch BaySecure MIB
- System Log MIB
- RapidCity Enterprise MIB
- rcDiag (Conversation steering) MIB
- rcVLAN MIB
- rcMLT MIB

SNMP trap support

The Ethernet Routing Switch 2500 supports an SNMP agent with industry standard SNMPv1 traps, as well as private SNMPv1 trap extensions ().

Table 66
Support SNMP traps

Trap name	MIB	Sent when
lldpRemTablesChange	LLDP-MIB	Changes in lldpStatsRemTableLastChangeTime occur.
risingAlarm	s5CtrMIB	A rising alarm is fired.
fallingAlarm	s5CtrMIB	A falling alarm is fired.
pethPsePortOnOffNotification	rfc3621MIB	Pse Port is delivering or is not delivering power to the PD.
pethMainPowerUsageOnNotification	rfc3621MIB	The usage power is above the threshold.
pethMainPowerUsageOffNotification	rfc3621MIB	The usage power is below the threshold

Trap name	MIB	Sent when
entConfigChange	rfc4133MIB	A change in either of these tables occurred: entPhysicalTable, entLogicalTable, entLPMappingTable, entAliasMappingTable.
coldStart	rfc3418MIB	The system is powered on.
warmStart	rfc3418MIB	The system restarts due to a management reset.
linkDown	rfc2863MIB	The link state changes to down on a port.
linkUp	rfc2863MIB	The link state changes to up on a port.
authenticationFailure	rfc3418MIB	SNMP authentication failure occurs.
lldpXMedTopologyChangeDetected	lldpExtMedMIB	A new remote device is attached to a local port, or a remote device is disconnected.
bsAdacPortConfigNotification	bayStackAdacMIB	The maximum number of devices supported per port is reached.
bsDhcpSnoopingBindingTableFull	bayStackDhcpSnoopingMIB	An attempt is made to add a new DHCP binding entry when the binding table is full .
bsDhcpSnoopingTrap	bayStackDhcpSnoopingMIB	A DHCP packet is dropped.
bsaiArpPacketDroppedOnUntrustedPort	bayStackArpInspectionMIB	An ARP packet is dropped on an untrusted port due to an invalid IP/MAC binding.
bsSourceGuardReachedMaxIpEntries	bayStackSourceGuardMIB	The maximum number of IP entries on a port has been reached.
bsSourceGuardCannotEnablePort	bayStackSourceGuardMIB	There are insufficient resources available to enable IP source guard checking on a port.
rcnBpduReceived	rcTrapsMIB	A BPDU is received on a port which has BPDU filtering enabled.
bsnConfigurationSavedToNvram	bsnMIB	All switch configuration is saved to NVRAM.
bsnEapAccessViolation	bsnMIB	An EAP access violation occurs.
bsnStackManagerReconfiguration	bsnMIB	The stack manager detects a problem with a link between stack members.
bsnLacTrunkUnavailable	bsnMIB	An attempt is made to form an 802.3ad LAG trunk, but there are no available resources to create a new trunk .

Trap name	MIB	Sent when
bsnLoginFailure	bsnMIB	An attempt to login to the system fails as a result of an incorrect password.
bsnLacPortDisabledDueToLossOfVLACPDU	bsnMIB	A port is disabled due to the loss of a VLACP PDU.
bsnLacPortEnabledDueToReceiptOfVLACPDU	bsnMIB	A port is enabled due to receipt of a VLACP PDU.
bsnStackConfigurationError	bsnMIB	The expected size of a stack is not equal to the actual size of the stack.
bsnEnteredForcedStackMode	bsnMIB	A switch has entered forced stack mode.
bsnEapRAVErrror	bsnMIB	An Eap client MAC address was authorized on a port, but the port could not be moved to the Radius-Assigned VLAN.
s5EtrNewSbsMacAccessViolation	s5CtrMIB	A MAC address violation is detected.
s5CtrHotSwap	s5CtrMIB	A unit is hot-swapped in an operational stack.
s5CtrProblem	s5CtrMIB	A component or subcomponent has a problem condition; either a warning, nonfatal, or fatal condition.
s5CtrUnitUp	s5CtrMIB	A unit is added to an operational stack.
s5CtrUnitDown	s5CtrMIB	A unit is removed from an operational stack.

Nortel Ethernet Routing Switch 2500 Series

Configuration — Security

Release: 4.3

Publication: NN47215-505

Document revision: 04.01

Document release date: 22 February 2010

Copyright © 2008-2010 Nortel Networks. All Rights Reserved.

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

THE SOFTWARE DESCRIBED IN THIS DOCUMENT IS FURNISHED UNDER A LICENSE AGREEMENT AND MAY BE USED ONLY IN ACCORDANCE WITH THE TERMS OF THAT LICENSE.

Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com

