# Configuring Security on Avaya Ethernet Routing Switch 3500 Series

Release 5.2
NN47203-504
Issue 03.02
January 2016

© 2012-2016, Avaya, Inc.
All Rights Reserved.

**Notice**

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

**Documentation disclaimer**

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

**Link disclaimer**

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

**Warranty**

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

**Hosted Service**

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

**License types**

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

**Heritage Nortel Software**

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

**Copyright**

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

**Virtualization**

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

**Third Party Components**

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

**Service Provider**

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

**Compliance with Laws**

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

**Preventing Toll Fraud**

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

**Avaya Toll Fraud intervention**

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

**Security Vulnerabilities**

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

**Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

**Contact Avaya Support**

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

**Trademarks**

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such

Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

# Contents

**Chapter 1: Introduction** ... 16
Purpose of this document ... 16
Related resources ... 16
Documentation ... 16
Training ... 16
Viewing Avaya Mentor videos ... 16
Searching a documentation collection ... 17
Subscribing to e-notifications ... 18
Support ... 20
**Chapter 2: New in this release** ... 21
Features ... 21
Unified authentication ... 22
Other changes ... 22
**Chapter 3: ACLI command modes** ... 23
**Chapter 4: Security fundamentals** ... 25
Management password configuration ... 25
Console TELNET password Configuration ... 25
Unified authentication ... 25
Logging on ... 26
MAC address-based security ... 26
MAC address-based security autolearning ... 27
Sticky MAC address ... 27
RADIUS-based network security ... 28
How RADIUS works ... 28
RADIUS server configuration ... 28
RADIUS EAP or non-EAP requests to different servers ... 28
RADIUS server reachability ... 32
RADIUS password fallback ... 33
RADIUS Interim Accounting Updates support ... 33
RADIUS Request use Management IP Address ... 33
Campus security example ... 34
EAPOL-based security ... 36
EAPOL Security Configuration ... 37
EAPOL with Guest VLAN ... 37
Advanced EAPOL features ... 38
Multiple Host with Multiple Authentication ... 38
RADIUS-assigned VLAN use in MHMA mode ... 39
Non-EAP IP Phone authentication ... 40
Unicast EAP Requests in MHMA ... 40

802.1X or non-EAP with VLAN names.... 40
802.1X or Non-EAP and Guest VLAN on the same port.... 40
Non-EAP hosts on EAP-enabled ports.... 41
Non-EAPOL MAC RADIUS authentication.... 42
Multiple Host with Single Authentication.... 43
802.1X Non-EAP client re-authentication.... 44
802.1X or non-EAP Last Assigned RADIUS VLAN.... 45
802.1X or non-EAP with Fail Open VLAN.... 45
802.1X dynamic authorization extension (RFC 3576).... 46
802.1X EAP and NEAP Accounting .... 48
802.1X EAP Separate enable/disable.... 49
TACACS+.... 50
TACACS+ architecture.... 51
Feature operation.... 51
TACACS+ authentication.... 51
TACACS+ authorization.... 52
Changing privilege levels at run time.... 52
TACACS+ server configuration example.... 53
TACACS+ accounting.... 54
Feature limitations.... 54
TACACS+ configuration.... 55
IP Manager.... 55
Password security.... 55
Custom user names and passwords.... 56
Password length and valid characters.... 56
Password retry.... 57
Password history.... 57
Password display.... 57
Password verification.... 57
Password aging time.... 57
Log on failure timeout.... 57
Password security features and requirements.... 58
Password upgrade considerations.... 58
Read-Only and Read-Write passwords must be different.... 59
Applicable passwords.... 59
Enabling and disabling password security.... 59
Default passwords.... 60
HTTP port number change.... 60
Simple Network Management Protocol.... 60
SNMP Version 1 (SNMPv1).... 60
SNMP Version 2 (SNMPv2).... 61
SNMP Version 3 (SNMPv3).... 61
Avaya Ethernet Routing Switch 3500 Series support for SNMP.... 61

SNMP MIB support.... 61
SNMP trap support.... 61
SNMP trap control.... 62
Per host notification control.... 62
Secure Socket Layer protocol.... 62
Secure versus non-secure mode.... 63
DHCP snooping.... 63
DHCP binding table.... 64
Dynamic ARP inspection.... 65
IP Source Guard.... 65
Secure File Transfer Protocol (SFTP over SSH).... 67
SSH enhancement to support RSA.... 67
Storm Control.... 67
Rate limiting configuration.... 68
**Chapter 5: IPv6 Management Fundamentals**.... 69
The IPv6 header.... 69
IPv6 addresses.... 70
Interface ID.... 70
Address formats.... 70
IPv6 extension headers.... 71
Comparison of IPv4 and IPv6.... 72
ICMPv6.... 72
Neighbor discovery.... 73
ND messages.... 74
Neighbor discovery cache.... 75
Router discovery.... 76
Router advertisement.... 77
Router solicitation.... 77
Path MTU discovery.... 77
**Chapter 6: Configuring and managing security using ACLI**.... 78
Configuring and managing security using ACLI.... 78
Setting the system user name and password using ACLI.... 78
Setting the password for selected types of access using ACLI.... 79
Enabling or disabling password security using ACLI.... 80
Displaying the security using ACLI.... 80
Displaying the status of password security on the switch using ACLI.... 81
Setting the password aging time using ACLI.... 81
Displaying the password aging-time using ACLI.... 81
Configuring the number of password logon attempts using ACLI.... 82
Changing the http port number using ACLI.... 82
Displaying the port number of the HTTP port.... 82
Setting the HTTP port number using ACLI.... 83
Setting Telnet access using ACLI.... 83

Displaying Telnet access settings using ACLI..... 83
Configuring Telnet connections using ACLI..... 84
Disabling Telnet access using ACLI..... 86
Setting the Telnet settings to default values using ACLI..... 86
Configuring SSL using ACLI..... 87
Enabling or disabling SSL using ACLI..... 87
Creating or deleting an SSL certificate using ACLI..... 87
Viewing the SSL server configuration using ACLI..... 87
Viewing the SSL certificate using ACLI..... 88
Configuring Secure Shell using ACLI..... 88
Displaying the secure shell configuration information using ACLI..... 89
Displaying the SSH session information using ACLI..... 89
Displaying SSH download DSA key information using ACLI..... 90
Generating the DSA host keys using ACLI..... 90
Deleting the DSA host key using ACLI..... 90
Enabling or disabling the SSH server in nonsecure mode using ACLI..... 91
Enabling the SSH server in secure mode using ACLI..... 91
Setting the timeout value for session authentication using ACLI..... 91
Enabling DSA authentication using ACLI..... 92
Enabling password authentication using ACLI..... 92
Setting the SSH connection port using ACLI..... 92
Downloading the client public key from the TFTP server using ACLI..... 93
Deleting the SSH DSA authentication key using ACLI..... 93
Resetting SSH configuration parameters to default using ACLI..... 94
Enabling SSH RSA authentication using ACLI..... 94
Generating the SSH RSA host key using ACLI..... 94
Configuring RADIUS Interim Accounting Updates support using ACLI..... 95
Configuring RADIUS Interim Accounting Updates support using ACLI..... 95
Disabling RADIUS Interim Accounting Updates support using ACLI..... 96
Configuring RADIUS Interim Accounting Updates support defaults using ACLI..... 96
Viewing RADIUS Interim Accounting Updates support status using ACL..... 97
Configuring RADIUS Request use Management IP using ACLI..... 97
Enabling RADIUS request use of Management IP using ACLI..... 97
Disabling RADIUS request use of Management IP using ACLI..... 98
Viewing RADIUS request use Management IP status using ACLI..... 98
Configuring RADIUS authentication using ACLI..... 98
Configuring switch RADIUS server settings using ACLI..... 98
Enabling or disabling RADIUS password fallback using ACLI..... 100
Viewing RADIUS information using ACLI..... 101
Configuring RADIUS server reachability using ACLI..... 102
Viewing the RADIUS server reachability method using ACLI..... 102
Configuring 802.1X dynamic authorization extension (RFC 3576) configuration using ACLI..... 103
Configuring RADIUS dynamic authorization extension (802.1X RFC 3576) using ACLI..... 103

Disabling RADIUS dynamic authorization extension (802.1X RFC 3576) using ACLI..... 104
Viewing RADIUS dynamic authorization client configuration using ACLI..... 104
Viewing RADIUS dynamic authorization client statistics using ACLI..... 105
Enabling or disabling RADIUS dynamic authorization extension (802.1X RFC 3576) on a port using ACLI..... 105
Viewing replay protection for RADIUS dynamic authorization extension using ACLI..... 106
Enabling or disabling replay protection for RADIUS dynamic authorization extension using ACLI..... 106
Setting SNMP parameters using ACLI..... 107
Enabling or disabling the SNMP server using ACLI..... 107
Disabling SNMP access using ACLI..... 107
Enabling disabling or restoring to default the generation of SNMP authentication failure traps using ACLI..... 107
Modifying the community strings for SNMPv1 and SNMPv2c access using ACLI..... 108
Clearing the SNMP server community configuration using ACLI..... 109
Restoring the community string configuration to default settings using ACLI..... 109
Displaying SNMP community string configuration using ACLI..... 109
Configuring the SNMP sysContact value using ACLI..... 110
Clearing or restoring the SNMP sysContact value to default value using ACLI..... 110
Configuring or clearing the SNMP sysLocation value using ACLI..... 111
Restoring the SNMP sysLocation to the default using ACLI..... 111
Configuring the SNMP sysName value using ACLI..... 111
Clearing the SNMP sysName value using ACLI..... 112
Enabling SNMP linkUp linkDown traps for a port using ACLI..... 112
Disabling the SNMP linkUp linkDown traps for a port using ACLI..... 113
Adding SNMP traps to a filter profile using ACLI..... 113
Deleting SNMP traps from a filter profile using ACLI..... 114
Displaying notify-filter details using ACLI..... 115
Enabling or disabling the generation of SNMP traps using ACLI..... 115
Using ACLI commands specific to SNMPv3..... 116
Creating an SNMPv3 user using ACLI..... 116
Removing an SNMPv3 user using ACLI..... 118
Creating an SNMPv3 view using ACLI..... 118
Removing an SNMPv3 view using ACLI..... 119
Adding trap receivers to SNMPv3 tables using ACLI..... 120
Deleting trap receivers or restoring the SNMPv3 table to defaults using ACLI..... 121
Displaying SNMP-server host-related information using ACLI..... 122
Setting SNMP community strings and access privileges using ACLI..... 123
Displaying SNMPv3 configuration using ACLI..... 124
Creating an initial set of configuration data for SNMPv3 using ACLI..... 125
Configuring MAC address filter-based security using ACLI..... 125
Displaying MAC address security settings using ACLI..... 125
Configuring MAC address security options using ACLI..... 126
Adding addresses to MAC security address table using ACLI..... 128

Assigning a list of ports to a security list using ACLI..... 128
Disabling MAC source address-based security using ACLI..... 129
Disabling MAC address auto-learning aging time using ACLI..... 129
Clearing the MAC address security table using ACLI..... 129
Clearing the port membership of a security list using ACLI..... 130
Configuring MAC security for specific ports using ACLI..... 130
Filtering packets from specified MAC DAs using ACLI..... 131
Configuring MAC address autolearning using ACLI..... 131
Configuring MAC address auto-learning aging time using ACLI..... 132
Disabling MAC address auto-learning aging time using ACLI..... 132
Configuring MAC address auto-learning aging time to default using ACLI..... 132
Viewing the current Sticky MAC address mode using ACLI..... 133
Enabling Sticky MAC address mode using ACLI..... 133
Disabling Sticky MAC address mode using ACLI..... 134
Configuring EAPOL-based security using ACLI..... 134
Enabling or disabling EAPOL-based security using ACLI..... 134
Modifying EAPOL-based security parameters for a specific port using ACLI..... 134
Setting the guest VLAN for EAPOL using ACLI..... 136
Disabling guest VLAN for EAPOL using ACLI..... 136
Displaying the current EAPOL-based security status using ACLI..... 137
Displaying EAPOL diagnostics using ACLI..... 137
Displaying EAPOL statistics using ACLI..... 138
Displaying EAPOL guest VLAN settings using ACLI..... 139
Configuring advanced EAPOL features using ACLI..... 139
Configuring global EAPOL multihost settings..... 139
Disabling EAPOL multihost settings using ACLI..... 140
Restoring EAPOL multihost settings to default using ACLI..... 141
Configuring EAPOL multihost settings for a specific port or ports on an interface using ACLI..... 142
Disabling EAPOL multihost settings for a specific port or for all ports on an interface using ACLI..... 143
Restoring EAPOL multihost settings to default for a specific port or for all ports on an interface using ACLI..... 143
Configuring non-EAPOL MAC addresses on a specific port or on all ports on an interface using ACLI..... 144
Displaying global settings for non-EAPOL hosts on EAPOL-enabled ports using ACLI..... 145
Displaying non-EAPOL support settings for each port using ACLI..... 146
Displaying non-EAPOL hosts information using ACLI..... 146
Configuring support for non-EAPOL hosts on EAPOL-enabled ports using ACLI..... 147
Configuring 802.1X or Non-EAP and Guest VLAN on the same port using ACLI..... 152
Enabling EAPOL VoIP VLAN using ACLI..... 152
Disabling EAPOL VoIP VLAN using ACLI..... 152
Configuring EAPOL VoIP VLAN as the default VLAN using ACLI..... 153
Viewing EAPOL VoIP VLAN using ACLI..... 153

Configuring TACACS+ using ACLI..... 154
Configuring switch TACACS+ server settings using ACLI..... 154
Disabling switch TACACS+ server settings using ACLI..... 155
Enabling remote TACACS+ services using ACLI..... 155
Enabling or disabling TACACS+ authorization using ACLI..... 155
Configuring TACACS+ authorization privilege levels using ACLI..... 156
Enabling or disabling TACACS+ accounting using ACLI..... 156
Configuring the switch TACACS+ level using ACLI..... 157
Viewing TACACS+ information using ACLI..... 157
Configuring IP Manager using ACLI..... 157
Enabling IP Manager using ACLI..... 157
Disabling IP Manager using ACLI..... 158
Configuring the IP Manager list for IPv4 addresses using ACLI..... 158
Configuring the IP Manager list for IPv6 addresses using ACLI..... 159
Removing IP Manager list entries using ACLI..... 160
Viewing the IP Manager configuration using ACLI..... 160
Configuring DHCP snooping using ACLI..... 161
Enabling DHCP snooping globally using ACLI..... 161
Disabling DHCP snooping globally using ACLI..... 162
Enabling DHCP snooping on a VLAN using ACLI..... 162
Disabling DHCP snooping on a VLAN using ACLI..... 162
Configuring DHCP snooping port trust using ACLI..... 162
Configuring DHCP snooping port trust to default using ACLI..... 163
Viewing global DHCP snooping configuration information using ACLI..... 163
Viewing VLAN DHCP snooping configuration information using ACLI..... 164
Viewing DHCP snooping port trust information using ACLI..... 164
Viewing the DHCP binding table using ACLI..... 164
Configuring DHCP Snooping Option 82 globally using ACLI..... 165
Configuring port-based DHCP Snooping Option 82 subscriber ID using ACLI..... 165
Configuring VLAN-based DHCP Snooping Option 82 using ACLI..... 166
Viewing DHCP Snooping using ACLI..... 167
Viewing DHCP Snooping for an interface using ACLI..... 167
Configuring dynamic ARP inspection using ACLI..... 168
Displaying the ARP table using ACLI..... 168
Enabling dynamic ARP inspection on a VLAN using ACLI..... 169
Disabling dynamic ARP inspection on a VLAN using ACLI..... 169
Configuring dynamic ARP inspection port trust using ACLI..... 170
Configuring dynamic ARP inspection port trust to default using ACLI..... 170
Viewing VLAN dynamic ARP inspection configuration information using ACLI..... 171
Viewing dynamic ARP inspection port trust information using ACLI..... 171
Configuring IP Source Guard using ACLI..... 171
Enabling IP Source Guard using ACLI..... 172
Viewing IP Source Guard port configuration information using ACLI..... 172

Viewing IP Guard-allowed addresses using ACLi..... 173
Disabling IP Source Guard using ACLI..... 173
Configuring 802.1X or non-EAP Last Assigned RADIUS VLAN using ACLI..... 174
Enabling use of the most recent RADIUS VLAN..... 174
Disabling use of the most recent RADIUS VLAN..... 174
Restoring use of the most recent RADIUS VLAN to default..... 175
Displaying EAPOL multihost status..... 175
Enabling EAPOL Fail Open VLAN..... 175
Disabling EAPOL Fail Open VLAN..... 176
Displaying EAPOL Fail Open VLAN..... 176
Configuring Secure File Transfer Protocol using ACLI..... 177
Viewing Secure File Transfer Protocol (SFTP)..... 177
Setting SSHC authentication timeout..... 178
Setting the SSHC port..... 178
Enabling DSA authentication using ACLI..... 179
Generating an SSHC DSA host key (public and private)..... 179
Deleting the SSHC DSA host keys (public and private)..... 179
Setting SSHC DSA host key size..... 180
Uploading the public host key..... 180
Enabling password authentication using ACLI..... 180
Uploading a config file to an SFTP server using ACLI..... 181
Downloading a config file from an SFTP server using ACLI..... 181
Configuring IPv6 management using ACLI..... 182
Enabling IPv6 globally using ACLI..... 182
Enabling IPv6 interface on the management VLAN using ACLI..... 183
Displaying the IPv6 interface information using ACLI..... 183
Displaying IPv6 interface addresses using ACLI..... 184
Configuring IPv6 interface properties using ACLI..... 184
Displaying the global IPv6 configuration using ACLI..... 185
Configuring an IPv6 default gateway using ACLI..... 185
Displaying the IPv6 default gateway using ACLI..... 186
Configuring the IPv6 neighbor cache using ACLI..... 186
Displaying the IPv6 neighbor information using ACLI..... 186
Displaying IPv6 interface ICMP statistics using ACLI..... 187
Displaying IPv6 interface statistics using ACLI..... 187
Displaying IPv6 TCP connections using ACLI..... 188
Displaying IPv6 TCP listeners using ACLI..... 188
Displaying IPv6 TCP statistics using ACLI..... 189
Displaying IPv6 UDP statistics and endpoints using ACLI..... 189
Configuring storm control using ACLI..... 189
Displaying rate limit configuration using ACLI..... 191
Configuring rate limiting using ACLI..... 191
**Chapter 7: Configuring and managing security using EDM**..... 193

Configuring and managing security using Enterprise Device Manager..... 193
Setting the switch HTTP/HTTPS port using EDM..... 193
Configuring EAPOL using EDM..... 194
Configuring EAPOL globally using EDM..... 194
Enabling or disabling non-EAP client re-authentication using EDM..... 196
Configuring multihost EAP VoIP VLAN using EDM..... 196
Configuring port-based EAPOL using EDM..... 197
Configuring advanced port-based EAPOL using EDM..... 199
Clearing Non-EAP authenticated clients from ports using EDM..... 201
Viewing Multihost status information using EDM..... 201
Viewing Multihost session information using EDM..... 202
Viewing Multihost DHCP authenticated information..... 202
Adding a MAC address to the allowed non-EAP MAC address list using EDM..... 203
Deleting a MAC address from the allowed non-EAP MAC address list using EDM..... 204
Viewing port non-EAP host support status using EDM..... 204
Graphing port EAPOL statistics using EDM..... 205
Graphing port EAPOL diagnostics using EDM..... 206
Configuring TACACS using EDM..... 208
Enabling or disabling TACACS+ accounting using EDM..... 208
Enabling or disabling TACACS+ authorization using EDM..... 209
Configuring the switch TACACS+ levels using EDM..... 210
Creating a TACACS+ server using EDM..... 210
Configuring general switch security using EDM..... 211
Adding ports to a security list using EDM..... 213
Deleting ports from a security list using EDM..... 214
Configuring AuthConfig list using EDM..... 215
Adding entries to the AuthConfig list using EDM..... 215
Deleting entries from the AuthConfig list using EDM..... 216
Configuring MAC Address autolearn using EDM..... 217
Viewing AuthStatus information using EDM..... 218
Viewing AuthViolation information using EDM..... 219
Viewing MacViolation information using EDM..... 220
Configuring a Web and Telnet password using EDM..... 220
Configuring a console password using EDM..... 221
Configuring the Secure Shell protocol using EDM..... 222
Viewing SSH Sessions information using EDM..... 224
Configuring an SSH Client..... 225
SSHC/SFTP tab field descriptions..... 225
Configuring SSL using EDM..... 227
Configuring RADIUS parameters..... 228
Configuring RADIUS globally using EDM..... 228
Configuring the Global RADIUS Server using EDM..... 229
Configuring the EAP RADIUS Server using EDM..... 231

Configuring the NEAP RADIUS Server using EDM..... 233
Viewing RADIUS Dynamic Authorization server information using EDM..... 235
802.1X dynamic authorization extension (RFC 3576) client configuration using EDM..... 236
Configuring an 802.1X dynamic authorization extension (RFC 3576) client using EDM..... 236
Deleting an 802.1X dynamic authorization extension (RFC 3576) client configuration using EDM..... 237
Modifying the 802.1X dynamic authorization extension (RFC 3576) client configuration using EDM..... 237
Viewing the 802.1X dynamic authorization extension (RFC 3576) client information using EDM..... 239
Editing the 802.1X dynamic authorization extension (RFC 3576) client secret word using EDM..... 240
Viewing RADIUS Dynamic Server statistics using EDM..... 240
Graphing RADIUS Dynamic Server statistics using EDM..... 241
DHCP snooping configuration using EDM..... 241
Configuring DHCP snooping and Option 82 globally using EDM..... 241
Configuring DHCP snooping and Option 82 on a VLAN using EDM..... 242
Configuring DHCP snooping port trust and DHCP Option 82 for a port using EDM..... 243
Viewing the DHCP binding information using EDM..... 244
Configuring dynamic ARP inspection on a VLAN using EDM..... 244
Configuring dynamic ARP inspection on a port using EDM..... 245
ARP Inspection-port tab field descriptions..... 245
Configuring IP Source Guard using EDM..... 246
Configuring IP Source Guard on a port using EDM..... 246
Filtering IP Source Guard addresses using EDM..... 247
Configuring SNMP using EDM..... 248
Viewing SNMP information using EDM..... 248
Defining a MIB view using EDM..... 249
Configuring an SNMP user using EDM..... 250
Viewing SNMP user details using EDM..... 251
Configuring an SNMP community..... 251
Viewing SNMP community details using EDM..... 252
Configuring an SNMP host using EDM..... 253
Configuring SNMP host notification using EDM..... 254
Configuring SNMP notification control using EDM..... 255
Configuring IPv6 management using EDM..... 256
Configuring IPv6 Management globally using EDM..... 256
IPv6 Interface configuration using EDM..... 257
Configuring an IPv6 address using EDM..... 264
Configuring IPv6 static routes using EDM..... 265
IPv6 neighbor cache configuration using EDM..... 266
Graphing IPv6 interface ICMP statistics using EDM..... 269
Viewing ICMP message statistics using EDM..... 270
Viewing global IPv6 TCP properties using EDM..... 270

Viewing IPv6 TCP connections using EDM..... 271
Viewing IPv6 TCP listeners using EDM..... 272
Viewing IPv6 UDP endpoints using EDM..... 273
Configuring Storm Control using EDM..... 273
Configuring Storm Control globally..... 274
Configuring Broadcast Storm Control..... 275
Configuring Multicast Storm Control..... 276
Configuring Unicast Storm Control..... 278
Configuring rate limiting using EDM..... 279
**Chapter 8: Appendix A**..... 281
TACACS+ server configuration examples..... 281
Configuration example Cisco ACS (Version 3.2) server..... 281
Configuration example ClearBox server..... 284
SNMP MIB support..... 290
Management Agent..... 291
SNMP trap support..... 292
Sticky MAC address configuration examples..... 294

# Chapter 1: Introduction

## Purpose of this document

This document provides procedures and conceptual information to administer and configure security features for the ERS 3500 Series, including MAC-based security, RADIUS, EAPOL, and SSH.

## Related resources

### Documentation

For a list of the documentation for this product, see *Documentation Roadmap Reference for Avaya Ethernet Routing Switch 3500 Series*, NN47203-101.

### Training

Ongoing product training is available. For more information or to register, see http://avaya-learning.com/.

Enter the course code in the **Search** field and click **Go** to search for the course.

| Course code | Course title |
|---|---|
| 8D00020E | Stackable ERS and VSP Products Virtual Campus Offering |

### Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

#### About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

### Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

**Note:**

Videos are not available for all products.

## Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

### Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

### Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments

6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

## Subscribing to e-notifications

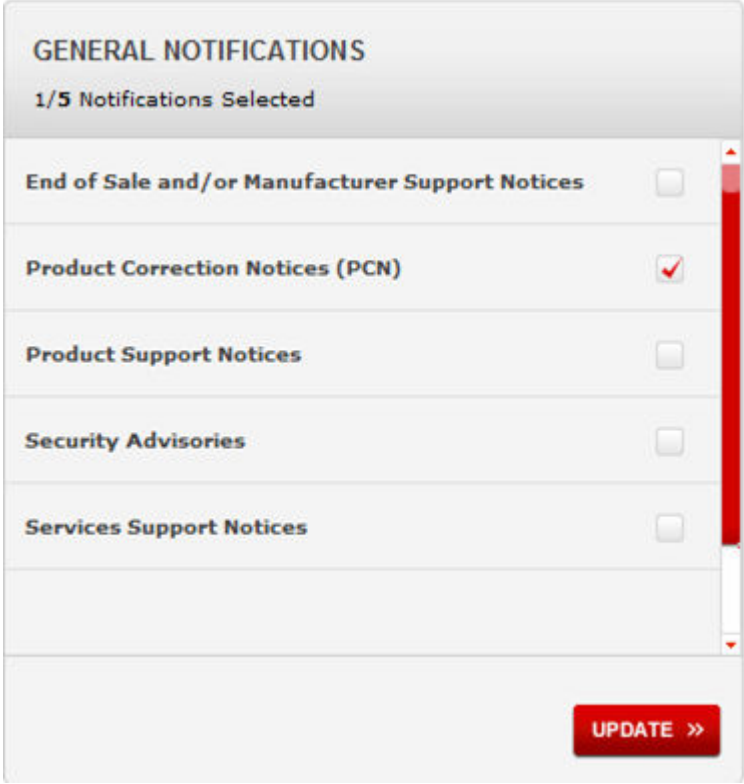
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

### About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing Switch 8800.

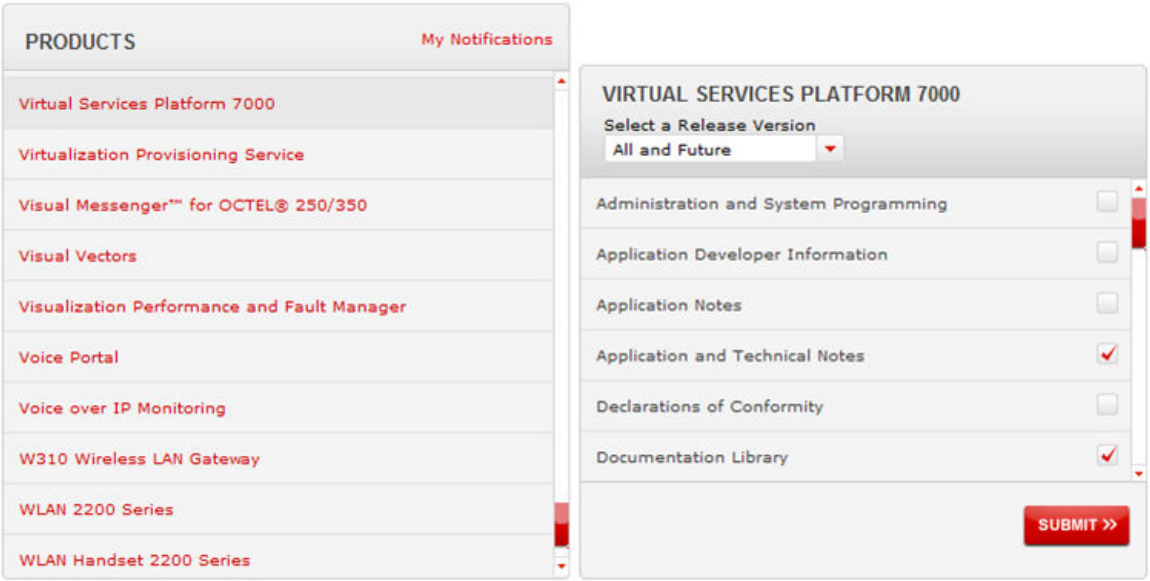
### Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.




6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.

8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.




11. Click **Submit**.

## Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

# Chapter 2: New in this release

The following hardware and software features are new in Avaya Ethernet Routing Switch (ERS) 3500 Series Release 5.2:

### ERS 3500 hardware

The following table lists and describes the new hardware supported in Release 5.2:

| Hardware | Description |
|---|---|
| **Modules** | |
| Avaya Ethernet Routing Switch 3549GTS | 48 10/100/1000 non-PoE and 2 shared SFP, plus 1 1/10 Gigabit SFP+ port, plus 2 rear dual mode/ stacking ports. |
| Avaya Ethernet Routing Switch 3549GTS-PWR+ | 48 10/100/1000 802.3at PoE+ and 2 shared SFP, plus 1 1/10 Gigabit SFP+ port, plus 2 rear dual mode/stacking ports. |

### ERS 3500 software features

The following software features are new for ERS 3500 Series Release 5.2:

- Avaya Energy Saver
- SLAMon enhancements
- Simple Loop Protection Protocol (SLPP) Guard
- Unified authentication
- Flash History
- Static LACP Key to Trunk ID binding

**Related links**

Features on page 21
Other changes on page 22

## Features

See the following sections for information about feature-related changes.

**Related links**

New in this release on page 21

Unified authentication on page 22

## Unified authentication

With the introduction of Unified authentication, you can now manage only one set of local usernames and passwords for switches, whether the units are operating in stacked or standalone mode. When in stacked mode, the authentication method, username, and local passwords are applied universally across all switches in a stack. If you use `the cli passwords` and `username` ACLI commands, the unified and previously used standalone authentication method, the username, and local passwords are updated on all switches in the stack.

The switch updates the obsolete standalone authentication method, username, and local passwords to ensure maximum compatibility, should it become necessary for you to downgrade the switch to a previous software release.

For more information, see Password security on page 55.

**Related links**

Features on page 21

# Other changes

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

### 802.1x standard

The 802.1x standard is changed from 802.1x-2001 to 802.1x-2004.

### Document title change

In Release 5.2, the title of this document changed from *Avaya Ethernet Routing Switch 3500 — Security*, NN47203-504 to *Configuring Security on Avaya Ethernet Routing Switch 3500 Series*, NN47203-504.

**Related links**

New in this release on page 21

# Chapter 3: ACLI command modes

Avaya command line interface (ACLI) provides the following configuration modes:

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

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

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

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

| Command mode and sample prompt | Entrance commands | Exit commands |
|---|---|---|
| User EXEC<br>`3526T>` | No entrance command, default mode. | Type `exit`or `logout` |
| Privileged EXEC<br>`3526T#` | From User EXEC mode, type: `enable` | Type `exit` or `logout` |
| Global Configuration<br>`3526T(config)#` | From Privileged EXEC mode, type: `configure` | To return to Privileged EXEC mode, type: `end` or `exit`<br><br>To exit ACLI completely, type: `logout` |
| Interface Configuration<br>`3526T(config-if)#` | From Global Configuration mode:<br>To configure a port, type: `interface fastethernet <port number>`<br>To configure a VLAN, type: `interface vlan <vlan number>` | To return to Global Configuration mode, type: `exit`<br>To return to Privileged EXEC mode, type: `end`<br>To exit ACLI completely, type: `logout` |

For more information about the ACLI configuration modes, see *Fundamentals of Avaya Ethernet Routing Switch 3500 Series*, NN47203-102.

# Chapter 4: Security fundamentals

This chapter describes the security features available with the Avaya Ethernet Routing Switch 3500 Series.

## Management password configuration

To provide security on your switch or stack, you can configure a local RADIUS or TACACS 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 Avaya Ethernet Routing Switch 3500 Series 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.

### Unified authentication

With the introduction of Unified authentication, you can now manage only one set of local usernames and passwords for switches, whether the units are operating in stacked or standalone mode. When in stacked mode, the authentication method, username, and local passwords are applied universally across all switches in a stack. If you use `the cli passwords` and `username` ACLI commands, the unified and previously used standalone authentication method, the username, and local passwords are updated on all switches in the stack.

The switch updates the obsolete standalone authentication method, username, and local passwords to ensure maximum compatibility, should it become necessary for you to downgrade the switch to a previous software release.

For more information, see Password security on page 55.

**Related links**

Features on page 21

## 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 figure below (default user names are RW and RO).

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

**Figure 1: Setting the user name and password using ACLI**

## 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 Avaya 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 to add 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.

## Sticky MAC address

Sticky MAC address provides a high level of control, and simpler configuration and operation for MAC address security, on a standalone switch or a switch that is part of a stack. With Sticky MAC address, you can secure the MAC address to a specified port so if the MAC address moves to another port, the system raises an intrusion event. When you enable Sticky MAC address, the switch performs the initial auto-learning of MAC addresses and can store the automatically-learned addresses across switch reboots.

For more information, see ACLI and EDM procedures and Sticky MAC address configuration examples.

# RADIUS-based network security

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

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

## How RADIUS works

A RADIUS application has two components:

- RADIUS server—a computer equipped with RADIUS server software (for example, a UNIX workstation). The RADIUS server stores client or user credentials, password, and access privileges, protected with a shared secret.
- RADIUS client—a router, PC, or a remote access server equipped with the appropriate client software.

A switch can be configured to use RADIUS authentication to authenticate users attempting to log on to the switch using telnet, SSH, EDM, or the console port.

Avaya recommends that you configure two RADIUS servers so that if one server is unreachable, the switch will attempt authentication using the secondary server. If the primary server is unavailable, the switch retries three times before moving to the secondary server. The retry interval can be configured according to network requirements so that false retries do not occur.

## RADIUS server configuration

You must set up specific user accounts on the RADIUS server before you can use RADIUS authentication in the Avaya Ethernet Routing Switch 3500 Series network. User account information about the RADIUS server contains user names, passwords, and service-type attributes.

Provide each user with the appropriate level of access.

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

For more information about configuring the RADIUS server, see the documentation that came with the server software.

## RADIUS EAP or non-EAP requests to different servers

You can manage EAP and Non-EAP (NEAP) functions on separate RADIUS servers.

EAP RADIUS servers: You can configure a maximum of two EAP RADIUS servers, either IPv4 or IPv6, for the authentication and accounting of EAP client requests. You can configure one EAP RADIUS server as the primary server and the other EAP RADIUS server as the secondary server.

Non-EAP RADIUS servers: You can configure a maximum of two non-EAP RADIUS servers, either IPv4 or IPv6, for the authentication and accounting of Non-EAP client requests. You can configure one non-EAP RADIUS server as the primary server and the other non-EAP RADIUS server as the secondary server.

Global RADIUS servers: Global RADIUS servers process both EAP and Non-EAP client requests if EAP or non-EAP RADIUS servers are not configured. You do not designate either EAP or Non-EAP client requests separately for management by a Global RADIUS server. You can configure one Global RADIUS server as the primary server and the other Global RADIUS server as the secondary server.

### RADIUS servers with SHSA, MHSA, and MHMA modes

When you use SHSA, MHSA and MHMA modes, if the primary RADIUS server is not reachable, the system attempts to connect to the secondary RADIUS server. If both the primary and secondary RADIUS servers cannot be reached, the EAP or Non-EAP client is not authenticated, and the system repeats the process with all RADIUS servers, in priority order, until an available server is found.

**Note:**

If the system cannot reach a RADIUS server with a valid IP address, it disconnects clients from the server at the next re-authentication.

### RADIUS server priority in SHSA and MHSA modes

For SHSA and MHSA modes, if you configure EAP RADIUS servers, only the EAP RADIUS servers are used in the following priority order:

- EAP RADIUS server – primary
- EAP RADIUS server – secondary

For SHSA and MHSA modes, if you do not configure EAP RADIUS servers, servers are used in the following priority order:

- Global RADIUS server – primary
- Global RADIUS server – secondary

**Note:**

The non-EAP RADIUS server is not used for ports in SHSA or MHSA mode since neither mode supports Non-EAP.

### RADIUS server priority in MHMA mode

Since MHMA mode is used when multiple authentications are required for a single port, and authenticated clients can be either EAP or Non-EAP, the client type determines which RADIUS server processes client requests.

### EAP clients

- If only EAP RADIUS servers are configured, all EAP clients are authenticated using an EAP server (primary or secondary). If both primary and secondary EAP RADIUS servers become unavailable, the EAP clients remain authenticated until the next reauthentication.
- If EAP and Global RADIUS servers are configured, all EAP clients are authenticated using only an EAP server (primary or secondary). If both primary and secondary EAP RADIUS servers become unavailable, the EAP clients remain authenticated until the next reauthentication.
- If only Global RADIUS servers are configured, all EAP clients are authenticated using a Global RADIUS server (primary or secondary). If both primary and secondary Global RADIUS servers become unavailable, the EAP clients remain authenticated until the next re-authentication.

### Non-EAP clients

- If only non-EAP RADIUS servers are configured, all Non-EAP clients are authenticated using the non-EAP RADIUS servers (primary or secondary). If both primary and secondary non-EAP RADIUS servers become unavailable, the Non-EAP clients remain authenticated until the next re-authentication.
- If Non-EAP and Global RADIUS servers are configured, all Non-EAP clients are authenticated using only the non-EAP RADIUS servers (primary or secondary). If both primary and secondary non-EAP RADIUS servers will become unavailable, the Non-EAP clients remain authenticated until the next re-authentication.
- If only Global RADIUS servers are configured, all Non-EAP clients are authenticated using a Global RADIUS server (primary or secondary). If both primary and secondary Global RADIUS servers become unavailable, the Non-EAP clients remain authenticated until the next re-authentication.

### Examples of RADIUS servers with MHMA mode

The following diagram illustrates a network that includes the following:

- an ERS 3500 switch with a port configured for MHMA
- the MHMA port connected to multiple EAP and Non-EAP clients
- a group of RADIUS servers configured as primary and secondary EAP RADIUS servers, non-EAP RADIUS servers, and Global RADIUS servers

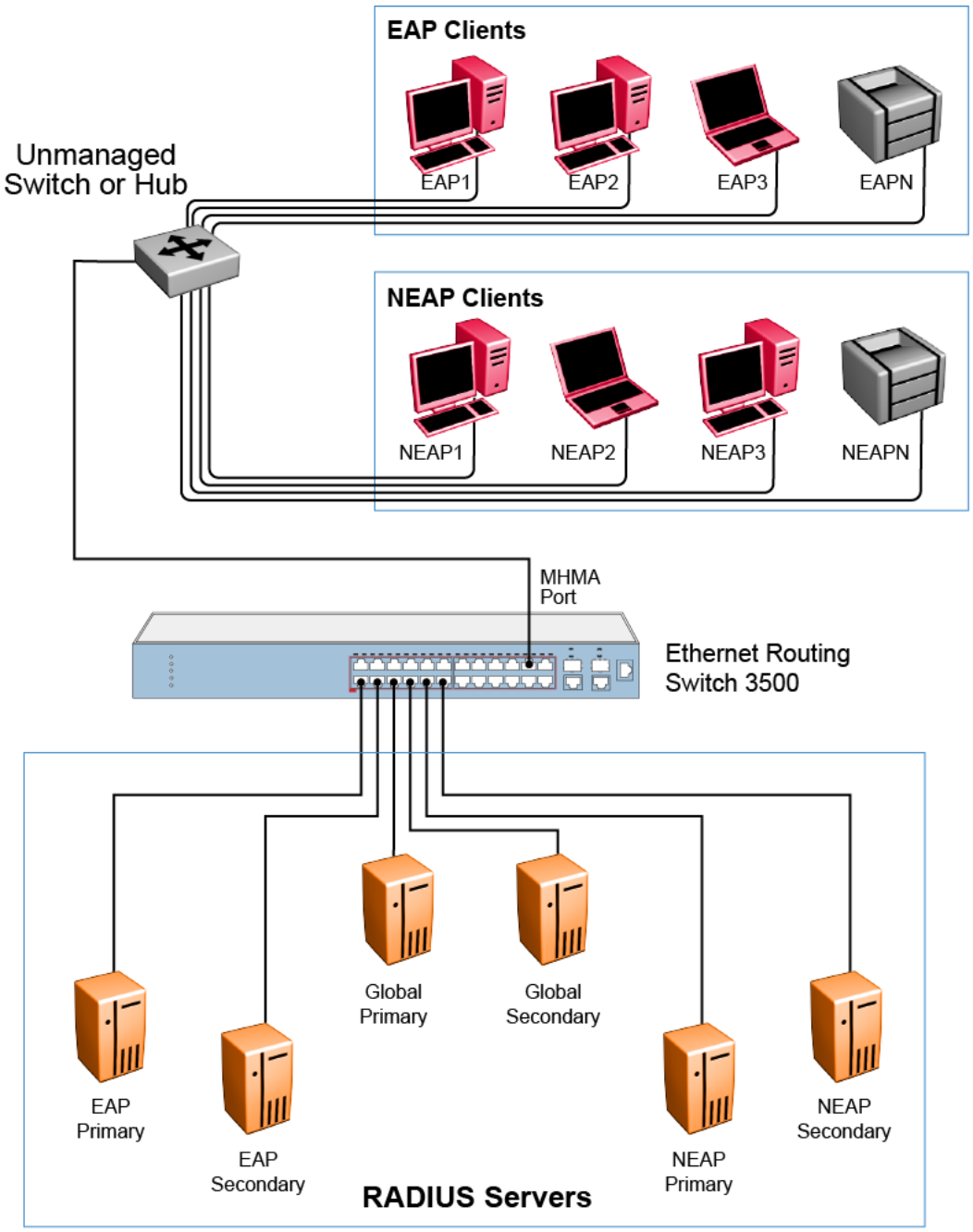



**Figure 2: EAP and non-EAP RADIUS servers in MHMA mode**

The following scenarios for EAP clients are based on the configuration in the preceding diagram:

1. EAP clients are authenticated on a Global RADIUS server and you configure the EAP RADIUS servers. At the next re-authentication, all EAP clients authenticate on the EAP RADIUS server.

2. Both the EAP RADIUS servers and the Global RADIUS servers are configured, with EAP clients authenticated on an EAP RADIUS server. In this case, the following can occur:
   - If the EAP RADIUS server becomes unavailable, the system disconnects the EAP clients at the next re-authentication, and the system does not reauthenticate the EAP clients on the Global RADIUS server.
   - If you reset the EAP RADIUS servers to default settings, where the IP addresses for both the primary and secondary hosts return to 0.0.0.0, at the RADIUS-based network security Configuration — Security August 2011 23 next re-authentication the system authenticates EAP clients on the Global RADIUS server.

   Assumptions:
   - If you configure an EAP RADIUS server, the system does not use the Global RADIUS server for EAP clients.
   - The system does not use the non-EAP RADIUS server for EAP clients.

The following scenarios for Non-EAP clients are based on the configuration in the preceding diagram:

1. Non-EAP clients are authenticated on a Global RADIUS server and you configure the non-EAP RADIUS servers. At the next re-authentication, all Non-EAP clients are authenticated using the non-EAP RADIUS server.
2. Both the non-EAP RADIUS servers and the Global RADIUS are configured; with Non-EAP clients authenticated on a non-EAP RADIUS server. In this case, the following can occur:
   - If the non-EAP RADIUS server becomes unavailable, the system disconnects the Non-EAP clients at the next re-authentication, and the system does not reauthenticate the Non-EAP clients on the Global RADIUS server.
   - If you reset the non-EAP RADIUS servers to default settings, where the IP addresses for both the primary and secondary hosts return to 0.0.0.0., at the next re-authentication, the system authenticates Non-EAP clients on the Global RADIUS server.

   Assumptions:
   - If you configure the non-EAP RADIUS server, the system does not use the Global RADIUS server for Non-EAP clients.
   - The system does not use the non-EAP RADIUS server for EAP clients.

## RADIUS server reachability

You can use RADIUS server reachability to configure the switch to use ICMP packets or dummy RADIUS requests to determine the reachability of the RADIUS server. The switch regularly performs the reachability test to determine if the switch should fail over to the secondary RADIUS server or to activate the fail open VLAN, if that feature is configured on the switch.

If you implement internal firewalls which limit the flow of ICMP reachability messages from the switch to the RADIUS server, you can configure the switch to use dummy RADIUS requests. If the switch is configured to use dummy RADIUS requests, the switch generates a regular dummy RADIUS request with the username 'avaya'. It is recommended that you set up a dummy account

with the user name avaya on the RADIUS server to avoid the generation of error messages indicating invalid user logins, if RADIUS server reachability is enabled.

The RADIUS reachability method you select applies to Global RADIUS servers, EAP RADIUS servers, and Non-EAP RADIUS servers.

By default, the switch uses ICMP packets to determine the reachability of the RADIUS server.

## RADIUS password fallback

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

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.

The RADIUS password fallback feature is enabled by default.

## RADIUS Interim Accounting Updates support

The Avaya Ethernet Routing Switch 3500 Series 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 Avaya Ethernet Routing Switch 3500 Series 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.

The RADIUS use Management IP Address feature is enabled by default.

# Campus security example

The following figure shows a typical campus configuration using the RADIUS-based and MACaddress- based security features for the Avaya Ethernet Routing Switch 3500 Series.

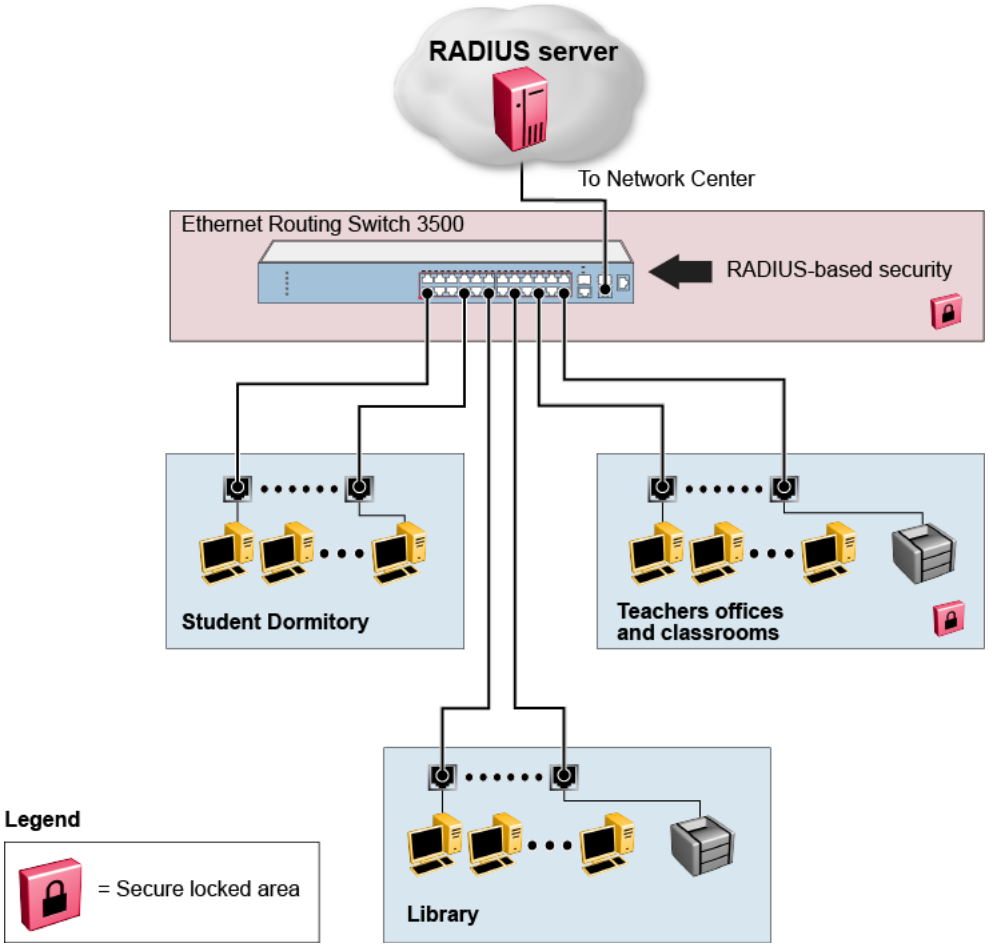



**Figure 3: Avaya Ethernet Routing Switch 3500 security feature**

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 on page 28).
  - 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 on page 26).
  - 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 addressbased 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 Avaya Ethernet Routing Switch 3500 Series 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 RADIUSbased server and to provide the advantages of remote authentication to internal LAN clients.

An example follows to show how an Avaya Ethernet Routing Switch 3500 Series 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:
  1. The switch asks for a User ID of the new client.
  2. The User ID is covered by EAPOL, and it passes to the RADIUS server.
  3. 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.

**Important:**

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.

**Important:**

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 on page 39.

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 it 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 and ADAC non-EAP IP Phone authentication can be used for IP Phones that cannot authenticate with EAP. 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 5.0, a match occurred based on the VLAN number of the Tunnel- Private-Group-Id attribute returned by the RADIUS server. Beginning with Release 5.0, 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.

## 802.1X or Non-EAP and Guest VLAN on the same port

The 802.1X or Non-EAP and Guest VLAN on the same port feature supports multiple modes simultaneously on the same port, removing the previous port restrictions. The feature allows Guest VLAN to function along with Non-EAP and various 802.1X operational modes.

For example, if EAPOL multihost VoIP VLAN is enabled, a Non-EAP phone is allowed on the VoIP VLAN. The switch authenticates the IP Phone using Non-EAP according to the DHCP signature of the phone. The data VLAN remains in the Guest VLAN until a device on the port authenticates using 802.1X and is optionally placed in the appropriate RADIUS assigned VLAN.

You can configure up to 5 EAP VoIP VLANs. A port is added as a member of a VoIP VLAN if the following are enabled: EAPoL both globally and per interface, on-eap-phone-enabled globally and per interface, and multihost per interface. VoIP VLANs are assumed to be enabled.

## Non-EAP hosts on EAP-enabled ports

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

- Hosts that match entries in a local list of allowed MAC addresses. You can specify the allowed MAC addresses when you configure the port to allow non-EAPOL access. These hosts are allowed on the port without authentication.
- Non-EAPOL hosts whose MAC addresses are authenticated by RADIUS.
- IP Phones configured for Auto-Detection and Auto-Configuration (ADAC).
- Avaya IP Phones using DHCP signatures for authentication.

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 on page 42.

    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.

For information about configuring non-EAPOL host support, see Configuring support for non-EAPOL hosts on EAPOL-enabled ports using ACLI on page 147

## 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.

**Important:**

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 5.0, 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, an 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, Avaya 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 Non-EAP client re-authentication

The Non-EAP (NEAP) client re-authentication feature supports the re-authentication of Non- EAP clients at defined intervals.

You can enable or disable NEAP client re-authentication globally for the switch, but the time interval for NEAP client re-authentication is determined by the value you set for EAP client reauthentication, at the port level. For information about setting the EAP client re-authentication timer, see either of the following sections:

- Configuring port-based EAPOL using EDM on page 197
- Modifying EAPOL-based security parameters for a specific port using ACLI on page 134

With the exception of the re-authentication interval timer, NEAP client re-authentication and EAP client re-authentication function independent of each other.

When you enable NEAP client re-authentication, an authenticated NEAP client is only removed from the authenticated client list if you remove the client account from the RADIUS server, or if you clear the NEAP authenticated client from the switch.

If an authenticated NEAP client does not generate traffic on the network, the system removes the MAC address for that client from the MAC address table after the aging time expires. Although the client MAC address is not displayed in MAC Address table, the client can appear as an authenticated client. If NEAP client re-authentication is enabled, the idle NEAP authenticated client is not removed from the authenticated client list.

When you disable NEAP client re-authentication, the switch cancels authentication for all authenticated NEAP clients, and automatically clears the MAC addresses of the NEAP clients from the forwarding database.

If you disconnect an authenticated NEAP client from a switch port, or if the port shuts down, the switch clears all NEAP clients authenticated on that port.

You cannot authenticate one NEAP client on more than one switch port simultaneously. If you connect NEAP clients to a switch port through a hub, those clients are authenticated on that switch port. If you disconnect a NEAP client from the hub and connect it directly to another switch port, the client is authenticated on the new port and its authentication is removed from the port to which the hub is connected.

If NEAP client re-authentication is enabled and the RADIUS server that the switch is connected to becomes unavailable, the system clears all authenticated NEAP and removes those clients from the switch NEAP client list.

For NEAP client re-authentication to function properly, you must enable the following features:

- MHMA at the port level
- RADIUS for Non-EAP clients globally
- RADIUS for Non-EAP clients at the port level

**Note:**

You do not have to enable the above features before you can enable or disable NEAP client re-authentication globally for the switch.

## 802.1X or non-EAP Last Assigned RADIUS VLAN

The 802.1X or non-EAP Last Assigned RADIUS VLAN functionality allows you to configure the switch so that the last received RADIUS assigned VLAN is always honored on a port. If enabled, the use most recent RADIUS assigned VLAN (either EAP or non-EAP) determines the VLAN membership and PVID replacing any previous RADIUS assigned VLAN values for that port.

The following are functional examples with last assigned RADIUS VLAN enabled:

- Multiple EAP and non-EAP clients can authenticate on a port
- The EAP and non-EAP clients can age out and re-authenticate. The last assigned VLAN setting for either EAP or non-EAP is always applied to the port.

**Important:**

This can move the port unexpectedly between VLANs.

## 802.1X or non-EAP with Fail Open VLAN

802.1X or non-EAP with Fail Open VLAN provides network connectivity when the switch cannot connect to the RADIUS server. Every three minutes, the switch verifies if the RADIUS servers are reachable. If the switch cannot connect to the primary and secondary RADIUS servers, then after a specified number of attempts to restore connectivity, the switch declares the RADIUS servers unreachable.

If the RADIUS servers are unreachable, all authenticated devices move into the configured Fail Open VLAN. This feature prevents disconnecting clients when the reauthentication timer expires. To provide connectivity requirements for corporate security policies, configure the Fail Open VLAN within the customer network.

For example, you can configure the Fail Open VLAN to provide access to corporate IT services, but restrict access to financial and other critical systems. In this configuration, if the RADIUS servers are unreachable, clients can connect to a limited level of the network.

In Fail Open mode with RADIUS servers unreachable, the switch regularly checks for RADIUS server connectivity. Once the RADIUS servers become reachable, client ports leave the Fail Open VLAN, and all MAC addresses are flushed, causing non-EAP clients to reauthenticate. The client ports return to the previous assigned VLANs, resuming normal network connectivity. When clients operate in the Fail Open VLAN with unreachable RADIUS servers, any 802.1X logoff messages received from the EAP supplicant are not processed by the switch.

For an EAP or non-EAP enabled port, the Fail Open VLAN feature is disabled by default. If the Fail Open VLAN is enabled and the RADIUS servers become unreachable, then:

- The port becomes a member of the EAP Fail Open VLAN. Ports belonging to an EAP VoIP VLAN become a member of both the EAP Fail Open VLAN and EAP VoIP VLAN
- The switch sets the PVID of the switch port to EAP Fail Open VLAN
- All EAP enabled ports move to the Fail Open VLANs across the units in a stack

**Important:**

When the switch is operating in Fail Open mode, it does not send EAP authentication requests to the RADIUS Server. If the RADIUS server is unreachable, all traffic is allowed from ports in the Fail Open VLAN, including previously non-authenticated devices.

**Important:**

When the port transitions from normal EAP operation to Fail Open, the end client is not aware that the port moves to a different VLAN. Depending upon the association of the IP addressing scheme to VLANs, it can be necessary for the client to obtain a new IP address when transitioning to or from the Fail Open VLAN.

Once the RADIUS server is reachable, the ports move to the Guest VLAN, or to configured VLANs, and age to allow the authentication of all incoming MAC addresses on the port. If at least one authenticated MAC address is on the port, it blocks all other unauthenticated MAC addresses on the port. You must turn on the debug counters to track server connectivity changes.

## 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 Avaya Ethernet Routing Switch 3500 Series 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.

  **Important:**

  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 Avaya Ethernet Routing Switch 3500 Series services.

**Important:**

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

An Avaya Ethernet Routing Switch 3500 Series 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 Avaya Ethernet Routing Switch 3500 Series, 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.

**Important:**

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. Avaya 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, Avaya 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

# 802.1X EAP and NEAP Accounting

In Release 5.0 RADIUS Accounting supports switch login events and EAP authentication, with RADIUS Interim Updates being supported for EAP clients. In Release 5.1 Accounting support is extended to generate accounting messages and interim updates for EAP and Non-EAP (NEAP) clients.

If a NEAP IP Phone is enabled, which authenticated a heritage Nortel IP Phone via its DHCP signature, then such authentication results in accounting messages being generated. If different servers are configured for EAP/NEAP servers then the accounting messages go to the respective servers.

**Note:**

EAP and NEAP accounting can be enabled when RADIUS accounting is enabled.

As the switch currently supports authentication for NEAP clients, accounting messages are generated for the following methods:

- ADAC based authentication
- MAC RADIUS authentication

- MHSA (Multiple Host Single Authentication) NEAP authentication
- Avaya IP phone DHCP signature authentication

The maximum number of clients for accounting is limited to the maximum configurable number of NEAP clients per port.

No additional CLI, MIB or EDM configuration is required for this feature.

# 802.1X EAP Separate enable/disable

The EAP/ NEAP separation command allows you to disable EAP clients without disabling NEAP clients.

When you enable EAPOL globally and per port, and enable or disable the EAP and NEAP clients, the following behaviors occur:

- At the switch, the default is enabled per port to keep the existing EAP clients enabled per port behavior.
- You can choose to enable NEAP clients. Detected NEAP clients are authenticated on the port.
- You can choose to disable the EAP clients and have only NEAP clients on a port or no client type enabled on port. In the case that EAP is disabled, the EAP packets that are not processed on port traffic from non-authenticated MACs are discarded. Authenticated MACs as NEAP clients can forward traffic on the port.
- If both EAP and NEAP clients are disabled on the port, no clients are authenticated and traffic will not be forwarded or received on the port.

If you do not enable EAPOL per port, then enabling or disabling these options have no effect on the authorized/forced unauthorized state of the port and on the processing of the traffic.

The following table describes the separation command behavior when applied to EAP per port features.

| Feature | Behavior |
|---|---|
| Single-Host | When in Single Host (multihost is disabled) this setting has no effect on the EAP packets – this setting is a multihost specific setting. |
| Multihost | Only when multihost is enabled per port than this setting will be applied to the port. |
| Non-EAP | When multihost and non-EAP are enabled per port, then the functionality is presented in the single-host and multi-host. |
| VLAN assignment for EAP clients | If the user decides to disable or enable EAP protocol on a port, then the VLAN assignment works for the |

*Table continues…*

| | |
|---|---|
| | remaining client types (non-EAP); the existing applied settings on a port for authenticated clients are kept. |
| VLAN assignment for NEAP clients | If you assign the VLAN for an authenticated EAP or NEAP client, then the VLAN is kept if authenticated clients are present on port. |
| VLAN assignment for EAP or NEAP clients | If you assign the VLAN for an authenticated EAP or NEAP client, then the VLAN is kept if authenticated clients are present on the port, no matter the client types. |
| Guest-VLAN | There is no restriction to disable the EAP protocol if you enable the Guest VLAN globally and per port (both EAP and non-EAP). |

# TACACS+

The Avaya Ethernet Routing Switch 3500 Series supports the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ is a security application implemented as a client/server-based protocol that provides centralized validation of users attempting to gain access to a router or network access server.

TACACS+ differs from RADIUS in two important ways:

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

**Important:**

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 ACLI.

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

The TACACS+ protocol is a draft standard available at https://datatracker.ietf.org/drafts/draftgrant-%20tacacs/

**Important:**

TACACS+ is not compatible with previous versions of TACACS.

## TACACS+ architecture

You can configure TACACS+ on the Avaya Ethernet Routing Switch 3500 Series 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 Avaya Ethernet Routing Switch 3500 Series.
- 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.

**Important:**

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 on page 53.

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

You can change privilege levels at run time. To change privilege levels at run time, use the following command:

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

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

**Important:**

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, enter the following command: `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 $enab<n>$ where <n> is the privilege level to which you want to allow access.

For an example of the configuration required on the TACACS+ server, see TACACS+ server configuration example on page 53.

## 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.

```
#Setting the accounting file on the server and server key
accounting file = /var/log/tac_plus.act
key = nOrt31
#Setting a user account used to log in
user = freddy {
     member=level6
     login=cleartext brody
     expires="Dec 31 2012"
}
#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
     }
}
```

**Figure 4: Example: TACACS+ server configuration**

## 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 ACLI terminal sessions within serial, Telnet, or SSH shells (from ACLI 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/SSHv2 session closed (not logged off)

## Feature limitations

The following features are not supported in the current implementation of TACACS+ in the Avaya Ethernet Routing Switch 3500 Series:

- 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 ACLI or EDM on the Avaya Ethernet Routing Switch 3500 Series. You can also use the console interface to enable or disable TACACS+ authentication on serial and Telnet connections.

For information about configuring TACACS+ using ACLI, see Configuring TACACS using ACLI on page 154.

For information about configuring TACACS+ using EDM, see Configuring TACACS using EDM on page 208.

# IP Manager

With IP Manager, you can limit access to the management features of the Avaya Ethernet Routing Switch 3500 Series 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.

**Important:**

To avoid locking a user out of the switch, Avaya recommends that you configure ranges of IP addresses that are allowed to access the switch. Changes you make to the IP Manager list are immediately applied for the new connection attempts. The sessions that were open at the time of configuring the IP Manager list remain unaffected.

# Password security

With unified password authentication you can manage the local authentication type username and password for a switch, whether it is part of a stack or a standalone unit.

For a stack environment, the local username and password authentication is applied universally across all switches in a stack.

If you insert a standalone switch with authentication credentials and mode already configured into an existing stack, both authentication credentials and mode of stack base unit are applied to the newly inserted switch. This maintains unified authentication management throughout the stack.

If you remove a switch from a stack to have it function as a standalone unit, that switch retains the unified stack authentication credentials until you manually change the credentials.

Switch authentication is identical to stack authentication except when RADIUS or TACACS+ authentication is used for the stack and there is no IP address configured for one or more of the stack units. In this case, the stack authentication type is set to RADIUS or TACACS+, the authentication type is automatically changed to “Local” for the units without IP addresses configured, and log messages are generated. This restriction is for any case where the user wants to set RADIUS or TACACS+ authentication and there is no stack or switch IP set. The setter checks for IP and if it not found then local authentication is used to avoid a lock-out of the user.

You can apply the following security methods to manage passwords for serial, Web, or Telnet access to a switch:

- local—uses the locally defined password
- none—disables the password
- RADIUS—uses RADIUS password authentication
- TACACS+—uses TACACS+ authentication, authorization, and accounting (AAA) services

With password security enabled, the following enhanced security features are applied.

## Custom user names and passwords

The Ethernet Routing Switch 3500 Series device provides the ability to create custom user names and passwords for accessing the switch or stack. User names and associated passwords can be defined at any time but only come into effect when password security is enabled. User names and passwords are created only by a user with read-write privileges.

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

## Password length and valid characters

Valid passwords 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 Avaya Ethernet Routing Switch 3500 Series keeps a history of the last three passwords. You cannot reuse a password stored in history. When you set the password for the fourth time, you can reuse the password that you used the first time.

## Password display

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

## Password verification

When you provide a new password, you must retype the 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.

## Log on failure timeout

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

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

## Password security features and requirements

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

**Table 1: Summary of password security features and requirements**

| Feature/Requirement | Description |
|---|---|
| Password composition | The password must contain a minimum of 2 of each of the following types of characters: lowercase letters, capital letters, numbers, and special symbols such as ! @#$%^&*(). |
| Password length | The password must consist of between 10 and 15 characters. |
| log on attempts | The switch allows only a specified maximum number of consecutive failed log on attempts. The number of allowed retries is configurable. The default is three. |
| Password history | The switch can be configured to store up to 10 previously used passwords. The passwords stored in the password history until they pass out of the history table. |
| Password update verification | Any password change must be verified by typing the new password twice. |
| Password aging time | Passwords expire after a specified period. The aging time is configurable. The default is 180 days. |
| Password display masking | Any time a password is displayed or entered in ACLI, each character of the password is displayed as an asterisk (*). |
| Password security factory default | By default, password security is enabled on the SSH software image and disabled on the non-SSH software image. |

## Password upgrade considerations

When you upgrade from a software image previous to Release 5.2 with separate switch and stack passwords, to the Release 5.2 or later with a unified password, only the stack set of credentials (password, username and authentication type) is preserved and used. The individual switch set of credentials is lost and overwritten by the new unified/stack set of credentials. Avaya recommends to set stack passwords and authentication type before you upgrade to Release 5.2

## 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 ACLI. 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.

**Important:**

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 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.

# Simple Network Management Protocol

The Avaya Ethernet Routing Switch 3500 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: readonly, 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.

## Avaya Ethernet Routing Switch 3500 Series support for SNMP

The SNMP agent in the Avaya Ethernet Routing Switch 3500 Series supports SNMPv1, SNMPv2c, and SNMPv3. Support for SNMPv2c introduces a standards-based GetBulk retrieval capability using SNMPv1 communities.

SNMPv3 support in the Avaya Ethernet Routing Switch 3500 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 Avaya Ethernet Routing Switch 3500 Series you can configure SNMPv3 by using Enterprise Device Manager, or ACLI.

## SNMP MIB support

The Avaya Ethernet Routing Switch 3500 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 Avaya Ethernet Routing Switch 3500 Series supports both industry-standard SNMP traps, as well as private Avaya 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 3500 series Release 5.0 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 (ACLI/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 (ACLI/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 Avaya command line interface (ACLI), Enterprise Device Manager (EDM), and SNMP.

## 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.

## DHCP Option 82

With DHCP Option 82, the switch can transmit information about the DHCP client and the DHCP agent relay to the DHCP server. The server can use the information from the switch to locate the DHCP client in the network and allocate a specific IP address to the DHCP client.

DHCP Option 82 function is controlled by the one switch at the edge of a network and not by any switches located between the network edge switch and the DHCP server.

DHCP Option 82 functions with DHCP Snooping (Layer 2 mode) or DHCP relay (Layer 3 mode) and cannot function independent of either of these features.

To use DHCP Snooping with DHCP Option 82 enable both features globally and for each client VLAN.

To use DHCP Option 82 with DHCP relay, you must enable DHCP relay globally on the switch and client VLANs.

For more information about DHCP Option 82 with DHCP relay, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 3500 Series*, NN47203-502.

# 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 on page 64.

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.

# 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 on page 63. 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 Avaya Ethernet Routing Switch 3500 Series by using Broadcom 569x ASICs and is implemented with the facility provided by the Fast Filter Processor (FFP) for each port, in the ASIC.

**Important:**

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

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

| IP Source Guard 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:<br>• DHCP is released<br>• the port link is down, or the administrator is disabled<br>• the lease time has expired | deletes the corresponding IP Filter and installs a default filter to block all IP traffic |
| enabled or disabled | enabled | not applicable | deletes the installed IP filter for the port |
| disabled | enabled | creates a binding entry | not applicable |
| disabled | enabled | deletes a binding entry | not applicable |

IP Source Guard does not support the following features:

- Manual assignment of IP addresses. DHCP snooping does not support static binding entries.

- IP and MAC address filter.

You can configure IP Source Guard by using the Avaya command line interface (ACLI), Enterprise Device Manager (EDM) and SNMP.

# Secure File Transfer Protocol (SFTP over SSH)

Using the SFTP protocol with SSH version 2, you can transfer a binary configuration file securely from a switch or stack to an SFTP server or from an SFTP server to a switch or stack.

Release 5.0 and up supports the following SFTP features:

- a binary configuration file upload to an SFTP server
- a binary configuration file download from an SFTP server
- DSA key authentication
- RSA key authentication
- password authentication
- host key generation
- 1024-bit DSA-key use for authentication. The DSA key range is 512-1024 and is multiple of 64.
- 2048-bit RSA-key use for authentication. The RSA key range is 1024-2048 and is multiple of 64.

# SSH enhancement to support RSA

When you select the RSA certificate option for a Secure Shell connection to the switch for a client PC, RSA public-private key encryption using a digital certificate with SSH login, is supported as a background option.

# Storm Control

This feature provides granular control of Broadcast, Multicast and Unicast traffic rates on a per-port basis. Broadcast, Multicast and Unicast traffic rates can be individually or collectively controlled on a switch or switch stack by setting the following: low-watermark and high watermark values in packets per second (pps), polling interval value, action type, and SNMP traps. When a high watermark is exceeded, an action of None, Drop or Shutdown can be applied to the traffic type.

A defined action is reversed, or ceases, when the traffic rate in pps falls below the low-watermark setting. When an action of ‘drop’ is used, traffic is dropped when traffic exceeds the high-watermark and will not resume forwarding until the traffic rate falls below the low-watermark. When the action of

‘shutdown’ is used, the switch port is administratively shutdown when traffic exceeds the high-watermark and requires administrator intervention to re-enable the switch port to resume traffic forwarding.

The Storm Control feature includes logging of watermark crossings and sending of traps for the high watermark crossings. Traps for high watermark exceeded may be sent repeatedly at a user specified interval.

Storm Control feature uses the rising and falling threshold levels to block and restore the forwarding of Broadcast, Multicast or Unicast packets. Storm Control feature is disabled by default.

# Rate limiting configuration

The Rate Limiting feature lets you configure the threshold limits for broadcast and multicast packets ingressing on a port for a given time interval. The Ethernet Routing Switch 3500 Series drops packets received above the threshold value if the traffic ingressing on the port exceeds the threshold. The hardware restrictions on this platform do not allow you to determine if the traffic from a port is the cause of excess broadcast or multicast traffic. Consequently you cannot perform port-specific actions such as disabling a port. You can generate a trap to detect the excess traffic or you can configure the switch to store a message in the system log when the traffic on the port exceeds the threshold value. This message in the system log conveys that some traffic to the switch is dropped.

When the volume of either packet type is high, placing severe strain on the network (often referred to as a "storm"), you can set the forwarding rate of those packet types to not exceed a specified percentage of the total available bandwidth. The pps (Packets Per Second) value you set is a small amount of the maximum value of pps for the maximum available bandwidth that is 262143 pps.

**Important:**

All Rate Limiting configuration settings are applied across the entire unit. You cannot set some ports in the unit to limit broadcast traffic with a value of X pps and some other ports in the same to limit multicast traffic with a value of Y pps.

You can view the rate limiting configuration settings and statistics with the **`show rate-limit`** command or the **`show running-config`** ACLI command. You can also limit the percentage of multicast traffic, or broadcast traffic, or both with **`rate-limit`** ACLI command.

**Note:**

With the Storm Control feature added in Release 5.1, both Storm Control and Rate Limiting are disabled by default. Only one of these features can be enabled at any one time. In order to use Rate Limiting, you must ensure that Storm Control is globally disabled.

# Chapter 5: IPv6 Management Fundamentals

This section provides information about the IPv6 management feature.

**Related links**

The IPv6 header on page 69
IPv6 addresses on page 70
Address formats on page 70
IPv6 extension headers on page 71
Comparison of IPv4 and IPv6 on page 72
ICMPv6 on page 72
Neighbor discovery on page 73
Router discovery on page 76
Path MTU discovery on page 77

## The IPv6 header

The IPv6 header contains the following fields:

- a 4-bit Internet Protocol version number, with a value of 6
- an 8-bit traffic class field, similar to Type of Service in IPv4
- a 20-bit flow label that identifies traffic flow for additional Quality of Service (QoS)
- a 16-bit unsigned integer, the length of the IPv6 payload
- an 8-bit next header selector that identifies the next header
- an 8-bit hop limit unsigned integer that decrements by 1 each time a node forwards the packet (nodes discard packets with hop limit values of 0)
- a 128-bit source address
- a 128-bit destination address

**Related links**

IPv6 Management Fundamentals on page 69

# IPv6 addresses

IPv6 addresses are 128 bits in length. The address identifies a single interface or multiple interfaces. IPv4 addresses, in comparison, are 32 bits in length. The increased number of possible addresses in IPv6 solves the inevitable IP address exhaustion inherent to IPv4.

The IPv6 address contains two parts: an address prefix and an IPv6 interface ID. The first 3 bits indicate the type of address that follow.

The Ethernet Routing Switch 3500 does not support stateless or stateful address configuration. The device does not try to obtain ipv6 parameters from a router and it does not query an IPv6 DHCP server, if it does not have an IPv6 address configured. The IPv6 global address of the 3500 series switch must be entered manually. The link-local IPv6 address is generated automatically, based on the MAC address of the device, once the IPv6 interface is attached to the management VLAN.

An example of a unicast IPv6 address is 1080:0:0:0:8:8000:200C:417A

**Related links**

IPv6 Management Fundamentals on page 69
Interface ID on page 70

## Interface ID

The interface ID is a unique number that identifies an IPv6 node (a host or a router). For stateless autoconfiguration, the ID is 64 bits in length.

In IPv6 stateless autoconfiguration, the interface ID is derived by a formula that uses the link layer 48-bit MAC address. (In most cases, the interface ID is a 64-bit interface ID that contains the 48-bit MAC address.) The IPv6 interface ID is as unique as the MAC address.

If you manually configure interface IDs or MAC addresses (or both), no relationship between the MAC address and the interface ID is necessary. A manually configured interface ID can be longer or shorter than 64 bits.

**Related links**

IPv6 addresses on page 70

# Address formats

The format for representing an IPv6 address is n:n:n:n:n:n:n:nn is the hexadecimal representation of 16 bits in the address.

An example is as follows: FF01:0:0:0:0:0:0:43

Each nonzero field must contain at least one numeral. Within a hexadecimal field, however, leading zeros are not required.

Certain classes of IPv6 addresses commonly include multiple contiguous fields containing hexadecimal 0. The following sample address includes six contiguous fields containing zeroes with a double colon (::):FF01::43

You can use a double colon to compress the leading zero fields in a hexadecimal address. A double colon can appear once in an address.

An IPv4-compatible address combines hexadecimal and decimal values as follows: x:x:x:x:x:x:d.d.d.d x:x:x:x:x:x is a hexadecimal representation of the six high-order 16- bit pieces of the address, and d.d.d.d is a decimal representation of the four 8-bit pieces of the address.

For example: 0:0:0:0:0:0:13.1.68.3

or

::13.1.68.3

**Related links**

IPv6 Management Fundamentals on page 69

# IPv6 extension headers

IPv6 extension headers describe processing options. Each extension header contains a separate category of options. A packet can include zero or more extension headers.

IPv6 examines the destination address in the main header of each packet it receives; this examination determines whether the router is the packet destination or an intermediate node in the packet data path. If the router is the destination of the packet, IPv6 examines the header extensions that contain options for destination processing. If the router is an intermediate node, IPv6 examines the header extensions that contain forwarding options.

By examining only the extension headers that apply to the operations it performs, IPv6 reduces the amount of time and processing resources required to process a packet.

IPv6 defines the following extension headers:

- The hop-by-hop extension header contains optional information that all intermediate IPv6 routers examine between the source and the destination.
- The end-to-end extension header contains optional information for the destination node.
- The source routing extension header contains a list of one or more intermediate nodes that define a path for the packet to follow through the network, to its destination. The packet source creates this list. This function is similar to the IPv4 source routing options.
- An IPv6 source uses the fragment header to send a packet larger than can fit in the path maximum transmission unit (MTU) to a destination. To send a packet that is too large to fit in the MTU of the path to a destination, a source node can divide the packet into fragments and send each fragment as a separate packet, to be reassembled at the receiver.
- The authentication extension header and the security encapsulation extension header, used singly or jointly, provide security services for IPv6 datagrams.

**Related links**

IPv6 Management Fundamentals on page 69

# Comparison of IPv4 and IPv6

The following table compares key differences between IPv4 and IPv6.

**Table 2: IPv4 and IPv6 differences**

| Feature | IPv4 | IPv6 |
|---|---|---|
| Address length | 32 bits | 128 bits |
| IPsec support (See Note 1) | Optional | Required |
| QoS support | Limited | Improved |
| Fragmentation | Hosts and routers | Hosts only |
| Minimum MTU (packet size) | 576 bytes | 1280 bytes |
| Checksum in header | Yes | No |
| Options in header | Yes | No |
| Link-layer address resolution | ARP (broadcast) | Multicast Neighbor Discovery Messages |
| Multicast membership | IGMP | Multicast Listener Discovery (MLD) |
| Router discovery (See Note 2) | Optional | Required |
| Uses broadcasts | Yes | No |
| Configuration (See Note 3) | Manual, DHCP | Manual |
| Note 1: Ethernet Routing Switch 3500 Series does not support IPsec.<br>Note 2: Ethernet Routing Switch 3500 Series does not perform Router discovery or advertise as a router.Note 3: Ethernet Routing Switch 3500 Series does not implement any form of automatic configuration of IPv6 address in Release 4.3. | | |

**Related links**

IPv6 Management Fundamentals on page 69

# ICMPv6

Internet Control Message Protocol (ICMP) version 6 maintains and improves upon features from ICMP for IPv4. ICMPv6 reports the delivery of forwarding errors, such as destination unreachable, packet too big, time exceeded, and parameter problem. ICMPv6 also delivers information messages such as echo request and echo reply.

**Important:**

ICMPv6 plays an important role in IPv6 features such as neighbor discovery, Multicast Listener Discovery, and path MTU discovery.

**Related links**

IPv6 Management Fundamentals on page 69

# Neighbor discovery

IPv6 nodes (routers and hosts) on the same link use neighbor discovery (ND) to discover link layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided for IPv4 with the Address Resolution Protocol (ARP) and router discovery. Neighbor discovery replaces ARP in IPv6.

Hosts use ND to discover the routers in the network that you can use as the default routers, and to determine the link layer address of their neighbors attached on their local links. Routers also use ND to discover their neighbors and their link layer information. Neighbor discovery also updates the neighbor database with valid entries, invalid entries, and entries migrated to different locations.

Neighbor discovery protocol provides you with the following:

- Address and prefix discovery: hosts determine the set of addresses that are on-link for the given link. Nodes determine which addresses or prefixes are locally reachable or remote with address and prefix discovery.
- Router discovery: hosts discover neighboring routers with router discovery. Hosts establish neighbors as default packet-forwarding routers.
- Parameter discovery: host and routers discover link parameters such as the link MTU or the hop limit value placed in outgoing packets.
- Address autoconfiguration: nodes configure an address for an interface with address autoconfiguration.
- Duplicate address detection: hosts and nodes determine if an address is assigned to another router or a host.
- Address resolution: hosts determine link layer addresses (MAC for Ethernet) of the local neighbors (attached on the local network), provided the IP address is known.
- Next-hop determination: hosts determine how to forward local or remote traffic with nexthop determination. The next hop can be a local or remote router.
- Neighbor unreachability detection: hosts determine if the neighbor is unreachable, and address resolution must be performed again to update the database. For neighbors you use as routers, hosts attempt to forward traffic through alternate default routers.
- Redirect: routers inform the host of more efficient routes with redirect messages.

Neighbor discovery uses three components:

- host-router discovery

- host-host communication component
- redirect

For more information, see for the ND components.

**Related links**

IPv6 Management Fundamentals on page 69
ND messages on page 74
Neighbor discovery cache on page 75

## ND messages

The following table shows new ICMPv6 message types.

**Table 3: IPv4 and IPv6 neighbor discovery comparison**

| IPv4 neighbor function | IPv6 neighbor function | Value |
|---|---|---|
| ARP Request message | Neighbor solicitation message | A node sends this message to determine the link-layer address of a neighbor or to verify that a neighbor is still reachable through a cached link-layer address. You can also use neighbor solicitations for duplicate address detection. |
| ARP Reply message | Neighbor advertisement | A node sends this message either in response to a received neighbor solicitation message or to communicate a link layer address change. |
| ARP cache | Neighbor cache | The neighbor cache contains information about neighbor types on the network. |
| Gratuitous ARP | Duplicate address detection | A host or node sends a request with its own IP address to determine if another router or host uses the same address. The source receives a reply from the duplicate device. Both hosts and routers use this function. |
| Router solicitation message (optional) | Router solicitation (required) | The host sends this message upon detecting a change in a network interface operational state. The message requests that routers generate router advertisement immediately rather than at the scheduled time. |

*Table continues…*

| IPv4 neighbor function | IPv6 neighbor function | Value |
|---|---|---|
| Router advertisement message (optional) | Router advertisement (required) | Routers send this message to advertise their presence together with various links and Internet parameters either periodically or in response to a router solicitation message. Router advertisements contain prefixes that you use for onlink determination or address configuration, and a suggested hop limit value. |
| Redirect message | Redirect message | Routers send this message to inform hosts of a better first hop for a destination. |

**Related links**

Neighbor discovery on page 73

## Neighbor discovery cache

The neighbor discovery cache lists information about neighbors in your network.

The neighbor discovery cache can contain the following types of neighbors

- static: a configured neighbor
- local: a device on the local system
- dynamic: a discovered neighbor

The following table describes neighbor cache states.

**Table 4: Neighbor cache states**

| State | Value |
|---|---|
| Incomplete | A node sends a neighbor solicitation message to a multicast device. The multicast device sends no neighbor advertisement message in response. Reachable You receive positive confirmation within the last reachable time period. |
| Stale | A node receives no positive confirmation from the neighbor in the last reachable time period. |
| Delay | A time period longer than the reachable time period passes since the node received the last positive confirmation, and a packet was sent within the last<br>DELAY_FIRST_PROBE_TIME period. If no reachability confirmation is received within |

*Table continues…*

| State | Value |
|---|---|
| | DELAY_FIRST_PROBE_TIME period of entering the DELAY state, neighbor solicitation is sent and the state is changed to |
| PROBE. | Probe Reachability confirmation is sought from the device every retransmit timer period. |

The following events involve Layer 2 and Layer 3 interaction when processing and affect the neighbor cache:

- flushing the Virtual Local Area Network (VLAN) media access control (MAC)
- removing a VLAN
- performing an action on all VLANs
- removing a port from a VLAN
- removing a port from a spanning tree group (STG)
- removing a multilink trunk group from a VLAN
- removing an Multi-Link Trunking port from a VLAN
- removing an Multi-Link Trunking port from an STG
- performing an action that disables a VLAN, such as removing all ports from a VLAN
- disabling a tagged port that is a member of multiple routable VLANs

**Related links**

Neighbor discovery on page 73

# Router discovery

IPv6 nodes discover routers on the local link with router discovery. The IPv6 router discovery process uses the following messages:

- router advertisement
- router solicitation

**Related links**

IPv6 Management Fundamentals on page 69
Router advertisement on page 77
Router solicitation on page 77

## Router advertisement

Configured interfaces on an IPv6 router send out router-advertisement messages. Router advertisements are also sent in response to router-solicitation messages from IPv6 nodes on the link.

**Related links**

Router discovery on page 76

## Router solicitation

An IPv6 host without a configured unicast address sends router solicitation Messages. Beginning with software release 5.0, the Ethernet Routing Switch 3500 does not support stateless automatic configuration. Therefore no router solicitation messages are sent by the switch.

**Related links**

Router discovery on page 76

# Path MTU discovery

IPv6 routers do not fragment packets. The source node sends a packet equal in size to the maximum transmission unit (MTU) of the link layer. The packet travels through the network to the source. If the packet encounters a link to a smaller MTU, the router sends the source node an ICMP error message containing the MTU size of the next link.

The source IPv6 node then resends a packet equal to the size of the MTU included in the ICMP message.

The default MTU value for a regular interface is 1500.

**Related links**

IPv6 Management Fundamentals on page 69

# Chapter 6: Configuring and managing security using ACLI

## Configuring and managing security using ACLI

This chapter describes the procedures necessary to configure security on the Avaya Ethernet Routing Switch 3500 Series, using the Avaya command line interface (ACLI).

## Setting the system user name and password using ACLI

Use the following procedure to configure the system user name and password for access through the serial console port and Telnet. This procedure supports only one read-only and one read-write user on the switch.

### Procedure

1. Log on to the Global Configuration command mode in ACLI.
2. Configure the username and password with the following command:

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

   - You can set the username and password back to the system default settings by using the following command:

     ```
     default username [ro|rw]
     ```

### Variable definitions

| Variable | Value |
|---|---|
| <username> <password> | 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. |
| ro\|rw | Specifies that you are modifying the read-only (ro) user name or the read-write (rw) user name.<br>The ro/rw variable is optional. If it is omitted, the command applies to the read-only mode. |

**Important:**

After you configure the user name and password with the **`username`** command, you can update the password without changing the username by using the **`cli password`** command, the console interface, or EDM.

## Setting the password for selected types of access using ACLI

Use the following procedure to set passwords for selected types of access (Telnet, TACACS, or RADIUS security) using ACLI.

The ACLI 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.
- Changes the password authentication type for serial console port or Telnet access to a switch.

**Important:**

The **`cli password`** command only changes the password, it does not affect the configured username.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. Configure the password for selected access or a specific authentication type by using the following commands:

```
cli password [serial | telnet] [local | none | radius | tacacs]
cli password {read-only | read-write} [<password>]
```

## Variable definitions

| Variable | Value |
|---|---|
| read-only \| read-write | Modify the read only password or the read/write password. |
| <password> | Enter your password.<br>**Important:**<br>This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password. |
| serial \| telnet | Modify the password for serial console access or for Telnet access. |
| none \| local \| radius \| tacacs | Indicates the password type you are modifying:<br>• none: disable the password |

*Table continues…*

| Variable | Value |
|---|---|
| | • local: uses the locally defined password for serial console or Telnet access.<br>• radius: uses RADIUS authentication for serial console or Telnet access.<br>• tacacs: uses TACACS+ authentication, authorization, and accounting (AAA) services for serial console or Telnet access. |

## Enabling or disabling password security using ACLI

When enabling password security with the command **`password security enable`**, if one of password does not comply with password security rules, the command fails and the user is asked to change it using **`cli password`** command according with these rules.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable password security, enter the following command:

   ```
   password security
   ```

   OR

   To disable password security, enter the following command:

   ```
   no password security
   ```

## Displaying the security using ACLI

### About this task

Use the following command to view the username / password settings:

### Procedure

1. Log on to the Priv Exec command mode.
2. Enter the following command at the command prompt:

   ```
   show cli password
   ```

   You can view the authentication using the following command:

   ```
   show cli password type
   ```

## Displaying the status of password security on the switch using ACLI

Use the following procedure to display the current status of password security on the switch.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show password security
   ```

### Example

The following figure provides a sample of the **`show password security`** command.

```
3524GT-PWR+#show password security
Password security is disabled
3524GT-PWR+#
```

## Setting the password aging time using ACLI

Use the following procedure to set the password aging time. Password security must be enabled for the command to be available.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   password aging-time day <1-2730>
   ```

   **Note:**

   If a new aging time is set from ACLI, the password aging couters are not reset.

## Displaying the password aging-time using ACLI

Use the following procedure to display the configured password aging-time.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show password aging-time
   ```

## Configuring the number of password logon attempts using ACLI

Use the following procedure to configure the number of times a user can attempt a password.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   telnet-access retry <1-100>
   ```

   **Note:**

   The default value for the allowed number of failed logon attempts is 3.

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

# Changing the http port number using ACLI

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 procedures.

## Displaying the port number of the HTTP port

Use the following procedure to display the port number of the HTTP port.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show http-port
   ```

### Example

The following figure provides a sample of the **show http-port** command.

```
3524GT-PWR+#show http-port
HTTP Port: 80
3524GT-PWR+#
```

## Setting the HTTP port number using ACLI

Use the following procedure to set the port number for the HTTP port, or to set the port number to the default value of 80.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To set the port number, enter the following command:

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

   OR

   To set the port number to the default value of 80, enter the following command:

   ```
   default http-port
   ```

# Setting Telnet access using ACLI

You can access ACLI through a Telnet session. To access ACLI remotely, the management port must have an assigned IP address and remote access must be enabled. You can log on to the switch using Telnet from a terminal that has access to the Avaya Ethernet Routing Switch 3500 Series.

**Important:**

Multiple users can access ACLI 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.

## Displaying Telnet access settings using ACLI

Use the following procedure to display the current settings for Telnet access.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show telnet-access
   ```

### Example

The following figure provides a sample of the **show telnet-access** command.

```
3524GT-PWR+#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
-------------------------  -------------------
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
----More (q=Quit, space/return=Continue)----
```

# Configuring Telnet connections using ACLI

Use the following procedure to configure the Telnet connection that is used to manage the switch.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   telnet-access [enable|disable] [login-timeout <0-10>] [retry
   <1-100>] [inactive-timeout <0-60>] [logging {none|access|failures|
   all}] [source-ip {<1-50> <A.B.C.D> | <51-100> <WORD>}]
   ```

## Variable definitions

The following table describes the parameters for the **telnet-access** command.

| Variable | Value |
|---|---|
| enable \| disable | Enables or disables Telnet connections. |
| login-timeout *<0–10>* | 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 0 and 10. Zero (0) is used to indicate no timeout. |

*Table continues…*

| Variable | Value |
|---|---|
| retry *<1–100>* | Specifies the number of times that the user can enter an incorrect password before closing the connection; enter an integer between 1 and 100. |
| inactive-timeout *<0–60>* | Specifies in minutes how long to wait before closing an inactive session; enter an integer between 0 and 60. |
| logging *{none\|access\|failures\|all}* | Specifies what types of events you want to save in the event log:<br>• **`all`**—Save all access events in the log:<br>- Telnet connect—indicates the IP address and access mode of a Telnet session.<br>- Telnet disconnect—indicates the IP address of the remote host and the access mode, due to either a log off or inactivity.<br>- 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.<br>• **`none`**—No Telnet events are saved in the event log.<br>• **`access`**—Connect and disconnect events are saved in the event log.<br>• **`failure`**—Only failed Telnet connection attempts are saved in the event log. |
| source-ip *[<1–50> <A.B.C.D> \| <51–100 <WORD>]* | The ERS 3500 supports a total of up to 50 IPv4 address/mask pairs (1–50) and 50 IPv6 address/prefix pairs (51–100). Specify the source IP addresses from which the connections are allowed:<br>• Enter the IPv4 addresses as a mask from 1 to 50 and an IP address in the format A.B.C.D.<br>• Enter the IPv6 addresses from 51–100 with a description.<br>**Important:**<br>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 ACLI on page 158 and Configuring the IP Manager list for IPv6 addresses using ACLI on page 159. |

# Disabling Telnet access using ACLI

Use the following procedure to disable the Telnet connection.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no telnet-access [source-ip [<1-50>|<51-100>]]
```

## Variable definitions

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

| Variable | Value |
|---|---|
| source-ip *<1–50>* \| *<51–100>* | Disables the Telnet access. 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 100th 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.<br>• Specify <1–50> to select the address/mask pair to be disabled.<br>• Specify <51–100> to select the IPv6 address/prefix to be disabled.<br>**Important:**<br>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 ACLI on page 158 and Configuring the IP Manager list for IPv6 addresses using ACLI on page 159. |

# Setting the Telnet settings to default values using ACLI

Use the following procedure to set the Telnet settings to the default values.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
default telnet-access
```

# Configuring SSL using ACLI

The following procedures describe how you can configure SSL to provide a secure Web management interface using ACLI.

## Enabling or disabling SSL using ACLI

Use the following procedure to enable SSL for the Web server to function in a secure mode or to disable SSL for the Web server to function in a nonsecure mode.

**Procedure**

1. Log on to ACLI in Global Configuration command mode.
2. To enable SSL, enter the following command:

   ```
   ssl
   ```

   OR

   To disable SSL, enter the following command:

   ```
   no ssl
   ```

## Creating or deleting an SSL certificate using ACLI

Use the following procedure to create an SSL certificate to replace the existing SSL certificate in NVRAM or to remove the existing certificate from NVRAM.

**Procedure**

1. Log on to ACLI in Global Configuration command mode.
2. To create an SSL certificate, enter the following command:

   ```
   ssl certificate
   ```

   OR

   To delete an SSL certificate, enter the following command:

   ```
   no ssl certificate
   ```

## Viewing the SSL server configuration using ACLI

Use the following procedure to view the SSL server configuration and SSL server state.

**Procedure**

1. Log on to ACLI in Privileged EXEC command mode.

2. At the command prompt, enter the following command:

```
show ssl
```

### Variable definitions

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

| Field | Description |
|---|---|
| WEB Server SLL Secured | Displays whether or not the Web server uses an SSL connection |
| **SSL server state** | |
| 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. |
| **SSL Certificate** | |
| Generation in progress | Shows whether SSL is generating a certificate. The SSL server generates a certificate during server startup initialization, or the ACLI 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 the ACLI 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 ACLI

Use the following procedure to display the SSL certificate stored in NVRAM.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show ssl certificate
```

# Configuring Secure Shell using ACLI

Use the procedures in the following sections to configure and manage SSH on the Ethernet Routing Switch 3500. The SSH protocol provides secure access to ACLI.

## Displaying the secure shell configuration information using ACLI

Use the following procedure to display the secure shell configuration information.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show ssh global
   ```

### Example

The following figure provides a sample of the **`show ssh global`** command.

```
3524GT-PWR+#show ssh global
Active SSH Sessions     :  0
Version                 :  Version 2 only
Port                    :  22
Authentication Timeout  :  60
DSA Authentication      :  True
RSA Authentication      :  True
Password Authentication :  True
Auth Key TFTP Server    :  172.16.3.2
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys           :  Exist
RSA Host Keys           :  Exist
Enabled                 :  False
3524GT-PWR+#
```

## Displaying the SSH session information using ACLI

Use the following procedure to display 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.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show ssh session
   ```

### Example

The following figure provides a sample of the **`show ssh session`** command.

```
3524GT-PWR+#show ssh session
Session  Host
-------  ---------------------------------------------
3524GT-PWR+#
```

## Displaying SSH download DSA key information using ACLI

Use the following procedure to display the results of the most recent attempt to download the DSA public key from the TFTP server.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

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

### Example

The following figure provides a sample of the **`show ssh download-auth-key`** command.

```
3524GT-PWR+#show ssh download-auth-key
Auth Key TFTP Server     :  172.16.3.2
DSA Auth Key File Name   :
RSA Auth Key File Name   :
Last Transfer Result     :  None
3524GT-PWR+#
```

## Generating the DSA host keys using ACLI

Use the following procedure to generate the DSA host keys. After the command is executed, you do not need to perform a reboot.

**Important:**

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

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Deleting the DSA host key using ACLI

Use the following procedure to delete the DSA host key in the switch.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Enabling or disabling the SSH server in nonsecure mode using ACLI

Use the following procedure to enable or disable the SSH server on the Avaya Ethernet Routing Switch 3500 in nonsecure mode. In addition to accepting SSH connections, the Avaya ERS 3500 Series continues to accept SNMP and Telnet connections while in this mode.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable the SSH server, enter the following command:

   ```
   ssh
   ```

   OR

   To disable the SSH server, enter the following command:

   ```
   no ssh
   ```

## Enabling the SSH server in secure mode using ACLI

Use the following procedure to enable the SSH server on the Avaya Ethernet Routing Switch 3500 Series in secure mode. In secure mode, the Avaya Ethernet Routing Switch 3500 Series does not accept SNMP, or Telnet connections.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   ssh secure
   ```

## Setting the timeout value for session authentication using ACLI

Use the following procedure to set the timeout value for session authentication.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

| Variable | Value |
|---|---|
| <1–120> | Specifies the timeout value for authentication.<br>DEFAULT: 60 seconds |

# Enabling DSA authentication using ACLI

Use the following procedure to enable DSA authentication. Note that DSA authentication can be disabled using the [no] parameter with this command.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
ssh dsa-auth
```

## Variable definitions

The following table describes the parameters for the **`ssh dsa-auth`** command.

| Variable | Value |
|---|---|
| no | Disables DSA authentication. |

# Enabling password authentication using ACLI

Use the following procedure to enable password authentication. Note that password authentication can be disabled using the [no] parameter with this command.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable password authentication, enter the following command:

```
ssh pass-auth
```

# Setting the SSH connection port using ACLI

Use the following procedure to set the SSH connection port.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

| Variable | Value |
|---|---|
| <1–65535> | Specifies the SSH connection port number.<br>DEFAULT: 22 |

## Downloading the client public key from the TFTP server using ACLI

Use the following procedure to download the client public key from the TFTP server to the Avaya Ethernet Routing Switch 3500 Series.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
ssh download-auth-key [address <A.B.C.D>] [key-name <file>]
```

### Variable definitions

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

| Variable | Value |
|---|---|
| address <*A.B.C.D*> | Specifies the IP address of the TFTP server. |
| dsa | Download SSH DSA auth key. |
| key-name <*file*> | Specifies the name of the public key file on the TFTP server. |
| rsa | Download the SSH RSA auth key. |

## Deleting the SSH DSA authentication key using ACLI

Use the following procedure to delete the SSH DSA authentication key.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

# Resetting SSH configuration parameters to default using ACLI

Use the following procedure to reset specific secure shell configuration parameters to the default values.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   default ssh [dsa-auth|pass-auth|port|rsa-auth|timeout]
   ```

## Variable definitions

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

| Variable | Value |
|---|---|
| dsa-auth | Enables SSH DSA authentication. |
| pass-auth | Enables SSH password authentication. |
| port | Resets the port number for SSH connections to the default.<br>DEFAULT: 22 |
| rsa-auth | Enables SSH RSA authentication. |
| timeout | Resets the timeout value for session authentication to the default.<br>DEFAULT: 60 |

# Enabling SSH RSA authentication using ACLI

Use the following procedure to enable RSA authentication.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   ssh rsa-auth
   ```

# Generating the SSH RSA host key using ACLI

Use the following procedure to generate the RSA host keys.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
ssh rsa-host-key
```

# Configuring RADIUS Interim Accounting Updates support using ACLI

Use the procedures in this section to configure RADIUS Interim Accounting Updates support on the Ethernet Routing Switch 3500 Series.

## Configuring RADIUS Interim Accounting Updates support using ACLI

Use the following 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

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
radius accounting interim-updates <enable> [interval <seconds>]
<use-server-interval>
```

### Variable definitions

The following table describes the parameters for the **`radius accounting interim-updates`** command.

| Variable | Value |
|---|---|
| enable | Enables RADIUS Interim Accounting Updates support statically on the switch. |
| interval *<seconds>* | Specifies the RADIUS Interim Accounting Updates support timeout interval in seconds.<br>DEFAULT: 600 seconds<br>RANGE: 60 to 3600 seconds |
| use-server-interval | Selects the value transmitted by the RADIUS server as the RADIUS Interim Accounting Updates support timeout interval. |

## Disabling RADIUS Interim Accounting Updates support using ACLI

Use the following procedure to 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

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **`no radius accounting interim-updates`** command.

| Variable | Value |
|---|---|
| enable | Disables RADIUS Interim Accounting Updates support statically on the switch. |
| use-server-interval | 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 ACLI

Use the following procedure to 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.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
default radius accounting interim-updates <enable> <interval> <use-server-interval>
```

### Variable definitions

The following table describes the parameters for the **`default radius accounting interim-updates`** command.

| Variable | Value |
|---|---|
| enable | Configures the RADIUS Interim Accounting Updates support default status on the switch as disabled. |
| interval | Configures the default RADIUS Interim Accounting Updates support default interval on the switch as 600 seconds. |
| use-server-interval | 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 ACL

Use the following procedure to 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.

### Procedure

1. Log on to ACLI in User EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show radius accounting interim-update
   ```

### Example

The following figure provides an example output of the **`show radius accounting interim-update`** command.

```
3524GT-PWR+>enable
3524GT-PWR+#show radius accounting interim-update
RADIUS accounting interim-updates: Disabled
RADIUS accounting interim-updates interval: 600
RADIUS accounting use-server-interval: Enabled
3524GT-PWR+#
```

# Configuring RADIUS Request use Management IP using ACLI

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

## Enabling RADIUS request use of Management IP using ACLI

Use the following procedure to enable RADIUS requests to use Management VLAN IP address.

**Procedure**

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   radius use-management-ip
   ```

   OR

   ```
   default radius use-management-ip
   ```

## Disabling RADIUS request use of Management IP using ACLI

Use the following procedure to disable RADIUS Request use to prevent the RADIUS requests from using the Management VLAN IP address.

**Procedure**

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   no radius use-management-ip
   ```

## Viewing RADIUS request use Management IP status using ACLI

Use the following procedure to display the RADIUS Request use Management IP status.

**Procedure**

1. Log on to ACLI in User EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show radius use-management-ip
   ```

# Configuring RADIUS authentication using ACLI

You can use the procedures in this section to help secure networks against unauthorized access, by configuring communication servers and clients to authenticate user identities through a central database.

## Configuring switch RADIUS server settings using ACLI

Use the following procedure to configure RADIUS server account information on the switch.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] [default] radius server host {ipaddr | ipv6addr} [key{key}]
[port <port>] [retry <1-5>] [secondary] [timeout <1-60>] [used-by
<eapol| non-eapol>]
```

## Variable definitions

The following table describes the parameters for the **`radius server host`** command.

| Variable | Value |
|---|---|
| <ipaddr> | Specifies the IPv4 address of the primary server you want to add or configure.<br>**Important:**<br>A value of 0.0.0.0 indicates that a primary RADIUS server is not configured. |
| <ipv6addr> | Specifies the IPv6 address of the primary server you want to add or configure.<br>**Important:**<br>A value of 0.0.0.0 indicates that a primary RADIUS server is not configured. |
| default | Restores the switch RADIUS server settings to default values.<br>To delete a RADIUS server and restore default RADIUS settings, use one of the following commands in the Global or Interface Command mode:<br>• `default radius server host`<br>• `default radius server host secondary`<br>• `default radius server host used-by eapol`<br>• `default radius server host secondary used-by eapol`<br>• `default radius server host used-by non-eapol`<br>• `default radius server host secondary used-by non-eapol` |
| key <*key*> | Specifies the secret authentication and encryption key used for all communications between the NAS |

*Table continues…*

| Variable | Value |
|---|---|
| | and the RADIUS server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to enter and confirm the key. |
| no | Deletes switch RADIUS server settings. |
| port *<port>* | Specifies the UDP port number for clients to use when trying to contact the RADIUS server at the corresponding RADIUS server IP address.<br>RANGE: 1 to 65535<br>DEFAULT port number: 1812 |
| retry *<1–5>* | Specifies the number of RADIUS retry attempts for a RADIUS Server instance.<br>RANGE: 1 to 5 |
| secondary | Specifies the RADIUS server you are configuring as the secondary server. The system uses the secondary server only if the primary server is not configured or is not reachable. |
| timeout *<timeout>* | Specifies the timeout interval between each retry for service requests to the RADIUS server.<br>RANGE: 1 to 60 seconds<br>DEFAULT: 2 seconds |
| used-by *<eapol \| non-eapol>* | Specifies the RADIUS server as an EAP RADIUS Server or a Non-EAP (NEAP) RADIUS Server.<br>• eapol—configures the RADIUS server to process EAP client requests only .<br>• non-eapol—configures the RADIUS server to process Non-EAP client requests only.<br>If you do not specify the RADIUS server as either EAP or Non-EAP, the system configures the server as a Global RADIUS Server, and processes client requests without designating them as separate EAP or Non-EAP. |

## Enabling or disabling RADIUS password fallback using ACLI

Use the following procedure to enable or disable the RADIUS password fallback feature for logging on to a switch by using the local password if the RADIUS server is unavailable or unreachable.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.

2. To enable RADIUS password fallback, enter the following command:

   `default radius-server password fallback`

   OR

   To disable RADIUS password fallback, enter the following command:

   `no radius-server password fallback`

## Viewing RADIUS information using ACLI

Use the following procedure to display RADIUS server configuration information.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   `show radius-server`

### Example

The following figure provides a sample of the **`show radius-server`** command.

```
3524GT-PWR+>enable
3524GT-PWR+#show radius-server
RADIUS Global Server
------------------------------------------------------------
Primary Host            : 0.0.0.0
Secondary Host          : 0.0.0.0
Port                    : 1812
Time-out                : 2
Key                     : ***************
Radius Retry Limit      : 3

RADIUS EAP Server
------------------------------------------------------------
Primary Host            : 0.0.0.0
Secondary Host          : 0.0.0.0
Port                    : 1812
Time-out                : 2
Key                     : ***************
Radius Retry Limit      : 3

RADIUS Non-EAP Server
------------------------------------------------------------
Primary Host            : 0.0.0.0
Secondary Host          : 0.0.0.0
----More (q=Quit, space/return=Continue)----
```

# Configuring RADIUS server reachability using ACLI

Use the following procedure to select and configure the method by which to determine the reachability of the RADIUS server.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
[default] radius reachability {use-icmp | use-radius [username
<username> | password <password>]}
```

## Variable definitions

The following table describes the parameters for the **`[default] radius reachability`** command.

| Variable | Value |
|---|---|
| default | Restores RADIUS server reachability to default values. |
| password *<password>* | Specifies a password for the RADIUS request. |
| use-icmp | Uses ICMP packets to determine reachability of the RADIUS server (default). |
| use-radius | Uses dummy RADIUS requests to determine reachability of the RADIUS server. |
| username *<username>* | Specifies a user name for the RADIUS request. |

# Viewing the RADIUS server reachability method using ACLI

Use the following procedure to display the configured RADIUS server reachability method.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show radius reachability
```

### Example

The following figure provides an example output of the **show radius reachability** command.

```
3524GT-PWR+#show radius reachability
RADIUS reachability: USE ICMP
3524GT-PWR+#
```

# Configuring 802.1X dynamic authorization extension (RFC 3576) configuration using ACLI

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

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

### Before you begin

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

**Important:**

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

### Procedure

1. Log on to ACLI Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Variable definitions

The following table describes the parameters for the **radius dynamic-server client** command.

| Variable | Value |
|---|---|
| <A.B.C.D> | Specifies the IP address of a new RADIUS dynamic authorization client or the IP address of an existing client for which you want to change the configuration. |
| enable | Enables packet receiving from the RADIUS Dynamic Authorization Client. |

*Table continues…*

| Variable | Value |
|---|---|
| port | Configures the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1024 to 65535. |
| process-change-of-auth-requests | Enables change-of-authorization (CoA) request processing. |
| process-disconnect-requests | Enables disconnect request processing. |
| secret | Configures the RADIUS Dynamic Authorization Client secret word. |

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

Use the following procedure to 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

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no radius dynamic-server client <A.B.C.D>
```

## Variable definitions

The following table describes the parameters for the **`no radius dynamic-server client`** command.

| Variable | Value |
|---|---|
| <A.B.C.D> | Specifies the IP address of the configured RADIUS Dynamic Authorization client that you want to disable. |

# Viewing RADIUS dynamic authorization client configuration using ACLI

Use the following procedure to display the configuration of RADIUS dynamic authorization client parameters.

### Procedure

1. Log on to ACLI in Privilege EXEC command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **`show radius dynamic-server client`** command.

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

## Viewing RADIUS dynamic authorization client statistics using ACLI

Use the following procedure to display RADIUS dynamic authorization client statistical information.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **`show radius dynamic-server statistics client`** command.

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

## Enabling or disabling RADIUS dynamic authorization extension (802.1X RFC 3576) on a port using ACLI

Use the following procedure to enable or disable RADIUS dynamic authorization extension on a port.

### Before you begin

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

**Important:**

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

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. To enable RADIUS dynamic authorization extension on a port, enter the following command:

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

   OR

   To disable RADIUS dynamic authorization extension on a port, enter the following command:

   ```
   no eapol radius-dynamic-server enable
   ```

## Viewing replay protection for RADIUS dynamic authorization extension using ACLI

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

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   show radius dynamic-server replay-protection
   ```

## Enabling or disabling replay protection for RADIUS dynamic authorization extension using ACLI

Use the following procedure to enable or disable replay protection for RADIUS dynamic authorization extension.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable or re-enable replay protection, enter the following command:

   ```
   default radius dynamic-server replay-protection
   ```

   OR

   To disable replay protection, enter the following command:

   ```
   no radius dynamic-server replay-protection
   ```

# Setting SNMP parameters using ACLI

## Enabling or disabling the SNMP server using ACLI

Use the following procedure to enable or disable the SNMP server.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Disabling SNMP access using ACLI

Use the following procedure to disable SNMP access

**Important:**

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

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   no snmp-server
   ```

## Enabling disabling or restoring to default the generation of SNMP authentication failure traps using ACLI

Use the following procedures to enable, disable, or restore SNMP authentication failure trap configuration to default settings using ACLI.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable the generation of SNMP authentication failure traps, enter the following command:

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

   OR

   To disable the generation of SNMP authentication failure traps, enter the following command:

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

OR

To restore SNMP authentication failure trap configuration to default settings, enter the following command:

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

# Modifying the community strings for SNMPv1 and SNMPv2c access using ACLI

Use the following procedure to modify the community strings for SNMPv1 and SNMPv2c access.

The following 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.

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

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Variable definitions

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

| Variable | Value |
|---|---|
| <community-string> | Changes community strings for SNMPv1 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.<br>**Important:**<br>This parameter is not available when Password Security is enabled, in which case, the switch prompts you to enter and confirm the new community string. |
| ro \| rw | Specifies read-only or read/write access. Stations with **ro** access can retrieve only MIB objects, and stations with **rw** access can retrieve and modify MIB objects. |

*Table continues…*

| Variable | Value |
|---|---|
| | **Important:**<br>If neither **ro** nor **rw** is specified, ro is assumed (default) |

## Clearing the SNMP server community configuration using ACLI

Use the following procedure to clear the snmp-server community configuration.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Restoring the community string configuration to default settings using ACLI

Use the following procedure to restore the community string configuration to the default settings.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

| Variable | Value |
|---|---|
| ro\|rw | Restores the read-only community to **public**, or the read/write community to **private**. |

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.

## Displaying SNMP community string configuration using ACLI

Use the following procedure to display the SNMP community string configuration.

**Note:**

The community strings are not displayed when Password Security is enabled.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show snmp-server community
   ```

## Configuring the SNMP sysContact value using ACLI

Use the following procedure to configure the SNMP sysContact value.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

| Variable | Value |
|---|---|
| <text> | Specifies the SNMP sysContact value; enter an alphanumeric string. |

## Clearing or restoring the SNMP sysContact value to default value using ACLI

Use the following procedure to clear or to restore the sysContact value to its default value.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To clear the sysContact value, enter the following command:

   ```
   no snmp-server contact
   ```

   OR

   To restore the sysContact value to the default value, enter the following command:

   ```
   default snmp-server contact
   ```

## Configuring or clearing the SNMP sysLocation value using ACLI

Use the following procedure to configure or to clear the SNMP sysLocation value.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To configure the SNMP sysLocation value, enter the following command:

   ```
   snmp-server location <text>
   ```

3. To clear the SNMP sysLocation value, enter the following command:

   ```
   no snmp-server location <text>
   ```

### Variable definitions

The following table describes the parameters for the **`[no] snmp-server location`** command.

| Variable | Value |
|---|---|
| <text> | Specifies the SNMP sysLocation value. Enter a string of up to 255 characters. |

## Restoring the SNMP sysLocation to the default using ACLI

Use the following procedure to restore the SNMP sysLocation to the default value.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   default snmp-server location
   ```

## Configuring the SNMP sysName value using ACLI

Use the following procedure to configure the SNMP sysName value.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   snmp-server name <text>
   ```

### Variable definitions

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

| Variable | Value |
|---|---|
| <text> | Specifies the SNMP sysName value; enter an alphanumeric string of up to 255 characters. |

## Clearing the SNMP sysName value using ACLI

Use the following procedure to clear the sysName value.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   `no snmp-server name`

   OR

   `default snmp-server name`

## Enabling SNMP linkUp linkDown traps for a port using ACLI

Use the following procedure to enable the linkUp/linkDown traps for a port.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   `snmp-server notification-control linkUp [<portlist>]` for linkUp trap.

   or

   `snmp-server notification-control linkDown [<portlist>]` for linkDown trap.

### Variable definitions

The following table describes the parameters for the **`snmp-server notification-control {linkUp|linkDown} [<portlist>]`** command.

| Variable | Value |
|---|---|
| port <portlist> | Specifies the port numbers on which to enable the linkUp/linkDown traps. Enter the port numbers or all.<br>**Important:**<br>If you omit this parameter, the status of the already configured list of ports is set to enabled. |

# Disabling the SNMP linkUp linkDown traps for a port using ACLI

Use the following procedure to disable the linkUp/linkDown traps for a port.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   no snmp-server notification-control linkUp [<portlist>]
   ```

   OR

   ```
   default snmp-server notification-control linkUp [<portlist>]
   ```

   for linkUp trap.

   Or

   ```
   no snmp-server notification-control linkDown [<portlist>]
   ```

   Or

   ```
   default snmp-server notification-control linkDown [<portlist>]
   ```

   for linkDown trap.

## Variable definitions

The following table describes the parameters for the **`{no|default} snmp-server notification-control {linkUp|linkDown} [<portlist>]`** command.

| Variable | Value |
|---|---|
| port <portlist> | Specifies the port numbers on which to disable the linkUp/linkDown traps. Enter the port numbers or all.<br>**Important:**<br>If you omit this parameter, the status of linkUp/linkDown trap is set to disabled for all ports, no matter what the already configured list of ports is. |

# Adding SNMP traps to a filter profile using ACLI

Use the following procedure to add SNMP traps to a filter profile (filter name).

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
snmp-server notify-filter <filterName:WORD> <OID:WORD> [<OID:WORD>
[<OID:WORD> [<OID:WORD> [<OID:WORD> [<OID:WORD> <OID:WORD>
[<OID:WORD> [<OID:WORD> [<OID:WORD>]]]]]]]]
```

## Variable definitions

The following table describes the parameters for the **snmp-server notify-filter** command.

| Variable | Value |
|---|---|
| <filterName> | Specifies the filter profile name. |
| <WORD> | Specifies the description of OID specification of the SNMP trap added to the filterName filter.<br><br>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. |

# Deleting SNMP traps from a filter profile using ACLI

Use the following procedure to delete SNMP traps from a filter profile (filter name).

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no snmp-server notify-filter <filterName:WORD> <OID:WORD>
[<OID:WORD>]
```

## Variable definitions

The following table describes the parameters for the **snmp-server notify-filter** command.

| Variable | Value |
|---|---|
| <filterName> | Specifies the filter profile name. |
| <WORD> | Specifies the description of OID specification of the SNMP trap added to the filterName filter.<br><br>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. |

## Displaying notify-filter details using ACLI

Use the following procedure to display notify-filter details.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

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

## Enabling or disabling the generation of SNMP traps using ACLI

Use the following procedure to enable or disable the generation of SNMP traps for specific ports, or for all switch ports.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable the generation of SNMP traps, enter the following command:

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

   OR

   To disable the generation of SNMP traps, enter one of the following commands:

   - `no snmp-server notification-control <notification> <WORD> <portlist>`
   - `default snmp-server notification-control <notification> <WORD> <portlist>`

### Variable definitions

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

| Variable | Value |
|---|---|
| <portlist> | Specifies a port or group of ports. If you do not specify a port or group of ports, the notification control is disabled for all switch ports. |
| <WORD> | Specifies a character string or OID describing the notification type.<br>An example of a character string describing the notification type is, **linkDown**, **linkup**.<br>An example of an OID describing the notification type is **1.3.1.6.1.3.1.1.5.3**, **1.3.6.1.6.3.1.1.5.4**. |

# Using ACLI commands specific to SNMPv3

## Creating an SNMPv3 user using ACLI

Use the following procedure to create an SNMPv3 user.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
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>]
```

## Variable definitions

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

| Variable | Value |
|---|---|
| engine-id *<engineid>* | Specifies the SNMP engine ID of the remote SNMP entity |
| *<username>* | Specifies the user names; enter an alphanumeric string of up to 255 characters. |

*Table continues…*

| Variable | Value |
|---|---|
| md5/sha *<password>* | Specifies the use of an md5/sha authentication pass phrase.<br>• *password*—specifies the new user md5 /sha authentication pass phrase; enter an alphanumeric string.<br>If this parameter is omitted, the user is created with only unauthenticated access rights.<br>**Important:**<br>This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password. |
| read-view *<view-name>* | Specifies the read view to which the new user has access:<br>• *view-name*—specifies the view name; enter an alphanumeric string of up to 255 characters. |
| write-view *<view-name>* | Specifies the write view to which the new user has access:<br>• *view-name*—specifies the view name; enter an alphanumeric string of up to 255 characters. |
| notify-view *<view-name>* | Specifies the notify view to which the new user has access:<br>• *view-name*— specifies the view name; enter an alphanumeric string of up to 255 characters. |
| des/aes/3des *<password>* | Specifies the use of a des/aes/3des privacy pass phrase.<br>• password—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.<br>**Important:**<br>This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password. |

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.

# Removing an SNMPv3 user using ACLI

Use the following procedure to delete a specified SNMPv3 user.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Variable definitions

The following table describes the parameters for the **no snmp-server user** command.

| Variable | Value |
|---|---|
| engine-id *<engineid>* | Specifies the SNMP engine ID of the remote SNMP entity. |
| *<username>* | Specifies the user to be removed. |

# Creating an SNMPv3 view using ACLI

Use the following procedure to create an SNMPv3 view. The view is a set of MIB object instance that can be assessed.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
snmp-server view <view-name> <OID> [<OID> [<OID> [<OID> [<OID>
[<OID> [<OID> [<OID> [<OID> [<OID>]]]]]]]]]
```

## Variable definitions

The following table describes the parameters for the **snmp-server view** command.

| Variable | Value |
|---|---|
| *<viewname>* | Specifies the name of the new view; enter an alphanumeric string. |
| *<OID>* | Specifies the Object identifier. *OID* can be entered as a MIB object English descriptor, a dotted form *OID*, or a mix of the two. Each *OID* 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 *OID* parameters are as follows:<br>• **`sysName`**<br>• **`+sysName`**<br>• **`-sysName`**<br>• **`+sysName.0`**<br>• **`+ifIndex.1`**<br>• **`-ifEntry.*.1`** (matches all objects in the if Table with an instance of 1, that is, the entry for interface #1)<br>• **`1.3.6.1.2.1.1.1.0`** (dotted form of **`sysDescr`**)<br>The plus (+) or minus (–) sign indicates whether the specified *OID* 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:<br>**`snmp-server view myview +system -sysDescr`**<br>and you use that view for the read-view of a user, then the user can read only the system group, except for **`sysDescr`**. |

## Removing an SNMPv3 view using ACLI

Use the following procedure to delete an SNMPv3 view.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Variable definitions

The following table describes the parameters for the **no snmp-server view** command.

| Variable | Value |
|---|---|
| <viewname> | Specifies the name of the view to be removed. If no view is specified, all views are removed. |

# Adding trap receivers to SNMPv3 tables using ACLI

Use the following procedure to add 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.

### Before you begin

- You must previously configure the community string or user that is specified with a notify-view.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
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>]>
```

## Variable definitions

The following table describes the parameters for the **snmp-server host** command.

| Variable | Value |
|---|---|
| port *<1-65535>* | Sets the SNMP trap port. |
| *A.B.C.D* | Specifies the dotted-decimal IP address of a host to be the trap destination. |
| *<community-string:WORD>* | 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. |
| filter *<WORD>* | Specifies the filter profile name. The **snmp-server host** command is improved with the filter parameter only for the hosts with a specified SNMP version (v1/v2c/v3). |

*Table continues…*

| Variable | Value |
|---|---|
| | Add the filter parameter only for the normal syntax form of the **snmp-server host** command. 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. |
| inform | Generates acknowledge inform requests. |
| *<ipv6addr>* | Specifies the IPv6 address of the SNMP notification host. |
| retries *<0-255>* | Specifies the number of retries for inform requests.<br>RANGE: 0-2147483647 |
| target-name *<WORD/1-32>* | Specifies the name of the target. |
| timeout *<1-2147483647>* | Specifies the timeout for inform requests.<br>RANGE: 1-2147483647 centi-seconds |
| *<username:WORD>* | Specifies the SNMPv3 user name for trap destination; enter an alphanumeric string. |
| v1 *<community-string:WORD>* | Creates v1 trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels. |
| v2c *<community-string:WORD>* | Creates v2c trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels. |
| v3 {auth\|no-auth\| auth-priv} | 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:<br>• **auth\|no-auth** —Specifies whether SNMPv3 traps can be authenticated.<br>• **auth-priv**—This parameter is only available if the image has full SHA/DES support. |

## Deleting trap receivers or restoring the SNMPv3 table to defaults using ACLI

Use the following procedure to delete trap receivers from the table or to restore the SNMPv3 MIB table to defaults (that is, to clear the table).

**Important:**

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.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To delete trap receivers, enter the following command:

   ```
   no snmp-server host {<A.B.C.D> | <ipv6addrr> } {v1 | v2c | v3}
   ```

3. To restore the table to defaults (to clear the table), enter the following command:

   ```
   default snmp-server host
   ```

## Variable definitions

The following table describes the parameters for the **`no snmp-server host`** command.

| Variable | Value |
|---|---|
| *<A.B.C.D>* | Specifies the IP address of a trap destination host. |
| *<ipv6addr>* | Specifies the IPv6 address of the SNMP notification host. |
| v1 \| v2c \| v3 | Specifies the trap receivers in the SNMPv3 MIBs. |

# Displaying SNMP-server host-related information using ACLI

Use the following procedure to display SNMP-server host-related information.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show snmp-server host
   ```

### Example

The following figure provides an example of **show snmp-server host** command.

```
3524GT-PWR+#show snmp-server host
---------------------------------------------------------------------------
Notify Group: inform
  Type        : Inform
  Storage Type: Read-Only
  Status      : Active

---------------------------------------------------------------------------
Notify Group: s5AgTrpRcvr
  Type        : Trap
  Storage Type: Read-Only
  Status      : Active

---------------------------------------------------------------------------
Notify Group: trap
  Type        : Trap
  Storage Type: Read-Only
  Status      : Active
```

```
IPv6 Trap Destinations:

----More (q=Quit, space/return=Continue)----
```

# Setting SNMP community strings and access privileges using ACLI

Use the following procedure to create community strings with varying levels of read, write, and notification access based on SNMPv3 views. These community strings are separate from those created 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.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   snmp-server community <community-string> {read-view <view-name>|
   write-view <view-name>| notify-view <view-name>}
   ```

## Variable definitions

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

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

*Table continues…*

| Variable | Value |
|---|---|
| write-view <*view-name*> | Changes the write view used by the new community string for different types of SNMP operations.<br>• *view-name*—specifies the name of the view that is a set of MIB objects/instances that can be accessed; enter an alphanumeric string. |
| notify-view <*view-name*> | Changes the notify view settings used by the new community string for different types of SNMP operations.<br>• *view-name*—specifies the name of the view that is a set of MIB objects/instances that can be accessed; enter an alphanumeric string. |

# Displaying SNMPv3 configuration using ACLI

Use the following procedure to display the SNMPv3 configuration.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show snmp-server [community|host|user|view]
   ```

## Variable definitions

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

| Variable | Value |
|---|---|
| community\|host\|user\|view | Displays NMPv3 configuration information:<br>• community strings as configured in SNMPv3 MIBs (this parameter is not displayed when Password Security is enabled)<br>• trap receivers as configured in SNMPv3 MIBs<br>• SNMPv3 users, including views accessible to each other<br>• SNMPv3 views |

## Creating an initial set of configuration data for SNMPv3 using ACLI

Use the following procedure to create 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.

**Important:**

This command deletes all existing SNMP configurations, so use with caution.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

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

# Configuring MAC address filter-based security using ACLI

## Displaying MAC address security settings using ACLI

Use the following procedure to display configuration information for the BaySecure application.

### Before you begin

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show mac-security {config|mac-address-table [address <macadd>]|port|
security-lists\mac-da-filter}
```

### Example

The following figure provides a sample of **show mac-security** <config>.

```
3510GT-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
MAC Auto-Learning Age-Time: 60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Disabled
Learn by Ports: NONE
3510GT-PWR+(config)#
```

## Variable definitions

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

| Variable | Value |
|---|---|
| config | Displays the general BaySecure configuration |
| mac-address-table [address <macaddr>] | Displays contents of the BaySecure table of allowed MAC addresses:<br>• address specifies a single MAC address to display |
| mac-da-filter | Displays MAC DA filtering addresses. |
| port | Displays the BaySecure status of all ports |
| security-lists | Displays the port membership of all security lists. |

# Configuring MAC address security options using ACLI

Use the following procedure to modify the BaySecure configuration.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
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}] ]
```

## Variable definitions

The following table describes the parameters for the command.

| Variable | Value |
|---|---|
| auto-learning aging-time *<0-65535>* | Configures the maximum MAC address autolearn aging time.<br>RANGE: 0 to 65535 |
| disable\|enable | Disables or enables MAC address-based security. |
| filtering {enable\|disable} | Enables or disables destination address (DA) filtering when an intrusion is detected. |
| intrusion-detect {enable\|disable\|forever} | Specifies the partitioning of a port when an intrusion is detected:<br>• *enable*— port is partitioned for a period of time.<br>• *disabled*— port is not partitioned on detection.<br>• *forever*— port is partitioned until manually changed. |
| intrusion-timer *<0-65535>* | Temporary partition time in seconds.<br>Default value is 0. |
| learning {enable\|disable} | Specifies MAC address learning:<br>• *enable*— enables learning by ports<br>• *disable*— disables learning by ports<br>**Important:**<br>The MAC address learning enable command must be executed to specify learning ports. |
| learning-ports *<portlist>* | Specifies MAC address learning. Learned addresses are added to the table of allowed MAC addresses. Enter the ports you want to learn; this can be a single port, a range of ports, several ranges, all, or none. |
| mac-address-table | Adds addresses to the MAC security address table. |
| mac-da-filter | Adds or deletes MAC DA filtering addresses. |
| security-list | Modifies security list port membership. |
| snmp-lock {enable\|disable} | Enables or disables a lock on SNMP write-access to the BaySecure MIBs. |

## Adding addresses to MAC security address table using ACLI

Use the following procedure to assign 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.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

| Variable | Value |
|---|---|
| <H.H.H> | Enter the MAC address in the form of H.H.H. |
| port <portlist> | Enter the port number or the security list number.<br>**Important:**<br>In this command, portlist must specify only a single port. |

## Assigning a list of ports to a security list using ACLI

Use the following procedure to assign a list of ports to a security list.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
mac-security security-list <1--32> [add|remove] <portlist>
```

### Variable definitions

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

| Variable | Value |
|---|---|
| <1–32> | Enter the number of the security list that you want to use. |
| <portlist> | Enter a list or range of port numbers. |

## Disabling MAC source address-based security using ACLI

Use the following procedure to disable MAC source address-based security.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no mac-security
```

## Disabling MAC address auto-learning aging time using ACLI

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Clearing the MAC address security table using ACLI

Use the following procedure to clear entries from the MAC address security table.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

| Variable | Value |
|---|---|
| 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. |

## Clearing the port membership of a security list using ACLI

Use the following procedure to clear the port membership of a security list.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

| Variable | Value |
|---|---|
| <1–32> | Enter the number of the security list that you want to clear. |

## Configuring MAC security for specific ports using ACLI

Use the following procedure to configure the BaySecure status of specific ports.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

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

**Note:**

Auto-learning option is available when you do not specify the port value in the command.

### Variable definitions

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

| Variable | Value |
|---|---|
| port *<portlist>* | Specifies the port numbers. |
| auto-learning\|disable\|enable\|learning | Directs the specific port:<br>• auto-learning — configures MAC Auto-Learning |

*Table continues…*

| Variable | Value |
|---|---|
| | • disable — disables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is performed<br>• enable — enables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is performed<br>• learning — disables BaySecure on the specified port and adds these port to the list of ports for which MAC address learning is performed |

## Filtering packets from specified MAC DAs using ACLI

Use the following procedure to filter packets from up to 10 specified MAC DAs. You can also delete such a filter and then receive packets from the specified MAC DA.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

| Variable | Value |
|---|---|
| add\|delete\|<H.H.H> | Add or delete the specified MAC address, enter the MAC address in the form of H.H.H |

**Important:**

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

## Configuring MAC address autolearning using ACLI

Use the following procedures to configure MAC address auto-learning to automatically add allowed MAC addresses to the MAC security address table.

## Configuring MAC address auto-learning aging time using ACLI

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

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **`mac-security auto-learning aging-time`** command.

| Variable | Value |
|---|---|
| *<0–65535>* | Specifies the aging time period in minutes. A value of 0 indicates an infinite aging time period.<br>DEFAULT: 60 minutes<br>RANGE: 0 to 65535 |

## Disabling MAC address auto-learning aging time using ACLI

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Configuring MAC address auto-learning aging time to default using ACLI

Use the following procedure to 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. The default value is 60 minutes.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

# Viewing the current Sticky MAC address mode using ACLI

Use the following procedure to view the current Sticky MAC address mode.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show mac-security config
   ```

### Example

The following figure provides an example output of the **`show mac-security config`** command.

```
3524GT-PWR+>enable
3524GT-PWR+#config
Configuring from terminal or network [terminal]? terminal
Enter configuration commands, one per line.  End with CNTL/Z.
3524GT-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
MAC Auto-Learning Age-Time:  60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Disabled
Learn by Ports: NONE
```

# Enabling Sticky MAC address mode using ACLI

Use the following procedure to enable Sticky MAC address mode so that the system can secure the MAC address to a specified port and store automatically-learned MAC addresses across switch reboots.

### Before you begin

Avaya recommends that you disable autosave using the **`no autosave enable`** command when you enable Sticky MAC address.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   mac-security auto-learning sticky
   ```

# Disabling Sticky MAC address mode using ACLI

Use the following procedure to disable Sticky MAC address mode. The default state is disabled.

**Procedure**

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   no mac-security auto-learning sticky
   ```

   OR

   ```
   default mac-security auto-learning sticky
   ```

# Configuring EAPOL-based security using ACLI

Use the following procedures to configure security based on the Extensible Authentication Protocol over LAN (EAPOL).

**Important:**

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

## Enabling or disabling EAPOL-based security using ACLI

Use the following procedure to enable or disable EAPOL-based security.

**Procedure**

1. Log on to ACLI in Global Configuration command mode.
2. To enable EAPOL-based security, enter the following command:

   ```
   eapol enable
   ```

3. To disable EAPOL-based security, enter the following command:

   ```
   eapol disable
   ```

## Modifying EAPOL-based security parameters for a specific port using ACLI

Use the following procedure to modify EAPOL-based security parameters for a specific port.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
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}]
```

## Variable definitions

The following table describes the parameters for the **eapol** command.

| Variable | Value |
|---|---|
| init | Reinitiates EAP authentication. |
| max-request <num> | Enter the number of times to retry sending packets to supplicant. |
| port <portllist> | Specifies the ports to configure for EAPOL; enter the port numbers you want to use.<br>**Important:**<br>If you omit this parameter, the system uses the port number that you specified when you issued the **interface** command. |
| quiet-interval <num> | 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. |
| radius-dynamic-server enable | Enables the switch to process requests from the RADIUS Dynamic Authorization server. |
| re-authentication {enable\|disable} | Enables or disables reauthentication. |
| re-authentication-period <1-604800> | Specifies the number of seconds that you want between re-authentication attempts. Use either this variable or the reauthentication-interval variable; do not use both variables because they control the same setting. |
| re-authenticate | Specifies an immediate reauthentication. |
| server-timeout <num> | Specifies a waiting period for response from the server. Enter the number of seconds that you want to wait; the range is 1-65535. |
| status {authorized\|unauthorized\|auto} | Specifies the EAP status of the port:<br>• *authorized*— Port is always authorized.<br>• *unauthorized*— Port is always unauthorized. |

*Table continues…*

| Variable | Value |
|---|---|
| | • *auto*— Port authorization status depends on the result of the EAP authentication. |
| supplicant-timeout <num> | Specifies a waiting period for response from supplicant for all EAP packets, except EAP Request/Identity packets. Enter the number of seconds that you want to wait; the range is 1-65535. |
| traffic-control {in-out\|in} | Sets the level of traffic control:<br>• *in-out*— If EAP authentication fails, both ingressing and egressing traffic are blocked.<br>• *in*— If EAP authentication fails, only ingressing traffic is blocked. |

# Setting the guest VLAN for EAPOL using ACLI

Use the following procedure to set the guest VLAN globally.

### Procedure

1. Log on to ACLI in Global Configuration or Interface Configuration command mode.
2. At the command prompt, enter the following command:

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

## Variable definitions

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

| Variable | Value |
|---|---|
| vid <1–4094> | Specifies the Guest VLAN ID |
| enable | Enables Guest VLAN |

# Disabling guest VLAN for EAPOL using ACLI

Use the following procedure to disable the guest VLAN.

### Procedure

1. Log on to ACLI in Global Configuration or Interface Configuration command mode.
2. At the command prompt, enter the following command:

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

   OR

   ```
   default eapol guest-vlan
   ```

## Displaying the current EAPOL-based security status using ACLI

Use the following procedure to display the status of the EAPOL-based security.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

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

### Example

The following figure provides a sample of **show eapol**.

```
3524GT-PWR+#show eapol
EAPOL Administrative State:  Enabled
Port:  1
    Admin Status:  F Auth
    Auth:  Yes
    Admin Dir:  Both
    Oper Dir:  Both
    ReAuth Enable:  No
    ReAuth Period:  3600
    Quiet Period:  60
    Xmit Period:  30
    Supplic Timeout:  30
    Server Timeout:  30
    Max Req:  2
    RDS DSE:  No
Port:  2
    Admin Status:  F Auth
    Auth:  Yes
    Admin Dir:  Both
    Oper Dir:  Both
    ReAuth Enable:  No
    ReAuth Period:  3600
    Quiet Period:  60
```

## Displaying EAPOL diagnostics using ACLI

Use the following procedure to display EAPOL diags.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

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

### Example

The following figure provides a sample of **show eapol auth-diags interface**:.

```
3524GT-PWR+>enable
3524GT-PWR+#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)----
```

# Displaying EAPOL statistics using ACLI

Use the following procedure to display EAPOL statistics.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

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

### Example

The following figure provides a sample of **show eapol auth-stats interface**.

```
3524GT-PWR+#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
    EapLengthErrorFramesRx:  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)----
```

## Displaying EAPOL guest VLAN settings using ACLI

Use the following procedure to display the current guest VLAN configuration.

### Procedure

1. Log on to ACLI in Global Configuration or Interface Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   show eapol guest-vlan
   ```

### Example

The following figure provides a sample of **show eapol guest-vlan**.

```
3524GT-PWR+#show eapol guest-vlan
EAPOL Guest Vlan   :  Disabled
EAPOL Guest Vlan ID:  1
3524GT-PWR+#
```

# Configuring advanced EAPOL features using ACLI

Avaya Ethernet Routing Switch 3500 Series supports advanced EAPOL features that allow multiple hosts and non-EAPOL clients on a port.

## Configuring global EAPOL multihost settings

Use the following procedure to control the global multihost settings.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

| Variable | Value |
|---|---|
| adac-non-eap-enable | Allows authentication of non-EAP Phones using ADAC. |
| allow-non-eap-enable | Enables MAC addresses of non-EAP clients. |
| auto-non-eap-mhsa-enable | Enables auto-authentication of non-EAP clients in MHSA mode. |
| eap-packet-mode | Selects the packet mode for EAP authentication. Values are:<br>• mulitcast<br>• unicast |
| non-eap-phone-enable | Enables the use of non-EAP IP phone clients. |
| non-eap-use-radius-assigned-vlan | Enables the use of VLAN IDs assigned by RADIUS for non-EAP clients. |
| radius-non-eap-enable | Enables RADIUS authentication of non-EAP clients. |
| use-radius-assigned-vlan | Allows the use of RADIUS-assigned VLAN IDs. |
| non-eap-pwd-fmt *{[ip-addr][mac-addr][port-number]}* | Sets bits in RADIUS non-EAPOL password format. |

# Disabling EAPOL multihost settings using ACLI

Use the following procedure to disable EAPOL multihost settings.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no eapol multihost { [adac-non-eap-enable] [allow-non-eap-enable]
[auto-non-eap-mhsa-enable] [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]}]}
```

## Variable definitions

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

| Variable | Value |
|---|---|
| adac-non-eap-enable | Disables authentication of non-EAP Phones using ADAC. |
| allow-non-eap-enable | Disables control of MAC addresses of non-EAP clients. |
| auto-non-eap-mhsa-enable | Disables auto-authentication of non-EAP clients in MHSA mode. |

*Table continues…*

| Variable | Value |
|---|---|
| non-eap-phone-enable | Disables the use of non-EAP IP phone clients. |
| non-eap-use-radius-assigned-vlan | Disables the use of VLAN IDs assigned by RADIUS for non-EAP clients. |
| radius-non-eap-enable | Disables RADIUS authentication of non-EAP clients. |
| use-radius-assigned-vlan | Disables the use of RADIUS-assigned VLAN IDs. |
| non-eap-pwd-fmt *{[ip-addr][mac-addr][port-number]}* | Clears bits in RADIUS non-EAPOL password format. |

# Restoring EAPOL multihost settings to default using ACLI

Use the following procedure to set the EAPOL multihost feature to default.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Variable definitions

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

| Variable | Value |
|---|---|
| adac-non-eap-enable | Resets authentication of non-EAP Phones using ADAC. |
| allow-non-eap-enable | Resets control of MAC addresses of non-EAP clients. |
| auto-non-eap-mhsa-enable | Disables auto-authentication of non-EAP clients in MHSA mode. |
| eap-packet-mode | Specifies the type of packet used for initial EAP request for IDs. |
| non-eap-phone-enable | Disables the use of non-EAP IP phone clients |
| non-eap-use-radius-assigned-vlan | Disables the use of VLAN IDs assigned by RADIUS for non-EAP clients |
| radius-non-eap-enable | Disables RADIUS authentication of non-EAP clients. |
| use-radius-assigned-vlan | Disables the use of RADIUS-assigned VLAN IDs. |
| non-eap-pwd-fmt *{[ip-addr][mac-addr][port-number]}* | Restores default format for RADIUS non-EAPOL password attribute. |

# Configuring EAPOL multihost settings for a specific port or ports on an interface using ACLI

Use the following procedure to configure the multihost settings for a specific port or for all ports on an interface.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
eapol multihost [adac-non-eap-enable] [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>] [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}]
```

## Variable definitions

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

| Variable | Value |
|---|---|
| adac-non-eap-enable | Enables authentication of non-EAP Phones using ADAC. |
| allow-non-eap-enable | Enables MAC addresses of non-EAP clients. |
| auto-non-eap-mhsa-enable | Enables auto-authentication of non-EAP clients in MHSA mode. |
| eap-mac-max <1–32> | Specifies the maximum number of EAP-authenticated MAC addresses allowed. |
| eap-packet-mode <multicast\|unicast> | Specifies the type of packet used for initial EAP request for IDs. |
| enable | Allows EAP clients (MAC addresses). |
| non-eap-mac-max <1–32> | Specifies the maximum number of non-EAP authenticated MAC addresses allowed. |
| non-eap-phone-enable | Allows the use of non-EAP IP phone clients. |
| non-eap-use-radius-assigned-vlan | Allows the use of RADIUS assigned VLAN IDs for non-EAP clients. |
| port <portlist> | Specifies the port number or list of ports on which to apply EAPOL multihost settings. |
| radius-non-eap-enable | Enables RADIUS authentication of non-EAP clients. |
| use-radius-assigned-vlan | Allows the use of RADIUS-assigned VLAN value. |
| non-eap-mac {H.H.H \| port} | Allows non-EAPOL MAC address. |

# Disabling EAPOL multihost settings for a specific port or for all ports on an interface using ACLI

Use the following procedure to disable the EAPOL multihost settings for a specific port or for all ports on an interface.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
no eapol multihost [adac-non-eap-enable] [allow-non-eap-enable]
[auto-non-eap-mhsa-enable] [enable] [port <portlist>] [radius-non-
eap-enable] [use-radius-assigned-vlan] [non-eap-mac {H.H.H | port}]
```

## Variable definitions

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

| Variable | Value |
|---|---|
| adac-non-eap-enable | Disables authentication of non-EAP Phones using ADAC. |
| allow-non-eap-enable | Disables MAC addresses of non-EAP clients |
| auto-non-eap-mhsa-enable | Disables auto-authentication of non-EAP clients in MHSA mode. |
| enable | Disallows EAP clients (MAC addresses). |
| non-eap-phone-enable | Disables the use of non-EAP IP phone clients. |
| non-eap-use-radius-assigned-vlan | Disables the use of RADIUS assigned VLAN IDs for non-EAP clients. |
| port <portlist> | Specifies the port number or list of ports on which to apply EAPOL multihost settings. |
| radius-non-eap-enable | Disables RADIUS authentication of non-EAP clients. |
| use-radius-assigned-vlan | Disallows the use of RADIUS-assigned VLAN value. |
| non-eap-mac {H.H.H \| port} | Disallows non-EAPOL MAC address. |

# Restoring EAPOL multihost settings to default for a specific port or for all ports on an interface using ACLI

Use the following procedure to set the multihost settings for a specific port or for all the ports on an interface to default.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
default eapol multihost [adac-non-eap-enable] [allow-non-eap-enable]
[auto-non-eap-mhsa-enable] [eap-mac-max <1-32>] [enable] [non-eap-
mac-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}]
```

## Variable definitions

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

| Variable | Value |
|---|---|
| adac-non-eap-enable | Resets authentication of non-EAP Phones using ADAC. |
| allow-non-eap-enable | Resets control of non-EAP clients (MAC addresses) to default. |
| auto-non-eap-mhsa-enable | Disables auto-authentication of non-EAP clients. |
| eap-mac-max <1–32> | Resets the maximum number of EAP-authenticated MAC addresses allowed to default. |
| enable | Resets control of wheter EAP clients (MAC addresses) are allowed to default. |
| non-eap-mac-max <1–32> | Resets maximum number of non-EAP authenticated MAC addresses allowed to default. |
| non-eap-phone-enable | Disables the use of non-EAP IP phone clients. |
| non-eap-use-radius-assigned-vlan | Disables the use of RADIUS assigned VLAN IDs for non-EAP clients. |
| port <portlist> | Specifies the port number or list of ports on which to default the EAPOL multihost configuration. |
| radius-non-eap-enable | Resets RADIUS authentication of non-EAP clients to default. |
| use-radius-assigned-vlan | Disallows the use of RADIUS-assigned VLAN value. |
| non-eap-mac {H.H.H \| port} | Resets the non-EAPOL MAC addresses to default. |

# Configuring non-EAPOL MAC addresses on a specific port or on all ports on an interface using ACLI

Use the following procedure to configure the MAC addresses of non-EAPOL hosts on a specific port or on all ports on an interface.

### Procedure

1. Log on to ACLI Interface Configuration command mode.
2. At the command prompt, enter the following command:

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

## Variable definitions

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

| Variable | Value |
|---|---|
| port <portlist> | Specify the port or ports on which to apply EAPOL settings. |
| <H.H.H> | Specifies the MAC address of the allowed non-EAPOL host. |

# Displaying global settings for non-EAPOL hosts on EAPOL-enabled ports using ACLI

Use the following procedure to display global settings for non-EAPOL hosts on EAPOL-enabled ports.

### Procedure

1. Log on to ACLI in Privileged EXEC, Global Configuration, or Interface Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   show eapol multihost
   ```

### Example

The following figure provides a sample of **show eapol multihost**.

```
<>#sh eapol multihost
Allow Non-EAPOL Clients:  Disabled
Use RADIUS To Authenticate Non-EAPOL Clients:  Disabled
Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
Allow Non-EAPOL VoIP Phone Clients:  Enabled
EAPOL Request Packet Generation Mode:  Multicast
Allow Use of RADIUS Assigned VLANs:  Disabled
Allow Use of Non-Eapol RADIUS Assigned VLANs:  Disabled
Non-EAPOL RADIUS Password Attribute Format:  IpAddr.MACAddr.PortNumber
EAPOL Protocol:  Enabled
Use most recent RADIUS VLAN:  Disabled
Non-EAP re-authentication:  Disabled
Allow ADAC Non-Eap Phone Authentication:  Disabled
Fail Open VLAN:  Disabled
Fail Open VLAN ID:  1
```

### Variable definitions

The following table describes the parameters for the **show eapol multihost** command.

| Variable | Value |
|---|---|
| interface | Displays EAPOL multihost port configuration. |
| non-eap-mac | Displays allowed non-EAPOL MAC address. |
| status | Displays EAPOL multihost port status. |

## Displaying non-EAPOL support settings for each port using ACLI

### Procedure

1. Log on to ACLI in Privileged EXEC, Global Configuration, or Interface Configuration command mode.
2. At the command prompt, enter the following command:

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

### Example

The following figure provides a sample of **show eapol multihost interface** [<portList>].

```
<>#sh eapol multihost interface
Unit/Port:  1/1
    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 MHSA:  Disabled
    Allow Non-EAP Phones:  Disabled
    RADIUS Req Pkt Send Mode:  Multicast
    Allow RADIUS VLANs:  Disabled
    Allow Non-EAP RADIUS VLANs:  Disabled
    EAPOL Protocol:  Enabled
    Use most recent RADIUS VLAN:  Disabled
    Allow ADAC Non-Eap Phone Authentication:  Disabled
```

## Displaying non-EAPOL hosts information using ACLI

Use the following procedure to display information about non-EAPOL hosts currently active on the switch.

### Procedure

1. Log on to ACLI in Privileged EXEC, Global Configuration, or Interface Configuration command mode.
2. At the command prompt, enter the following command:

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

**Example**

The following figure provides a sample of **show eapol multihost non-eap-mac status**:.

```
3524GT-PWR+>enable
3524GT-PWR+#show eapol multihost non-eap-mac status
Port Client MAC Address State
---- ------------------ ------------------------------
Total number of authenticated clients: 0
3524GT-PWR+#
```

# Configuring support for non-EAPOL hosts on EAPOL-enabled ports using ACLI

Use the following procedures to configure non-EAPOL authentication.

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

1. Enable non-EAPOL support globaly on the switch and locally (for the desired interface ports), using one or both of the following authentication methods:
   a. local authentication
   b. RADIUS authentication
2. Enable EAPOL multihost on ports.
3. Specify the maximum number of non-EAPOL MAC addresses allowed on a port.
4. For local authentication only, identify the MAC addresses of non-EAPOL hosts allowed on the ports.

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 ACLI

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.

**Procedure**

1. To enable local authentication of non-EAPOL hosts globally on the switch, perform the following:
   a. Log on to ACLI in Global Configuration command mode.
   b. At the command prompt, enter the following command:

      ```
      eapol multihost allow-non-eap-enable
      ```
2. To enable local authentication of non-EAPOL hosts for a specific port or for all ports on an interface, perform the following:
   a. Log on to ACLI in Interface Configuration command mode.

b. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **eapol multihost** command.

| Variable | Value |
|---|---|
| port <portlist> | Specifies the port or list of ports on which you want to enable non-EAPOL hosts using local authentication. If you do not specify a port parameter, the command applies to all ports on the interface. |

## Enabling RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports using ACLI

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.

### Procedure

1. To enable RADIUS authentication of non-EAPOL hosts globally on the switch, perform the following:.
   a. Log on to ACLI in Global Configuration command mode.
   b. At the command prompt, enter the following command:

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

2. To enable RADIUS authentication of non-EAPOL hosts for a specific port or for all ports on an interface, perform the following:
   a. Log on to ACLI in Interface Configuration command mode.
   b. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **eapol multihost** command.

| Variable | Value |
|---|---|
| port <portlist> | Specifies the port or ports on which you want RADIUS authentication enabled. If you do not specify a port parameter, the command applies to all ports on the interface. |

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

Use the following procedure to configure the format of the RADIUS password when authenticating non-EAP MAC addresses using RADIUS.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **`eapol multihost non-eap-pwd-fmt`** command.

| Variable | Value |
|---|---|
| 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.

## Configuring the maximum number of non-EAPOL hosts allowed using ACLI

Use the following procedure to configure the maximum number of non-EAPOL hosts allowed for a specific port or for all ports on an interface.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
eapol multihost [port <portlist>] non-eap-mac-max <1-32>
```

### Variable definitions

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

| Variable | Value |
|---|---|
| port <portlist> | Specifies the port or ports to which you want the setting to apply. If you do not specify a port |

*Table continues…*

| Variable | Value |
|---|---|
| | parameter, the command sets the value for all ports on the interface. |
| <1–32> | Specifies the maximum number of non-EAPOL clients allowed on the port at any one time. The default is 1. |

**Important:**

The configurable maximum number of non-EAPOL clients for each port is 32, however Avaya expects that the usual maximum allowed for each port be lower. Avaya expects that the combined maximum will be approximately 200 per switch.

## Creating the allowed non-EAPOL MAC address list using ACLI

Use the following procedure to specify the MAC addresses of non-EAPOL hosts allowed on a specific port or on all ports on an interface for local authentication.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

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

| Variable | Value |
|---|---|
| port <portlist> | Specifies the port or ports on which you want to allow the specified non-EAPOL hosts. If you do not specify a port parameter, the command applies to all ports on the interface. |
| <H.H.H> | Specifies the MAC address of the allowed non-EAPOL host. |

## Enabling or disabling Non-EAP client re-authentication using ACLI

Use the following procedure to enable or disable non-EAP (NEAP) re-authentication for the switch.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable non-EAP re-authentication, enter the following command:

```
eapol multihost non-eap-reauthentication-enable
```

3. To disable non-EAP re-authentication, enter the following command:

```
no eapol multihost non-eap-reauthentication-enable
```

OR

```
default eapol multihost non-eap-reauthentication-enable
```

## Viewing the non-EAP client re-authentication status using ACLI

Use the following procedure to display the configuration status of NEAP re-authentication for the switch.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   show eapol multihost
   ```

### Example

The following figure provides a sample of **show eapol multihost**.

```
3524GT-PWR+>enable
3524GT-PWR+#show eapol multihost
Allow Non-EAPOL Clients:  Disabled
Use RADIUS To Authenticate Non-EAPOL Clients:  Disabled
Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
Allow Non-EAPOL VoIP Phone Clients:  Disabled
EAPOL Request Packet Generation Mode:  Multicast
Allow Use of RADIUS Assigned VLANs:  Disabled
Allow Use of Non-Eapol RADIUS Assigned VLANs:  Disabled
Non-EAPOL RADIUS Password Attribute Format:  IpAddr.MACAddr.PortNumber
Use most recent RADIUS VLAN:  Disabled
Non-EAP re-authentication:  Disabled
3524GT-PWR+#
```

## Clearing non-EAP authenticated clients from ports using ACLI

Use the following procedure to clear authenticated NEAP clients from a specified port.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   clear eapol non-eap [<portlist>] [address <H.H.H>]
   ```

### Variable definitions

The following table describes the parameters for the **`clear eapol non-eap`** command.

| Variable | Value |
|---|---|
| <portlist> | Specifies a port or ports from which to clear authenticated NEAP clients. If you do not specify a port parameter, the command applies to all ports. |
| address <H.H.H> | Specifies the MAC address of an authenticated NEAP client to clear from the port. |

*Table continues…*

| Variable | Value |
|---|---|
| | If you enter a MAC address value of 00:00:00:00:00:00, all authenticated NEAP clients are cleared from the specified port. |

# Configuring 802.1X or Non-EAP and Guest VLAN on the same port using ACLI

Use the following sections to allow 802.1X or Non-EAP devices to function with Guest VLAN enabled on the same port.

## Enabling EAPOL VoIP VLAN using ACLI

Use the following procedure to enable the EAPOL multihost VoIP VLAN.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
eapol multihost voip-vlan <1-5> {[enable] [vid <1-4094>}
```

### Variable definitions

The following table describes the parameters for the **`eapol multihost voip-vlan`** command.

| Variable | Value |
|---|---|
| enable | Enables the VoIP VLAN. |
| *<1–5>* | Specifies the number of VoIP VLAN.<br>RANGE: 1 to 5 |
| vid *<1–4094>* | Specifies the VLAN ID.<br>RANGE: 1 to 4094 |

## Disabling EAPOL VoIP VLAN using ACLI

Use the following procedure to disable the EAPOL multihost VoIP VLAN.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no eapol multihost voip-vlan <1-5> [enable]
```

### Variable definitions

The following table describes the parameters for the **no eapol multihost voip-vlan** ommand.

| Variable | Value |
|---|---|
| enable | Disables the VoIP VLAN. |
| <1–5> | Specifies the number of VoIP VLAN, range of 1 to 5. |

## Configuring EAPOL VoIP VLAN as the default VLAN using ACLI

Use the following procedure to configure the EAPOL multihost VoIP VLAN as the default setting.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
default eapol multihost voip-vlan <1-5> [enable] [vid]
```

### Variable definitions

The following table describes the parameters for the **default eapol mulihost voip-vlan** command.

| Variable | Value |
|---|---|
| enable | Enables the VoIP VLAN. |
| <1–5> | Specify the number of VoIP VLAN, range of 1 to 5. |
| vid | Default VoIP VLAN ID. |

## Viewing EAPOL VoIP VLAN using ACLI

Use the following procedure to display EAPOL multihost VoIP VLAN information.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
show eapol multihost voip-vlan
```

# Configuring TACACS+ using ACLI

Use the following section to configure TACACS+ to perform AAA services for system users.

## Configuring switch TACACS+ server settings using ACLI

Use the following procedure to configure switch TACACS+ server settings to add a TACACS+ server to your system.

### Before you begin

- Configure the TACACS+ server to add to your system.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
tacacs server {[host <A.B.C.D> | key <key> | port <1-65535> |
secondary-host <A.B.C.D> ]}
```

## Variable definitions

The following table describes the parameters for the **`tacacs server`** command.

| Variable | Value |
|---|---|
| host *<A.B.C.D>* | Specifies the IP address of the primary server to add or configure. |
| key *<key>* | Specifies the secret authentication and encryption key used for all communications between the NAS and the TACACS+ server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to confirm the key when you enter it.<br>**Important:**<br>The key parameter is a required parameter when you create a new server entry. The parameter is optional when you modify an existing entry. |
| port *<1–65535>* | Specifies the TCP port for TACACS+.<br>DEFAULT: 49 |
| secondary-host *<A.B.C.D>* | 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 ACLI

Use the following procedure to disable switch TACACS+ server settings to discontinue using TACACS+ services in your system.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   no tacacs server
   ```

   OR

   ```
   default tacacs server
   ```

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

## Enabling remote TACACS+ services using ACLI

Use the following procedure to enable remote TACACS+ services to provide services to remote users over serial or Telnet/SSH connections.

### Before you begin

- Configure a TACACS+ server on the switch before you enable remote TACACS+ services. See Configuring switch TACACS+ server settings using ACLI on page 154

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable remote TACACS+ services for serial connections, enter the following command:

   ```
   cli password serial tacacs
   ```

3. To enable remote TACACS+ services for Telnet connections, enter the following command:

   ```
   cli password telnet tacacs
   ```

## Enabling or disabling TACACS+ authorization using ACLI

Use the following procedure to enable or disable TACACS+ authorization globally on the switch.

TACACS+ authorization is disabled by default.

### Procedure

1. Log on to ACLI in Global Configuration command mode.

2. To enable TACACS+ authorization, enter the following command:

   ```
   tacacs authorization enable
   ```

3. To disable TACACS+ authorization, enter the following command:

   ```
   tacacs authorization disable
   ```

# Configuring TACACS+ authorization privilege levels using ACLI

Use the following procedure to configure TACACS+ authorization privilege levels to specify the privilege levels to which TACACS+ authorization applies.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   tacacs authorization level { ALL | <LINE> | NONE }
   ```

## Variable definitions

The following table describes the parameters 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 or a list of numerical values 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.<br><br>The default authorization level is NONE. |

# Enabling or disabling TACACS+ accounting using ACLI

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable TACACS+ accounting, enter the following command:

   ```
   tacacs accounting enable
   ```

3. To disable TACACS+ accounting, enter the following command:

   ```
   tacacs accounting disable
   ```

## Configuring the switch TACACS+ level using ACLI

Use the following procedure to configure the switch TACACS+ level to select a new level for a switch or use the last configured level.

**Procedure**

1. Log on to ACLI in Global Configuration command mode.
2. To configure a new TACACS+ level for a switch, enter the following command:

   ```
   tacacs switch level <1-15>
   ```

   If no level is specified, the switch TACACS+ level defaults to 15.
3. To use the last configured TACACS+ level for a switch, enter the following command:

   ```
   tacacs switch back
   ```

## Viewing TACACS+ information using ACLI

Use the following procedure to display TACACS+ configuration status.

**Procedure**

1. Log on to ACLI in Privilege EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show tacacs
   ```

# Configuring IP Manager using ACLI

## Enabling IP Manager using ACLI

Use the following procedure to enable IP Manager to control Telnet, SNMP, SSH, or HTTP access.

**Procedure**

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **ipmgr** command.

| Variable | Value |
|---|---|
| snmp | Enables the IP Manager list check for SNMP including Enterprise Device Manager. |
| ssh | Enables the IP Manager list check for SSH access. |
| telnet | Enables the IP Manager list check for telnet access. |
| web | Enables the IP Manager list check for web-based management system. |

## Disabling IP Manager using ACLI

Use the following procedure to disable IP Manager to discontinue controlling Telnet, SNMP, SSH, or HTTP access.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no ipmgr {snmp | ssh | telnet | web}
```

### Variable definitions

The following table describes the parameters for the **no ipmgr** command.

| Variable | Value |
|---|---|
| snmp | Enables the IP Manager list check for SNMP including Enterprise Device Manager. |
| ssh | Enables the IP Manager list check for SSH access. |
| telnet | Enables the IP Manager list check for telnet access. |
| web | Enables the IP Manager list check for web-based management system. |

## Configuring the IP Manager list for IPv4 addresses using ACLI

Use the following procedure to configure the IP Manager list to specify the source IP addresses or address ranges, with list IDs between 1 and 50, that have access to the switch when IP Manager is enabled.

### Procedure

1. Log on to ACLI in Global Configuration command mode.

2. At the command prompt, enter the following command:

```
ipmgr source-ip <listID> <ipv4addr> [mask <mask>]
```

## Variable definitions

The following table describes the parameters for the **ipmgr source-ip** command.

| Variable | Value |
|---|---|
| *<ipv4addr>* | Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation. |
| *<listID>* | Specifies an integer in the range 1 to 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 ACLI

Use the following procedure to configure the IP Manager list to specify the source IP addresses or address ranges, with list IDs between 51 and 100, that have access to the switch when IP Manager is enabled.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
ipmgr source-ip <listID> <ipv6addr/prefix>
```

## Variable definitions

The following table describes the parameters for the **ipmgr source-ip** command.

| Variable | Value |
|---|---|
| *<ipv6addr/prefix>* | Specifies the source IPv6 address and prefix from which access is allowed. |
| *<listID>* | Specifies an integer in the range 1 to 50 for IPv4 entries and 51–100 for IPv6 entries that uniquely identifies the entry in the IP Manager list. |

# Removing IP Manager list entries using ACLI

Use the following procedure to remove IP Manager list entries to deny access to the switch for specified source IP addresses or address ranges.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   no ipmgr source-ip [<listID>]
   ```

   The command sets both the IP address and mask for the specified entry to 255.255.255.255 for IPv4 entries, and to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/128 for IPv6 entries.

## Variable definitions

The following table describes the parameters for the **`no ipmgr source-ip`** command.

| Variable | Value |
|---|---|
| *<listID>* | 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.<br>If you do not specify a <listID>, the command resets the entire list to factory defaults. |

# Viewing the IP Manager configuration using ACLI

Use the following procedure to view the IP Manager configuration to review current IP manager configuration information.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show ipmgr
   ```

### Example

The following figure provides a sample of the **`show ipmgr`** command for IPv4 addresses (1–50).

```
3510GT-PWR+(config)#show ipmgr
TELNET Access: Enabled
SNMP Access:   Enabled
WEB Access:    Enabled
TELNET IP List Access Control:  Enabled
SNMP IP List Access Control:    Enabled
WEB IP List Access Control:     Enabled
Allowed Source IP Address   Allowed Sourced 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
----More   (q=Quit, space/return=Continue) ----
```

The following figure provides a sample of the **`show ipmgr`** command for IPv6 addresses (51–100).

```
Allowed Source IPv6 Address
-------------------------------------
51   ::/0
52  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
53  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
54  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
55  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
56  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
57  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
58  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
59  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
60  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
61  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
62  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
63  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
64  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
----More   (q=Quit, space/return=Continue) ----
```

# Configuring DHCP snooping using ACLI

## Enabling DHCP snooping globally using ACLI

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.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   ip dhcp-snooping enable
   ```

## Disabling DHCP snooping globally using ACLI

Disable DHCP snooping globally to discontinue DHCP snooping functionality at the VLAN and port level on the switch.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   no ip dhcp-snooping
   ```

   OR

   ```
   default ip dhcp-snooping
   ```

## Enabling DHCP snooping on a VLAN using ACLI

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.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   ip dhcp-snooping vlan <vlanID>
   ```

## Disabling DHCP snooping on a VLAN using ACLI

Disable DHCP snooping on a VLAN to discontinue DHCP snooping functionality on the VLAN.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   no ip dhcp-snooping vlan <vlanID>
   ```

## Configuring DHCP snooping port trust using ACLI

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

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
ip dhcp-snooping [port <portlist>] <trusted|untrusted>
```

## Variable definitions

The following table describes the parameters for the **ip dhcp-snooping** 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 ACLI

Configure DHCP snooping port trust to default to specify that a particular port or range of ports is untrusted.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
default ip dhcp-snooping <portlist>
```

## Variable definitions

The following table describes the parameters for the **default ip dhcp-snooping** 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 ACLI

View global DHCP snooping configuration information to review and confirm the DHCP snooping configuration for the switch.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
show ip dhcp-snooping
```

## Viewing VLAN DHCP snooping configuration information using ACLI

View VLAN DHCP snooping configuration information to review and confirm the DHCP snooping configuration for VLANs on the switch.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
show ip dhcp-snooping vlan
```

## Viewing DHCP snooping port trust information using ACLI

View DHCP snooping port trust information to review and confirm the port trust configuration for a port or list of ports.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
show ip dhcp-snooping interface [<interface type>] [<port>]
```

### Variable definitions

The following table describes the parameters for the **`show ip dhcp-snooping interface`** 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 ACLI

View the DHCP binding table to review current DHCP lease information.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Configuring DHCP Snooping Option 82 globally using ACLI

Before DHCP Snooping can function on a VLAN or port, you must enable DHCP Snooping globally. If DHCP Snooping is disabled globally, the switch forwards DHCP reply packets to all applicable ports, regardless of whether the port is trusted or untrusted.

Use this procedure to enable or disable DHCP Snooping for the switch.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
[default] [no] ip dhcp-snooping <enable> <option82>
```

### Variable definitions

The following table describes the parameters for the **`ip dhcp-snooping`** command.

| Variable | Value |
|---|---|
| enable | Enables DHCP Snooping globally on the switch. |
| default | Configures DHCP Snooping on the switch to default values. |
| no | Disables DHCP Snooping globally on the switch. |
| option82 | Enables DHCP Snooping with Option 82 globally on the switch. |

## Configuring port-based DHCP Snooping Option 82 subscriber ID using ACLI

Configure port-based DHCP Snooping to specify whether a port or group of ports are trusted or untrusted, and to assign an Option 82 subscriber ID to the port or ports.

For trusted ports, DHCP replies are forwarded automatically.

For untrusted ports, DHCP replies are filtered through DHCP Snooping.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. To configure port-based DHCP Snooping, enter the following command:

```
[default] [no] ip dhcp-snooping [port <portlist>] <trusted |
untrusted> option82-subscriber-id <WORD>
```

3. To return DHCP Snooping to default values for all interface ports, enter the following command:

```
[default] ip dhcp-snooping port all
```

## Variable definitions

The following table describes the parameters for the **`ip dhcp-snooping`** command.

| Variable | Value |
|---|---|
| default | Returns a port, or range of ports, to default DHCP Snooping values. |
| no | Removes the Option 82 for DHCP Snooping subscriber ID from a port. |
| option82 | Enables DHCP Snooping with Option 82 on a VLAN. |
| trusted | Specifies that the port or ports automatically forward DHCP replies. |
| untrusted | Specifies that the port or ports filter DHCP replies through DHCP Snooping. |
| WORD | Specifies the DHCP Option 82 subscriber ID for the port. The value is a character string between 1 and 255 characters. |

# Configuring VLAN-based DHCP Snooping Option 82 using ACLI

You must enable DHCP Snooping separately for each VLAN.

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

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] ip dhcp-snooping vlan <vlanID> <option82>
```

## Variable definitions

The following table describes the parameters for the **`ip dhcp-snooping vlan`** command.

| Variable | Value |
|---|---|
| default | Configures DHCP Snooping on a VLAN to the default value.<br>DEFAULT: disabled |

*Table continues…*

| Variable | Value |
|---|---|
| no | Disables DHCP Snooping on a VLAN. If you do not specify a VLAN ID, DHCP Snooping is disabled on all VLANs. |
| option82 | Enables DHCP Snooping with Option 82 on a VLAN. |
| vlanID | Specifies the ID of the preconfigured VLAN on which you want to enable DHCP Snooping.<br>RANGE: 1 to 4094 |

## Viewing DHCP Snooping using ACLI

Use the following procedure to display the state of DHCP Snooping and DHCP Snooping Option 82.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   show ip dhcp-snooping
   ```

### Example

The following figure provides an example output of the **`show ip dhcp-snooping`** command.

```
3524GT-PWR+#show ip dhcp-snooping
Global DHCP snooping state: Enabled
DHCP Snooping option82 is Disabled
       DHCP    DHCP Snooping
VLAN Snooping    option82
---- --------  -------------
1    Disabled   Disabled
3524GT-PWR+#
```

## Viewing DHCP Snooping for an interface using ACLI

Use the following procedure to display the state of DHCP Snooping and DHCP Snooping Option 82 for an interface.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   show ip dhcp-snooping interface
   ```

### Example

The following figure provides an example output of the **show ip dhcp-snooping interface** command.

```
3524GT-PWR+#show ip dhcp-snooping interface
       DHCP        ARP        Source        DHCP Snooping
Port Snooping   Inspection  Guard Mode  Option82 Subscriber Id
---- ---------  ----------  ----------  ----------------------
1    Untrusted  Untrusted   Disabled
2    Untrusted  Untrusted   Disabled
3    Untrusted  Untrusted   Disabled
4    Untrusted  Untrusted   Disabled
5    Untrusted  Untrusted   Disabled
6    Untrusted  Untrusted   Disabled
7    Untrusted  Untrusted   Disabled
8    Untrusted  Untrusted   Disabled
9    Untrusted  Untrusted   Disabled
10   Untrusted  Untrusted   Disabled
11   Untrusted  Untrusted   Disabled
12   Untrusted  Untrusted   Disabled
13   Untrusted  Untrusted   Disabled
14   Untrusted  Untrusted   Disabled
15   Untrusted  Untrusted   Disabled
16   Untrusted  Untrusted   Disabled
17   Untrusted  Untrusted   Disabled
18   Untrusted  Untrusted   Disabled
19   Untrusted  Untrusted   Disabled
----More (q=Quit, space/return=Continue)----
```

# Configuring dynamic ARP inspection using ACLI

## Displaying the ARP table using ACLI

Use this procedure to display the arp table of the device.

### Procedure

1. Log on to ACLI in User EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show arp-table
   ```

### Example

The following figure provides a sample of the **show arp-table** command.

```
3524GT-PWR+#show arp-table
Port IP Address      MAC Address
---- --------------- ----------------
2    172.16.120.1    00:0E:62:77:64:60
3524GT-PWR+#
```

## Enabling dynamic ARP inspection on a VLAN using ACLI

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.

### Before you begin

- Enable DHCP snooping globally on the switch. See Enabling DHCP snooping globally using ACLI on page 161

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
ip arp-inspection vlan <vlanID>
```

### Variable definitions

The following table describes the parameters for the **`ip arp-inspection vlan`** command.

| Variable | Value |
|---|---|
| <vlanID> | Specifies the VLAN in your network. Values range from 1 to 4094. |

## Disabling dynamic ARP inspection on a VLAN using ACLI

Disable dynamic ARP inspection on a VLAN to discontinue validating ARP packets transmitted.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no ip arp-inspection vlan <vlanID>
```

### Variable definitions

The following table describes the parameters for the **`no ip arp-inspection vlan`** command.

| Variable | Value |
|---|---|
| <vlanID> | Specifies the VLAN in your network. Values range from 1 to 4094. |

# Configuring dynamic ARP inspection port trust using ACLI

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.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
ip arp-inspection [port <LINE>] <trusted|untrusted>
```

## Variable definitions

The following table describes the parameters for the **`ip arp-inspection`** command.

| Variable | Value |
|---|---|
| port *<LINE>* | Specifies a port or list of ports. Use the format {slot/port[-slot/port][,...]}. |

# Configuring dynamic ARP inspection port trust to default using ACLI

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.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. Configure dynamic ARP inspection port trust to default on a single port or list of ports by using the following command:

```
default ip arp-inspection port <LINE>
```

3. Configure dynamic ARP inspection port trust to default on all ports on the switch by using the following command

```
default ip arp-inspection port all
```

## Variable definitions

The following table describes the parameters for the **`default ip arp-inspection port`** 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 ACLI

View VLAN dynamic ARP inspection configuration information to review VLANs on which dynamic ARP inspection is enabled.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
show ip arp-inspection vlan
```

## Viewing dynamic ARP inspection port trust information using ACLI

View dynamic ARP inspection port trust information to review and confirm the port trust configuration for a port or list of ports.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
show ip arp-inspection interface [<interface type>] [<port>]
```

### Variable definitions

The following table describes the parameters for the **`show ip arp-inspection interface`** command.

| Variable | Value |
|---|---|
| <interface type> | Specifies the type of interface (FastEthernet). |
| <port> | Specifies a port or list of ports. Use the format {slot/port[-slot/port][,...]}. |

# Configuring IP Source Guard using ACLI

### Before you begin

Before you can configure IP Source Guard, you must ensure the following:

- Dynamic Host Control Protocol (DHCP) snooping is globally enabled.

- The port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- The bsSourceGuardConfigMode MIB object exists.

  This MIB object is used to control the IP Source Guard mode on an interface.
- the following applications are not enabled:
  - IP Fix
  - Baysecure
  - EAPOL

**Important:**

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

# Enabling IP Source Guard using ACLI

Enable IP Source Guard to increase the security level to a port or ports by preventing IP spoofing.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

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

## Variable definitions

The following table describes the parameters for the **`ip verify source interface`** command.

| Variable | Value |
|---|---|
| <interface type> | Specifies the interface type of the interface on which you want IP Source Guard enabled. |
| <port> | Specifies the interface type of the interface on which you want IP Source Guard enabled |

# Viewing IP Source Guard port configuration information using ACLI

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

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.

2. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **show ip verify source** command.

| Variable | Value |
|---|---|
| <port> | Specifies the interface type of the interface on which you want IP Source Guard enabled. |
| <interface type> | Specifies the interface on which you want IP Source Guard enabled. |

## Viewing IP Guard-allowed addresses using ACLi

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

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **show ip source binding** command.

| Variable | Value |
|---|---|
| <A.B.C.D> | Specifies the IP address or group of addresses that IP Source Guard allowed. |
| <port> | Specifies the interface type of the interface on which you want IP Source Guard enabled. |
| <interface type> | Specifies the type of interface for which you want IP Source Guard-allowed addresses displayed. |

## Disabling IP Source Guard using ACLI

Disable IP Source Guard to transmit all IP traffic unfiltered.

### Procedure

1. Log on to ACLI in Ethernet, FastEthernet, or GigabitEthernet Interface Configuration command mode.

2. At the command prompt, enter the following command:

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

### Variable definitions

The following table describes the parameters for the **`no ip verify source interface`** command.

| Variable | Value |
|---|---|
| <port> | Specifies the interface type of the interface on which you want IP Source Guard enabled. |
| <interface type> | Specifies the interface on which you want IP Source Guard disabled. |

# Configuring 802.1X or non-EAP Last Assigned RADIUS VLAN using ACLI

## Enabling use of the most recent RADIUS VLAN

Use the following procedure to enable use of the most recent RADIUS assigned VLAN.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Disabling use of the most recent RADIUS VLAN

Use the following procedure to disable use of the most recent RADIUS assigned VLAN.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Restoring use of the most recent RADIUS VLAN to default

Use the following procedure to restore the use most recent RADIUS assigned VLAN status to default.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

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

## Displaying EAPOL multihost status

Use the following procedure to display EAPOL multihost information.

### Procedure

1. Log on to ACLI Privilege EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show eapol multihost
   ```

### Example

The following figure provides a sample of the **`show eapol multihost`** command.

```
3524GT-PWR+>enable
3524GT-PWR+#show eapol multihost
Allow Non-EAPOL Clients:  Disabled
Use RADIUS To Authenticate Non-EAPOL Clients:  Disabled
Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
Allow Non-EAPOL VoIP Phone Clients:  Disabled
EAPOL Request Packet Generation Mode:  Multicast
Allow Use of RADIUS Assigned VLANs:  Disabled
Allow Use of Non-Eapol RADIUS Assigned VLANs:  Disabled
Non-EAPOL RADIUS Password Attribute Format:  IpAddr.MACAddr.PortNumber
Use most recent RADIUS VLAN:  Disabled
Non-EAP re-authentication:  Disabled
3524GT-PWR+#
```

## Enabling EAPOL Fail Open VLAN

Use this procedure to enable the Fail Open VLAN.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   eapol multihost fail-open-vlan {[enable] [vid <1-4094>]}
   ```

### Variable definitions

The following table describes the parameters for the **`eapol multihost fail-open-vlan`** command.

| Variable | Value |
|---|---|
| enable | Enables the Fail Open VLAN. |
| vid *<1–4094>* | Specifies a Fail Open VLAN ID.<br>RANGE: 1 to 4094 |

## Disabling EAPOL Fail Open VLAN

Use this procedure to disable the Fail Open VLAN.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no eapol multihost fail-open-vlan [enable]
```

### Variable definitions

The following table describes the parameters for the **`no eapol multihost fail-open-vlan`** command.

| Variable | Value |
|---|---|
| [enable] | Disables the Fail Open VLAN.<br>**Note:**<br>This parameter is optional — not required to disable eapol multihost fail-open-vlan. |

## Displaying EAPOL Fail Open VLAN

Use the following procedure to display EAPOL Fail Open VLAN information.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

```
show eapol multihost fail-open-vlan
```

# Configuring Secure File Transfer Protocol using ACLI

## Viewing Secure File Transfer Protocol (SFTP)

Use the following procedure to view the current SFTP configuration.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   show sshc
   ```

### Example

The following figure provides an example output of the **show sshc** command.

```
3524GT-PWR+#show sshc
GLOBAL:
    Version                 :  Version 2 only
    DSA Auth Key            :  Does Not Exist
    DSA key size            :  512
    RSA Auth Key            :  Does Not Exist
    RSA key size            :  1024

SFTP:
    DSA Authentication      :  True
    RSA Authentication      :  False
    Password Authentication :  False
    User Name               :  admin
    SFTP Server Address     :  0.0.0.0
    Port                    :  22
```

## Variable definitions

The following table describes the parameters for the **show sshc** command.

| Variable | Value |
|---|---|
| Version | Displays the SSH version. Option 2 is the only valid option. |
| Port | Displays the SSH connection port.<br>RANGE: 1 to 65535<br>DEFAULT: 22 |
| Authentication Timeout | Displays the timeout interval in seconds.<br>DEFAULT: 30 |
| DSA Authentication | Displays the DSA Authentication state.<br>DEFAULT: True |

*Table continues…*

| Variable | Value |
|---|---|
| RSA Authentication | Displays the RSA Authentication state.<br>DEFAULT: True |
| User Name | Displays the user name.<br>DEFAULT: admin |
| SFTP Server Address | Displays the SFTP server IP address. |
| DSA Auth Key | Displays the authentication key if it is configured. |
| DSA key size | Displays the DSA key size as an integer.<br>RANGE: 512 to 1024<br>DEFAULT: 1024 |
| RSA Auth Key | Displays the authentication key if it is configured. |
| RSA key size | Displays the RSA key size as an integer (multiple of 128).<br>RANGE: 1024-2048<br>DEFAULT: 2048 |

# Setting SSHC authentication timeout

Use the following procedure to set the SSHC authentication timeout, in seconds, for a session.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   sshc timeout <1-120>
   ```

   The default is 30.

# Setting the SSHC port

Use the following procedure to set the SSHC port to accept new connections.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   sshc port <portnumber>
   ```

## Variable definitions

The following table describes the parameters for the **`sshc port`** command.

| Variable | Value |
|---|---|
| *<portnumber>* | Specifies the TCP port as a value from 1–65535. The default port is 22. |

## Enabling DSA authentication using ACLI

Use the following procedure to enable DSA authentication. Note that DSA authentication can be disabled using the [no] parameter with this command.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
ssh dsa-auth
```

### Variable definitions

The following table describes the parameters for the **`ssh dsa-auth`** command.

| Variable | Value |
|---|---|
| no | Disables DSA authentication. |

## Generating an SSHC DSA host key (public and private)

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
sshc dsa-host-key [force]
```

### Variable definitions

The following table describes the parameters for the **`sshc dsa-host-key`** command.

| Variable | Value |
|---|---|
| force | Specifies generation of a new SSHC DSA host key. No reset is required. |

## Deleting the SSHC DSA host keys (public and private)

Use the following procedure to delete the SSHC DSA host keys from the NVRAM. The DSA authentication state does not change.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
no sshc dsa-host-key
```

## Setting SSHC DSA host key size

Use the following procedure to set the SSHC DSA host key size and generate a new key at the next system reboot.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
sshc dsa-key <512-1024>
```

## Uploading the public host key

Use the following procedure to upload the SSHC auth key.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
sshc upload-host-key address <A.B.C.D | WORD> key-name <WORD>
```

### Variable definitions

The following table describes the parameters for the **`ssh upload-host-key`** command.

| Variable | Value |
|---|---|
| address <*A.B.C.D* \| *WORD*> | Specifies the TFTP server address.<br>• A.B.C.D is the IPv4 address format<br>• WORD is the IPv6 address format |
| key-name <*WORD*> | Specifies the TFTP filename. |

## Enabling password authentication using ACLI

Use the following procedure to enable password authentication. Note that password authentication can be disabled using the [no] parameter with this command.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable password authentication, enter the following command:

   ```
   ssh pass-auth
   ```

## Uploading a config file to an SFTP server using ACLI

Use the following procedure to upload a configuration file to an SFTP server using the SFTP protocol.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   copy config sftp address <A.B.C.D | WORD> filename [username <WORD>
   password <WORD>]
   ```

   **Notes:**

   - If you enter the **address** parameter, the system saves it as the default values.
   - If you do not enter the password and username, the command fails.
   - If you disable password authentication (that is, you enabled DSA key authentication), the command parameters **password** and **username** are optional and are not saved.

### Variable definitions

The following table describes the parameters for the **`copy config sftp`** command.

| Variable | Value |
|---|---|
| address <A.B.C.D \| WORD > | Specifies the address of the SFTP server as follows:<br>• A.B.C.D is the IPv4 address format<br>• WORD is the IPv6 address format |
| filename <WORD> | Specifies the configuration file name. |
| password <WORD> | Specifies the password. |
| username <WORD> | Specifies the username |

## Downloading a config file from an SFTP server using ACLI

Use the following procedure to download a configuration file from an SFTP server using the SFTP protocol.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   copy sftp config address <A.B.C.D | WORD> filename [username <WORD>
   password <WORD>]
   ```

   **Notes:**

   - If you enter the **address** and **filename** parameters, the system saves them as the default values.
   - If you enable password authentication (that is, you disabled the DSA key authentication), the command parameters **password** and **username** are required.
   - If you do not enter the password and username, the command fails.
   - If you disable password authentication (that is, you enabled DSA key authentication), the command parameters **password** and **username** are optional and are not saved.

## Variable definitions

The following table describes the parameters for the **`copy sftp config address`** command.

| Variable | Value |
|---|---|
| <A.B.C.D \| WORD> | Specifies the address of the SFTP server as follows:<br>• A.B.C.D is the IPv4 address format<br>• WORD is the IPv6 address format |
| filename <WORD> | Specifies the configuration file name. |
| password <WORD> | Specifies the password. |
| username <WORD> | Specifies the username. |

# Configuring IPv6 management using ACLI

## Enabling IPv6 globally using ACLI

Use the following procedure to enable IPv6 administration status for the switch.

IPv6 administration is disabled by default.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
ipv6 enable
```

## Enabling IPv6 interface on the management VLAN using ACLI

Use the following procedure to enable IPv6 administration for a VLAN.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

   ```
   interface vlan 1
   ipv6 interface enable
   ```

## Displaying the IPv6 interface information using ACLI

Use the following procedure to display IPv6 interface information.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show ipv6 interface
   ```

### Example

The following figure provides a sample of the **`show ipv6 interface`** command.

```
3524GT-PWR+#show ipv6 interface
==========================================================================
                                      Interface Information
==========================================================================
IFINDX VLAN-ID  MTU  PHYSICAL         ADMIN    OPER  RCHBLE  RETRAN  TYPE
                     ADDRESS          STATE    STATE TIME    TIME

--------------------------------------------------------------------------

==========================================================================
                                      Address Information
==========================================================================
INTF   IPV6                                    TYPE    ORIGIN    STATUS
INDEX  ADDRESS

--------------------------------------------------------------------------

0 out of 0 Total Num of Interface Entries displayed.

0 out of 0 Total Num of Address Entries displayed.
```

# Displaying IPv6 interface addresses using ACLI

Use the following procedure to view IPv6 interface addresses to learn the addresses.

### Procedure

1. Log on to ACLI in User EXEC command mode.
2. At the command prompt, enter the following command:

```
show ipv6 address interface [<WORD>]
```

## Variable definitions

The following table describes the parameters for the **`show ipv6 address`** command.

| Variable | Value |
|---|---|
| <WORD> | Specifies the IPv6 address. Length is 0 to 45. |

# Configuring IPv6 interface properties using ACLI

Use the following procedure to configure the IPv6 interface, create the VLAN IPv6 interface, and set the parameters.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:

```
ipv6 interface [address <ipv6_address/prefix_length>]
```

## Variable definitions

The following table describes the parameters for the **`ipv6 interface`** command.

| Variable | Value |
|---|---|
| all | Sets all variables to default settings. |
| address *<ipv6_address/prefix_length>* | Interface IPv6 address and mask prefix. |
| default ipv6 interface *[enable]* | Defaults all IPv6 interface parameters. |
| link-local *<WORD 0-19>* | Local link identifier. An alphanumeric value with a maximum of 19 characters. |
| mtu *<1280-9600>* | Default status: MTU 1500. |
| name *<1-255>* | Name: character string, from 1 to 255 in length. |

*Table continues…*

| Variable | Value |
|---|---|
| reachable-time *<0-3600000>* | Time in milliseconds neighbor is considered reachable after a reachable confirmation message. Default: 30000. |
| retransmit-timer *<0-3600000>* | Time in milliseconds between retransmissions of neighbor solicitation messages to a neighbor. Default: 1000. |

## Displaying the global IPv6 configuration using ACLI

Use the following procedure to display the IPv6 global configuration.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show ipv6 global
   ```

### Example

The following figure provides a sample of the **`show ipv6 global`** command.

```
3524GT-PWR+>enable
3524GT-PWR+#show ipv6 global
forwarding                      : disabled
default-hop-cnt                 : 30
number-of-interfaces            : 0
admin-status                    : disabled
icmp-error-interval             : 1000
icmp-redirect-msg               : disabled
icmp-unreach-msg                : disabled
multicast-admin-status          : disabled
icmp-error-quota                : 50
block-multicast-replies         : disabled
3524GT-PWR+#
```

## Configuring an IPv6 default gateway using ACLI

Use the following procedure to enable or disable an IPv6 default gateway.

### Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. To enable a default gateway, enter the following command:

   ```
   ipv6 default-gateway <WORD>
   ```

3. To disable a default gateway, enter the following command:

   ```
   no ipv6 default-gateway
   ```

## Displaying the IPv6 default gateway using ACLI

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show ipv6 default-gateway
   ```

## Configuring the IPv6 neighbor cache using ACLI

Use the following procedure to add or remove a static neighbor cache entry.

### Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To add a static neighbor cache entry, enter the following command:

   ```
   ipv6 neighbor <ipv6_address> port <unit/port> mac <mac_addr>
   ```

3. To remove a static neighbor cache entry, enter the following command:

   ```
   no ipv6 neighbor <ipv6_address>
   ```

## Displaying the IPv6 neighbor information using ACLI

Use the following command to display IPv6 neighbor information.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show ipv6 neighbor [<ipv6_address>] [type {other | dynamic | static
   | local}]
   ```

### Example

The following figure provides a sample of the **`show ipv6 neighbor`** command.

```
3524GT-PWR+#show ipv6 neighbor

NET ADDRESS/           PHYS     TYPE    STATE
LAST
PHYSICAL ADDRESS       INTF   UPD
-------------------------------------------------------------------------------
2000::31/                      1/11   DYNAMIC REACHABLE  118
fc:a8:41:fb:c8:00
2000::40/                      V-1    LOCAL   REACHABLE  70
a0:51:c6:51:5c:00
```

```
2000::55/                       1/11   DYNAMIC STALE      121
1c:6f:65:a7:35:f6
fe80::1e6f:65ff:fea7:35f6/      1/11   DYNAMIC REACHABLE  102
1c:6f:65:a7:35:f6
fe80::a251:c6ff:fe51:5c00/      V-1    LOCAL   REACHABLE  70
a0:51:c6:51:5c:005

out of 5 Total Num of Neighbor Entries displayed.
```

# Displaying IPv6 interface ICMP statistics using ACLI

Use the following procedure to display IPv6 interface ICMP statistics.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   `show ipv6 interface icmpstatistics`

### Example

The following figure provides a sample of the **`show ipv6 interface icmpstatistics`** command.

```
3524GT-PWR+#show ipv6 interface icmpstatistics
================================================================================
                                        Icmp Stats
================================================================================
0 out of 0 Total Num of Interface Entries displayed.
3524GT-PWR+#
```

# Displaying IPv6 interface statistics using ACLI

Use the following procedure to display IPv6 interface statistics.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   `show ipv6 interface statistics`

### Example

The following figure provides a sample of the **`show ipv6 interface statistics`** command.

```
3524GT-PWR+#show ipv6 interface statistics
=========================================================================
                                        Interface Stats
=========================================================================

Icmp stats for IfIndex = 10001
IcmpInMsgs: 11
IcmpInErrors: 0
IcmpInDestUnreachs : 1
```

```
IcmpInAdminProhibs : 0
IcmpInTimeExcds : 0
IcmpInParmProblems : 0
IcmpInPktTooBigs : 0
IcmpInEchos : 1
IcmpInEchoReplies : 3
IcmpInRouterSolicits : 0
IcmpInRouterAdverts : 0
InNeighborSolicits : 3
InNbrAdverts : 3
IcmpInRedirects : 0
IcmpInGroupMembQueries : 0
IcmpInGroupMembResponses : 0
IcmpInGroupMembReductions : 0
IcmpOutMsgs : 22
IcmpOutErrors : 1
IcmpOutDestUnreachs : 0
IcmpOutAdminProhibs : 0
IcmpOutTimeExcds : 0
IcmpOutParmProblems : 0
IcmpOutPktTooBigs : 0
IcmpOutEchos : 4
IcmpOutEchoReplies : 1
IcmpOutRouterSolicits : 3
IcmpOutRouterAdvertisements : 0
IcmpOutNeighborSolicits : 8
IcmpOutNeighborAdvertisements : 5
IcmpOutRedirects : 0
IcmpOutGroupMembQueries : 0
IcmpOutGroupMembResponses : 7
IcmpOutGroupMembReductions : 0

1 out of 1 Total Num of Interface Entries displayed.
```

## Displaying IPv6 TCP connections using ACLI

Use the following procedure to display IPv6 TCP connections.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show ipv6 tcp connections
   ```

## Displaying IPv6 TCP listeners using ACLI

Use the following procedure to display IPv6 TCP listeners.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show ipv6 tcp listener
   ```

## Displaying IPv6 TCP statistics using ACLI

Use the following procedure to display IPv6 TCP statistics.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:

   ```
   show ipv6 tcp
   ```

### Example

The following figure provides a sample of the **`show ipv6 tcp`** command.

```
3524GT-PWR+#show ipv6 tcp

show ipv6 tcp global statistics:
------------------
ActiveOpens:        0
PassiveOpens:       0
AttemptFails:       0
EstabResets:        0
CurrEstab:          0
InSegs:             0
OutSegs:            0
RetransSegs:        0
InErrs:             0
OutRsts:            0
HCInSegs:           0
HCOutSegs:          0
3524GT-PWR+#
```

## Displaying IPv6 UDP statistics and endpoints using ACLI

Use the following procedure to display IPv6 UDP statistics and endpoints.

### Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. To display UDP statistics, enter the following command:

   ```
   show ipv6 udp
   ```

3. To display UDP endpoints, enter the following command:

   ```
   show ipv6 udp endpoints
   ```

# Configuring storm control using ACLI

Use the following procedures to configure storm control using ACLI

### Configuring storm control globally

1. Enter the Global Configuration mode in ACLI.
2. Enter the following command:

   **storm-control [broadcast | multicast | unicast | all] [action [none | drop | shutdown ]] [enable] [high-watermark <10-100000000>] [low-watermark <10-100000000>] [poll-interval <5-300>] [trap-interval <0-1000]**

Variable definitions

| Variable | Value |
|---|---|
| action | Sets the storm Control action |
| enable | Enable storm control |
| high-watermark | Set high-watermark in pps |
| low-watermark | Set low-watermark in pps |
| poll-interval | Set interval for watermark checking (seconds) |
| trap-interval | Set trap sending interval in poll-intervals when above high-watermark (0= do not send) |

### Disabling storm control

Use the following command to disable Storm Control

1. Enter the Global Configuration mode in ACLI.
2. Enter the following command at the command prompt:

   **no storm-control [broadcast | multicast | unicast | all] enable**

### Displaying Global Storm Control state

Use the following command to display the Global Storm Control state:

1. Enter the Pvil Exec mode in ACLI.
2. Enter the following command at the command prompt:

   **show storm-control [broadcast | multicast | unicast | all]**

### Configuration example for displaying the Global Storm Control state

```
3526T-PWR+(config)#show storm-control all
Storm Control Status   High Wm     Low Wm     Poll    Action      Trap
--------------------   --------   --------   -----   ---------   ----
Unicast     Disabled    1000        100        5       none        0
Broadcast   Disabled    1000        100        5       none        0
Multicast   Disabled    1000        100        5       none        0
```

# Displaying rate limit configuration using ACLI

Display rate limit configuration to view settings and statistics.

### Procedure

1. Logon to the ACLI in Privileged EXEC mode.
2. At the command prompt, enter the following command:

   ```
   show rate-limit
   ```

3. 

### Example

The following figure displays sample output from the **`show rate-limit`** command.

```
3510GT-PWR+show rate-limit
Packet Type     Limit
-----------     -----
Both            0 pps
3510GT-PWR+#
```

# Configuring rate limiting using ACLI

Configure rate limiting in packets per second for the specified traffic type: either multicast, broadcast, or both.

### Procedure

1. Logon to the ACLI Global Configuration Mode.
2. At the command prompt, enter the following command:

   ```
   [no] [default] rate-limit [multicast|broadcast|both] <0-262143>
   ```

## Variable definitions

The following table describes the parameters for the **`rate-limit`** command.

| Variable | Value |
|---|---|
| multicast \|broadcast \| both | Applies rate limiting, in packets/second, to the specified type of traffic:<br>• multicast — applies rate limiting to multicast packets<br>• broadcast — applies rate limiting to broadcast packets |

*Table continues…*

| Variable | Value |
| --- | --- |
| | • both — applies rate limiting to both multicast and broadcast packets |
| *<0–262143>* | Sets the pps (Packets Per Second) upper threshold limit for the traffic type. When the volume of packets exceeds this threshold, packets are dropped. The pps value you set is a small percent of the maximum value of pps for the total available bandwidth (262143 pps). |
| no | Disables rate limiting on the switch or stack |
| default | Restores the default value for rate limiting for the switch or stack |

# Chapter 7: Configuring and managing security using EDM

## 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. Use the procedures in this chapter to configure switch security using Enterprise Device Manager (EDM).

## Setting the switch HTTP/HTTPS port using EDM

Use the following procedure to configure HTTP/HTTPS port parameters for the switch:

### Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **General**.
3. On the **Http/Https** tab, configure the HTTP/HTTPS parameters as required.
4. On the toolbar, click **Apply**.

### Variable definitions

The following table describes the fields of Http/Https tab.

| Variable | Value |
|---|---|
| HttpPort | Specifies a value for the switch HTTP port, ranging from 1024 to 65535. The default value is 80. |
| HttpsPort | Specifies a value for the switch HTTPS port, ranging from 1024 to 65535. The default value is 443. |
| SecureOnly | Configures the Web server to respond to HTTPS only, or both HTTPS and HTTP client browser requests. |

*Table continues…*

| Variable | Value |
|---|---|
| | **Note:**<br>If you configure the Web server to respond to HTTPS client browser requests only, all existing non-secure connections with the browser are terminated. |

# Configuring EAPOL using EDM

Use the procedures in this section to configure network access control on an internal Local Area Network (LAN) with Extensible Authentication Protocol over LAN (EAPOL), using Enterprise Device Manager..

**Important:**

You must enable EAPOL before you enable features, such as UDP Forwarding and IP Source Guard, that use QoS policies.

## Configuring EAPOL globally using EDM

Use this procedure to configure EAPOL globally and to set and view EAPOL security information for the switch.

**Important:**

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

### Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, 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**.

## EAPOL tab field descriptions

The following table describes the fields on the EAPOL tab.

| Name | Description |
|---|---|
| **SystemAuthControl** | Enables or disables EAPOL for your switch. When this field is set to disabled (the default state), the |

*Table continues…*

| Name | Description |
|---|---|
| | 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.<br><br>The GuestVlanEnabled field must be selected to provide ports with access to the global default Guest VLAN. |
| **MultiHostAllowNonEapClient (MAC addresses)** | This object controls whether locally authenticated 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 Avaya 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 |
| **MultiHostUseMostRecentRadiusAssignedVlan** | Enables or disables the use of the most recent RADIUS VLAN.<br><br>**Note:**<br><br>You must also enable MultiHostUseMostRecentRadiusAssignedVlan on each port to enable the feature. |
| **MultiHostEapPacketMode** | Specifies the packet mode, either unicast or multicast, in the Multihost mode. |
| **MultiHostFailOpenVlanEnabled** | Enables or disables the EAPOL multihost Fail Open VLAN. Default is disabled. |
| **MultiHostFailOpenVlanId** | Configure the VLAN ID of the Fail Open VLAN or accept the default of VLAN ID 1. |

*Table continues…*

| Name | Description |
| --- | --- |
| | **Note:**<br>The switch does not validate that the RADIUS-assigned VLAN attribute is different than the Fail Open VLAN. Do not configure a Fail Open VLAN name or ID with the same name of a RADIUS VLAN name or ID. Using the same name can cause EAP or Non-EAP clients to assign to the Fail Open VLAN even if a RADIUS server connection failure did not occur. |
| **NonEAPRadiusPasswordAttributeFormat** | Specifies the format of the RADIUS Server password attribute for non-EAP clients; either IP address, MAC address, or port number. |
| **MultiHostNeapReauthenticationEnabled** | Enables or disables the non-EAP client re-authentication. Default is disabled. |
| **MultiHostAdacNonEapEnabled** | Enables or disables the non-EAP multihost ADAC settings. |

## Enabling or disabling non-EAP client re-authentication using EDM

Use this procedure to enable or disable Non-EAP (NEAP) re-authentication for the switch.

### Procedure

1. In the navigation tree, double-click **Security**.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **EAPOL** tab.
4. Perform one of the following:
   - Select the **MultiHostNeapReauthenticationEnabled** checkbox to enable NEAP re-authentication.
   - Clear the **MultiHostNeapReauthenticationEnabled** checkbox to disable NEAP re-authentication.
5. On the toolbar, click **Apply**.

## Configuring multihost EAP VoIP VLAN using EDM

Use this procedure to activate the multihost VoIP VLAN. You can allow 802.1X or Non-EAP devices to function with the Guest VLAN enabled on the same port.

### Procedure

1. In the navigation tree, double-click **Security** to open the security tree.

2. In the security tree, click **802.1X/EAP**.
3. In the work area, click the **EAP VoIP VLAN** tab.
4. In the table, double-click the cell under the column you want to edit.
5. Select a parameter or value form the drop-down list
6. Repeat steps 4 and 5 to configure other parameters.
7. On the toolbar, click **Apply**.

## EAP VoIP Vlan tab field descriptions

The following table describes the fields on the EAP VoIP VLAN tab.

| Name | Description |
|---|---|
| **MultiHostVoipVlanIndex** | Indicates the multihost VoIP VLAN index, range of 1 to 5. |
| **MultiHostVoipVlanEnabled** | Enables (true) or disables (false) the multihost VoIP VLAN. |
| **MultiHostVoipVlanId** | Indicates the VLAN ID, range of 1 to 4094. |

# Configuring port-based EAPOL using EDM

Use this procedure to configure EAPOL security parameters for an individual port or multiple ports.

### Procedure

1. In the navigation tree, double-click **Security** to open the security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **EAPOL Ports** tab.
4. In a port row, double-click a cell under the column heading for the parameter you want to change.
5. Select a parameter or value from the drop-down list.
6. Repeat the previous two steps to configure other parameters.
7. On the toolbar, click **Apply**.

## EAPOL Ports tab field descriptions

The following table describes the fields on the EAPOL Ports tab.

| Name | Description |
|---|---|
| **PortNumber** | Indicates the port number. |

*Table continues…*

| Name | Description |
|---|---|
| **PortProtocolVersion** | Indicates the EAP Protocol version that is running on this port. |
| **PortCapabilities** | Indicates the PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable. |
| **PortInitialize** | Enables and disables EAPOL authentication for the specified port. |
| **PortReauthenticateNow** | Enables (true) EAPOL authentication for the specified port immediately, without waiting for the Re-Authentication Period to expire. |
| **PaeState** | Indicates the EAPOL authorization status for the switch: |
| **BackendAuthState** | Indicates the current state of the Backend Authentication state for the switch. |
| **AdminControlledDirections** | Indicates the current EAPOL authentication for the port:<br>• **both**: Incoming and outgoing traffic<br>• **in**: Incoming traffic only<br>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** | Indicates the current operational value for the traffic control direction for the port (see the preceding field description). |
| **AuthControlledPortStatus** | Indicates the current EAPOL authorization status for the port:<br>• **authorized**<br>• **unauthorized** |
| **AuthControlledPortControl** | Indicates the EAPOL authorization status for the port:<br>• **Force Authorized**: The authorization status is always authorized<br>• **Force Unauthorized**: The authorization status is always unauthorized<br>• **Auto**: The authorization status depends on the EAP authentication |
| **QuietPeriod** | Indicates the current value of the time interval between any single EAPOL authentication failure |

*Table continues…*

| Name | Description |
|---|---|
| | and the start of a new EAPOL authentication attempt. |
| **TransmitPeriod** | Indicates the time to wait for response from supplicant for EAP requests/Identity packets. |
| **SupplicantTimeout** | Indicates the time to wait for response from supplicant for all EAP packets, except EAP Request/Identity. |
| **ServerTimeout** | Indicates the time to wait for a response from the RADIUS server for all EAP packets. |
| **MaximumRequests** | Indicates the number of times the switch attempts to resend EAP packets to a supplicant. |
| **ReAuthentication Period** | Indicates the 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** | Indicates if reauthentication is 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** | Indicates 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** | Indicates the protocol version number carried in the most recently received EAPOL frame. |
| **LastEapolFrame Source** | Indicates the source MAC address carried in the most recently received EAPOL frame. |

## Configuring advanced port-based EAPOL using EDM

Use this procedure to configure advanced port-based EAPOL for an individual port or multiple ports.

### Procedure

1. In 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 Advance Ports** tab.
4. In a port row, double-click a cell under the column heading for the parameter you want to change.

5. Select a parameter or value from the drop-down list.
6. Repeat the previous two steps to configure other parameters.
7. On the toolbar, click **Apply**.

## EAPOL Advance Ports tab field descriptions

The following table describes the fields on the EAPOL Advance Ports tab.

| Name | Description |
|---|---|
| **PortNumber** | Specifies the port number. |
| **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 is 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 Avaya 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). |
| **ProcessRadiusRequestsServerPackets (RADIUS Dynamic Authorization Server)** | Enables or disables the processing of RADIUS requests-server packets that are received on this port. |
| **MultiHostClearNeap** | Clears a specific, or all authenticated, NEAP clients from the port. To clear a specific client on a port, |

*Table continues…*

| Name | Description |
|---|---|
| | enter the MAC address of the client. To clear all clients on a port, enter 00:00:00:00:00:00. |
| **MultiHostAdacNonEapEnabled** | Enables or disables the non-EAP multihost ADAC settings. |

# Clearing Non-EAP authenticated clients from ports using EDM

Use this procedure to clear authenticated NEAP clients from a specified port.

### Procedure

1. In the navigation tree, double-click **Security** .
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **EAPOL Advance Ports** tab.
4. Click a port row to select a port.
5. Double-click the cell under the **MultiHostClearNeap** column heading.
6. Perform one of the following:
   - To clear a specific authenticated NEAP client from the specified port, type the MAC address of that client in the box.
   - To clear all authenticated NEAP clients from the specified port, type a MAC address of 00:00:00:00:00:00 in the box.
7. On the toolbar, click **Apply**.

# Viewing Multihost status information using EDM

Use this procedure to display multiple host status for a port.

### Procedure

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**.
5. Click the **Multi Host Status** tab.

## Multi Host Status tab field descriptions

The following table describes the fields on the Multi Host Status tab.

| Name | Description |
|---|---|
| **PortNumber** | The port number in use. |
| **ClientMACAddr** | The MAC address of the client. |
| **PaeState** | The current state of the authenticator PAE state machine. |
| **BackendAuthState** | The current state of the Backend Authentication state machine. |
| **Reauthenticate** | The current reauthentication state of the machine. When the reauthenticate attribute is set to True, the client reauthenticates. |

# Viewing Multihost session information using EDM

Use this procedure to view Multihost session information for a port.

### Procedure

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.

## Multi Host Session tab field descriptions

The following table describes the fields on the Multi Host Session tab.

| Name | Description |
|---|---|
| **PortNumber** | The port number in use. |
| **ClientMACAddr** | The MAC address of the client. |
| **AuthenticMethod** | The authentication method used to establish the session. |
| **Time** | The elapsed time of the session. |
| **UserName** | The user name representing the identity of the supplicant PAE. |

# Viewing Multihost DHCP authenticated information

Use this procedure to display mutiple host DHCP authenticated information for a port.

### Procedure

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 DHCP Authenticated** tab.

## Multi Host DHCP Authenticated tab field descriptions

The following table describes the fields on the Multi Host DHCP Authenticated tab.

| Name | Description |
|---|---|
| **PortNumber** | Specifies the port number. |
| **ClientMACAddr** | Specifies the MAC address of the client. |
| **UserName** | Specifies the user name representing the identity of the supplicant PAE. |

# Adding a MAC address to the allowed non-EAP MAC address list using EDM

Use 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

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**.

## Allowed non-EAP MAC tab field descriptions

The following table describes the fields on the Allowed non-EAP MAC tab.

| Name | Description |
|---|---|
| **PortNumber** | The port number in use. |
| **ClientMACAddr** | The MAC address of the client. |

# Deleting a MAC address from the allowed non-EAP MAC address list using EDM

Use 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

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.

## Allowed non-EAP MAC tab field descriptions

The following table describes the fields on the Allowed non-EAP MAC tab.

| Name | Description |
|---|---|
| **PortNumber** | The port number in use. |
| **ClientMACAddr** | The MAC address of the client. |

# Viewing port non-EAP host support status using EDM

Use this procedure to view non-EAP host support status for a port.

### Procedure

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.

## Non-EAP Status tab field descriptions

The following table describes the fields on the Non-EAP Status tab.

| Name | Description |
|---|---|
| **PortNumber** | The port number in use. |
| **ClientMACAddr** | The MAC address of the client. |
| **State** | The authentication status. Possible values are:<br>• **rejected**: the MAC address cannot be authenticated on this port.<br>• **locallyAuthenticated**: the MAC address was authenticated using the local table of allowed clients.<br>• **radiusPending**: the MAC address is awaiting authentication by a RADIUS server.<br>• **radiusAuthenticated**: the MAC address was authenticated by a RADIUS server.<br>• **adacAuthenticated**: the MAC address was authenticated using ADAC configuration tables.<br>• **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

Use this procedure to create a graph of port EAPOL statistics.

### Procedure

1. In 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 Stats** tab.
4. Click a row to graph.
5. From the toolbar, select a graph type to create a graph.

## EAPOL Stats tab field descriptions

The following table describes the fields on the EAPOL Stats tab.

| Name | Description |
|---|---|
| **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

Use this procedure to create a graph of port EAPOL diagnostic statistics.

### Procedure

1. In the navigation tree, double-click **Graph** to open the Graph tree.
2. From the Graph tree, 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.

## EAPOL Diag tab field descriptions

The following table describes the fields on the EAPOL Diag tab.

| Name | Description |
|---|---|
| **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. |
| **AuthSuccessWhileAuthenticating** | 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. |
| **AuthTimeoutsWhileAuthenticating** | 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. |
| **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, |

*Table continues…*

| Name | Description |
|---|---|
| | 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. |
| **BackendOtherRequestsTo Supplicant** | 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. |
| **BackendNonNakResponsesFromSupplicant** | 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. |

# Configuring TACACS using EDM

Use the procedures in this section to configure TACACS+ to perform AAA services for system users.

## Enabling or disabling TACACS+ accounting using EDM

Use this procedure to enable or disable TACACS+ accounting using EDM.

### Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **TACACS+**
3. In the work area, click the **Globals** tab.
4. Perform one of the following:
   - To enable accounting, select the **Accounting** checkbox.
   - To disable accounting, deselect the **Accounting** checkbox.
5. On the toolbar, click **Apply**.

## Globals tab field descriptions

The following table describes the fields on the Globals tab.

| Name | Description |
|---|---|
| **Accounting** | Enables or disables accounting:<br>• Select the checkbox to enable accounting<br>• Deselect the checkbox to disable accounting |

# Enabling or disabling TACACS+ authorization using EDM

Use this procedure to enable or disable TACACS+ accounting using EDM.

### Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **TACACS+**
3. In the work area, click the **Globals** tab.
4. Perform one of the following:
   - To enable authorization, select the **AuthorizationEnabled** checkbox .
   - To disable authorization, deselect the **AuthorizationEnabled** checkbox.
5. On the toolbar, click **Apply**.

## Globals tab field descriptions

The following table describes the fields on the Globals tab.

| Name | Description |
|---|---|
| **AuthorizationEnabled** | Enable or disable the authorization feature. |

## Configuring the switch TACACS+ levels using EDM

Use this procedure to configure the switch TACACS+ levels using EDM.

### Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, 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**.

### Globals tab field descriptions

The following table describes the fields on the Globals tab.

| Name | Description |
|---|---|
| **AuthorizationLevels <0–15>** | This object controls which ACLI command privilege levels will be authorized by TACACS+. |

## Creating a TACACS+ server using EDM

Use this procedure to create a TACACS+ server.

### Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, 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 **Address** field, enter the IP address of the TACACS+ server.
6. In the **PortNumber** field, enter the TCP port on which the client establishes a connection to the server.
7. In the **Key** field, enter the secret key shared with this TACACS+ server.
8. In the **Confirm Key** field, reenter the secret key shared with this TACACS+ server.
9. In the **Priority** field, click **Primary** or **Secondary** to determine the order in which the TACACS+ server is used.
10. Click **Insert** to accept the change and return to the work area.

### TACACS+ Server tab field descriptions

The following table describes the fields on the TACACS+ Server tab.

| Name | Description |
|---|---|
| **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. |
| **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. |
| **Key** | Secret key to be shared with this TACACS+ server. |
| **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

Use this procedure to configure general switch security.

### Procedure

1. In the navigation tree, double-click **Security** to open the Security tree..
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **Mac Security** tab.
4. Configure switch security parameters as required.
5. On the toolbar, click **Apply**.

## MAC Security tab field descriptions

The following table describes the fields on the MAC Security tab.

| Name | Description |
|---|---|
| **AuthSecurityLock** | If this parameter is listed as *locked*, the agent refuses all requests to modify the security configuration. Entries also include:<br>• **other**<br>• **notlocked** |

*Table continues…*

| Name | Description |
|---|---|
| **AuthCtlPartTime** | 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. |
| **SecurityStatus** | Indicates whether or not the switch security feature is enabled. |
| **SecurityMode** | Mode of switch security. Entries include:<br>• **macList**: Indicates that the switch is in the MAC-list mode. You can configure more than one MAC address for each port.<br>• **autoLearn**: Indicates that the switch learns the first MAC address on each port as an allowed address of that port. |
| **SecurityAction** | Actions performed by the software when a violation occurs (when SecurityStatus is enabled). The security action specified here applies to all ports of the switch.<br>A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include:<br>• **noAction**: Port does not have any security assigned to it, or the security feature is turned off.<br>• **trap**: Listed trap.<br>• **partitionPort**: Port is partitioned.<br>• **partitionPortAndsendTrap**: Port is partitioned, and traps are sent to the trap receiver.<br>• **daFiltering**: Port filters out the frames where the destination address field is the MAC address of the unauthorized station.<br>• **daFilteringAndsendTrap**: Port filters out the frames where the desitnation address field is the MAC address of unauthorized station. Traps are sent to trap receivers.<br>• **partitionPortAnddaFiltering**: Port is partitioned and filters out the frames with the destination address field is the MAC address of unauthorized station.<br>• **partitionPortdaFilteringAndsendTrap**: Port is partitioned and filters out the frames where the destination address field is the MAC address of the |

*Table continues…*

| Name | Description |
|---|---|
| | 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. |
| **AutoLearningSticky (sticky-mac)** | When selected, the learning mechanism used is the same as when auto-learning is enabled, with the exception that:<br>• when the Sticky MAC feature is enabled, migration and auto-deletion on link-down are blocked and the addresses are not aged out<br>• when Sticky mode is enabled, the aging timer is automatically set to zero<br>• Sticky MAC addresses are saved into NVRAM config file and ASCII files<br>• administrative removal of sticky addresses is possible |

**Important:**

You cannot assign a port or ports to the PortLearnStatus field if you have enabled AutoLearn for the port or ports.

# Adding ports to a security list using EDM

Use this procedure to add ports to the security list to insert new port members into a security list.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.

3. In the work area, click the **SecurityList** tab.
4. On the toolbar, click **Insert**.
5. Perform one of the following:
   - In the **SecurityListIndx** 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:
   - 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**.

## SecurityList tab field descriptions

The following table describes the fields on the SecurityList tab.

| Name | Description |
|---|---|
| **SecurityListIndx** | 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 ports from a security list using EDM

Use this procedure to delete ports from a security list.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, 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.

## SecurityList tab field descriptions

The following table describes the fields on the SecurityList tab.

| Name | Description |
|---|---|
| **SecurityListIndx** | A numerical identifier for a security list. Values range from 1 to 32. |
| **SecurityListMembers** | Defines the security list port members. |

# Configuring AuthConfig list 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.

## Adding entries to the AuthConfig list using EDM

Use this procedure to add entries to the AuthConfig list.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **AuthConfig** tab.
4. On the tool bar, click **Insert** to open the Insert AuthConfig window.
5. Type a value in the **BrdIndx** field.
6. Type a value in the **PortIndx** field.
7. Type a value in the **MACIndx** field.
8. Select the **AutoLearningSticky (sticky-mac)** check box to enable Sticky MAC address, or clear the check box to disable.

   **Important:**

   Avaya recommends you to disable autosave if you enable Sticky MAC address.
9. Select the **AccessCtrlType** check box to enable a MAC address on multiple ports, or clear the check box to disable.
10. Click **Insert** .

11. Type a value in the **SecureList** field.
12. On the toolbar, click **Apply**.

## AuthConfig tab field descriptions

The following table describes the fields on the AuthConfig tab.

| Name | Description |
|---|---|
| **BrdIndx** | Index of the slot that contains the board on which the port is located. If you specify SecureList, this field must be zero. |
| **PortIndx** | Index of the port on the board. If you specify SecureList, this field must be zero. |
| **MACIndx** | An index of MAC addresses that are designated as allowed (station). |
| **AutoLearningSticky (sticky-mac)** | Enables or disables Sticky MAC. Sticky MAC can store automatically learned MAC addresses across switch reboots and secure MAC addresses to a specified port.<br>**Note:**<br>If AutoLearningSticky is enabled, you cannot modify AccessCtrolType and SecureList. |
| **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 BrdIndx and PortIndx values are zero. For other board and port index values, this index must also have a value of zero.<br>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

Use this procedure to remove entries from the AuthConfig list for boards, ports and MAC addresses that have the security configuration.

### Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, 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**.

# Configuring MAC Address autolearn using EDM

Use this procedure to configure automatic learning of MAC Addresses.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **AutoLearn**.
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 to 25.
8. On the toolbar, click **Apply**.

## AutoLearn tab field descriptions

The following table describes the fields on the AutoLearn tab.

| Name | Description |
|---|---|
| **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. |

**Important:**

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.

# Viewing AuthStatus information using EDM

Use 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

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **AuthStatus** tab.

## AuthStatus tab field descriptions

The following table describes the fields on the AuthStatus tab.

| Name | Description |
|---|---|
| **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 `node allowed` or `node blocked` type. |
| **CurrentActionMode** | A value representing the type of information contained, including:<br>• **noAction**: Port does not have any security assigned to it, or the security feature is turned off..<br>• **partitionPort**: Port is partitioned.<br>• **partitionPortAndsendTrap**: Port is partitioned and traps are sent to the trap receiver. |

*Table continues…*

| Name | Description |
|---|---|
| | • **Filtering**: Port filters out the frames where the destination address field is the MAC address of the unauthorized station.<br>• **FilteringAndsendTrap**: Port filters out the frames where the destination address field is the MAC address of the unauthorized station. Traps are sent to the trap receiver.<br>• **sendTrap**: A trap is sent to the trap receiver(s).<br>• **partitionPortAnddaFiltering**: Port is partitioned and filters out the frames where the destination address field is the MAC address of the unauthorized station<br>• **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). |
| **CurrentPortSecurStatus** | Displays the security status of the current port, including:<br>• If the port is disabled, notApplicable is returned.<br>• If the port is in a normal state, portSecure is returned.<br>• If the port is partitioned, portPartition is returned. |

# Viewing AuthViolation information using EDM

Use 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

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **AuthViolation** tab.

## AuthViolation tab field descriptions

The following table describes the fields on the AuthViolation tab.

| Name | Description |
|---|---|
| **BrdIndx** | The index of the board. This corresponds to the unit containing the board. The index will be 1 where it is not applicable. |
| **PortIndx** | The index of the port on the board. This corresponds to the port on that a security violation was seen. |
| **MACAddress** | The MAC address of the device attempting unauthorized network access (MAC address-based security). |

# Viewing MacViolation information using EDM

Use this procedure to view MAC Violation information.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, 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.

## MacViolation tab field descriptions

The following table describes the fields on the MacViolation tab.

| Name | Description |
|---|---|
| **Address** | The MAC address of the device attempting unauthorized network access (MAC address-based security). |
| **Brd** | The index of the board. This corresponds to the slot containing the board. The index is 1 when it is not applicable. |
| **Port** | The index of the port on the board. This corresponds to the port on which a security violation was seen. |

# Configuring a Web and Telnet password using EDM

Use this procedure to configure a Web and Telnet password for an individual switch.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
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. On the toolbar, click **Apply**.

## Web/Telnet Password tab field descriptions

The following table describes the fields on the Web/Telnet Password tab.

| Name | Description |
|---|---|
| **Web/Telnet Switch Password Type** | Specifies the password type. Values include:<br>• **None**<br>• **Local Password**<br>• **RADIUS Authentication**<br>Default is None. |

# Configuring a console password using EDM

Use this procedure to configure a Console password for an individual switch.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, 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 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. On the toolbar, click **Apply**.

## Console Password tab field descriptions

The following table describes the fields on the Console Password tab.

| Name | Description |
|---|---|
| **Console Password Type** | Specifies the password type. Values include:<br>• **None**<br>• **Local Password**<br>• **RADIUS Authentication**<br>Default is None. |

# Configuring the Secure Shell protocol using EDM

Use this procedure to configure the Secure Shell (SSH) protocol to provide secure access to the switch.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **SSH/SSL**.
3. In the work area, click the **SSH** tab.
4. Configure SSH parameters as required.
5. On the toolbar, click **Apply**.

## SSH tab field descriptions

The following table describes the fields on the SSH tab.

| Name | Description |
|---|---|
| **Enable** | Indicates the SSH status. Values include:<br>• **false**: Disabled<br>• **true**: Enabled<br>• **secure**: SSH enabled, turns off all remote access, takes effect after a reboot<br>Default is false. |
| **Version** | Indicates the SSH version. The default is v2only. |
| **Port** | Indicates the SSH connection port. Value range of 1 to 65535, default is 22. |
| **Timeout** | Indicates the SSH connection timeout in seconds. Value range of 1 to 120, default is 60. |
| **KeyAction** | Indicates the SSH key action. Values include:<br>• **generateDsa**<br>• **generateRsa**<br>• **deleteDsa**<br>• **deleteRsa** |
| **DsaAuth** | Enables or disables SSH with DSA public key authentication. The default is enabled. |
| **PassAuth** | Enables or disables SSH with password authentication. The default is enabled. |
| **DsaHostKeyStatus** | Indicates the current status of the SSH DSA host key:<br>• **notGenerated**: DSA host key has not yet been generated.<br>• **generated**: DSA host key is generated.<br>• **generating**: DSA host key is currently being generated. |
| **RsaAuth** | Enables or disables SSH with RSA public key authentication. The default is enabled. |
| **RsaHostKeyStatus** | Indicates the current status of the SSH DSA host key:<br>• **notGenerated**: RSA host key has not yet been generated.<br>• **generated**: RSA host key is generated.<br>• **generating**: RSA host key is currently being generated. |

*Table continues…*

| Name | Description |
|---|---|
| **TftpServerInetAddressType** | Indicates the type of address stored in the TFTP server. Values include:<br>• **IPv4**<br>• **IPv6**<br>The default is IPv4. |
| **TftpServerInetAddress** | Specifies the IP address of TFTP server for all TFTP operations. |
| **TftpFile** | Indicates the name of the file for the TFTP transfer. |
| **TftpAction** | Indicates the SSH public keys that are set to initiate a TFTP download. Values include:<br>• **none**<br>• **downloadSshDsaPublicKeys**<br>• **deleteSshDsaAuthKey**<br>• **downloadSshRsaPublicKeys**<br>• **deleteSshRsaAuthKey**<br>The default is none |
| **TftpResult** | Indicates the retrieved value of the TFTP transfer. Values include:<br>• **none**<br>• **success**<br>• **transferError** |

# Viewing SSH Sessions information using EDM

Use this procedure to display currently active SSH sessions.

### Procedure

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.

## SSH Sessions tab field descriptions

The following table describes the fields on the SSH Sessions tab.

| Name | Description |
|---|---|
| **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 an SSH Client

Use this procedure to configure and manage a Secure Shell (SSH) Client.

### Procedure

1. In the navigation tree, double-click **Security**.
2. In the Security tree, click **SSH/SSL**.
3. In the work area, click the **SSHC/SFTP** tab.
4. Configure SSHC parameters as required.
5. Click **Apply**.

# SSHC/SFTP tab field descriptions

The following table describes the fields on the SSHC/SFTP tab.

| Name | Description |
|---|---|
| **KeyAction** | Specifies the action to take for the SSH Client host key. Values include:<br>• **none**: take no host key action<br>• **generateDsa**: generates a DSA host key for the SSH Client<br>• **generateRsa**: generates an RSA host key for the SSH Client<br>• **deleteDsa**: deletes the SSH Client DSA host key.<br>• **deleteRsa**: deletes the SSH Client DSA host key.<br>• **generateDsaForce**:<br>• **generateRsaForce**: |
| **KeyFileName** | Speicifies the SSH Client host key file name. |

*Table continues…*

| Name | Description |
|---|---|
| **TftpAction** | Specifies the type of SSH Client authentication key to upload using TFTP. Values include:<br>• **none**: do not upload an SSH Client authentication key using TFTP<br>• **uploadSshcDsaAuthKey**: uploads a DSA SSH Client authentication key using TFTP<br>• **uploadSshcRsaAuthKey**: uploads an RSA SSH Client authentication key using TFTP |
| **TftpServerInetAddressType** | Specifies whether the IP address is IPv4 or IPv6. |
| **TftpServerInetAddress** | Specifies the IP address of the TFTP server. |
| **DsaKeySize** | Specifies the DSA key size. Values range from 512 to 1024. Default value: 512. |
| **RsaKeySize** | Specifies the RSA key size. Values range from 1024 to 2048. Default value: 1024. |
| **DSAHostKeyStatus** | Indicates the current status of the SSH Client DSA host key. Values include:<br>• notGenerated<br>• generated<br>• generating |
| **RsaHostKeyStatus** | Indicates the current status of the SSH Client RSA host key. Values include:<br>• notGenerated<br>• generated<br>• generating |
| **SFTP** | |
| **Port** | Specifies the TCP port number for the SFTP file transfer. Values range from 1 to 65535. Default value: 22. |
| **DsaAuthentication** | When selected, enables SFTP DSA authentication for SSH Client (default). |
| **RsaAuthentication** | When selected, enables SFTP password authentication for SSH Client. |
| **PasswordAuthentication** | When selected, enables SFTP RSA authentication for SSH Client. |
| **SftpServerInetAddressType** | Specifies whether the IP address is IPv4 or IPv6. |
| **SftpServerInetAddress** | Specifies the IP address of the SFTP server. |
| **UserName** | Specifies the user name. |
| **SftpServerPassword** | Specifies the password for the SFTP server. |

*Table continues…*

| Name | Description |
|---|---|
| **Confirm SftpServerPassword** | Confirm the password for the SFTP server. |

# Configuring SSL using EDM

Use this procedure to configure Secure Socket Layer (SSL) to provide your network with a secure Web management interface.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **SSH/SSL**.
3. In the work area, click the **SSL** tab.
4. Configure SSL parameters as required.
5. On the toolbar, click **Apply**.

## SSL tab field descriptions

The following table describes the fields on the SSL tab.

| Name | Description |
|---|---|
| **Enabled** | Enables or disables SSL. |
| **CertificateControl** | Enables the creation and deletion of SSL certificates.<br>• **create**: creates an SSL certificate<br>• **delete**: deletes an SSL certificate.<br>• **other**: results in a wrongValue error |
| **CertificateExists** | Indicates if a valid SSL certificate is created.<br>• **true**: a valid SSL certificate is created<br>• **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.<br>• **inProgress**: the operation is not yet completed<br>• **success**: the operation is complete<br>• **failure**: the operation failed |

*Table continues…*

| Name | Description |
|---|---|
| | • **other**: the s5AgSslCertificateControl object was never set |
| **ServerControl** | Resets the SSL server. Values are reset and other. The default is other. |

**Important:**

You cannot reset the SSL server while creating the SSL certificate.

# Configuring RADIUS parameters

Use the following procedures to configure the RADIUS parameters on the Globals tab.

## Configuring RADIUS globally using EDM

Use this procedure to configure RADIUS security for the switch.

### Procedure

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. Perform one of the following:
   - In the RADIUS section, select the **UseMgmtIp** checkbox, to enable RADIUS request use management.
   - In the RADIUS section, clear the **UseMgmtIp** checkbox, to disable RADIUS request use management.
5. Perform one of the following:
   - In the RADIUS section, select the **PasswordFallbackEnabled** checkbox, to enable RADIUS password fallback.
   - In the RADIUS section, clear the **PasswordFallbackEnabled** checkbox. to disable RADIUS password fallback.
6. Perform one of the following:
   - In the RADIUS section, select the **DynAuthReplayProtection** checkbox, to enable RADIUS replay protection.
   - In the RADIUS section, clear the **DynAuthReplayProtection** checkbox, to disable RADIUS replay protection .
7. In the RADIUS section, click a **RadiusReachability** radio button.

8. On the toolbar, click **Apply**.

## Globals tab field descriptions

The following table describes the fields on the Globals tab.

| Name | Description |
|---|---|
| **UseMgmtIp** | When selected, RADIUS uses the system management IP address as the source address for RADIUS requests. |
| **PasswordFallbackEnabled** | When selected, enables RADIUS password fallback. |
| **DynAuthReplayProtection** | When selected, enables RADIUS replay protection. |
| **Reachability** | Specifies the RADIUS server reachability mode. Values include:<br>• **useRadius**: Uses dummy RADIUS requests to determine reachability of the RADIUS server.<br>• **useIcmp**: Uses ICMP packets to determine reachability of the RADIUS server (default). |

# Configuring the Global RADIUS Server using EDM

Use this procedure to configure the RADIUS server globally for processing client requests without designating separate EAP or Non-EAP

### Procedure

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 **Global RADIUS Server** tab.
4. Select an IPv4 or IPv6 address type in the **PrimaryRadiusServerAddressType** box.
5. Type an IPv4 or IPv6 address in the **PrimaryRadiusServer** field.
6. Select an IPv4 or IPv6 address type in the **SecondaryRadiusServerAddressType** box.
7. Type an IPv4 or IPv6 address in the **SecondaryRadiusServer** field.
8. Type a UDP port number in the **RadiusServerUdpPort** field.
9. Type a timeout value in the **RadiusServerTimeout** field.
10. To change the shared secret key, type a value in the **SharedSecret(Key)** field.
11. Confirm the new shared secret key value in the **ConfirmSharedSecret(Key)** field.
12. Type a value in the **RetryLimit** field.
13. On the toolbar, click **Apply**.

## Global RADIUS Server tab field descriptions

The following table describes the fields on the Global RADIUS Server tab.

| Name | Description |
|---|---|
| **PrimaryRadiusServerAddressType** | Specifies the IP address type for the primary Global RADIUS server. Values include unknown, IPv4, and IPv6. |
| **PrimaryRadiusServer** | Specifies the IPv4 or IPv6 address of the primary Global RADIUS server (default: 0.0.0.0).<br>**Important:**<br>An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a primary Global RADIUS Server is not configured. |
| **SecondaryRadiusServerAddressType** | Specifies the IP address type for the secondary Global RADIUS server. Values include unknown, IPv4, and IPv6. |
| **SecondaryRadiusServer** | Specifies the IPv4 or IPv6 address of the secondary Global RADIUS server (default: 0.0.0.0). The secondary Global RADIUS server is used if the primary Global RADIUS server is unavailable or unreachable.<br>**Important:**<br>An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a secondary Global RADIUS Server is not configured. |
| **RadiusServerUdpPort** | Specifies the UDP port number clients use to contact the Global RADIUS Server at the Global RADIUS Server IP address.<br>RANGE: 1 to 65535<br>DEFAULT: 1812 |
| **RadiusServerTimeout** | Specifies the timeout interval between each retry for service requests to the Global RADIUS server.<br>DEFAULT: 2 seconds<br>RANGE: 1 to 60 seconds |
| **SharedSecret(key)** | Specifies the value for the Global RADIUS Server shared secret key. |

*Table continues…*

| Name | Description |
| --- | --- |
| | **Important:**<br>The shared secret key has a maximum of 16 characters. |
| **ConfirmedSharedSecret(key)** | Confirms the value of the shared secret key specified in the SharedSecret(Key) field. Entering a value in this field is only required if you changed the SharedSecret(Key). |
| **RetryLimit** | Specifies the number of RADIUS retry attempts for a Global RADIUS Server instance.<br>RANGE: 1 to 5 |

# Configuring the EAP RADIUS Server using EDM

Use this procedure to configure an EAP RADIUS Server for processing EAP client requests only.

### Procedure

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 **EAP RADIUS Server** tab.
4. Select an IPv4 or IPv6 address type in the **PrimaryRadiusServerAddressType** field.
5. Type an IPv4 or IPv6 address in the **PrimaryRadiusServer** box.
6. Select an IPv4 or IPv6 address type in the **SecondaryRadiusServerAddressType** field.
7. Type an IPv4 or IPv6 address in the **SecondaryRadiusServer** field.
8. Type a UDP port number in the **RadiusServerUdpPort** box.
9. Type a timeout value in the **RadiusServerTimeout** box.
10. To change the shared secret key, type a value in the **SharedSecret(Key)** box.
11. Confirm the new shared secret key value in the **ConfirmSharedSecret(Key)** box.
12. Perform one of the following:
    - To enable accounting, check the **AccountingEnabled** checkbox.
    - To disable accounting, clear the **AccountingEnabled** checkbox.
13. Type a value in the **AccountingPort** box.
14. Type a value in the **RetryLimit** field.
15. On the toolbar, click **Apply**.

## EAP RADIUS Server tab field descriptions

The following table describes the fields on the EAP RADIUS Server tab.

| Name | Description |
|---|---|
| **PrimaryRadiusServerAddressType** | Specifies the IP address type for the primary EAP RADIUS server. Values include IPv4 and IPv6. |
| **PrimaryRadiusServer** | Specifies the IPv4 or IPv6 address of the primary EAP RADIUS server (default: 0.0.0.0).<br>**Important:**<br>An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a primary EAP RADIUS Server is not configured. |
| **SecondaryRadiusServerAddressType** | Specifies the IP address type for the secondary EAP RADIUS server. Values include IPv4 and IPv6. |
| **SecondaryRadiusServer** | Specifies the IPv4 or IPv6 address of the secondary EAP RADIUS server (default: 0.0.0.0). The secondary EAP RADIUS server is used if the primary EAP RADIUS server is unavailable or unreachable.<br>**Important:**<br>An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a secondary EAP RADIUS Server is not configured. |
| **RadiusServerUdpPort** | Specifies the UDP port number clients use to contact the EAP RADIUS Server at the EAP RADIUS Server IP address. The port number can range between 1 and 65535, the default is 1812. |
| **RadiusServerTimeout** | Specifies the timeout interval between each retry for service requests to the EAP RADIUS server. The default is 2 Seconds. Value range of 1 to 60 seconds. |
| **SharedSecret(key)** | Specifies the value for the EAP RADIUS Server shared secret key.<br>**Important:**<br>The shared secret key has a maximum of 16 characters. |
| **ConfirmedSharedSecret(key)** | Confirms the value of the shared secret key specified in the SharedSecret(Key) field. Entering a value in this field is only required if you changed the SharedSecret(Key). |

*Table continues…*

| Name | Description |
|---|---|
| **AccountingEnabled** | Enables or disables RADIUS accounting for a Global RADIUS Server instance. |
| **AccountingPort** | Specifies the UDP accounting port number for clients to use when trying to contact the RADIUS server at the corresponding Global RADIUS Server IP address. Values range from 0 to 65535. |
| **RetryLimit** | Specifies the number of RADIUS retry attempts for a EAP RADIUS Server instance. Value range of 1 to 5. |

# Configuring the NEAP RADIUS Server using EDM

Use this procedure to configure an NEAP RADIUS Server for processing NEAP client requests only.

### Procedure

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 **NEAP RADIUS Server** tab.
4. Select an IPv4 or IPv6 address type in the **PrimaryRadiusServerAddressType** field.
5. Type an IPv4 or IPv6 address in the **PrimaryRadiusServer** box.
6. Select an IPv4 or IPv6 address type in the **SecondaryRadiusServerAddressType** field.
7. Type an IPv4 or IPv6 address in the **SecondaryRadiusServer** box.
8. Type a UDP port number in the **RadiusServerUdpPort** box.
9. Type a timeout value in the **RadiusServerTimeout** box.
10. To change the shared secret key, type a value in the **SharedSecret(Key)** box.
11. Confirm the new shared secret key value in the **ConfirmSharedSecret(Key)** box.
12. Perform one of the following:
    - To enable accounting, check the **AccountingEnabled** checkbox.
    - To disable accounting, clear the **AccountingEnabled** checkbox.
13. Type a value in the **AccountingPort** box.
14. Type a value in the **RetryLimit** box.
15. On the toolbar, click **Apply**.

## NEAP RADIUS Server tab field descriptions

The following table describes the fields on the NEAP RADIUS Server tab.

| Name | Description |
|---|---|
| **PrimaryRadiusServerAddressType** | Specifies the IP address type for the primary NEAP RADIUS server. Values include IPv4 and IPv6. |
| **PrimaryRadiusServer** | Specifies the IPv4 or IPv6 address of the primary NEAP RADIUS server (default: 0.0.0.0).<br>**Important:**<br>An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a primary NEAP RADIUS Server is not configured. |
| **SecondaryRadiusServerAddressType** | Specifies the IP address type for the secondary NEAP RADIUS server. Values include IPv4 and IPv6. |
| **SecondaryRadiusServer** | Specifies the IPv4 or IPv6 address of the secondary NEAP RADIUS server (default: 0.0.0.0). The secondary NEAP RADIUS server is used if the primary NEAP RADIUS server is unavailable or unreachable.<br>**Important:**<br>An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a secondary NEAP RADIUS Server is not configured. |
| **RadiusServerUdpPort** | Specifies the UDP port number clients use to contact the NEAP RADIUS Server at the NEAP RADIUS Server IP address. The port number can range between 1 and 65535, the default is 1812. |
| **RadiusServerTimeout** | Specifies the timeout interval between each retry for service requests to the NEAP RADIUS server. The default is 2 Seconds. Value range of 1 to 60 seconds. |
| **SharedSecret(key)** | Specifies the value for the NEAP RADIUS Server shared secret key.<br>**Important:**<br>The shared secret key has a maximum of 16 characters. |

*Table continues…*

| Name | Description |
|---|---|
| **ConfirmedSharedSecret(key)** | Confirms the value of the shared secret key specified in the SharedSecret(Key) field. Entering a value in this field is only required if you changed the SharedSecret(Key). |
| **AccountingEnabled** | Enables or disables RADIUS accounting for a Global RADIUS Server instance. |
| **AccountingPort** | Specifies the UDP accounting port number for clients to use when trying to contact the RADIUS server at the corresponding Global RADIUS Server IP address. Values range from 0 to 65535. |
| **RetryLimit** | Specifies the number of RADIUS retry attempts for a NEAP RADIUS Server instance. Value range of 1 to 5. |

# Viewing RADIUS Dynamic Authorization server information using EDM

Use this procedure to display RADIUS Dynamic Authorization server information for the switch.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Server** tab.

# RADIUS Dynamic Auth. Server tab field descriptions

The following table describes the fields on the RADIUS Dynamic Auth. Server tab.

| Name | Description |
|---|---|
| **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) client configuration using EDM

Use the following procedures to create, delete, or modify a RADIUS Dynamic Authorization client configuration.

## Configuring an 802.1X dynamic authorization extension (RFC 3576) client using EDM

Use this procedure to create and configure a RADIUS Dynamic Authorization client for the switch.

**Procedure**

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.
4. On the tool bar, click **Insert**.
5. In the **Address** dialog box, type an IP address.
6. Perform one of the following:
   - To enable the RADIUS Dynamic Authorization client, select the **Enabled** checkbox.
   - To disable the RADIUS Dynamic Authorization client, clear the **Enabled** checkbox.
7. In the **UdpPort** dialog box, type a port number.
8. Perform one of the following:
   - To enable change of authorization request processing, select the **ProcessCoARequests** checkbox.
   - To disable change of authorization request processing, clear the **ProcessCoARequests** checkbox.
9. Perform one of the following:
   - To enable disconnect request processing, select the **ProcessDisconnectRequests** checkbox.
   - To disable disconnect request processing, clear the **ProcessDisconnectRequests** checkbox.
10. In the **Secret** dialog box, type a shared secret word.
11. In the **Confirm Secret** dialog box, retype the same shared secret word.
12. Click **Insert**.
13. On the toolbar, click **Apply**.

## RADIUS Dynamic Auth. Client tab field descriptions

The following table describes the fields on the RADIUS Dynamic Auth. Client tab.

| Name | Description |
|---|---|
| **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 or disables 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. |

# Deleting an 802.1X dynamic authorization extension (RFC 3576) client configuration using EDM

Use this procedure to delete an existing RADIUS Dynamic Authorization client configuration.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.
4. To select a RADIUS Dynamic Authorization client to delete, click the client row.
5. On the toolbar, click **Apply**.

# Modifying the 802.1X dynamic authorization extension (RFC 3576) client configuration using EDM

Use this procedure to edit an existing RADIUS Dynamic Authorization client configuration.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.
4. To select a RADIUS Dynamic Authorization client to edit, click the client row.
5. In the client row, double-click the cell in the **Enabled** column.
6. Select a value from the list—**true** to enable RADIUS Dynamic Authorization client, or **false** to disable RADIUS Dynamic Authorization client for the VLAN.
7. In the client row, double-click the cell in the **UdpPort** column.
8. Edit the UDP port number as required.
9. In the client row, double-click the cell in the **ProcessCoARequests** column.
10. Select a value from the list—**true** to enable CoA request processing, or **false** to disable CoA request processing.
11. In the client row, double-click the cell in the **ProcessDisconnectRequests** column.
12. Select a value from the list—**true** to enable disconnect request processing, or **false** to disable disconnect request processing.
13. On the toolbar, click **Apply**.

## RADIUS Dynamic Auth. Client tab field descriptions

The following table describes the fields on the RADIUS Dynamic Auth. Client tab.

| Name | Description |
|---|---|
| **AddressType** | Indicates the IP address type for the RADIUS Dynamic Authorization Client. This is a read-only cell. |
| **Address** | Indicates the IP address of the RADIUS Dynamic Authorization Client. This is a read-only cell. |
| **Enabled** | Enables or disables packet receiving from the RADIUS Dynamic Authorization Client.<br>• **enable**: True<br>• **disable**: False |
| **UdpPort** | Defines the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1024 to 65535. |
| **ProcessCoARequests** | Enables or disables change of authorization (CoA) request processing. |
| **ProcessDisconnectRequests** | Enables or disables disconnect request processing. |

*Table continues…*

| Name | Description |
|---|---|
| **Secret** | The RADIUS Dynamic Authorization Client secret word. This cell remains empty. |

# Viewing the 802.1X dynamic authorization extension (RFC 3576) client information using EDM

Use this procedure to display existing RADIUS Dynamic Authorization client configurations for the switch.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.

## RADIUS Dynamic Auth. Client tab field descriptions

The following table describes the fields on the RADIUS Dynamic Auth. Client tab.

| Name | Description |
|---|---|
| **AddressType** | Indicates the IP address type for the RADIUS Dynamic Authorization Client. |
| **Address** | Indicates the IP address of the RADIUS Dynamic Authorization Client. |
| **Enabled** | Indicates whether packet receiving from the RADIUS Dynamic Authorization Client is enabled (true) or disabled (false). |
| **UdpPort** | Indicates the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1024–65535. |
| **ProcessCoARequests** | Indicates whether change of authorization (CoA) request processing is enabled or disabled. |
| **ProcessDisconnectRequests** | Indicates whether disconnect request processing is enabled or disabled. |
| **Secret** | Indicates the secret word shared between the RADIUS Dynamic Authorization Client and the RADIUS server. |

## Editing the 802.1X dynamic authorization extension (RFC 3576) client secret word using EDM

Use this procedure to change the existing RADIUS Dynamic Authorization client secret word.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**
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. On the toolbar, click **Apply**.

# Viewing RADIUS Dynamic Server statistics using EDM

Use this procedure to display RADIUS Dynamic Server statistical information.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Server Stats** tab.

## RADIUS Dynamic Server Stats tab field descriptions

The following table describes the fields on the RADIUS Dynamic Server Stats tab.

| Name | Description |
|---|---|
| **ClientIndex** | Indicates the RADIUS Dynamic Server client index. |
| **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

Use this procedure to display a graphical representation of statistics for a RADIUS Dynamic Server client.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Server Stats** tab.
4. To select a server, click the client row.
5. On the tool bar, click **Graph**.
6. Click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

# 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.

## Configuring DHCP snooping and Option 82 globally using EDM

Use this procedure to enable or disable global DHCP Snooping parameters for the switch.

### Before you begin

- In Layer 3 mode, DHCP Snooping must be enabled on Layer 3 VLANs spanning toward DHCP servers.
- Enable DHCP Relay.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping Globals** tab.
4. For DHCP Snooping, perform one of the following:
   - Select the **DhcpSnoopingEnabled** check box to enable DHCP snooping.
   - Clear the **DhcpSnoopingEnabled** check box to disable DHCP snooping.
5. For Option 82 for Snooping, perform one of the following:
   - Select the **DhcpSnoopingOption82Enabled** box.
   - Clear the **DhcpSnoopingOption82Enabled** box

6. On the toolbar, click **Apply**.

## Configuring DHCP snooping and Option 82 on a VLAN using EDM

Use this procedure to enable or disable DHCP Snooping and DHCP Snooping with Option 82 parameters on the VLAN.

### Before you begin

### About this task

- Enable DHCP snooping separately for each VLAN ID.

**Important:**

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

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping-VLAN** tab.
4. To select a VLAN to edit, click the **VLAN ID**.
5. In the VLAN row, double-click the cell in the **DhcpSnoopingEnabled** column.
6. Select a value from the following List:
   - **true** to enable DHCP Snooping for the VLAN
   - **false** to disable DHCP Snooping for the VLAN
7. In the VLAN row, double-click the cell in the **VlanOption82Enabled** column.
8. Select one of the values from the following list:
   - **true** to enable DHCP Snooping with Option 82 for the VLAN
   - **false** to disable DHCP Snooping with Option 82 for the VLAN.
9. On the toolbar, click **Apply**.

## DHCP Snooping-VLAN tab field descriptions

The following table describes the fields on the DHCP Snooping-VLAN tab.

| Name | Description |
|---|---|
| **VlanId** | Identifies the VLANs configured on the switch. |
| **DhcpSnoopingEnabled** | Enables or disables DHCP snooping on a VLAN. |
| **VlanOption82Enabled** | Enables or disables DHCP Snooping Option 82 on a VLAN. |

# Configuring DHCP snooping port trust and DHCP Option 82 for a port using EDM

Use this procedure to configure DHCP Snooping on a port to configure port trust and to enable or disable DHCP Snooping with Option 82 for a port. Used with DHCP Snooping, DHCP Option 82 assists in tracking of end device locations.

Ports are untrusted by default.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping-port** tab.
4. To select a port to edit, click a **Port** row.
5. In the port row, double-click the cell in the **DhcpSnoopingIfTrusted** column
6. Select a value from the following list:
   - trusted.
   - untrusted
7. Repeat the previous two steps for each port you want to configure.
8. Double-click the **DhcpSnoopingIfOption82SubscriberId** for a port.
9. Type a subscriber ID value for the port.
10. Repeat the previous two steps for each port you want to configure
11. On the toolbar, click **Apply**.

## DHCP Snooping-port tab field descriptions

The following table describes the fields on the DHCP Snooping-port tab.

| Name | Description |
|---|---|
| **Port** | Identifies the ports on the switch. |
| **DhcpSnoopingIfTrusted** | Specifies if the port is trusted or untrusted. Default is false. |
| **DhcpSnoopingIfOption82Subscribed** | Specifies the DHCP Option 82 subscriber ID for the port.<br>The value is a character string from 1 to 64 characters. |

# Viewing the DHCP binding information using EDM

Use this procedure to view the current DHCP snooping binding table.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Bindings** tab.

## DHCP Bindings tab field descriptions

The following table describes the fields on the DHCP Bindings tab.

| Name | Description |
|---|---|
| **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. |
| **Source** | Indicates the source of the binding table entry. |

# Configuring dynamic ARP inspection on a VLAN using EDM

Use this procedure to enable or disable dynamic ARP inspection on the VLAN.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, 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 toolbar, click **Apply**.

## ARP inspection-VLAN tab field descriptions

The following table describes the fields on the ARP inspection-VLAN tab.

| Name | Description |
|---|---|
| **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

Use this procedure to enable or disable dynamic ARP inspection on a port.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **Dynamic ARP Inspection (DAI)**.
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 toolbar, click **Apply**.

## ARP Inspection-port tab field descriptions

The following table describes the fields on the ARP Inspection-port tab.

| Name | Description |
|---|---|
| **Port** | Identifies ports on the switch, using the unit/port format. |
| **ARPInspectionIfTrusted** | Configures a port as trusted or untrusted for ARP inspection. |

# Configuring IP Source Guard 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.

### Before you begin

- Globally enable Dynamic Host Control Protocol (DHCP) snooping.
- For information see Configuring DHCP snooping and Option 82 on a VLAN using EDM on page 242
- Ensure that the port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- 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)

**Important:**

Avaya 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.

# Configuring IP Source Guard on a port using EDM

Use this procedure to enable or disable a higher level of security on a port or ports.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree
2. From the Security tree, 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. Perform one of the following:
   - From the list, select **ip** to enable IP Source Guard
   - From the list, select **disabled** to disable IP Source Guard on the port.
6. On the toolbar, click **Apply**.

## IP Source Guard-port tab field descriptions

The following table describes the fields on the IP Source Guard-port tab.

| Name | Description |
|---|---|
| **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

Use this procedure to display IP Source Guard information for specific IP addresses.

### Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, 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**.

## IP Source Guard-addresses Filter dialog field descriptions

The following table describes the fields on the IP Source Guard-addresses Filter dialog.

| Name | Description |
|---|---|
| **Condition** | Defines the search condition.<br>• **AND**: Includes keywords specified in both the Port and Address fields while filtering results<br>• **OR**: Includes either one of the keywords specified in the Port and Address fields while filtering results |
| **Ignore Case** | Ignores the letter case while searching. |
| **Column** | Specifies the content of the column search.<br>• **Contains**<br>• **Does not contain**<br>• Equals to |
| **All records** | Displays all entries in the table. |

# Configuring SNMP 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.

## Viewing SNMP information using EDM

Use this procedure to view read-only information about the addresses that the agent software uses to identify the switch.

Perform this procedure to view SNMP information.

### Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. From the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the work area, click the **SNMP** tab.

## SNMP tab field descriptions

The following table describes the fields on the SNMP tab.

| Name | Description |
|---|---|
| **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. |

*Table continues…*

| Name | Description |
|---|---|
| **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. |

# Defining a MIB view using EDM

Use this procedure to assign MIB view access for an object.

### Procedure

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, 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 toolbar, click **Apply**.

## MIB View tab field descriptions

The following table describes the fields on the MIB View tab.

| Name | Description |
|---|---|
| **ViewName** | Specifies a name for the new entry in a range from 1 to 32 characters. |
| **Subtree** | Specifies any valid object identifiers that define 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:<br>• **included**: Granted<br>• **excluded**: Denied |
| **Storage Type** | Select one of the following:<br>• **volatile**: Entry does not persist if switch loses power |

*Table continues…*

| Name | Description |
|---|---|
| | • **nonVolatile**: Entry persists if switch loses power |

# Configuring an SNMP user using EDM

Use this procedure to create an SNMP user.

### Procedure

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, click **User**.
4. On the User tab tool bar, click **User**.
5. Click **Insert**.
6. Enter the parameters to describe the user.
7. Click **Insert**.
8. On the toolbar, click **Apply**.

## User tab field descriptions

The following table describes the fields on the User tab.

| Name | Description |
|---|---|
| **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:<br>• **None**<br>• **MD5**<br>• **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:<br>• **None**<br>• **DES**<br>• **3DES** |

*Table continues…*

| Name | Description |
|---|---|
| | • **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. |
| **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:<br>• **volatile**: Entry does not persist if switch loses power<br>• **nonVolatile**: Entry persists if switch loses power |

## Viewing SNMP user details using EDM

Use this procedure to view SNMP user details.

### Procedure

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, click **User**.
4. In the work area, on the User tab, select a user.
5. On the toolbar, click the **Details** button.

## Configuring an SNMP community

A community string is a passphrase used by the switch in snmpv1 and snmpv2 operations. Use this procedure to configure an SNMP community string.

### Procedure

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, 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**.

## Community tab field descriptions

The following table describes the fields on the Community tab.

| Name | Description |
|---|---|
| **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. |
| **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** | If you need to describe a series of choices for the field, use an unordered list as follows:<br>• **volatile**: Entry does not persist if switch loses power<br>• **nonVolatile**: Entry persists if switch loses power |

# Viewing SNMP community details using EDM

Use this procedure to view SNMP community details.

### Procedure

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, click **Community**.

4. In the work area, on the Community tab, select a community.
5. On the toolbar, click **Details**.

## Configuring an SNMP host using EDM

Use this procedure to create an SNMP host.

### Procedure

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, 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 toolbar, click **Apply**.

## Insert Host tab field descriptions

The following table describes the fields on the Insert Host tab.

| Name | Description |
|---|---|
| **Domain** | Select one of the following:<br>• **IPv4**<br>• **IPv6**<br>The default value is IPv4. |
| **DestinationAddr (Port)** | 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:<br>• **trap**<br>• **inform** |
| **Version** | Specifies the SNMP version as one of the following:<br>• **SNMPv1**<br>• **SNMPv2c** |

*Table continues…*

| Name | Description |
|---|---|
| | • **SNMPv3/USM** |
| **SecurityName** | Specifies security name used for generating SNMP messages. |
| **SecurityLevel** | Specifies the security level for SNMP messages as one of the following:<br>• **noAuthNoPriv**<br>• **authNoPriv**<br>• **authPriv** |
| **Storage Type** | Select one of the following:<br>• **volatile**: Entry does not persist if switch loses power<br>• **nonVolatile**: Entry persists if switch loses power |

# Configuring SNMP host notification using EDM

Use this procedure to configure SNMP trap notification.

### Procedure

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, 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 toolbar, click **Apply**.

## Host tab field descriptions

The following table describes the fields on the Host tab.

| Name | Description |
|---|---|
| **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. |

*Table continues…*

| Name | Description |
|---|---|
| **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 priviliges, authorization and no privileges, or authorization and privileges. |
| **StorageType** | Select one of the following:<br>• **volatile**: Entry does not persist if switch loses power<br>• **nonVolatile**: Entry persists if switch loses power |

# Configuring SNMP notification control using EDM

Use this procedure to enable or disable SNMP traps in the list. Notification Control is the Trap Web Page.

### Procedure

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, click **Notification Control**.
4. In the NotifyControlEnabled column, double-click the cell in the NotifyControlType (SNMP trap) row that you wish to modify.
5. Perform one of the following:
   - Select a value from the list: **true** to enable the SNMP trap.
   - Select a value from the list: **false** to disable SNMP trap.
   - On the toolbar, click the **Enable All** to enable all SNMP traps available on the switch.
   - On the toolbar, click the **Disble All** to disable all SNMP traps available on the switch.
6. On the toolbar, click **Apply**.

## Notification Control tab field descriptions

The following table describes the fields on the Notification Control tab.

| Name | Description |
|---|---|
| **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. |
| **NotifyControlPortListEnabled** | Indicates the port list for which the notification is enabled or disabled. Whether or not this field is configurable is dependent on the NotifyControlType value. |

# Configuring IPv6 management using EDM

Use the procedures in this section to configure IPv6 on the ERS 3500 Series.

**Related links**

Configuring IPv6 Management globally using EDM on page 256
IPv6 Interface configuration using EDM on page 257
Configuring an IPv6 address using EDM on page 264
Configuring IPv6 static routes using EDM on page 265
IPv6 neighbor cache configuration using EDM on page 266
Graphing IPv6 interface ICMP statistics using EDM on page 269
Viewing ICMP message statistics using EDM on page 270
Viewing global IPv6 TCP properties using EDM on page 270
Viewing IPv6 TCP connections using EDM on page 271
Viewing IPv6 TCP listeners using EDM on page 272
Viewing IPv6 UDP endpoints using EDM on page 273

## Configuring IPv6 Management globally using EDM

Use this procedure to enable and configure IPv6 Management globally.

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Globals** tab.
4. To enable IPv6 Management globally, select the **AdminEnabled** check box.
5. Control the sending of icmpv6 unreachable messages by clicking the **IcmpNetUnreach**.
6. To control the rate of icmpv6 error messages, type a value in the **IcmpErrorInterval** dialog box.

7. On the toolbar, click **Apply**.

**Related links**

Configuring IPv6 management using EDM on page 256
Globals tab field descriptions on page 257

## Globals tab field descriptions

The following table describes the fields on the Globals tab.

| Name | Description |
|---|---|
| **AdminEnabled** | Enables or disables IPv6 Management globally. |
| **OperEnabled** | Indicates if IPv6 Management is operationally enabled or disabled. Values are true (enabled) or false (disabled). |
| **Forwarding** | Indicates if IPv6 forwarding is enabled (Forwarding) or disabled (notForwarding). IPv6 forwarding (routing) is not supported, only management interface functions are supported. |
| **DefaultHopLimit** | Indicates the default hop limit value. |
| **IcmpNetUnreach** | Enables or disables ICMP net unreach. |
| **IcmpRedirectMsg** | Indicates if ICMP redirect is enabled (true) or disabled (false). |
| **IcmpErrorInterval** | Defines the time (in milliseconds) to wait before sending an ICMP error message. Values range from 0 to 2147483647 ms. A value of 0 means the system does not send an ICMP error message. |
| **IcmpErrorQuota** | Indicates the number of ICMP error messages that the system can send during ICMP error interval. A value of 0 means that the system cannot send ICMP error messages. |
| **MulticastAdminStatus** | Indicates if the global multicast admin status is enabled (true) or disabled (false). |

**Related links**

Configuring IPv6 Management globally using EDM on page 256

# IPv6 Interface configuration using EDM

Use the following procedures to create, configure, or view IPv6 interface information.

**Related links**

Configuring IPv6 management using EDM on page 256
Creating an IPv6 interface using EDM on page 258
Configuring the IPv6 management interface using EDM on page 259

Graphing IPv6 Interface Statistics using EDM on page 261

## Creating an IPv6 interface using EDM

Use this procedure to create an IPv6 interface

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6** to open the IPv6 work area.
3. In the work area, click the **Interfaces** tab.
4. Click **Insert**.
5. In the **IfIndex** box, type the interface index of the management VLAN.
6. In the **Identifier** box, type the identifier portion of the address or leave the field blank to use the default MAC-based identifier that is created automatically. This is the IPv6 link-local address.
7. In the **Descr** box, type a description for this IPv6 interface (255 characters maximum length).
8. In the **ReasmMaxSize(MTU)** box, type a value in the MTU field to set the maximum size of an IPv6 packet, in bytes. The range is 1280 to 9600 and the default is 1500.
9. Click the **AdminStatus** box to create and enable the IPv6 interface at the same time.
10. In the **ReachableTime** box, you can type the reachable time. The range is 0 to 3600000 milliseconds.
11. In the **RetransmitTime** box, you can type the retransmit time. The range is 0 to 3600000 milliseconds.
12. Click **Insert**.

### Related links

IPv6 Interface configuration using EDM on page 257
Interfaces tab field descriptions on page 258

## Interfaces tab field descriptions

The following table describes the fields on the Interfaces tab.

| Name | Description |
|---|---|
| **IfIndex** | Specifies the Ifindex of the VLAN. |
| **Identifier** | Indicates the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order. |
| **IdentifierLength** | Specifies the length of the interface identifier in bits. |

*Table continues…*

| Name | Description |
|---|---|
| **Descr** | Specifies a text string containing information about the interface. The network management system also sets this string. |
| **VlanId** | Identifies the VLAN associated with the entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag. |
| **Type** | Specifies Unicast, the only supported type. |
| **ReasmMaxSize(MTU)** | Specifies the MTU for this IPv6 interface. The range is from 1280 to 9600, and the default value is 1500. |
| **PhysAddress** | Spedifies the media-dependent physical address. For Ethernet, this is a MAC address. |
| **AdminStatus** | Specifies whether the administration status of the interface is enabled (true) or disabled (false). The default is enabled (true). |
| **OperStatus** | Specifies whether the operation status of the interface is up or down. |
| **ReachableTime** | Specifies the time that a neighbor is considered reachable after receiving a reachability confirmation. Values range from 0 to 30000 milliseconds. This is an optional field. |
| **RetransmitTime** | Specifies the RetransmitTime, which is the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Values range from 0 to 3600000 milliseconds. This is an optional field. |
| **MulticastAdminStatus** | Specifies the multicast status as either True or False. |

### Related links

Creating an IPv6 interface using EDM on page 258

## Configuring the IPv6 management interface using EDM

Use this procedure to configure the IPv6 management interface, to change IPv6 parameters for the management VLAN and to view IPv6 VLAN configuration information.

### Before you begin

- An IPv6 interface must be created and attached to a VLAN before having any kind of connectivity on IPv6. One interface is permitted, and it must be attached to the management vlan. This VLAN can be the default management VLAN 1 or a custom port-based vlan that must be set as management.

### Procedure

1. In the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, click **IPv6**.

3. In the work area, click the **Interfaces** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. In the VLAN row, double-click the cell in the **Descr** column.
6. Type a descriptor for the VLAN.
7. In the VLAN row, double-click the cell in the **ReasmMaxSize(MTU)** column.
8. Type an MTU value.
9. In the VLAN row, double-click the cell in the **AdminStatus** column.
10. Select a value from the list—`true` to enable the administration status for the VLAN, or `false` to disable the administration status for the VLAN.
11. In the VLAN row, double-click the cell in the **ReachableTime** column.
12. Type a neighbor reachable time value.
13. In the VLAN row, double-click the cell in the **RetransmitTime** column.
14. Type a retransmit time value.
15. On the toolbar, click **Apply**.

**Related links**

IPv6 Interface configuration using EDM on page 257
Interfaces tab field descriptions on page 260

## Interfaces tab field descriptions

The following table describes the fields on the Interfaces tab.

| Name | Description |
|---|---|
| **IfIndex** | Specifies the Ifindex of the VLAN. |
| **Identifier** | Indicates the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order. |
| **IdentifierLength** | Indicates the length of the interface identifier in bits. |
| **Descr** | Specifies a text string containing information about the interface. The network management system also sets this string. |
| **Vlanid** | Indicates the Virtual LAN associated with the entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag. |
| **Type** | Indicates the interface port type. |
| **ReasmMaxSize(MTU)** | Specifies the MTU for this IPv6 interface. The range is from 1280 to 9600, and the default value is 1500. |

*Table continues…*

| Name | Description |
|---|---|
| **PhysAddress** | Indicates the media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address. |
| **AdminStatus** | Specifies whether the administration status of the interface is enabled (true) or disabled (false). The default is enabled (true). |
| **OperStatus** | Indicates whether the operation status of the interface is up or down. |
| **ReachableTime** | Specifies the time that a neighbor is considered reachable after receiving a reachability confirmation. Values range from 0 to 30000 milliseconds. This is an optional field. |
| **RetransmitTime** | Specifies the RetransmitTime, which is the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Values range from 0 to 3600000 milliseconds. This is an optional field. |
| **MulticastAdminStatus** | Indicates the multicast administration status as either true or false. |

**Related links**

Configuring the IPv6 management interface using EDM on page 259

## Graphing IPv6 Interface Statistics using EDM

Use this procedure to view and graph IPv6 interface statistics using EDM.

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Interfaces** tab.
4. Click **Graph**.
5. To clear the interface statistics counters, click **Clear Counters**.
6. Click the arrow on the **Poll Interval:** box.
7. Select a value from the list.
8. Select **Line Chart**, **Area Chart**, or **Bar Chart** graph type.

**Related links**

IPv6 Interface configuration using EDM on page 257
Interfaces Graph tab field descriptions on page 262

## Interfaces Graph tab field descriptions

The following table describes the fields on the Interfaces Graph tab.

| Name | Description |
|---|---|
| **InReceives** | The total number of input datagrams received from interfaces, including those received in error. |
| **InHdrErrors** | The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, and errors discovered in processing their IP options. |
| **InNoRoutes** | The number of input IP datagrams discarded because no route could be found to transmit them to their destination. |
| **InAddrErrors** | The number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |
| **InUnknownProtos** | The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. |
| **InTruncatedPkts** | The number of input IP datagrams discarded because the datagram frame did not carry enough data. |
| **InDiscards** | The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include datagrams discarded while awaiting reassembly. |
| **InDelivers** | The total number of input datagrams successfully delivered to IP user-protocols (including ICMP). |
| **OutForwDatagrams** | The number of datagrams for which this entity was not their final IP destination and for which it was successful in finding a path to their final destination. In entities that do not act as IP routers, this counter includes only those datagrams that were Source-Routed through this entity, and the Source-Route processing was successful. |

*Table continues…*

| Name | Description |
|---|---|
| **OutRequests** | The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include datagrams counted in ipForwDatagrams. |
| **OutDiscards** | The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). This counter includes datagrams counted in ipForwDatagrams if such packets met this (discretionary) discard criterion. |
| **OutFragOKs** | The number of IP datagrams that have been successfully fragmented. |
| **OutFragFails** | The number of IP datagrams that have been discarded because they needed to be fragmented but could not be. This includes IPv4 packets that have the DF bit set and IPv6 packets that are being forwarded and exceed the outgoing link MTU. |
| **OutFragCreates** | The number of output datagram fragments that have been generated because IP fragmentation. |
| **ReasmReqds** | The number of IP fragments received which needed to be reassembled at this entity. |
| **ReasmOKs** | The number of IP datagrams successfully reassembled. |
| **ReasmFails** | The number of failures detected by the IP reassembly algorithm (for whatever reason: for example, timed out, and errors). This is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. |
| **InMcastPkts** | The number of IP multicast datagrams received. |
| **OutMcastPkts** | The number of IP multicast datagrams transmitted. |

**Important:**

You can also change the Poll Interval by selecting and clicking on a value from the list. The default value for the Poll Interval is 10 ms.

**Related links**

Graphing IPv6 Interface Statistics using EDM on page 261

## Configuring an IPv6 address using EDM

Use this procedure to configure an IPv6 address for the switch using EDM.

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Addresses** tab.
4. Click **Insert**.
5. Accept the default **IfIndex** value which is the management VLAN of the switch.
6. In the **Addr** box, type an IPv6 address.
7. In the **AddrLen** box, type the IPv6 prefix length.
8. In the **Type** section, click a radio button.
9. Click **Insert**.
10. On the toolbar, click **Apply**.

### Related links

Configuring IPv6 management using EDM on page 256
Addresses tab field descriptions on page 264

## Addresses tab field descriptions

The following table describes the fields on the Addresses tab.

| Name | Description |
|---|---|
| **IfIndex** | Specifies the Ifindex of the VLAN. |
| **Addr** | Indicates the interface IPv6 address. |
| **AddrLen** | Indicates the interface IPv6 prefix length. |
| **Type** | Specifies the interface address type. Only unicast is supported for IPv6 management functions. |
| **Origin** | Indicates the origin of the interface address. Values include<br>• **other**<br>• **manual**.<br>• **dhcp**<br>• **linklayer**.<br>• **random** |

*Table continues…*

| Name | Description |
|---|---|
| **Status** | Indicates the status of the interface address. Values include<br>• **preferred**<br>• **deprecated**.<br>• **invalid**<br>• **inaccessible**.<br>• **unknown**<br>• **tentative**.<br>• **duplicate** |
| **Created** | Indicates the value of the system up time when this address was created. A value of 0 indicates that this address was created before the last network management subsystem initialization. |
| **LastChanged** | Indicates the value of the system up time when this address was last updated. A value of 0 indicates that this address was updated before the last network management subsystem initialization. |

**Related links**

Configuring an IPv6 address using EDM on page 264

# Configuring IPv6 static routes using EDM

Use this procedure to configure IPv6 static routes using EDM.

**Important:**

If the switch is not enabled for IPv6 forwarding, only the default gateway IPv6 address can be set. This is done by leaving the all zeros address unchanged, as it is automatically entered in the destination field, and entering a next-hop address in the corresponding field. In this case the next-hop is the default gateway for the switch

## Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Static Routes** tab.
4. Click **Insert**.
5. In the **Dest:** dialog box, type a value.
6. In the **PrefixLength** dialog box, type a value.

7. In the **NextHop** dialog box, type a value.
8. Perform one of the following:
   - Accept the default **IfIndex** value.
   - Click **Vlan** to select a value from the list.
9. Click **Insert**.
10. On the toolbar, click **Apply**.

**Related links**

Configuring IPv6 management using EDM on page 256
Static Routes tab field descriptions on page 266

## Static Routes tab field descriptions

The following table describes the fields on the Static Routes tab.

| Name | Description |
|---|---|
| **Dest** | Specifies the destination IP address of this route. An entry with a value of 0:0:0:0:0:0:0:0 is considered a default route. |
| **PrefixLength** | Specifies the number of leading one bits which form the mask to be logical-ANDed with the destination address before being compared to the value in the rcIpv6StaticRouteDestAddr field. |
| **NextHop** | Specifies the IP address of the next hop of this route. (In the case of a route bound to an interface which is realized using a broadcast media, the value of this field is the agent IP address on that interface). |
| **IfIndex** | Specifies the index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex. |
| **Status** | Indicates the status of the static route. |

**Related links**

Configuring IPv6 static routes using EDM on page 265

# IPv6 neighbor cache configuration using EDM

Use the following procedures to configure or view the IPv6 neighbor cache configuration.

**Related links**

Configuring IPv6 management using EDM on page 256
Configuring the IPv6 neighbor cache using EDM on page 267

Viewing the neighbor cache using EDM on page 267

## Configuring the IPv6 neighbor cache using EDM

Use this procedure to configure the IPv6 neighbor cache using EDM.

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Neighbors** tab.
4. Click **Insert**.
5. Configure IPv6 neighbor cache parameters as required.
6. Click **Insert** to save your changes.

### Related links

IPv6 neighbor cache configuration using EDM on page 266
Neighbors tab field descriptions on page 267

### Neighbors tab field descriptions

The following table describes the fields on the Neighbors tab.

| Name | Description |
|---|---|
| **IfIndex** | A unique value to identify a physical interface or a logical interface (VLAN). For the VLAN, the value is the Ifindex of the VLAN. |
| **NetAddress** | The IP address corresponding to the media-dependent physical address. |
| **PhysAddress** | The media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address. |
| **Interface** | Either a physical port ID or the Multi-Link Trunking port ID. This entry is associated either with a port or with the Multi-Link Trunking in a VLAN. |

### Related links

Configuring the IPv6 neighbor cache using EDM on page 267

## Viewing the neighbor cache using EDM

Use this procedure to view the neighbor cache to discover information about neighbors in your network. Neighbor cache in IPv6 is similar to the IPv4 Address Resolution Protocol (ARP) table. The neighbor cache is a set of entries for individual neighbors to which traffic was sent recently. You make entries on the neighbor on-link unicast IP address, including information such as the link-layer address. A neighbor cache entry contains information used by the Neighbor Unreachability

Detection algorithm, including the reachability state, the number of unanswered probes, and the time the next Neighbor Unreachability Detection event is scheduled.

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Neighbors** tab.

**Related links**

IPv6 neighbor cache configuration using EDM on page 266
Neighbors tab field descriptions on page 268

## Neighbors tab field descriptions

The following table describes the fields on the Neighbors tab.

| Name | Description |
|---|---|
| **IfIndex** | A unique value to identify a physical interface or a logical interface (VLAN). For the VLAN, the value is the Ifindex of the VLAN. |
| **NetAddress** | The IP address corresponding to the media-dependent physical address. |
| **PhysAddress** | The media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address. |
| **Interface** | Either a physical port ID or the Multi-Link Trunking port ID. This entry is associated either with a port or with the Multi-Link Trunking in a VLAN. |
| **LastUpdated** | The value of sysUpTime at the time this entry was last updated. If this entry was updated prior to the last reinitialization of the local network management subsystem, this object contains a zero value. |
| **Type** | The type of mapping is as follows:<br>• **Dynamic type**: Indicates that the IP address to the physical address mapping is dynamically resolved using, for example, IPv4 ARP or the IPv6 Neighbor Discovery Protocol..<br>• **Static type**: Indicates that the mapping is statically configured.<br>• **Local type**: Indicates that the mapping is provided for the interface address. |
| **State** | Specifies the Neighbor Unreachability Detection state for the interface when the address mapping in this entry is used. If Neighbor Unreachability |

*Table continues…*

| Name | Description |
|---|---|
| | Detection is not in use (for example, for IPv4), this object is always unknown. Options include the following:<br>• **reachable**: confirmed reachability<br>• **stale**: unconfirmed reachability<br>• **delay**: waiting for reachability confirmation before entering the probe state<br>• **probe**: actively probing<br>• **invalid**: an invalidated mapping<br>• **unknown**: state cannot be determined<br>• **incomplete**:address resolution is being performed |

**Related links**

Viewing the neighbor cache using EDM on page 267

# Graphing IPv6 interface ICMP statistics using EDM

Use this procedure to display and graph IPv6 interface ICMP statistics.

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **ICMP Stats** tab.
4. To clear the interface statistics counters, click **Clear Counters**.
5. Click the arrow on the **Poll Interval:** box.
6. Select a value from the list.
7. To select data to graph, click a data row under a column heading.
8. Click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

**Related links**

Configuring IPv6 management using EDM on page 256
ICMP Stats tab field descriptions on page 269

## ICMP Stats tab field descriptions

The following table describes the fields on the ICMP Stats tab.

| Name | Description |
|---|---|
| **InMsgs** | Number of ICMP messages received. |
| **InErrors** | Number of ICMP error messages received |
| **OutMsgs** | Number of ICMP messages sent. |
| **OutErrors** | Number of ICMP error messages sent. |
| **Poll Interval** | Sets polling interval. Value: 2 to 60 s. |

**Related links**

Graphing IPv6 interface ICMP statistics using EDM on page 269

# Viewing ICMP message statistics using EDM

Use this procedure to view the IPv6 interface ICMP message statistics using EDM

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **ICMP Msg Stats** tab.
4. Click **Refresh** to update the ICMP message statistics.

**Related links**

Configuring IPv6 management using EDM on page 256
ICMP Msg Stats tab field descriptions on page 270

## ICMP Msg Stats tab field descriptions

The following table describes the fields on the ICMP Msg Stats tab.

| Name | Description |
|---|---|
| **Type** | Type of packet received or sent. |
| **InPkts** | Number of packets received. |
| **OutPkts** | Number of packets sent. |

**Related links**

Viewing ICMP message statistics using EDM on page 270

# Viewing global IPv6 TCP properties using EDM

Use this procedure to view IPv6 TCP properties for the switch.

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **TCP/UDP**.
3. In the work area, click the **TCP Globals** tab.
4. Click **Refresh** to update the information.

### Related links

Configuring IPv6 management using EDM on page 256
TCP Globals tab field descriptions on page 271

## TCP Globals tab field descriptions

The following table describes the fields on the TCP Globals tab.

| Name | Description |
|---|---|
| **RtoAlgorithm** | Algorithm identifier. |
| **RtoMin** | Minimum value in milliseconds. |
| **RtoMax** | Maximum value in milliseconds. |
| **MaxConn** | Maximum number of connections. |

### Related links

Viewing global IPv6 TCP properties using EDM on page 270

# Viewing IPv6 TCP connections using EDM

Use this procedure to view IPv6 TCP connections using EDM.

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **TCP/UDP**.
3. In the work area, click the **TCP connections** tab.
4. Click **Refresh** to update the information.

### Related links

Configuring IPv6 management using EDM on page 256
TCP connections tab field descriptions on page 271

## TCP connections tab field descriptions

The following table describes the fields on the TCP connections tab.

| Name | Description |
|---|---|
| **LocalAddressType** | Local address type |
| **LocalAddress** | Local address |
| **LocalAddress Port** | Local address port |
| **LocalPort** | Local port IP |
| **RemAddress Type** | Remote address type |
| **RemAddress** | Remote address |
| **RemPort** | Remote port IP |
| **State** | State<br>• Enabled<br>• Disabled |

**Related links**

Viewing IPv6 TCP connections using EDM on page 271

# Viewing IPv6 TCP listeners using EDM

Use this procedure to view IPv6 TCP listeners using EDM.

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **TCP/UDP**.
3. In the work area, click the **TCP Listeners** tab.
4. Click **Refresh** to update the information.

**Related links**

Configuring IPv6 management using EDM on page 256
TCP Listeners tab field descriptions on page 272

## TCP Listeners tab field descriptions

The following table describes the fields on the TCP Listeners tab.

| Name | Description |
|---|---|
| **LocalAddressType** | Local address type |
| **LocalAddress** | Local address |
| **Local Port** | Local port |

**Related links**

Viewing IPv6 TCP listeners using EDM on page 272

## Viewing IPv6 UDP endpoints using EDM

Use this procedure to view IPv6 UDP endpoints using EDM

### Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **TCP/UDP**.
3. In the work area, click the **UDP Endpoints** tab.
4. Click **Refresh** to update the information.

### Related links

Configuring IPv6 management using EDM on page 256
UDP Endpoints tab field descriptions on page 273

## UDP Endpoints tab field descriptions

The following table describes the fields on the UDP Endpoints tab.

| Name | Description |
|---|---|
| **LocalAddressType** | Local address |
| **LocalAddress** | Local address port |
| **Local Port** | Local port IP |
| **RemoteAddressType** | Remote address type |
| **RemoteAddress** | Remote address |
| **RemotePort** | Remote port IP |
| **Instance** | Indicates the instance. |
| **Process** | Indicates the process. |

### Related links

Viewing IPv6 UDP endpoints using EDM on page 273

# Configuring Storm Control using EDM

Use the procedures in this section to configure Storm Control globally and for specific traffic type.

### Related links

Configuring Storm Control globally on page 274
Configuring Broadcast Storm Control on page 275
Configuring Multicast Storm Control on page 276
Configuring Unicast Storm Control on page 278

# Configuring Storm Control globally

## About this task

Use the following procedure to globally configure Storm Control using EDM

## Procedure

1. In the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree double-click **Storm Control**.
3. In the work area, click the **Globals** tab.
4. Configure the Storm Control parameters as required.
5. On the toolbar, click **Apply**.

# Global Storm Control field descriptions

| Name | Description |
|---|---|
| **TrafficType** | Indicates the different types of traffic for Storm Control Settings.<br>• **unicast**: Indicates the unicast storm control settings<br>• **broadcast**: Indicates the broadcast Storm Control settings<br>• **multicast**: Indicates the multicast Storm Control settings |
| **Enabled** | Indicates the current setting for the port. Values include:<br>• **true**: enables Storm Control on the port<br>• **false**: disables Storm Control on the port |
| **LowWatermark(pps)** | Indicates the low-watermark value for the port in packets per second (pps).<br>RANGE: 10 to 100000000 |
| **HighWatermark(pps)** | Indicates the high-watermark value for the port in packets per second (pps).<br>RANGE: 10 to 100000000 |
| **PollInterval(secs)** | Indicates the interval for watermark checking, the value varies in seconds.<br>RANGE: 5 to 300 |
| **TrapInterval** | Indicates the interval for sending traps when the poll-intervals exceed. |

*Table continues…*

| Name | Description |
|---|---|
| | RANGE: 0 to 1000<br>**Note:**<br>Value 0 means disabled (high watermark traps will not be repeated) |
| **ActionType** | Indicates the Storm Control action for the specified port.<br>• **drop**: Set Storm Control action to drop<br>• **none**<br>• **shutdown**: Set Storm Control action to shutdown |

# Configuring Broadcast Storm Control

## About this task

Use the following procedure to configure the Broadcast Storm Control settings.

## Procedure

1. In the navigation tree double-click **Edit** to open the Edit tree.
2. In the Edit tree, double-click **Storm Control**.
3. In the work area click the **Broadcast** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **Enabled** column.
6. Set a value from the drop-down list — **true** to enable Storm Control, or **false** to disable Storm Control for the specified port.
7. In the port row, double-click the cell in the **LowWatermark(pps)** column, and enter a value in the range `<10-100000000>`.
8. In the port row, double-click the cell in the **HighWatermark(pps)** column, and enter a value in the range `<10-100000000>`.
9. In the port row, double-click the cell in the **PollInterval(secs)**column, and enter a value in the range `<5-300>`.
10. In the port row, double-click the cell in the **TrapInterval**column, and enter a value in the range `<0-1000>`.
11. In the port row, double-click the cell in the **ActionType** column.
12. Set a value from the drop-down list — **none** to take no action, **drop** , or **shutdown** to shutdown Storm Control for specified port.
13. Click **Apply Selection**.

14. On the toolbar, click **Apply**.

## Broadcast Storm Control field descriptions

| Name | Description |
|---|---|
| **Index** | Indicates the port number. |
| **Enabled** | Indicates the current setting for the port. Values include:<br>• **true**: enables Storm Control on the port<br>• **false**: disables Storm Control on the port |
| **LowWatermark(pps)** | Indicates the low-watermark value for the port in packets per second (pps).<br>RANGE: 10 to 100000000 |
| **HighWatermark(pps)** | Indicates the high-watermark value for the port in packets per second (pps).<br>RANGE: 10 to 100000000 |
| **PollInterval(secs)** | Indicates the interval for watermark checking, the value varies in seconds.<br>RANGE: 5 to 300 |
| **TrapInterval** | Indicates the interval for sending traps when the poll-intervals exceed.<br>RANGE: 0 to 1000<br>**Note:**<br>Value 0 means disabled (high watermark traps will not be repeated) |
| **ActionType** | Indicates the Storm Control action for the specified port.<br>• **drop**: Set Storm Control action to drop<br>• **none**:<br>• **shutdown**: Set Storm Control action to shutdown |

# Configuring Multicast Storm Control

### About this task

Use the following procedure to configure the Multicast Storm Control setting

### Procedure

1. In the navigation tree double-click **Edit** to open the Edit tree.
2. In the Edit tree, double-click **Storm Control**.

3. In the work area click the **Multicast** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **Enabled** column.
6. Set a value from the drop-down list — **true** to enable Storm Control, or **false** to disable Storm Control for the specified port.
7. In the port row, double-click the cell in the **LowWatermark(pps)** column, and enter a value in the range `<10-100000000>`.
8. In the port row, double-click the cell in the **HighWatermark(pps)** column, and enter a value in the range `<10-100000000>`.
9. In the port row, double-click the cell in the **PollInterval(secs)column**, and enter a value in the range `<5-300>`.
10. In the port row, double-click the cell in the **TrapIntervalcolumn**, and enter a value in the range `<0-1000>`.
11. In the port row, double-click the cell in the **ActionType** column.
12. Set a value from the drop-down list — **none** to take no action, **drop** , or **shutdown** to shutdown Storm Control for specified port.
13. Click **Apply Selection**.
14. On the toolbar, click **Apply**.

## Multicast Storm Control field descriptions

| Name | Description |
|---|---|
| **Index** | Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell. |
| **Enabled** | Indicates the current setting for the port. Values include:<br>• **true**: enables Storm Control on the port<br>• **false**: disables Storm Control on the port |
| **LowWatermark(pps)** | Indicates the low-watermark value for the port in packets per second (pps).<br>RANGE: 10 to 100000000 |
| **HighWatermark(pps)** | Indicates the high-watermark value for the port in packets per second (pps).<br>RANGE: 10 to 100000000 |
| **PollInterval(secs)** | Indicates the interval for watermark checking, the value varies in seconds.<br>RANGE: 5 to 300 |

*Table continues…*

| Name | Description |
|---|---|
| **TrapInterval** | Indicates the interval for sending traps when the poll-intervals exceed.<br>RANGE: 0 to 1000<br>**Note:**<br>Value 0 means disabled (high watermark traps will not be repeated) |
| **ActionType** | Indicates the Storm Control action for the specified port.<br>• **drop**: Set Storm Control action to drop<br>• **none**:<br>• **shutdown**: Set Storm Control action to shutdown |

# Configuring Unicast Storm Control

## About this task

Use the following procedure to configure the Unicast Storm Control settings.

## Procedure

1. In the navigation tree double-click **Edit** to open the Edit tree.
2. In the Edit tree, double-click **Storm Control**.
3. In the work area click the **Unicast** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **Enabled** column.
6. Set a value from the drop-down list — **true** to enable Storm Control, or **false** to disable Storm Control for the specified port.
7. In the port row, double-click the cell in the **LowWatermark(pps)** column, and enter a value in the range `<10-100000000>`.
8. In the port row, double-click the cell in the **HighWatermark(pps)** column, and enter a value in the range `<10-100000000>`.
9. In the port row, double-click the cell in the **PollInterval(secs)** column, and enter a value in the range `<5-300>`.
10. In the port row, double-click the cell in the **TrapIntervalcolumn**, and enter a value in the range `<0-1000>`.
11. In the port row, double-click the cell in the **ActionType** column.
12. Set a value from the drop-down list — **none** to take no action, **drop** , or **shutdown** to shutdown Storm Control for specified port.

13. Click **Apply Selection**.
14. On the toolbar, click **Apply**.

## Unicast Storm Control field descriptions

| Name | Description |
|---|---|
| **Index** | Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell. |
| **Enabled** | Indicates the current setting for the port. Values include:<br>• **true**: enables Storm Control on the port<br>• **false**: disables Storm Control on the port |
| **LowWatermark(pps)** | Indicates the low-watermark value for the port in packets per second (pps).<br>RANGE: 10 to 100000000 |
| **HighWatermark(pps)** | Indicates the high-watermark value for the port in packets per second (pps).<br>RANGE: 10 to 100000000 |
| **PollInterval(secs)** | Indicates the interval for watermark checking, the value varies in seconds.<br>RANGE: 5 to 300 |
| **TrapInterval** | Indicates the interval for sending traps when the poll-intervals exceed.<br>RANGE: 0 to 1000<br>**Note:**<br>Value 0 means disabled (high watermark traps will not be repeated) |
| **ActionType** | Indicates the Storm Control action for the specified port.<br>• **drop**: Set Storm Control action to drop<br>• **none**:<br>• **shutdown**: Set Storm Control action to shutdown |

# Configuring rate limiting using EDM

Use this procedure to display and configure rate limiting on a switch.

### Procedure

1. From the Device Physical View, click a unit.
2. From the navigation tree, click **Edit**.
3. In the Edit tree, click **Unit**.
4. In the work area, select the **Rate Limit** tab.
5. To a rate limit, click a TrafficType row.
6. Double-click the cell in the **AllowedRatePps** column.
7. Type a value.
8. Double-click the cell in the **Enable** column.
9. Select a value from the list — true to enable the traffic type, or false to disable the traffic type.
10. On the toolbar, click **Apply**.

## Rate Limit tab field descriptions

The following table describes the fields on the Rate Limit tab.

| Name | Description |
|---|---|
| **Traffic Type** | Specifies the traffic type. |
| **AllowedRatePps** | Allowed traffic rate packets/second. It is in the range of 0–262143.<br>**Important:**<br>Rate Limiting feature is disabled when AllowedRatePps is set to 0. |
| **Enable** | When Enable is set to True, the TrafficType can either be multicast, broadcast, or both.<br>**Important:**<br>You cannot set the Enabled field for both multicast and broadcast TrafficType to False at the same time. This is an illegal configuration. |

# Chapter 8: Appendix A

This section contains information about the following topics:

- TACACS+ server configuration examples
- SNMP MIB support

## TACACS+ server configuration examples

This section describes basic configuration examples of the TACACS+ server.

### Configuration example Cisco ACS (Version 3.2) server

The following figure shows the main administration window.

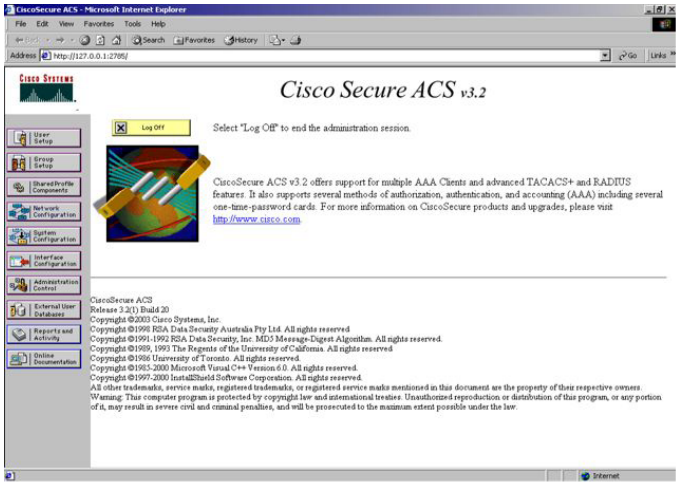



**Figure 5: Cisco ASC (version 3.2) main administration window**

1. Define the users and the corresponding authorization levels.

   If you map users to default group settings, it is easier to remember which user belongs to each group. For example, the rwa user belongs to group 15 to match Privilege level 15. All rwa user settings are picked up from group 15 by default.

   The following figure shows a sample Group Setup window.

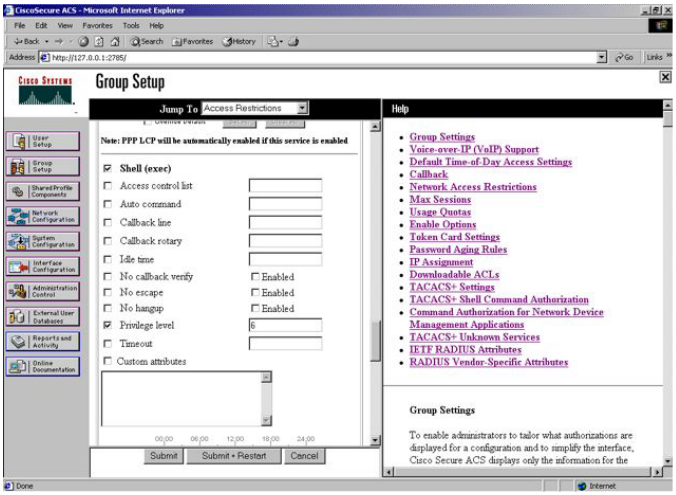



**Figure 6: Group Setup window - Cisco ACS server configuration**

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+.

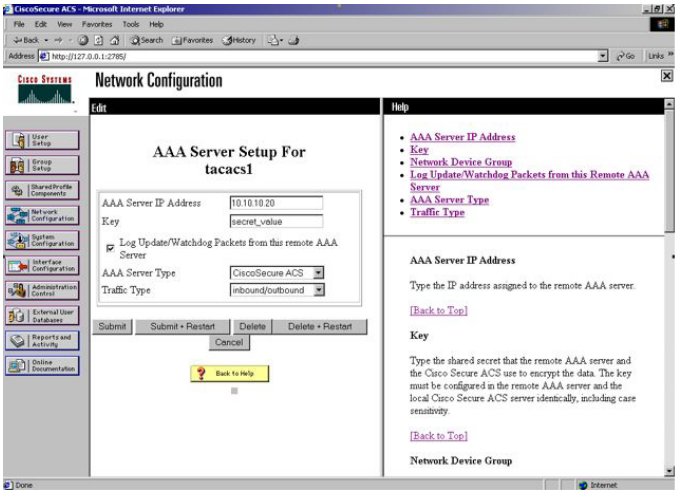



**Figure 7: Network Configuration window - server setup**

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 Avaya Ethernet Routing Switch 3500.

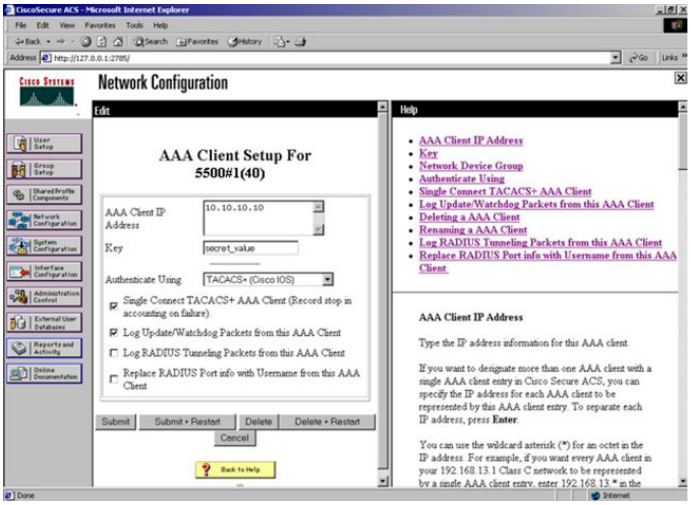



**Figure 8: Network Configuration window - client setup**

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.

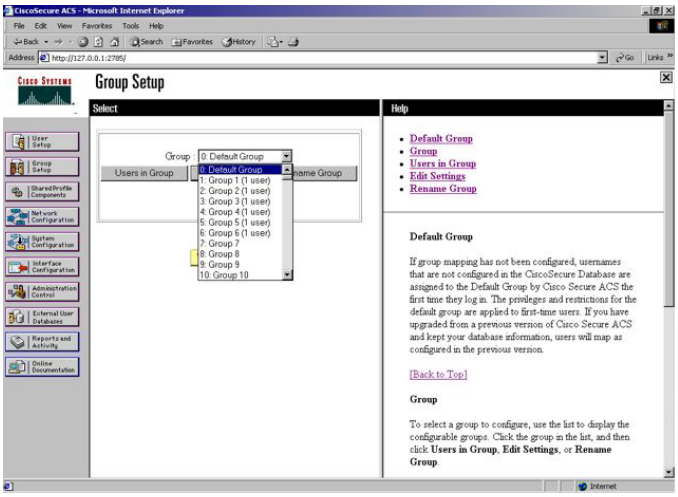



**Figure 9: Group Setup window - viewing the group setup**

5. Go to **Shared Profile Components , Shell Command Authorization Set.**

   The Shell Command Authorization Set screen appears.

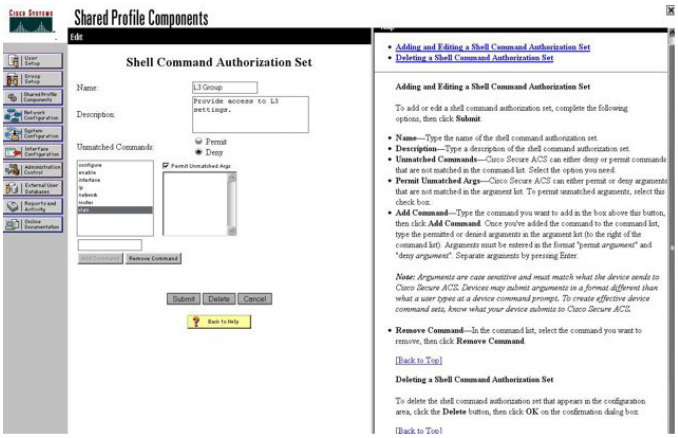



**Figure 10: Shared Profile Components window - defining the command set**

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.

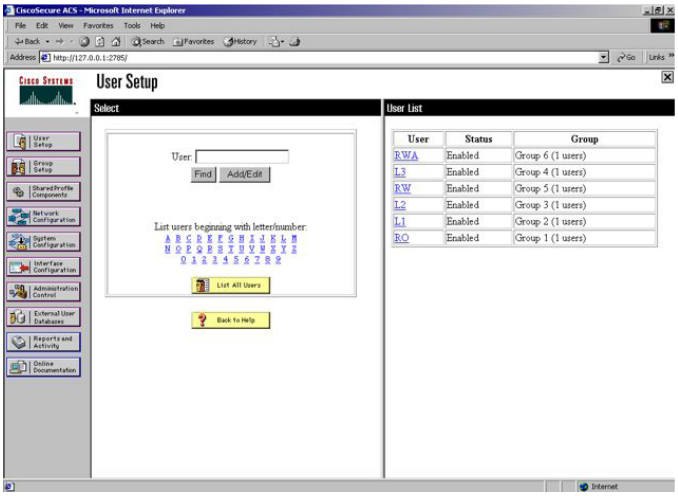



**Figure 11: User Setup window - Cisco ACS server configuration**

# Configuration example ClearBox server

1. Run the General Extension Configurator and configure the user data source.

   In this example, Microsoft Access was used to create a database of user names and authorization levels; the general.mdb file needs to include these users.

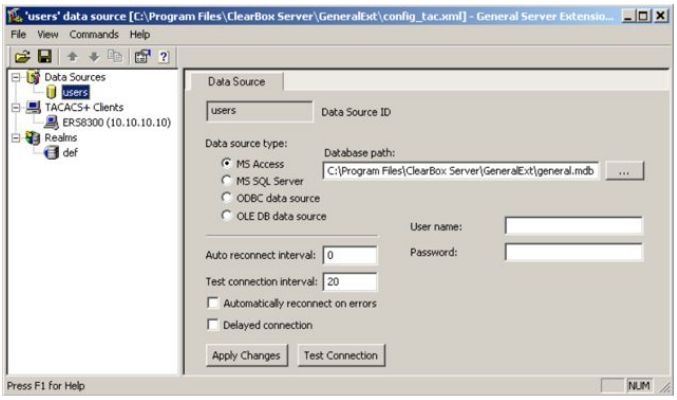



**Figure 12: General Extension Configurator**

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 Avaya Ethernet Routing Switch 3500. Enter the appropriate information. The shared secret must match the value configured on the Avaya Ethernet Routing Switch 3500.

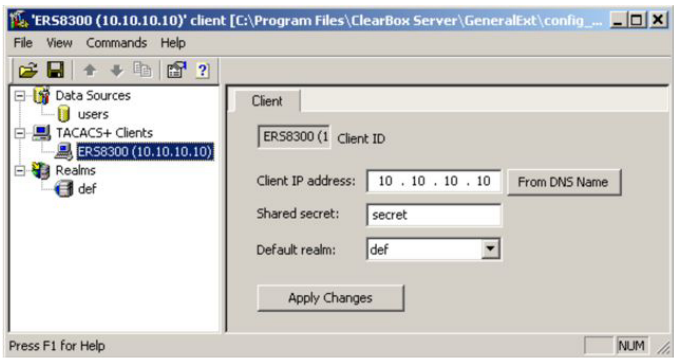



**Figure 13: Creating a client entry**

The default realm Authentication tab looks like the following figure.

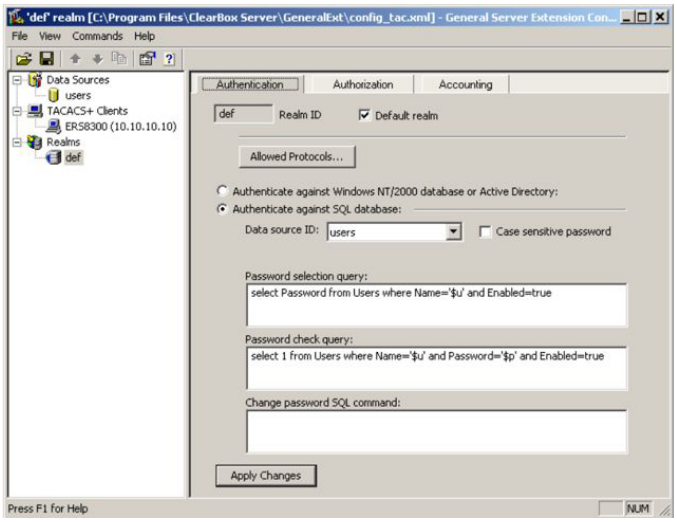



**Figure 14: Default realm - Authentication tab**

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 .

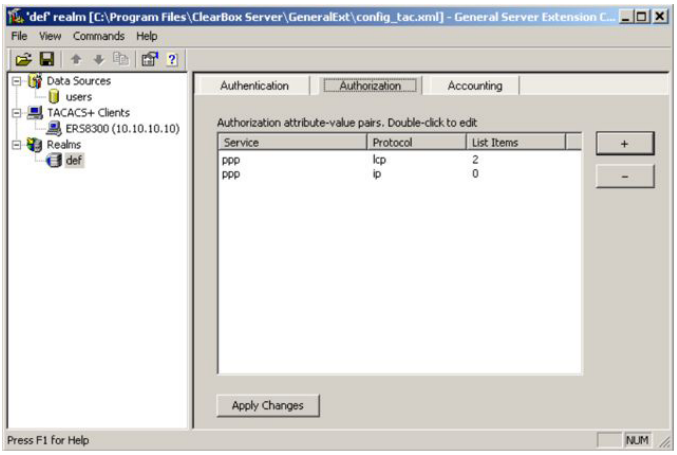



**Figure 15: Default realm - Authorization tab**

5. Enter information in the window as shown in the following figure to specify the query parameters.

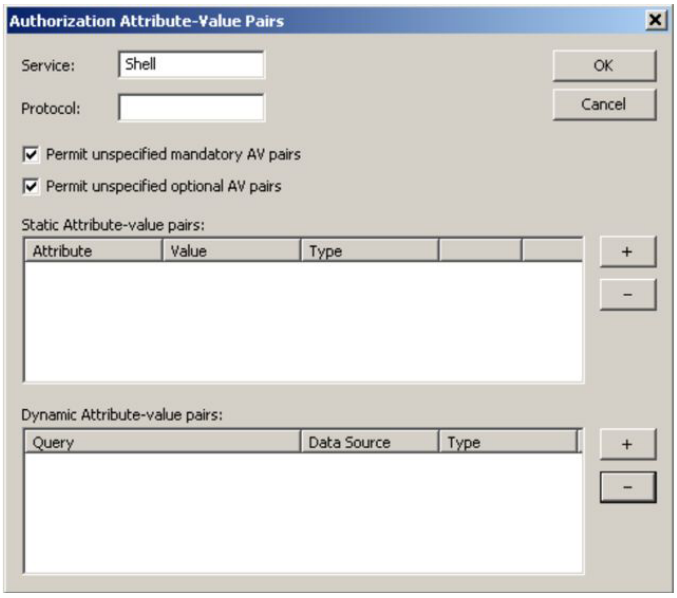
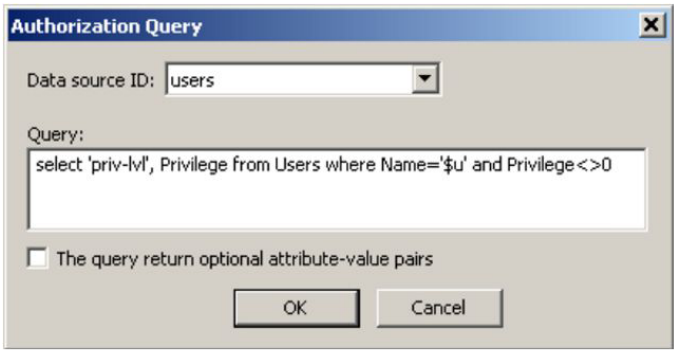
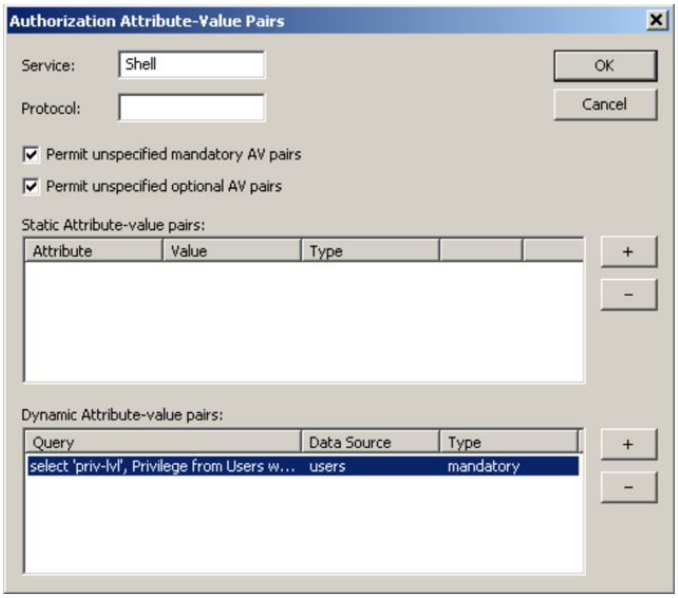



**Figure 16: Adding parameters for the query**

6. Click the **+** button to add the parameters to the query.
7. Use the string shown in the following figure for the authorization query.




The following figure shows the final window.




8. Click **OK**.

   The information appears on the **Authorization** tab.

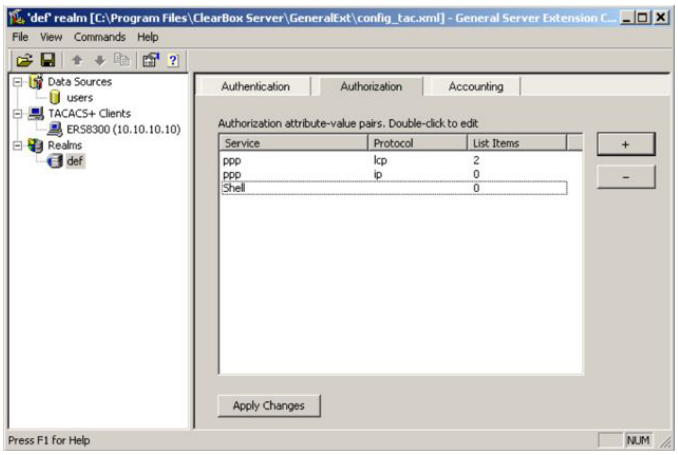



**Figure 17: Authorization attribute-value pairs added to Authorization tab**

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 18: Users table - Microsoft Access**

10. Run the Server Manager.

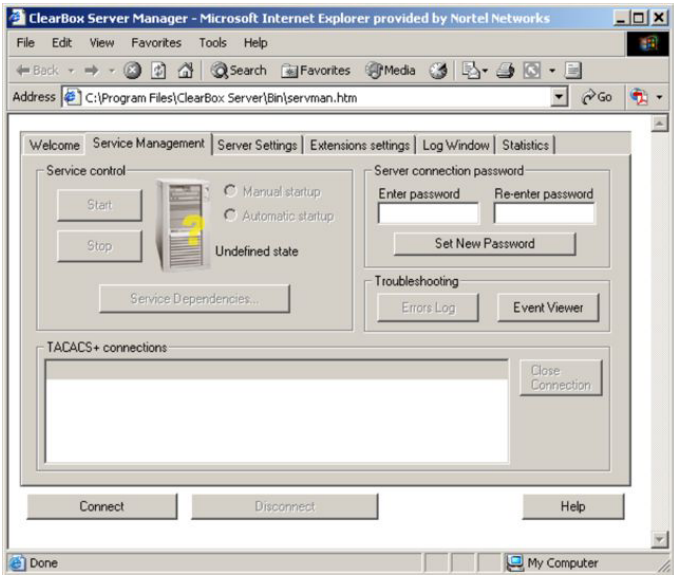



**Figure 19: ClearBox Server Manager**

11. Click the **Connect** button.

    The **Connect to...** dialog box appears.

**Figure 20: Connect to... dialog box**

12. Click **OK** (do not fill in fields).
13. Click **OK** at the warning message.
14. Click **Start**.

    Changes to the General Server Extension Configurator require that the server be restarted.

# SNMP MIB support

The Avaya Ethernet Routing Switch 3500 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.

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 5: SNMP MIB support**

| Application | Standard MIBs | Proprietary MIBs |
|---|---|---|
| **S5 Chassis MIB** | | s5cha127.mib |
| **S5Agent 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 Avaya Ethernet Routing Switch 3500 Series supports an SNMP agent with industry standard SNMPv1 traps, as well as private SNMPv1 trap extensions.

| 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. |
| **entConfigChange** | rfc4133MIB | A change in either of these tables occurred: entPhysicalTable, |

*Table continues…*

| Trap name | MIB | Sent when |
|---|---|---|
| | | 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** | bayStackDhcpSnoopi ngMIB | An attempt is made to add a new DHCP binding entry when the binding table is full. |
| **bsDhcpSnoopingTrap** | bayStackDhcpSnoopi ngMIB | A DHCP packet is dropped. |
| **bsaiArpPacketDroppedOnUntrustedPort** | bayStackArpInspectio nMIB | An ARP packet is dropped on an untrusted port due to an invalid IP/MAC binding. |
| **bsSourceGuardReachedMaxIpEntries** | bayStackSourceGuar dMIB | The maximum number of IP entries on a port has been reached. |
| **bsSourceGuardCannotEnablePort** | bayStackSourceGuar dMIB | 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. |
| **bsnLacTrunkUnavailable** | bsnMIB | An attempt is made to form an 802.3ad LAG trunk, but there are no available resources to create a new trunk. |
| **bsnLoginFailure** | bsnMIB | An attempt to login to the system fails as a result of an incorrect password. |

*Table continues…*

| Trap name | MIB | Sent when |
|---|---|---|
| **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. |
| **bsnEapRAVError** | 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. |
| **s5CtrFanDirectionError** | s5CtrMIB | A fan component's direction is incorrect |
| **s5CtrHighTemperatureError** | s5CtrMIB | The system is overheated. |

# Sticky MAC address configuration examples

The following configuration examples describe the basic steps required to:

- configure a device to learn sticky MAC addresses on a range of ports
- manually configure sticky MAC address on an individual port

**Note:**

Avaya recommends that you disable autosave when sticky mac is enabled.

## Before you begin

Globally enable the following:

- MAC security
- autolearning mode

For the specific interfaces on which you are configuring sticky MAC address, enable the following :

- MAC security
- autolearning sticky mode

**Configuring a device to learn sticky MAC addresses on a range of ports:**

Ports 1/6 through 1/14 are used for this example.

1. Enable MAC security and auto-learning globally.

```
ERS3500(config)#mac-security enable
ERS3500(config)#mac-security auto-learning sticky
ERS3500(config)#no autosave enable
ERS3500(config)#copy config nvram
```

2. Enable MAC security and auto-learning on ports 1/6-14.

```
ERS3500(config)#interface fastEthernet 1/6-14
ERS3500(config-if)#mac-security enable
```

```
ERS3500(config-if)#mac-security auto-learning enable
ERS3500(config-if)#mac-security auto-learning max-addrs
<1-25>
ERS3500(config-if)#no mac-security autolearning
ERS3500(config-if)#mac-security enable
ERS3500(config-if)#exit
```

3. Verify the MAC security configuration for the interfaces.

```
ERS3500(config)#show mac-security port 1/6-14
```

```
Unit        Port      Trunk        Security      Auto-Learning  MAC Number
--------    --------  --------     --------      ------         ------
    1         6                    Enabled       Enabled            2
    1         7                    Enabled       Enabled            2
    1         8                    Enabled       Enabled            2
    1         9                    Enabled       Enabled            2
    1        10                    Enabled       Enabled            2
    1        11                    Enabled       Enabled            2
    1        12                    Enabled       Enabled            2
    1        13                    Enabled       Enabled            2
    1        14                    Enabled       Enabled            2
```

4. Connect a PC to port 1/8 and verify the configuration by displaying the MAC security MAC address table.

```
ERS3500#show mac-security mac-address-table
```

```
Number of addresses:  1


Unit        Port      Allowed MAC Address         Type
--------    --------  --------                    -------
1           8         00-02-A5-E9-00-28           Sticky


Security List         Allowed MAC Address         Type
--------              --------                    -------
```