



# Configuring Security on Ethernet Routing Switch 3500 Series

Release 5.3.6  
9035601  
July 2018

© 2018, Extreme Networks, 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, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. 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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks 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 or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks' 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

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks 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. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

#### Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks' standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: <http://www.extremenetworks.com/support> under the link "Policies" or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

"Hosted Service" means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks 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 Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

#### Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, 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.

#### Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS, INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS 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 EXTREME NETWORKS, INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE ("EXTREME NETWORKS").

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. 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 Extreme Networks or an Extreme Networks 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 set of Designated Processors that hosts (physically or virtually) 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 type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks 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 Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

#### 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 Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks 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 Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks 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, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks 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 Extreme Networks' website at: <http://www.extremenetworks.com/support/policies/software-licensing> or such successor site as designated by Extreme Networks. 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 only 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](http://WWW.MPEGLA.COM).

### Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS 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 EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS 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](http://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](http://WWW.MPEGLA.COM).

### Compliance with Laws

You acknowledge and agree that it is Your responsibility 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 Extreme Networks 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.

### Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at <https://gtacknowledge.extremenetworks.com/>.

### Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: <http://documentation.extremenetworks.com>, or such successor site as designated by Extreme Networks.

### Contact Extreme Networks Support

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

### Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks 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 Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the U.S. and other countries.

For additional information on Extreme Networks trademarks, please see: <http://www.extremenetworks.com/company/legal/>

# Contents

<b>Chapter 1: Preface</b> .....	14
Purpose.....	14
Training.....	14
Providing Feedback to Us.....	14
Getting Help.....	14
Extreme Networks Documentation.....	15
Subscribing to Service Notifications.....	15
<b>Chapter 2: New in this document</b> .....	17
Other Changes.....	17
<b>Chapter 3: CLI command modes</b> .....	18
<b>Chapter 4: Security fundamentals</b> .....	20
Management password configuration.....	20
Console TELNET password Configuration.....	20
Unified authentication.....	20
Logging on.....	20
MAC address-based security.....	21
MAC address-based security autolearning.....	21
Sticky MAC address.....	22
Block subsequent MAC authentication.....	22
RADIUS-based network security.....	24
How RADIUS works.....	24
RADIUS server configuration.....	24
RADIUS EAP or non-EAP requests to different servers.....	25
RADIUS server reachability.....	28
RADIUS password fallback.....	29
RADIUS Interim Accounting Updates support.....	29
RADIUS Request use Management IP Address.....	29
Campus security example.....	30
EAPOL-based security.....	32
EAPOL Security Configuration.....	33
EAPOL with Guest VLAN.....	34
Advanced EAPOL features.....	34
Multiple Host with Multiple Authentication.....	34
RADIUS-assigned VLAN use in MHMA mode.....	35
Non-EAP IP Phone authentication.....	36
Unicast EAP Requests in MHMA.....	36
802.1X or non-EAP with VLAN names.....	36
802.1X or Non-EAP and Guest VLAN on the same port.....	37
Non-EAP hosts on EAP-enabled ports.....	37

Non-EAPOL MAC RADIUS authentication.....	38
Multiple Host with Single Authentication.....	39
MHSA No-Limit.....	40
802.1X Non-EAP client re-authentication.....	40
NEAP Not Member of VLAN.....	41
802.1X or non-EAP Last Assigned RADIUS VLAN.....	41
802.1X or non-EAP with Fail Open VLAN.....	42
Fail Open VLAN Continuity Mode.....	43
Fail Open UBP.....	44
802.1X dynamic authorization extension (RFC 3576).....	44
802.1X EAP and NEAP Accounting .....	46
802.1X EAP Separate enable/disable.....	47
TACACS+.....	48
TACACS+ architecture.....	49
Feature operation.....	49
TACACS+ authentication.....	49
TACACS+ authorization.....	50
Changing privilege levels at run time.....	50
TACACS+ server configuration example.....	51
TACACS+ accounting.....	53
Feature limitations.....	54
TACACS+ configuration.....	54
IP Manager.....	54
Password security.....	55
Custom user names and passwords.....	55
Log on failure timeout.....	56
Password security.....	56
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
Support for SNMP in the switch.....	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
SHA-2 Support for SSL Certificates.....	63
DHCP snooping.....	63
DHCP binding table.....	64
Dynamic ARP inspection.....	65
IP Source Guard.....	66
Secure File Transfer Protocol (SFTP over SSH).....	67
SSH enhancement to support RSA.....	68
Storm Control.....	68
Rate limiting configuration.....	68
<b>Chapter 5: Configuring and managing security using CLI.....</b>	<b>70</b>
Configuring and managing security using CLI.....	70
Setting the system user name and password .....	70
Setting the password for selected types of access using CLI.....	71
Enabling or disabling password security using CLI.....	72
Displaying the security .....	72
Displaying the status of password security on the switch .....	73
Configuring the number of password logon attempts.....	73
Configuring password aging-time.....	74
Configuring password check-repeated.....	74
Configuring password check-sequential.....	75
Configuring password complexity.....	76
Configuring minimum password length.....	77
Changing the http port number.....	78
Displaying the port number of the HTTP port.....	78
Setting the HTTP port number .....	79
USB port and serial console port control .....	79
Disabling serial console ports.....	79
Enabling serial console ports.....	80
Viewing serial console port status.....	80
Disabling USB ports.....	81
Enabling USB ports.....	81
Viewing USB port status.....	82
Setting Telnet access using CLI.....	82
Displaying Telnet access settings.....	83
Configuring Telnet connections .....	83
Disabling Telnet access.....	85
Setting the Telnet settings to default values .....	86
Configuring SSL using CLI.....	86
Enabling or disabling SSL .....	86
Creating or deleting an SSL certificate.....	87
Viewing the SSL server configuration.....	87
Viewing the SSL certificate.....	88

Regenerating the SSL Certificate.....	89
Secure Shell protocol configuration using CLI.....	90
Displaying SSH information .....	90
Configuring SSH.....	91
Generating the DSA host keys.....	91
Generating the SSH RSA host key.....	92
Downloading DSA or RSA authentication keys.....	92
Deleting the SSH DSA authentication key .....	93
Deleting the SSH RSA authentication key.....	93
Enabling user log-on with an SSH DSA key.....	93
Enabling user log-on with an SSH RSA key .....	94
Enabling user log-on with SSH password authentication .....	94
Disabling SNMP and Telnet With SSH .....	94
Configuring the TCP port for SSH daemon.....	95
Configuring the timeout value for session authentication .....	95
<b>Configuring and clearing the SSH banner.....</b>	<b>96</b>
<b>Configuring and clearing the SSH banner.....</b>	<b>97</b>
Secure Shell Client configuration.....	97
Configuring SFTP authentication for SSH Client .....	98
Generating an SSHC DSA host key.....	98
Generating an SSHC RSA host key (public and private).....	99
Configuring SSHC DSA host key size.....	99
Configuring SSHC RSA host key size.....	100
Configuring the SSHC port.....	100
Viewing Secure File Transfer Protocol (SFTP).....	101
Uploading the public host key.....	102
Uploading a config file to an SFTP server .....	103
Downloading a config file from an SFTP server.....	103
Configuring RADIUS Interim Accounting Updates support using CLI.....	104
Configuring RADIUS Interim Accounting Updates support .....	104
Disabling RADIUS Interim Accounting Updates support.....	105
Configuring RADIUS Interim Accounting Updates support defaults .....	106
Viewing RADIUS Interim Accounting Updates support status .....	106
Configuring RADIUS Request use Management IP using CLI.....	107
Enabling RADIUS request use of Management IP .....	107
Disabling RADIUS request use of Management IP.....	107
Viewing RADIUS request use Management IP status .....	108
Configuring RADIUS authentication using CLI.....	108
Configuring switch RADIUS server settings .....	108
Enabling or disabling RADIUS password fallback .....	110
Viewing RADIUS information .....	110
Configuring RADIUS server reachability.....	111
Viewing the RADIUS server reachability method .....	112

Configuring 802.1X dynamic authorization extension (RFC 3576) configuration using CLI.....	112
Configuring RADIUS dynamic authorization extension (802.1X RFC 3576) .....	112
Disabling RADIUS dynamic authorization extension (802.1X RFC 3576).....	113
Viewing RADIUS dynamic authorization client configuration .....	114
Viewing RADIUS dynamic authorization client statistics .....	114
Enabling or disabling RADIUS dynamic authorization extension (802.1X RFC 3576) on a port .....	115
Viewing replay protection for RADIUS dynamic authorization extension.....	116
Enabling or disabling replay protection for RADIUS dynamic authorization extension .....	116
Setting SNMP parameters using CLI.....	116
Enabling or disabling the SNMP server .....	117
Disabling SNMP access .....	117
Enabling disabling or restoring to default the generation of SNMP authentication failure traps .....	117
Modifying the community strings for SNMPv1 and SNMPv2c access.....	118
Clearing the SNMP server community configuration.....	119
Restoring the community string configuration to default settings.....	119
Displaying SNMP community string configuration.....	120
Configuring the SNMP sysContact value.....	120
Clearing or restoring the SNMP sysContact value to default value .....	120
Configuring or clearing the SNMP sysLocation value.....	121
Restoring the SNMP sysLocation to the default.....	121
Configuring the SNMP sysName value.....	122
Clearing the SNMP sysName value.....	122
Enabling SNMP linkUp linkDown traps for a port.....	122
Disabling the SNMP linkUp linkDown traps for a port.....	123
Adding SNMP traps to a filter profile .....	124
Deleting SNMP traps from a filter profile.....	124
Displaying notify-filter details.....	125
Enabling or disabling the generation of SNMP traps.....	125
Using CLI commands specific to SNMPv3.....	126
Creating an SNMPv3 user.....	126
Removing an SNMPv3 user.....	128
Creating an SNMPv3 view.....	129
Removing an SNMPv3 view .....	130
Adding trap receivers to SNMPv3 tables.....	130
Deleting trap receivers or restoring the SNMPv3 table to defaults.....	132
Displaying SNMP-server host-related information.....	133
Setting SNMP community strings and access privileges.....	133
Displaying SNMPv3 configuration .....	134
Creating an initial set of configuration data for SNMPv3 .....	135
Configuring MAC address filter-based security using CLI.....	136
Displaying MAC address security settings.....	136
Configuring MAC address security options.....	137



Adding addresses to MAC security address table.....	138
Assigning a list of ports to a security list.....	139
Disabling MAC source address-based security .....	139
Disabling MAC address auto-learning aging time .....	140
Clearing the MAC address security table .....	140
Clearing the port membership of a security list .....	140
Configuring MAC security for specific ports .....	141
Filtering packets from specified MAC DAs .....	142
Configuring MAC address autolearning using CLI.....	142
Configuring MAC address auto-learning aging time .....	142
Disabling MAC address auto-learning aging time .....	143
Configuring MAC address auto-learning aging time to default .....	143
Enabling or disabling block subsequent MAC authentication.....	144
Viewing the current Sticky MAC address mode .....	144
Enabling Sticky MAC address mode .....	145
Disabling Sticky MAC address mode .....	145
Configuring EAPOL-based security.....	146
Enabling or disabling EAPOL-based security .....	146
Modifying EAPOL-based security parameters for a specific port .....	146
Setting the guest VLAN for EAPOL .....	148
Disabling guest VLAN for EAPOL .....	148
Displaying the current EAPOL-based security status .....	148
Resetting EAP settings globally.....	149
Resetting EAP settings at the port level.....	150
Displaying EAPOL diagnostics .....	150
Displaying EAPOL statistics.....	151
Displaying EAPOL guest VLAN settings.....	151
Configuring advanced EAPOL features using CLI.....	152
Configuring global EAPOL multihost settings.....	152
Disabling global EAPOL multihost settings.....	153
Restoring global EAPOL multihost settings to default .....	154
Configuring EAPOL multihost settings for a specific port or ports on an interface .....	155
Disabling EAPOL multihost settings for a specific port or for all ports on an interface.....	157
Restoring EAPOL multihost settings to default for a specific port or for all ports on an interface .....	158
Setting the maximum number of clients allowed per port.....	159
Configuring non-EAPOL MAC addresses on a specific port or on all ports on an interface...	161
Displaying global settings for non-EAPOL hosts on EAPOL-enabled ports.....	161
Displaying non-EAPOL support settings for each port.....	162
Displaying non-EAPOL hosts information.....	163
Configuring support for non-EAPOL hosts on EAPOL-enabled ports.....	163
Configuring 802.1X or Non-EAP and Guest VLAN on the same port using CLI.....	168
Enabling EAPOL VoIP VLAN .....	168

Disabling EAPOL VoIP VLAN .....	169
Configuring EAPOL VoIP VLAN as the default VLAN .....	169
Viewing EAPOL VoIP VLAN .....	170
Configuring TACACS+ using CLI.....	170
Configuring switch TACACS+ server settings .....	170
Disabling switch TACACS+ server settings.....	171
Enabling remote TACACS+ services .....	171
Enabling or disabling TACACS+ authorization .....	172
Configuring TACACS+ authorization privilege levels .....	172
Enabling or disabling TACACS+ accounting .....	173
Configuring the switch TACACS+ level .....	173
Viewing TACACS+ information .....	174
Configuring IP Manager using CLI.....	174
Configuring IP Manager.....	174
Configuring the IP Manager list for IPv4 addresses .....	175
Configuring the IP Manager list for IPv6 addresses .....	175
Removing IP Manager list entries .....	176
Displaying the IP Manager configuration.....	176
Configuring DHCP snooping using CLI.....	177
Configuring DHCP snooping globally .....	178
Configuring DHCP snooping on a VLAN .....	178
Configuring DHCP snooping port trust.....	178
Displaying global DHCP snooping configuration information.....	179
Displaying VLAN DHCP snooping configuration information.....	179
Displaying DHCP snooping port trust information .....	180
Displaying the DHCP binding table .....	180
Configuring DHCP Snooping Option 82 globally .....	180
Configuring VLAN-based DHCP Snooping Option 82 .....	181
Displaying DHCP Snooping .....	182
Displaying DHCP Snooping for an interface .....	182
Configuring dynamic ARP inspection using CLI.....	183
Displaying the ARP table.....	183
Configuring dynamic ARP inspection on a VLAN .....	184
Configuring dynamic ARP inspection port trust .....	184
Configuring dynamic ARP inspection port trust to default .....	185
Displaying VLAN dynamic ARP inspection configuration information.....	185
Displaying dynamic ARP inspection port trust information.....	186
Configuring IP Source Guard .....	186
Configuring IP Source Guard.....	187
Displaying IP Source Guard port configuration information .....	187
Displaying IP Guard-allowed addresses.....	188
Configuring 802.1X or non-EAP Last Assigned RADIUS VLAN .....	188
Configuring use of the most recent RADIUS VLAN.....	188

Restoring use of the most recent RADIUS VLAN to default.....	189
Displaying EAPOL multihost status.....	189
Configuring EAPOL Fail Open VLAN.....	189
Displaying EAPOL Fail Open VLAN.....	190
Configuring storm control .....	190
Configuring storm control .....	191
Displaying global storm control state.....	192
Displaying rate limit configuration.....	193
Configuring rate limiting .....	193
<b>Chapter 6: Security configuration and management using Enterprise Device Manager.....</b>	<b>195</b>
Setting the switch HTTP/HTTPS port using EDM.....	195
<b>Chapter 7: Configuring EAPOL using EDM.....</b>	<b>196</b>
Configuring EAPOL globally using EDM.....	196
EAPOL tab field descriptions.....	196
Enabling or disabling non-EAP client re-authentication using EDM.....	198
Configuring port based EAPOL.....	199
Configuring port-based EAPOL using EDM.....	200
EAPOL Ports tab field descriptions.....	201
Configuring advanced port-based EAPOL using EDM.....	203
EAPOL Advance Ports tab field descriptions.....	203
Configuring multihost EAP VoIP VLAN using EDM.....	204
EAP VoIP Vlan tab field descriptions.....	205
Clearing Non-EAP authenticated clients from ports using EDM.....	205
Viewing Multihost status information using EDM.....	206
Multi Host Status tab field descriptions.....	206
Viewing Multihost session information using EDM.....	206
Multi Host Session tab field descriptions.....	207
Viewing Multihost DHCP authenticated information.....	207
Multi Host DHCP Authenticated tab field descriptions.....	207
Configuring RADIUS globally using EDM.....	207
Globals tab field descriptions.....	209
Track all MACs per port.....	210
Displaying all MACs.....	210
Adding a MAC address to the allowed non-EAP MAC address list using EDM.....	213
Allowed non-EAP MAC tab field descriptions.....	213
Deleting a MAC address from the allowed non-EAP MAC address list using EDM.....	213
Allowed non-EAP MAC tab field descriptions.....	214
Viewing port non-EAP host support status using EDM.....	214
Non-EAP Status tab field descriptions.....	214
Graphing port EAPOL statistics using EDM.....	215
EAPOL Stats tab field descriptions.....	215
Graphing port EAPOL diagnostics using EDM.....	216

EAPOL Diag tab field descriptions.....	216
<b>Chapter 8: Configuring and managing security using EDM.....</b>	<b>219</b>
Configuring TACACS using EDM.....	219
Enabling or disabling TACACS+ accounting using EDM.....	219
Enabling or disabling TACACS+ authorization using EDM.....	219
Configuring the switch TACACS+ levels using EDM.....	220
Creating a TACACS+ server using EDM.....	220
Configuring general switch security using EDM.....	221
Adding ports to a security list using EDM.....	224
Deleting ports from a security list using EDM.....	225
Configuring AuthConfig list using EDM.....	225
Adding entries to the AuthConfig list using EDM.....	225
Deleting entries from the AuthConfig list using EDM.....	227
Configuring MAC Address autolearn using EDM.....	227
Viewing AuthStatus information using EDM.....	228
Viewing AuthViolation information using EDM.....	230
Configuring a Web and Telnet password using EDM.....	230
Configuring a console password using EDM.....	231
Configuring the Secure Shell protocol using EDM.....	232
Viewing SSH Sessions information using EDM.....	234
Configuring an SSH Client.....	234
Configuring SSL using EDM.....	236
Configuring the Global RADIUS Server using EDM.....	237
Configuring the EAP RADIUS Server using EDM.....	239
Configuring the NEAP RADIUS Server using EDM.....	241
Viewing RADIUS Dynamic Authorization server information using EDM.....	243
Configuring RADIUS parameters.....	244
Configuring RADIUS globally using EDM.....	244
802.1X dynamic authorization extension (RFC 3576) client configuration using EDM.....	246
Configuring an 802.1X dynamic authorization extension (RFC 3576) client using EDM.....	246
Deleting an 802.1X dynamic authorization extension (RFC 3576) client configuration using EDM.....	248
Modifying the 802.1X dynamic authorization extension (RFC 3576) client configuration using EDM.....	248
Viewing the 802.1X dynamic authorization extension (RFC 3576) client information using EDM.....	249
Editing the 802.1X dynamic authorization extension (RFC 3576) client secret word using EDM.....	250
Viewing RADIUS Dynamic Server statistics using EDM.....	250
Graphing RADIUS Dynamic Server statistics using EDM.....	251
DHCP snooping configuration using EDM.....	251
Configuring DHCP snooping and Option 82 globally using EDM.....	251
Configuring DHCP snooping and Option 82 on a VLAN using EDM.....	252

Configuring DHCP snooping port trust and DHCP Option 82 for a port using EDM.....	253
Viewing the DHCP binding information using EDM.....	254
Configuring dynamic ARP inspection on a VLAN using EDM.....	255
Configuring dynamic ARP inspection on a port using EDM.....	255
Configuring IP Source Guard using EDM.....	256
Configuring IP Source Guard on a port using EDM.....	256
Filtering IP Source Guard addresses using EDM.....	257
Configuring SNMP using EDM.....	258
Viewing SNMP information using EDM.....	258
Defining a MIB view using EDM.....	259
Configuring an SNMP user using EDM.....	260
Viewing SNMP user details using EDM.....	261
Configuring an SNMP community.....	262
Viewing SNMP community details using EDM.....	263
Configuring an SNMP host using EDM.....	263
Configuring SNMP host notification using EDM.....	264
Configuring SNMP notification control using EDM.....	265
Configuring Storm Control using EDM.....	266
Configuring Storm Control globally.....	266
Configuring Broadcast Storm Control.....	268
Configuring Multicast Storm Control.....	269
Configuring Unicast Storm Control.....	271
Configuring port-based storm control.....	272
Configuring rate limiting using EDM.....	273
<b>Chapter 9: Configuration examples.....</b>	<b>275</b>
TACACS+ server configuration examples.....	275
Extreme Networks Identity Engine Ignition Server TACACS+ configuration example.....	275
Configuration example: Linux freeware server.....	278
SNMP MIB support.....	280
Management Agent.....	280
SNMP trap support.....	281
Sticky MAC address configuration examples.....	283
MHMA authentication mode (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes.....	285
Scenario.....	286
Configuration example.....	290

# Chapter 1: Preface

---

## Purpose

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

---

## Training

Ongoing product training is available. For more information or to register, you can access the Web site at [www.extremenetworks.com/education/](http://www.extremenetworks.com/education/).

---

## Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at [internalinfodev@extremenetworks.com](mailto:internalinfodev@extremenetworks.com)

---

## Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- [GTAC \(Global Technical Assistance Center\) for Immediate Support](#)
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact)

- Email: [support@extremenetworks.com](mailto:support@extremenetworks.com). To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

---

## Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation

[www.extremenetworks.com/documentation/](http://www.extremenetworks.com/documentation/)

Archived Documentation (for previous versions and legacy products)

[www.extremenetworks.com/support/documentation-archives/](http://www.extremenetworks.com/support/documentation-archives/)

Release Notes

[www.extremenetworks.com/support/release-notes](http://www.extremenetworks.com/support/release-notes)

### Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: [www.extremenetworks.com/support/policies/software-licensing](http://www.extremenetworks.com/support/policies/software-licensing).

---

## Subscribing to Service Notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

### **About this task**

You can modify your product selections at any time.

### **Procedure**

1. In an Internet browser, go to <http://www.extremenetworks.com/support/service-notification-form/>.
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.



# Chapter 2: New in this document

There are no new feature changes in this release.

---

## Other Changes

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

### **SHA-256 Support for SSL Certificates**

Starting with Release 5.3.1, only the SHA-256 hash algorithm is supported to compute the SSL certificate signature. Support for SHA-1 is deprecated and trusting SHA-1 generated certificates is stopped.

For information about SHA-2 support for SSL certificates, see [SHA-2 Support for SSL Certificates](#) on page 63.

# Chapter 3: CLI command modes

Command Line Interface (CLI) provides the following command modes:

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

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

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

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

**Table 1: CLI command modes**

Command mode and sample prompt	Entrance commands	Exit commands
User Executive Switch>	No entrance command, default mode	exit or logout
Privileged Executive Switch#	enable	exit or logout
Global Configuration Switch (config)#	From Privileged Executive mode, enter configure terminal	To return to Privileged Executive mode, enter end or exit To exit CLI completely, enter

*Table continues...*

Command mode and sample prompt	Entrance commands	Exit commands
		logout
<b>Interface Configuration</b> Switch (config-if)#	From Global Configuration mode: To configure a port, enter interface fastethernet <port number> To configure a VLAN, enter interface vlan <vlan number> To configure a loopback, enter interface loopback <loopback number>	To return to Global Configuration mode, enter exit To return to Privileged Executive mode, enter end To exit CLI completely, enter logout
<b>Application Configuration</b> Switch (config-app)#	From Global, or Interface Configuration mode, enter application	To return to Global Configuration mode, enter exit To return to Privileged Executive mode, enter end To exit CLI completely, enter logout

# Chapter 4: Security fundamentals

This chapter describes the security features available with the ERS 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 switch 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` CLI 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.

---

## 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 CLI.



Figure 1: Setting the user name and password using CLI

---

## 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 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 CLI and EDM procedures and Sticky MAC address configuration examples.

---

## Block subsequent MAC authentication

When a new EAP or Non-EAP client is added to a port with a valid RAV it is assigned the same RADIUS as the first EAP or Non-EAP client present on port.

In order to be enabled, the option must be enabled both globally and per port.

EAP and Non-EAP clients are blocked dependent on whether MultiVlan is disabled or enabled and in the following situations:

**MultiVlan Disabled:**

All clients on a specific port are authenticated on a single VLAN.

**EAP clients are blocked in the following situations:**

- EAP client comes without any VLAN
- EAP client comes with a VLAN that does not exist on the switch
- EAP client comes with a VLAN different from the one specified by the first EAP client present on port
- “use-radius-assignment-vlan” is disabled on port

**\* Note:**

In all the preceding cases, information is logged with details about the fail reasons.

**Non-EAP clients are blocked in following situations:**

- Non-EAP client comes without any VLAN
- Non-EAP client comes with a VLAN that does not exist on the switch
- Non-EAP client comes with a VLAN different from the one specified by the first EAP client present on port or by first non-EAP client if no EAP clients are present.
- “non-eap-radius-assignment-vlan” is disabled per port

**\* Note:**

In all the preceding cases, information is logged with details about fail reasons.

PVID is set according to VLAN available for EAP/non-EAP clients.

**MultiVlan Enabled:**

In this situation there are 2 VLANs available (1 for EAP clients and 1 for non-EAP clients). The 2 VLANs are determined by the first EAP/non-EAP successful authentication.

**EAP clients are blocked in the following situations:**

- EAP client comes without any VLAN
- EAP client comes with a VLAN that does not exist on the switch
- EAP client comes with a VLAN different from the one specified by the first EAP client present on port
- “use-radius-assignment-vlan” is disabled on port
- EAP client comes with a VLAN for Non-EAP clients

**Non-EAP clients are blocked in the following situations:**

- Non-EAP client comes without any VLAN

- Non-EAP client comes with a VLAN that does not exist on the switch
- Non-EAP client comes with a VLAN different from the one specified by the first Non-EAP client present on port
- “non-eap-radius-assignment-vlan” is disabled per port
- Non-EAP client comes with a VLAN for EAP clients

**\* Note:**

No PVID changes.

---

## 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.

Extreme Networks 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 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.

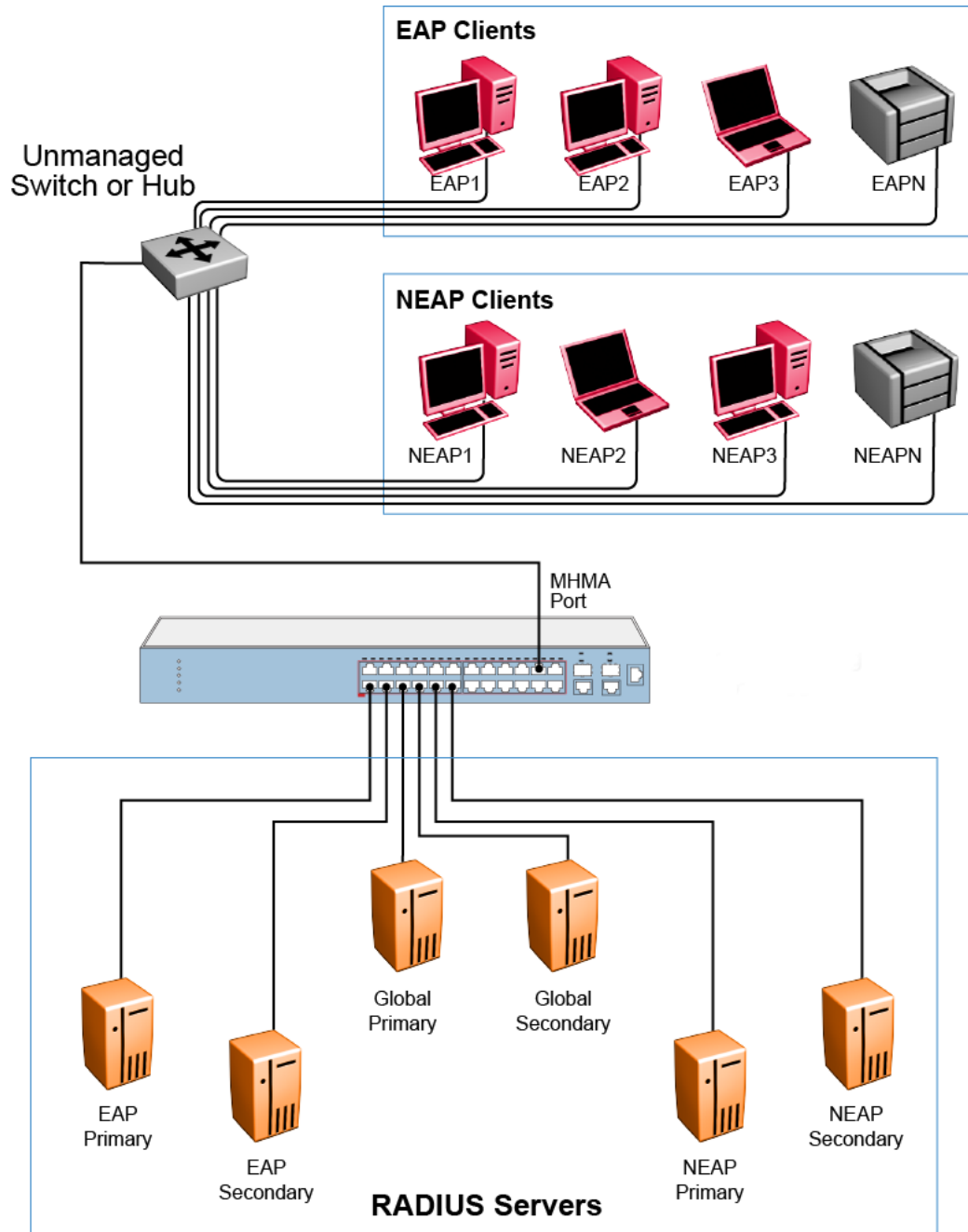
#### **Non-EAP clients**

- 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:

- a 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 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. You can configure both a username and a password for the dummy account using CLI. Because the switch interprets either Request Accept or Request Reject responses as a confirmation for reachability, you do not have to add the credentials on server in order to test for server reachability. Extreme Networks recommends that you set up a dummy account with a user name and password 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

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 switch 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

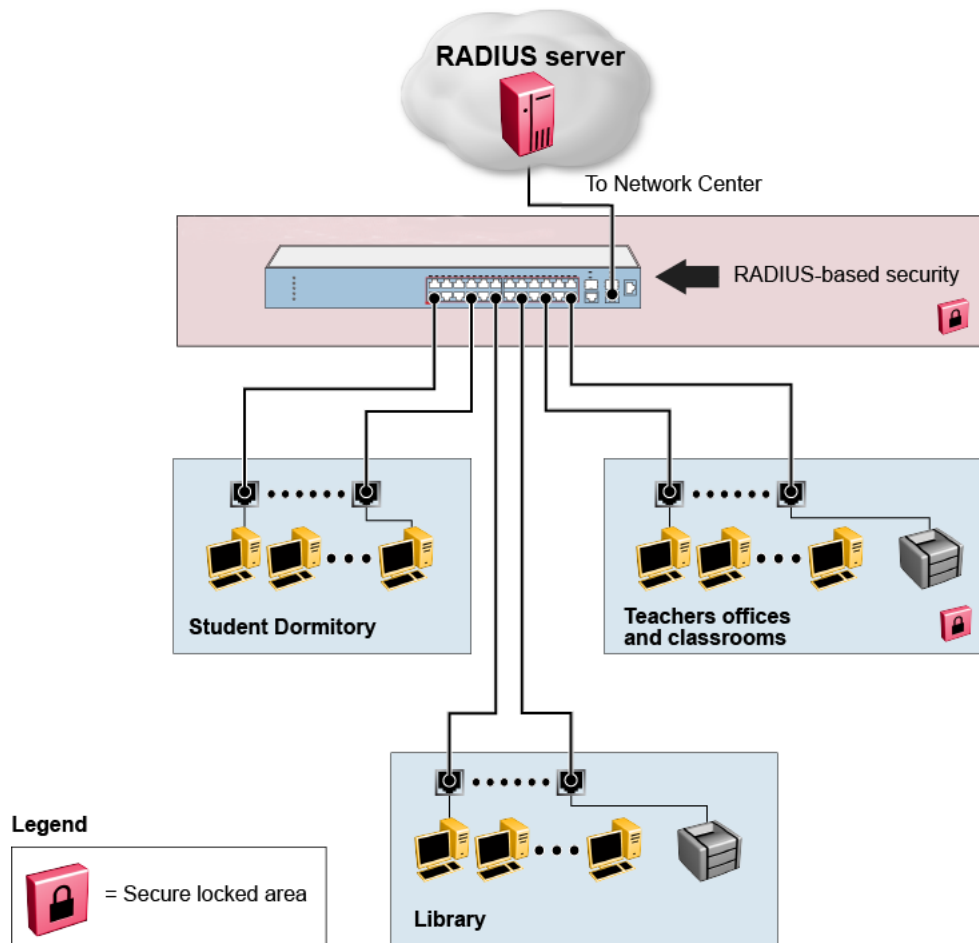
This is normal behavior in Layer 2 mode; if the Management VLAN is unavailable, there is no active Management IP instance. In Layer 3 mode, if RADIUS Request Use Management IP is enabled, the switch does not use any of the other routing instances to send RADIUS requests when the management VLAN is inactive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



**Figure 3: Security features**

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 24).
  - 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 21).
  - 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

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

An example follows to show how a switch 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 35.

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).
- 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 38.

If the MAC address is authenticated by RADIUS, the host is allowed.

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

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.

---

## 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, Extreme Networks 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.

---

## MHSA No-Limit

The MHSA No-Limit feature accommodates the scenario when an access point is connected to the switch. Only the access point performs authentication. The hosts connected behind the access point access the network without any authentication.

The **mhsa-no-limit** option allows an unlimited number of hosts behind the access point. This is a per-port option. If the **mhsa-no-limit** option is enabled on a port, all traffic will be allowed on that port after the first successful client authentication.

---

## 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 200
- [Modifying EAPOL-based security parameters for a specific port using CLI](#) on page 146

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.

---

## NEAP Not Member of VLAN

The NEAP Not Member of VLAN feature ensures that ports configured with RADIUS Non-EAP authentication are assigned to at least one VLAN to make authentication possible for Non-EAP clients.

When the RADIUS Non-EAP configuration is ready, the port is automatically assigned to default VLAN.

**\* Note:**

For the NEAP Not Member of VLAN feature to function properly, you must enable the following features:

- EAPOL globally and at the port level
- multihost at the port level
- non-EAP RADIUS authentication globally and at the port level

---

## 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.

---

## Fail Open VLAN Continuity Mode

The Fail Open VLAN Continuity Mode feature introduces a new mode of operation for EAP/NEAP clients when the RADIUS server become unreachable.

RADIUS Server reachability is checked periodically. When the RADIUS server is unreachable, the interval is one minute. When the RADIUS server is reachable, the interval is 3 minutes. This can lead to a delay of up to 3 minutes, from the moment when the RADIUS Server becomes unreachable until the movement to Fail Open VLAN is performed.

When Fail Open VLAN Continuity Mode is enabled and if the RADIUS client does not receive any response from RADIUS Server, the EAP or Non-EAP MACs are not flushed. The RADIUS reachability is triggered, and the port is moved or copied to Fail Open VLAN.

With Fail Open VLAN Continuity Mode enabled, the switch operates as follows:

- The authenticated state of a client is not altered if RADIUS reachability changes.
- If a client performs reauthentication (either EAP or NEAP), and the RADIUS Server is unreachable, then the current state of the client is preserved.

Fail Open VLAN Continuity Mode is a global configuration that applies to all switches in a stack.

**\* Note:**

It is recommended that the RADIUS Reachability to be set on Use RADIUS. If Use ICMP is used and the RADIUS server is reachable, but the RADIUS Server Service is stopped, an ICMP packet is sent for every authentication. If there are many EAP/Non-EAP clients in the setup, this flood with ICMP packets can be disturbing.

This is a corner case and can be avoided using RADIUS packets for reachability, as recommended, or starting RADIUS Server Service if Use ICMP is used for reachability.

This situation appears because with Fail Open Continuity Mode enabled, the RADIUS Reachability mechanism is triggered when no response is received from the RADIUS Server.

**\* Note:**

When an EAP or NEAP client tries to re-authenticate and the RADIUS server is not reachable, the switch keeps the client in the VLAN currently assigned by RADIUS and maintains any

applicable policies. If necessary, the switch provides appropriate communication back to the EAP supplicant to indicate that re-authentication was successful.

---

## Fail Open UBP

If Fail open UBP is configured and the QoS support for UBP is enabled, the configured UBP classifier gets installed with the source MAC for every new MAC address learned on the port while the port is in FailOpenVLAN (FOV) Mode. The UBP is deleted when the MAC ages, migrates, or authenticates, or when the port exits the FailOpenVLAN.

The filter on-mac option from regular UBP is disabled by default. If the UBP cannot be installed in the hardware, a log message is generated from EAP, containing the MAC address and the unit and port where the operation failed. QoS sends detailed logs with more information on the error.

If the UBP is not created in QoS, the installation operation creates only a software user-policy association, by issuing “show qos user-policy”. On proceeding to create the filter in the QoS settings, an auto-installation takes place in the hardware. This is inherited from UBP behavior with EAP or NEAP clients.

When a port is removed from FailOpenVLAN state, Fail Open UBP is uninstalled on that port and all clients are re-authenticated.

### Limitations:

The following are the limitations for UBP installation related to EAP and QoS:

- When the port transitions to FOV, all authenticated clients retain the UBPs, if they are received from the RADIUS server. Depending on the EAP settings, the filters can be applied with or without filter-on-mac, therefore the traffic flow may vary.
- The FOV UBP is applied only for new MACs that send traffic while in FOV. MACs that had been intruders prior to the port entering FOV are still treated as intruders, and no FOV UBP are installed for them.
- UBP cannot be changed while EAP is enabled globally, and per port is not permitted.
- UBP support must be enabled from QoS.
- The filter can fail the Fail Open VLAN installation for reasons such as QoS resource exhaustion.
- Some combinations of QoS rules do not work, since the source MAC is added into the classifier when installing it.

---

## 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 switch 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 switch services.

**! Important:**

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

A switch 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 switch, 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. It is recommended 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, Extreme Networks 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

**\* Note:**

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

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

## EAP (802.1X) accounting

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

The RADIUS accounting protocol is defined in RFC 2866. RADIUS accounting in the switch utilizes the same RADIUS server used for RADIUS authentication.

By default, the RADIUS accounting UDP port is the RADIUS authentication port + 1. You can configure RADIUS accounting separately.

## Non-EAP accounting

EAP (802.1X) accounting is extended to non-EAP (NEAP) clients.

If you configure EAP clients and non-EAP clients on different servers, the system directs accounting messages to the appropriate EAP and non-EAP servers.

The maximum number of clients for NEAP accounting permitted on a switch port is limited to the maximum number of configurable NEAP clients on the port (32).

Because the switch can only report statistics for individual ports, NEAP accounting information for MultiHost modes reflects the total network activity on a port.

NEAP accounting supports the following authentication methods:

- IP phone DHCP signature authentication
- ADAC based authentication
- MAC RADIUS authentication
- MHS (Multiple Host Single Authentication) NEAP authentication

---

## 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 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+

Terminal Access Controller Access Control System plus (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 CLI.



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/doc/draft-ietf-opsawg-tacacs><https://datatracker.ietf.org/drafts/draftgrant-%20tacacs/>

**!** **Important:**

TACACS+ is not compatible with previous versions of TACACS.

---

## TACACS+ architecture

You can configure TACACS+ 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 switch.
- 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 51.

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 51.

---

## TACACS+ server configuration example

The following example shows a configuration sample for a Linux TACACS+ 4.0.4 server.

```
#Set the server key. You must configure an identical key on the switches communicating
with the TACACS+ server.

key = bayproject

#Set the accounting file on the server. All accounting records are written as text to
this filename.

accounting file = /usr/local/var/log/tac_plus.act

# You can configure user authentication separately for PAP, ARAP, CHAP, and normal
logins. You can also configure a global authentication method to be used if a per-
protocol method is not specified.
# You cannot use a global user password for outbound PAP.
# The following example assigns to a user four different passwords for inbound and
outbound:
# user = user1 {
#     chap = cleartext "chap_password"
#     pap = cleartext "inbound_pap_password"
#     opap = cleartext "outbound_pap_password"
#     login = des XQj4892fjk
# }

# You can set the default authentication to use a passwd(5) file. With this option, when
a user does not appear in the configuration file, the daemon attempts to authenticate the
user using passwords from this file.
# default authentication = file /etc/passwd

# Configure groups:

group = vlan {
    login = cleartext vlan

# Specify the permitted commands:

    cmd = enable { permit .* }
    cmd = configure { permit .* }
    cmd = vlan { permit .* }
    cmd = show { permit .* }
    cmd = exit { permit .* }
    cmd = logout { permit .* }
    cmd = tacacs { permit .* }
}

group = trunk {
    login = cleartext trunk
    cmd = enable { permit .* }
    cmd = configure { permit terminal }
```

## Security fundamentals

```
cmd = mlt { permit .* }
cmd = show { permit .* }
cmd = exit { permit .* }
cmd = logout { permit .* }
cmd = tacacs { permit .* }
}

group = mirror {
  login = cleartext mirror
  cmd = enable { permit .* }
  cmd = configure { permit terminal }
  cmd = port-mirroring { permit .* }
  cmd = show { permit .* }
  cmd = exit { permit .* }
  cmd = logout { permit .* }
  cmd = tacacs { permit .* }
}

group = ipmgr {
  login = cleartext ipmgr
  cmd = enable { permit .* }
  cmd = configure { permit terminal }
  cmd = ipmgr { permit .* }
  cmd = show { permit .* }
  cmd = exit { permit .* }
  cmd = logout { permit .* }
  cmd = tacacs { permit .* }
}

# Configure the user accounts and assign the users to groups:

user = vlan1 {

  member = vlan # assigns the user vlan1 to the vlan group
  service = exec {
    priv-lvl = 0 # the CLI level displayed on switch
  }
}

user = trunk1 {
  member = trunk
  service = exec {
    priv-lvl = 1
  }
}

user = mirror1 {
  member = mirror
  service = exec {
    priv-lvl = 2
  }
}

user = ipmgr1 {
  member = ipmgr
  service = exec {
    priv-lvl = 3
  }
}

# You can configure an expiry date for a user password. Starting on the expiry date, the
user password becomes invalid. A warning message is sent to the user prior to the
expiration date.
```

```
# The 'expires' field in the configuration file is not consulted if passwd(5) files are used for authentication. In this case, the 'shell' field of the password file is checked for the expiry date.
```

```
#user = user2 {  
#   expires = "MMM DD YYYY"  
#   password = cleartext "user2_pass"  
#}
```

```
# To check the configuration file syntax, use the tac_plus -P -C command. Any error messages will be displayed on the terminal.
```

---

## 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 CLI terminal sessions within serial, Telnet, or SSH shells (from CLI 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+:

- 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 CLI or EDM. You can also use the console interface to enable or disable TACACS+ authentication on serial and Telnet connections.

For information about configuring TACACS+ using CLI, see [Configuring TACACS using CLI](#) on page 170.

For information about configuring TACACS+ using EDM, see [Configuring TACACS using EDM](#) on page 219.

---

## IP Manager

With IP Manager, you can limit access to the management features 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, it is recommended 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

Custom user names and passwords can be created 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.

## 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

The password security feature, if enabled, enhances password security for the switch or stack read-only password and read-write passwords. By default, password security is disabled for the standard software image and enabled for the secure software image. If password security is disabled, there is no minimum restriction on number of characters required or are there any other restrictions. You can enable password security from CLI only.

When you enable password security, the following happens:

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

When you disable password security, the following happens:

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

With password security enabled, the following features and requirements are active:

### **Password length and valid characters**

Valid passwords are from 8 to 255 characters long.

Where, x-y-z-t specifies the number of characters from each character type that need to be included in the password. Their minimum values can be configured.

- minimum w lower-case characters
- minimum y numeric characters
- minimum z special characters
- minimum t upper-case characters

The password is case-sensitive.



**\* Note:**

The RO and RW passwords cannot be the same.

### Password retry

If the user fails to provide the correct password after a number of consecutive retries, the switch resets the log-on process. You can configure the number of retries, using CLI. The default is three.

### Password history

You can configure the switch to keep a maximum history of the last twelve passwords. If you set the password for the fourth time and the history size is set to 3, you can reuse the password that you used the first time. You cannot reuse a password stored in history.

### Password aging time

Passwords expire after a specified aging period. The aging period is configurable, with a range of 0 day to approximately 365 days. The default is 0 days. When a password has aged out, you are prompted to create a new password. Only users with a valid Read-Write (RW) password can create a new RW password or Read-Only (RO) password.

### Password check sequential and repeated characters

You cannot use passwords that contains sequential characters, such as ab, ba, qw, wq, 12, 21, !@, @! or repeated characters, such as 11, aa, @@.

### Password verification

When you provide a new password, you must confirm it by retying the password. If the two passwords do not match, the password update process fails. In this case, you must try to update the password again. No limit exists on the number of times you are allowed to update the password.

### Password display masking

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

## Password complexity

Password complexity feature enforces complexity password rules. The rules are different when the switch is upgraded from an unsupported to a supported release for the first time.

The following password complexity rules are applicable when the feature is enabled.

**Table 2: Password complexity rules**

Type	Description	Value range	Minimum length	Default value when the feature is enabled	Default value when switch is upgraded from an unsupported to a supported release for first time
Length	Specifies number of characters in password.	8 to 255	8 characters	8	10

*Table continues...*

Type	Description	Value range	Minimum length	Default value when the feature is enabled	Default value when switch is upgraded from an unsupported to a supported release for first time		
Character	Specifies the number of character from each character type that need to be included in password.			0-0-0-0	2-2-2-2		
		Where, x-y-z-t specify the number of characters from each character type. Following are the details:					
		<ul style="list-style-type: none"> <li>• x — lowercase</li> <li>• y — uppercase</li> <li>• z — numeric</li> <li>• t — special characters</li> </ul>					
		Character type					
		lowercase	a to z	0 to 9	0	2	
uppercase	A to Z	0 to 9	0	2			
numeric	0 to 9	0 to 9	0	2			
special characters	(!, @, #, \$, %, ^, &, *, (, ), -, +, =, _	0 to 9	0	2			
History	Number of passwords retained in history	0 to 12		1	3		
Sequential	Checks for sequential characters within passwords when enabled.  For example, abcdefgh.	Enable or Disable		Enable	Enable		
Check-repeated	Checks for repeated characters within passwords when enabled.  For example, aa.	Enable or Disable		Enable	Enable		

## Password upgrade considerations

When you upgrade from a software image previous to Release 5.3 with separate switch and stack passwords to Release 5.3 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. Extreme Networks recommends to set stack passwords and authentication type before you upgrade to Release 5.3.

---

## 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 CLI. 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

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.

---

## Support for SNMP in the switch

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

SNMPv3 support introduces industrial-grade user authentication and message security. This includes MD5- and SHA-based user authentication and message integrity verification, as well as AES, DES, and 3DES-based privacy encryption.

You can configure SNMPv3 using CLI or Enterprise Device Manager (EDM).

---

## SNMP MIB support

SNMP agent with industry standard Management Information Bases (MIB) is supported, 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.

Industry-standard SNMP traps and private Extreme Networks enterprise traps are supported.

## 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

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

In the secure mode, the Web server listens on TCP port 443 and responds only to HTTPS client browser requests. All existing non-secure connections with the browser are closed down. In the non-secure mode, the Web server listens on TCP port 80, 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.

---

## SHA-2 Support for SSL Certificates

In Release 5.3.1 or later, only the SHA-256 hash algorithm is supported to compute the SSL certificate signature. Support for SHA-1 is deprecated and trusting SHA-1 generated certificates is stopped.

### Important:

When you upgrade from a release that uses SHA-1 based certificates to Release 5.3.1 or later, the old certificate is used with the upgraded software. In this case, SSL negotiation sessions fail because SHA-1 is not supported on Release 5.3.1 or later. To successfully negotiate an SSL session that uses SHA-1, you must first upgrade to a release that supports SHA-256 and then regenerate the SSL certificate.

For information about regenerating certificates, see [Regenerating the SSL Certificate using CLI](#) on page 89.

---

## 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 Command Line Interface (CLI), 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 Ethernet Routing Switch 3500 Series* .

---

## 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 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

*Table continues...*

IP Source Guard configuration state	DHCP snooping configuration state	DHCP snooping Binding Entry action (untrusted ports)	IP Source Guard action
enabled	enabled	deletes binding entries when one of the following conditions occurs: <ul style="list-style-type: none"> <li>• DHCP is released</li> <li>• the port link is down, or the administrator is disabled</li> <li>• the lease time has expired</li> </ul>	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 Command Line Interface (CLI), 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.

The following SFTP features are supported:

- 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 128.

---

## 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 switch 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` CLI command. You can also limit the percentage of multicast traffic, or broadcast traffic, or both with `rate-limit` CLI command.

**\*** **Note:**

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: Configuring and managing security using CLI

---

## Configuring and managing security using CLI

This chapter describes the procedures necessary to configure security using the Command Line Interface (CLI).

---

### Setting the system user name and password

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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.

*Table continues...*

Variable	Value
	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 CLI

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

The CLI 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. Enter Global Configuration mode:

```
enable
configure terminal
```


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.

*Table continues...*

Variable	Value
	 <b>Important:</b> 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: <ul style="list-style-type: none"> <li>• none: disable the password</li> <li>• local: uses the locally defined password for serial console or Telnet access.</li> <li>• radius: uses RADIUS authentication for serial console or Telnet access.</li> <li>• tacacs: uses TACACS+ authentication, authorization, and accounting (AAA) services for serial console or Telnet access.</li> </ul>

---

## Enabling or disabling password security using CLI

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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



## Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the prompt, enter the following command:

```
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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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.

```
Switch#show password security
Password security is disabled
```

---

## Configuring the number of password logon attempts

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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 CLI, the password aging counters are not reset.

## Configuring password aging-time

### About this task

Use this procedure to configure password validity period. By default, the value is 0 and the password does not age-out.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. Configure password aging time:
 

```
password aging-time [username <name>]<0-365>
```
3. Return password aging-time to default value:
 

```
default password aging-time
```
4. Verify the settings:
 

```
show password aging-time
```

### Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#password aging-time 10
Switch(config)#show password aging-time
Global aging time: 10 days
Switch(config)#default password aging-time
Switch(config)#show password aging-time
Global aging time: 0 days
```

## Variable definitions

The following table describes variables that you use with the `password aging-time` command.

Variable	Definition
<0-365>	Specifies the number of days the password remains valid.  By default, the password aging-time is 0 (disabled) and it will not age out. If the password aging-time is 1, the password must be changed every day.
username	Sets the number of days the password remains valid for a specific user.

## Configuring password check-repeated

## About this task

Use this procedure to allow or forbid repeated consecutive characters within password. For example, aadfjkl, 12245678, bbbbbbbb, and others.

By default, this feature is enabled and repeated characters within password are not allowed.

## Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. Configure password check-repeated:
 

```
password check-repeated [enable | disable]
```
3. Return check-repeated to default value (enabled):
 

```
default password check-repeated
```
4. Verify the settings:
 

```
show password check-repeated
```

## Example

```
Switch# show password check-repeated
Check-repeated-characters option is enabled
```

## Variable definitions

The following table describes variables that you use with the `password check-repeated` command.

Variable	Definition
disable	Accepts repeated consecutive characters.
enable	Forbids repeated consecutive characters. Default is enabled.

## Configuring password check-sequential

### About this task

Use this procedure to allow or forbid sequential characters in the password.

By default, this feature is enabled and you cannot create password with sequential characters. For example, password with sequential characters can be abcdefgh, hgfedcba, qwertyui, iuytrewq, 12345678, or 87654321.

### Procedure

1. Enter Global Configuration mode:

- ```
enable
```
- ```
configure terminal
```
2. Configure password check-sequential:

```
password check-sequential [enable | disable]
```
  3. Return check-sequential to default value (enabled):

```
default password check-sequential
```
  4. Verify the settings:

```
show password check-sequential
```

### Example

```
Switch# show password check-sequential
Check-sequential-characters option is enabled
```

## Variable definitions

The following table describes variables that you use with the `password check-sequential` command.

Variable	Definition
disable	Accepts repeated sequential characters.
enable	Forbids repeated sequential characters. Default is enabled.

---

## Configuring password complexity

### About this task

You can configure minimum number of characters that must be used in the password from each character type. The character types are lowercase, uppercase, number and special characters. By default, the value of each character type is 0 and the complexity rule is not applied.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```
2. Configure password complexity:

```
password complexity [lower-case <0-9> | numeric <0-9> | special <0-9> | upper-case <0-9>]
```
3. Return password complexity to default value:

```
default password complexity
```

#### 4. Verify the settings:

```
show password complexity
```

#### Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#password complexity lower-case 0
Switch(config)#password complexity numeric 3
Switch(config)#password complexity special 1
Switch(config)#password complexity upper-case 2
Switch(config)#show password complexity
Complexity:2-0-3-1
Upper-case: 2
Lower-case: 0
Numeric: 3
Special: 1
```

## Variable definitions

The following table describes variables that you use with the `password complexity` command.

Variable	Definition
0.0.0.0	Complexity default value.
lower-case	Specifies the minimum number of lower-case characters that can be included in the password.
numeric	Specifies the minimum number of numeric characters that can be included in the password.
special	Specifies the minimum number of special characters (!, @, #, \$, %, ^, &, *, (, ), -, +, =, _) that can be included in the password.
upper-case	Specifies the minimum number of upper-case characters that can be included in the password.

## Configuring minimum password length

### About this task

Configure minimum password length. By default, the password minimum length is eight characters.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. Configure the minimum length for a password:
 

```
password min-length <8-255>
```
3. Restore the minimum length of a password to default value:

```
default password min-length
```

4. Verify the settings:

```
show password min-length
```

**Example**

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#password min-length 10
Switch(config)#show password min-length
Minimum password length: 10

Switch(config)#default password min-length
Switch(config)#show password min-length
Minimum password length: 8
```

## Variable definitions

The following table describes variables that you use with the `password min-length` command.

Variable	Definition
<8-255>	Specifies the length interval. Default is 8.

---

## Changing the http port number

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

You can configure this feature by using the following procedures.

---

## Displaying the port number of the HTTP port

### Procedure

1. Enter Privileged EXEC mode:  

```
enable
```
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.

```
Switch#show http-port
HTTP Port: 80
```

---

## Setting the HTTP port number

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, 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
```

---

## USB port and serial console port control

This section describes how you can control access to the switch by enabling or disabling the USB port or serial console port. All serial console ports on the switch are enabled by default.

---

## Disabling serial console ports

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
no serial-console <enable>
```

3. Disable the serial console port on a specific switch unit in a stack:

```
no serial-console [unit <1-8>] <enable>
```

## Variable definitions

Use the data in the following table to use the `no serial-console [unit <1-8>] <enable>` command.

Variable	Value
unit <1-8>	Identifies the unit number of the switch in a stack. Values range from 1 to 8.

## Enabling serial console ports

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
[default] serial-console <enable>
```
3. Enable the serial console port on a specific switch unit in a stack:  

```
[default] serial-console [unit <1-8>] <enable>
```

### Variable definitions

Use the data in the following table to use the `no serial-console [unit <1-8>] <enable>` command.

Variable	Value
unit <1-8>	Identifies the unit number of the switch in a stack. Values range from 1 to 8.

## Viewing serial console port status

### Procedure

1. Enter Privileged EXEC mode:  

```
enable
```
2. View the status of all serial console ports on the switch:  

```
show serial-console
```
3. View the status of a specific serial console port on the switch:  

```
show serial-console [unit <1-8>]
```

### Example

```
Switch>enable
Switch>show serial-console
Serial Console: Disabled
```



## Variable definitions

Use the data in the following table to use the `no serial-console [unit <1-8>] <enable>` command.

Variable	Value
unit <1-8>	Identifies the unit number of the switch in a stack. Values range from 1 to 8.

---

## Disabling USB ports

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. Disable USB ports on all switches in a stack:
 

```
no usb-host-port [unit <1-8>] <enable>
```
3. Disable the USB port on a stand-alone switch:
 

```
no usb-host-port <enable>
```

## Variable definitions

Use the data in the following table to use the `no serial-console [unit <1-8>] <enable>` command.

Variable	Value
unit <1-8>	Identifies the unit number of the switch in a stack. Values range from 1 to 8.

---

## Enabling USB ports

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. Enable USB ports on all switches in a stack:
 

```
[default] usb-host-port [unit <1-8>] <enable>
```
3. Enable USB ports on a stand-alone switch:
 

```
[default] usb-host-port <enable>
```

## Variable definitions

Use the data in the following table to use the `no serial-console [unit <1-8>] <enable>` command.

Variable	Value
unit <1-8>	Identifies the unit number of the switch in a stack. Values range from 1 to 8.

---

## Viewing USB port status

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. View the status of USB ports on all switches in a stack:  
`show usb-host-port [unit <1-8>]`
3. View the status of the USB port a stand-alone switch:  
`show usb-host-port`

## Variable definitions

Use the data in the following table to use the `no serial-console [unit <1-8>] <enable>` command.

Variable	Value
unit <1-8>	Identifies the unit number of the switch in a stack. Values range from 1 to 8.

---

## Setting Telnet access using CLI

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

### Important:

Multiple users can access CLI 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

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

### Procedure

1. Enter Privileged EXEC mode:  
enable
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.

```
Switch#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  255.255.255.0   255.255.255.0
3  255.255.255.0   255.255.255.0
4  255.255.255.0   255.255.255.0
5  255.255.255.0   255.255.255.0
6  255.255.255.0   255.255.255.0
7  255.255.255.0   255.255.255.0
8  255.255.255.0   255.255.255.0
9  255.255.255.0   255.255.255.0
10 255.255.255.0   255.255.255.0
11 255.255.255.0   255.255.255.0
12 255.255.255.0   255.255.255.0
13 255.255.255.0   255.255.255.0
14 255.255.255.0   255.255.255.0
15 255.255.255.0   255.255.255.0
----More (q=Quit, space/return=Continue)----
```

## Configuring Telnet connections

### Procedure

1. Enter Global Configuration mode:  
enable  
configure terminal
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.
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}	<p>Specifies what types of events you want to save in the event log:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Save all access events in the log: <ul style="list-style-type: none"> <li>- Telnet connect—indicates the IP address and access mode of a Telnet session.</li> <li>- Telnet disconnect—indicates the IP address of the remote host and the access mode, due to either a log off or inactivity.</li> <li>- 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.</li> </ul> </li> <li>• <b>none</b>—No Telnet events are saved in the event log.</li> <li>• <b>access</b>—Connect and disconnect events are saved in the event log.</li> <li>• <b>failure</b>—Only failed Telnet connection attempts are saved in the event log.</li> </ul>
source-ip [<1-50> <A.B.C.D>   <51-100 <WORD>]	Up to 50 IPv4 address/mask pairs (1-50) and 50 IPv6 address/prefix pairs (51-100) are supported.

*Table continues...*

Variable	Value
	<p>Specify the source IP addresses from which the connections are allowed:</p> <ul style="list-style-type: none"> <li>• Enter the IPv4 addresses as a mask from 1 to 50 and an IP address in the format A.B.C.D.</li> <li>• Enter the IPv6 addresses from 51–100 with a description.</li> </ul> <p><b>!</b> <b>Important:</b></p> <p>These are the same source IP addresses as in the IP Manager list. For more information about the IP Manager list, see <a href="#">Configuring the IP Manager list for IPv4 addresses using CLI</a> on page 175 and <a href="#">Configuring the IP Manager list for IPv6 addresses using CLI</a> on page 175.</p>

## Disabling Telnet access

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```


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>	<p>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.</p> <ul style="list-style-type: none"> <li>• Specify &lt;1–50&gt; to select the address/mask pair to be disabled.</li> <li>• Specify &lt;51–100&gt; to select the IPv6 address/prefix to be disabled.</li> </ul>

Variable	Value
	<p> <b>Important:</b></p> <p>These are the same source IP addresses as in the IP Manager list. For more information about the IP Manager list, see <a href="#">Configuring the IP Manager list for IPv4 addresses using CLI</a> on page 175 and <a href="#">Configuring the IP Manager list for IPv6 addresses using CLI</a> on page 175.</p>

---

## Setting the Telnet settings to default values

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
default telnet-access
```

---

## Configuring SSL using CLI

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

---

## Enabling or disabling SSL

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. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show ssl
```

### Example

The following is a sample output of the **show ssl** command:

```
Switch #show ssl
WEB Server SSL secured: No
SSL server state      : Active
SSL Certificate       :
    Generation in progress: No
    Saved in NVRAM       : Yes
    Certificate file size : 804 bytes
    RSA host key length  : 2048 bits
```

## 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
<b>SSL server state</b>	
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.
<b>SSL Certificate</b>	
Generation in progress	Shows whether SSL is generating a certificate. The SSL server generates a certificate during server startup initialization, or the CLI 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 CLI 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

### Procedure

1. Enter Privileged EXEC mode:  

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

```
show ssl certificate
```

### Example

The following is an example of the `show ssl certificate` command:

```
Issuer      : Extreme Networks
Start Date  : May 26 2003, 00:01:26
End Date    : May 24 2033, 23:01:26
```

```
RSA Host Key (length = 2048 bits):
b199777714196fad8575948047b2f15fcd944a6bbf897e634c3c2898665f457a
e93de38acf5733786bb76a6d21f001835f55c710ddd476c51a525da60f526b47
be8ef3aa2119046e54402da7b3180d6948a1bd4fbab740f231968b29dc55ceb6
194547a853847a02d05bf9ea8e918f456fe8490a7b64d0903417f917bc22569d
c3790bd3c59ddcee00bd4cd8b006cee26c0337065453badb192e934aae416244
315cdbb77bf4f69a1e3a48dee0e3d5554a05605f6d961500fb5f7279394845d7
99ce1b5b4ae4e5d4fecala3435a778ee8680ab99aa907d18b98e1144fb731c5f
6c62054a3f3ac43a9ff25ccf5ce418a3d0f680c89f53d4829bd62dac60aed2c5
```



## Regenerating the SSL Certificate

Use the steps in the following procedure to regenerate the SSL certificate after you upgrade the software to a release that supports SHA-256 and to reset the SSL server to use the new certificate.

### Before you begin

Upgrade the software to a release that supports SHA-256.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command to regenerate the SSL certificate.

```
ssl certificate
```

The SSL certificate regenerates in the background. It might take several minutes to regenerate the SSL certificate.

3. Enter the following command to check the progress of the regeneration process:

```
show ssl
```

#### Important:

You must wait until the SSL certificate is fully complete before you reset the SSL server.

If the output displays `Generation in progress: Yes`, SSL certificate regeneration is not completed. Do not reset the SSL server.

If the output displays `Generation in progress: No`, SSL certificate regeneration is completed. You can now reset the SSL server.

4. Enter the following command to reset the SSL server to use the new SSL certificate.

```
ssl reset
```

### Example

The following output displays when SSL certificate regeneration is in progress:

```
Switch #show ssl
WEB Server SSL secured: No
SSL server state : Active
Generation in progress: Yes
Saved in NVRAM : Yes
Certificate file size : 804 bytes
RSA host key length : 2048 bits
```

The following output displays when SSL certificate regeneration is in complete:

```
Switch #show ssl
WEB Server SSL secured: No
SSL server state : Active
```

```
Generation in progress: No
Saved in NVRAM : Yes
Certificate file size : 804 bytes
RSA host key length : 2048 bits
```

---

## Secure Shell protocol configuration using CLI

Secure Shell (SSH) protocol is used to improve Telnet and provide a secure access to the CLI interface. There are two versions of the SSH Protocol (SSH1 and SSH2). The switch supports SSH2.

You can use the information in this section to configure and manage SSH.

---

## Displaying SSH information

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

### Example

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

```
Switch#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 Retries            : 3
Auth Key TFTP Server    : 192.0.2.1
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys           : Exist
RSA Host Keys           : Exist
Enabled                  : False
```

The following example displays sample output for the **show ssh download-auth-key** command:

```
Switch#show ssh download-auth-key
Auth Key TFTP Server : 192.0.2.1
DSA Auth Key File Name :
RSA Auth Key File Name :
Last Transfer Result  : None
```

## Variable definitions

The following table describes the parameters for the `show ssh` command.

Variable	Value
download-auth-key	Displays authorization key and TFTP server IP address
global	Displays general SSH settings.
session	Displays SSH session info.

---

## Configuring SSH

Use this procedure to enable SSH in a non-secure mode. The switch continues to accept SNMP and Telnet connections while in this mode.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
ssh
```

3. Disable SSH for the switch:

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

---

## Generating the DSA host keys

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

3. Delete the switch SSH DSA host key:

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

---

## Generating the SSH RSA host key

Use the following procedure to generate the RSA host keys.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

3. Delete the SSH RSA host key on the switch:

```
no ssh rsa-host-key
```

---

## Downloading DSA or RSA authentication keys

Use this procedure to download the DSA or RSA authentication key into the switch.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
ssh download-auth-key {[address <A.B.C.D > | <WORD>] usb [unit
<1-8>]}[key-name <WORD>][dsa | rsa ]
```

## Variable definitions

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

Variable	Value
address <A.B.C.D> <WORD>	Specifies the IP address of the TFTP server. <ul style="list-style-type: none"> <li>• A.B.C.D—specifies the IP address</li> <li>• WORD—specifies the IPv6 address</li> </ul>
dsa	Download SSH DSA auth key.

*Table continues...*

Variable	Value
key-name <WORD>	Specifies the TFTP filename.
rsa	Download the SSH RSA auth key.
unit <1-8>	Specifies the unit number in a stack from which to download the SSH auth key using USB.

---

## Deleting the SSH DSA authentication key

### Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
2. At the command prompt, enter the following command:  

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

---

## Deleting the SSH RSA authentication key

### Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
2. At the command prompt, enter the following command:  

```
no ssh rsa-auth-key
```

---

## Enabling user log-on with an SSH DSA key

### Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
2. At the command prompt, enter the following command:  

```
[default] ssh dsa-auth
```
3. Disable user log-on with SSH DSA key authentication:  

```
no ssh dsa-auth
```

## Variable definitions

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

Variable	Value
no	Disables DSA authentication.

---

## Enabling user log-on with an SSH RSA key

### Procedure

1. Enter Global Configuration mode:  

```
enable  
configure terminal
```
2. At the command prompt, enter the following command:  

```
[default] ssh rsa-auth
```
3. Disable user log-on with SSH RSA key authentication:  

```
no ssh rsa-auth
```

---

## Enabling user log-on with SSH password authentication

### Procedure

1. Enter Global Configuration mode:  

```
enable  
configure terminal
```
2. At the prompt, enter the following command:  

```
[default] ssh pass-auth
```
3. Disable user log-on using the SSH password authentication method:  

```
no ssh pass-auth
```

---

## Disabling SNMP and Telnet With SSH

Use this procedure to disable SNMP and Telnet management interfaces permanently.

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command to disable SNMP and Telnet management interfaces permanently:

```
ssh secure [force]
```

## Variable definitions

The following table describes the parameters for the `ssh secure` command.

Variable	Value
force	Skips the confirmation step.

---

## Configuring the TCP port for SSH daemon

### Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

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

- Configure the default TCP port for the SSH daemon:

```
default ssh port
```

## Variable definitions

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

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

---

## Configuring the timeout value for session authentication

### Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

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

3. Configure the SSH authentication timeout to the default value of 60 seconds:

```
default ssh timeout
```

## Variable definitions

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

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

---

## Configuring and clearing the SSH banner

Use this procedure to download a custom SSH banner from the TFTP server.

**\* Note:**

The maximum size of the SSH banner is 1564 characters.

### Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

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

```
ssh download-banner address [<A.B.C.D> | <WORD>] <filename>
```

3. Display the banner:

```
show ssh banner
```

4. (Optional) Clear the SSH banner:

```
clear ssh banner
```

### Example

The following is an example of the `show ssh banner` command.

```
Switch(config)#show ssh banner  
This system is for authorized users only. All activity is logged and regularly checked  
by systems personal. Individuals using this system without authority or in excess of  
their authority are subject to having all their services revoked. Any illegal services  
run by user or attempts to take down this server or its services will be reported to  
local law enforcement, and said user will be punished to the full extent of the law.  
Anyone using this system consents to these terms.
```



## Variable definitions

The following table describes the parameters for the `ssh download-banner address` command.

Variable	Value
<A.B.C.D>	Specifies the TFTP IPv4 address.
<filename>	Specifies the file to be downloaded from the TFTP server.
<WORD>	Specifies the TFTP IPv6 address.

---

## Configuring and clearing the SSH banner

Use this procedure to configure the number of SSH authentication retries.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
ssh retries <1-100>
```
3. (Optional) Set SSH retries to default value:
 

```
default ssh retries
```

---

## Secure Shell Client configuration

Use the procedures in this section to configure and manage Secure Shell Client.

Opening and closing an SSH session involves three actions:

- Connect - make the connection from the CLI user interface
- Authenticate - the SSH Client uses DSA or RSA authentication keys. If key authentication fails due to non-existent or unaccepted DSA/RSA keys, you can enter a username and password (three tries allowed).
- Close the session - end the SSH session and return to CLI by using by typing a '~' followed by a period (~.).

## Configuring SFTP authentication for SSH Client

Use this procedure to configure the SFTP authentication method the SSH Client uses for transferring files.

### Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
2. Configure the SFTP authentication method the SSH Client uses for transferring files:  

```
sshc authentication {dsa | password | rsa}
```
3. Configure the SFTP authentication method SSH Client to the default of DSA:  

```
default sshc authentication
```

OR

```
no sshc authentication
```

### Variable definitions

The following table describes the parameters for the `sshc authentication` command.

Variable	Value
dsa	Enables SFTP DSA authentication for SSH Client (default).
password	Enables SFTP password authentication for SSH Client.
rsa	Enables SFTP RSA authentication for SSH Client.

## Generating an SSHC DSA host key

### Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
2. At the command prompt, enter the following command:  

```
sshc dsa-host-key [force]
```
3. Delete the public or private DSA host keys from NVRAM:

```
no sshc dsa-host-key
```

## 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.

---

## Generating an SSHC RSA host key (public and private)

### Procedure

1. Enter Global Configuration mode:
 

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:
 

```
sshc rsa-host-key [force]
```
3. Delete the public or private DSA host keys from NVRAM
 

```
no sshc rsa-host-key
```

## Variable definitions

The following table describes the parameters for the `sshc rsa-host-key` command.

Variable	Value
force	Specifies generation of a new SSHC RSA host key. No reset is required.

---

## Configuring 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. Enter Global Configuration mode:
 

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:

```
sshc dsa-key <512-1024>
```

## Variable definitions

The following table describes the parameters for the `sshc dsa-key` command.

Variable	Value
<512-1024>	Specifies the key size (multiple of 64).

---

## Configuring SSHC RSA host key size

Use the following procedure to set the SSHC RSA host key size and generate a new key at the next system reboot.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
sshc rsa-key <1024-2048>
```

## Variable definitions

The following table describes the parameters for the `sshc rsa-key` command.

Variable	Value
<1024-2048>	Specifies the key size (multiple of 128).

---

## Configuring the SSHC port

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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.

## Viewing Secure File Transfer Protocol (SFTP)

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
show sshc
```

### Example

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

```
Switch(config)#show sshc
GLOBAL:
  Version           : Version 2 only
  DSA Auth Key      : Does Not Exist
  DSA key size      : 1024
  RSA Auth Key      : Exist
  RSA key size      : 2048

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. RANGE: 1 to 65535 DEFAULT: 22
Authentication Timeout	Displays the timeout interval in seconds. DEFAULT: 30
DSA Authentication	Displays the DSA Authentication state.

*Table continues...*

Variable	Value
	DEFAULT: True
RSA Authentication	Displays the RSA Authentication state. DEFAULT: True
User Name	Displays the user name. 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 (multiple of 64). RANGE: 1024 to 1024 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). RANGE: 1024 to 2048 DEFAULT: 2048

## Uploading the public host key

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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 **sshc upload-host-key** command.

Variable	Value
address <A.B.C.D   WORD>	Specifies the TFTP server address. <ul style="list-style-type: none"> <li>• A.B.C.D is the IPv4 address format</li> <li>• WORD is the IPv6 address format</li> </ul>
key-name <WORD>	Specifies the TFTP filename.

---

## Uploading a config file to an SFTP server

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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: <ul style="list-style-type: none"> <li>• A.B.C.D is the IPv4 address format</li> <li>• WORD is the IPv6 address format</li> </ul>
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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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: <ul style="list-style-type: none"> <li>• A.B.C.D is the IPv4 address format</li> <li>• WORD is the IPv6 address format</li> </ul>
filename <WORD>	Specifies the configuration file name.
password <WORD>	Specifies the password.
username <WORD>	Specifies the username.

---

## Configuring RADIUS Interim Accounting Updates support using CLI

Use the procedures in this section to configure RADIUS Interim Accounting Updates support.

---

### Configuring RADIUS Interim Accounting Updates support

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. Enter Global Configuration mode:
 

```
enable
configure terminal
```
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.  DEFAULT: 600 seconds 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

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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 CLI to enter User EXEC 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.

```
Switch#show radius accounting interim-update
RADIUS accounting interim-updates: Disabled
RADIUS accounting interim-updates interval: 600
RADIUS accounting use-server-interval: Enabled
```

---

## Configuring RADIUS Request use Management IP using CLI

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

---

### Enabling RADIUS request use of Management IP

#### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
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

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

#### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. At the command prompt, enter the following command:  
`no radius use-management-ip`

## Viewing RADIUS request use Management IP status

### Procedure

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

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

## Configuring RADIUS authentication using CLI

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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.  <b>!</b> <b>Important:</b> 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.

*Table continues...*

Variable	Value
	<p> <b>Important:</b></p> <p>A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.</p>
default	<p>Restores the switch RADIUS server settings to default values.</p> <p>To delete a RADIUS server and restore default RADIUS settings, use one of the following commands in the Global or Interface Command mode:</p> <ul style="list-style-type: none"> <li>• <code>default radius server host</code></li> <li>• <code>default radius server host secondary</code></li> <li>• <code>default radius server host used-by eapol</code></li> <li>• <code>default radius server host secondary used-by eapol</code></li> <li>• <code>default radius server host used-by non-eapol</code></li> <li>• <code>default radius server host secondary used-by non-eapol</code></li> </ul>
key <key>	<p>Specifies the secret authentication and encryption key used for all communications between the NAS and the RADIUS server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to enter and confirm the key.</p>
no	<p>Deletes switch RADIUS server settings.</p>
port <port>	<p>Specifies the UDP port number for clients to use when trying to contact the RADIUS server at the corresponding RADIUS server IP address.</p> <p>RANGE: 1 to 65535</p> <p>DEFAULT port number: 1812</p>
retry <1–5>	<p>Specifies the number of RADIUS retry attempts for a RADIUS Server instance.</p> <p>RANGE: 1 to 5</p>
secondary	<p>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.</p>
timeout <timeout>	<p>Specifies the timeout interval between each retry for service requests to the RADIUS server.</p>

*Table continues...*

Variable	Value
	RANGE: 1 to 60 seconds DEFAULT: 2 seconds
used-by <i>&lt;eapol   non-eapol&gt;</i>	Specifies the RADIUS server as an EAP RADIUS Server or a Non-EAP (NEAP) RADIUS Server. <ul style="list-style-type: none"> <li>• eapol—configures the RADIUS server to process EAP client requests only .</li> <li>• non-eapol—configures the RADIUS server to process Non-EAP client requests only.</li> </ul> <p>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.</p>

---

## Enabling or disabling RADIUS password fallback

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. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <vlan ID>
```

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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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.

```
Switch#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

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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 `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

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

### Procedure

1. Enter Privileged EXEC mode:  

```
enable
```
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.

```
Switch#show radius reachability
RADIUS reachability: USE ICMP
```

---

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

---

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

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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.
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)**

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. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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

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

### Procedure

1. Enter Privileged EXEC mode:  

```
enable
```
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

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

**Procedure**

1. Enter Privileged EXEC mode:

```
enable
```

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**

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 port on which the feature is not enabled.

**Procedure**

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface fastEthernet <port>
```

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

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

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

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

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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 CLI

---

## Enabling or disabling the SNMP server

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

### Procedure

1. Enter Global Configuration mode:  

```
enable  
configure terminal
```
2. At the command prompt, enter the following command:  

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

---

## Disabling SNMP access

### Important:

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

### Procedure

1. Enter Global Configuration mode:  

```
enable  
configure terminal
```
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

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

### Procedure

1. Enter Global Configuration mode:  

```
enable  
configure terminal
```
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

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.

These community strings have a fixed MIB view.

### Procedure

1. Enter Global Configuration mode:

```
enable
```


```
configure terminal
```

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>	<p>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 <b>NONE</b>, it is disabled.</p> <p> <b>Important:</b></p> <p>This parameter is not available when Password Security is enabled, in which case, the switch prompts you to enter and confirm the new community string.</p>
ro   rw	<p>Specifies read-only or read/write access. Stations with <b>ro</b> access can retrieve only MIB objects, and</p>

*Table continues...*

Variable	Value
	stations with <b>rw</b> access can retrieve and modify MIB objects.   <b>Important:</b> If neither <b>ro</b> nor <b>rw</b> is specified, <b>ro</b> is assumed (default)

## Clearing the SNMP server community configuration

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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 <b>public</b> , or the read/write community to <b>private</b> .

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

**\* Note:**

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

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show snmp-server community`

---

## Configuring the SNMP sysContact value

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
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

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`



- 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

### Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- To configure the SNMP `sysLocation` value, enter the following command:

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

- 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 <code>sysLocation</code> value. Enter a string of up to 255 characters.

---

## Restoring the SNMP `sysLocation` to the default

### Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

```
default snmp-server location
```

---

## Configuring the SNMP sysName value

Use the following procedure to configure the SNMP sysName value.

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```

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

## Disabling the SNMP linkUp linkDown traps for a port

### Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- 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>	<p>Specifies the port numbers on which to disable the linkUp/linkDown traps. Enter the port numbers or all.</p> <p><b>!</b> <b>Important:</b></p> <p>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.</p>

## Adding SNMP traps to a filter profile

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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>]]]]]]]
```

### Variable definitions

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

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

## Deleting SNMP traps from a filter profile

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- 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.  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

### Procedure

- Enter Privileged EXEC mode:

```
enable
```

- 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 filter subtree address.
Mask	Specifies the filter mask.

---

## Enabling or disabling the generation of SNMP traps

### Procedure

- Enter Global Configuration mode:

```
enable  
configure terminal
```

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.  An example of a character string describing the notification type is, <b>linkDown</b> , <b>linkup</b> .  An example of an OID describing the notification type is <b>1.3.1.6.1.3.1.1.5.3</b> , <b>1.3.6.1.6.3.1.1.5.4</b> .

---

## Using CLI commands specific to SNMPv3

---

### Creating an SNMPv3 user

#### Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

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.
md5/sha <password>	<p>Specifies the use of an md5/sha authentication pass phrase.</p> <ul style="list-style-type: none"> <li>• <i>password</i>—specifies the new user md5 /sha authentication pass phrase; enter an alphanumeric string.</li> </ul> <p>If this parameter is omitted, the user is created with only unauthenticated access rights.</p> <p><b>!</b> <b>Important:</b></p> <p>This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password.</p>
read-view <view-name>	<p>Specifies the read view to which the new user has access:</p> <ul style="list-style-type: none"> <li>• <i>view-name</i>—specifies the view name; enter an alphanumeric string of up to 255 characters.</li> </ul>
write-view <view-name>	<p>Specifies the write view to which the new user has access:</p> <ul style="list-style-type: none"> <li>• <i>view-name</i>—specifies the view name; enter an alphanumeric string of up to 255 characters.</li> </ul>
notify-view <view-name>	<p>Specifies the notify view to which the new user has access:</p> <ul style="list-style-type: none"> <li>• <i>view-name</i>— specifies the view name; enter an alphanumeric string of up to 255 characters.</li> </ul>
des/aes/3des <password>	<p>Specifies the use of a des/aes/3des privacy pass phrase.</p> <ul style="list-style-type: none"> <li>• <i>password</i>—specifies the new user des/aes/3des privacy pass phrase; enter an alphanumeric string</li> </ul>

*Table continues...*

Variable	Value
	<p>of minimum 8 characters. If this parameter is omitted, the user is created with only authenticated access rights.</p> <p><b>!</b> <b>Important:</b> This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password.</p>

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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>	<p>Specifies the Object identifier. <i>OID</i> can be entered as a MIB object English descriptor, a dotted form <i>OID</i>, or a mix of the two. Each <i>OID</i> 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 <i>OID</i> parameters are as follows:</p> <ul style="list-style-type: none"> <li>• <code>sysName</code></li> <li>• <code>+sysName</code></li> <li>• <code>-sysName</code></li> <li>• <code>+sysName.0</code></li> <li>• <code>+ifIndex.1</code></li> <li>• <code>-ifEntry.*.1</code> (matches all objects in the if Table with an instance of 1, that is, the entry for interface #1)</li> <li>• <code>1.3.6.1.2.1.1.1.0</code> (dotted form of <code>sysDescr</code>)</li> </ul> <p>The plus (+) or minus (-) sign indicates whether the specified <i>OID</i> is included in or excluded from, respectively, the set of MIB objects that are accessible by using this view. For example, if you create a view as follows:</p>

*Table continues...*

Variable	Value
	<pre>snmp-server view myview +system - sysDescr</pre> <p>and you use that view for the read-view of a user, then the user can read only the system group, except for <code>sysDescr</code>.</p>

## Removing an SNMPv3 view

### Procedure

1. Enter Global Configuration mode:
 

```
enable
```

```
configure terminal
```
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

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. Enter Global Configuration mode:
 

```
enable
```

```
configure terminal
```
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 <b>snmp-server host</b> command is improved with the filter parameter only for the hosts with a specified SNMP version (v1/v2c/v3).  Add the filter parameter only for the normal syntax form of the <b>snmp-server host</b> command. When you delete a specific SNMP-server host with the <b>no</b> command or delete all configured SNMP-server hosts with the <b>default</b> 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. RANGE: 0-2147483647
target-name <WORD/1-32>	Specifies the name of the target.
timeout <1-2147483647>	Specifies the timeout for inform requests. 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.

*Table continues...*

Variable	Value
v3 {auth no-auth  auth-priv}	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>auth no-auth</b> —Specifies whether SNMPv3 traps can be authenticated.</li> <li>• <b>auth-priv</b>—This parameter is only available if the image has full SHA/DES support.</li> </ul>

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

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. Enter Global Configuration mode:

```
enable
configure terminal
```

2. To delete trap receivers, enter the following command:

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

### Procedure

1. Enter Privileged EXEC mode:  
enable
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.

```
Switch#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

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. Enter Privileged EXEC mode:  
enable
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
<i>&lt;community-string&gt;</i>	Enter a community string to be created with access to the specified views.  <b>! Important:</b> 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 <i>&lt;view-name&gt;</i>	Changes the read view used by the new community string for different types of SNMP operations.  • <i>view-name</i> —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.
write-view <i>&lt;view-name&gt;</i>	Changes the write view used by the new community string for different types of SNMP operations.  • <i>view-name</i> —specifies the name of the view that is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.
notify-view <i>&lt;view-name&gt;</i>	Changes the notify view settings used by the new community string for different types of SNMP operations.  • <i>view-name</i> —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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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: <ul style="list-style-type: none"> <li>• community strings as configured in SNMPv3 MIBs (this parameter is not displayed when Password Security is enabled)</li> <li>• trap receivers as configured in SNMPv3 MIBs</li> <li>• SNMPv3 users, including views accessible to each other</li> <li>• SNMPv3 views</li> </ul>

## Creating an initial set of configuration data for SNMPv3

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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.

*Table continues...*

Variable	Value
<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 CLI

### Displaying MAC address security settings

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

#### Before you begin

#### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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>**.

```
Switch(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
```

### Variable definitions

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

Variable	Value
config	Displays the general BaySecure configuration

*Table continues...*



Variable	Value
mac-address-table [address <macaddr>]	Displays contents of the BaySecure table of allowed MAC addresses: <ul style="list-style-type: none"> <li>• address specifies a single MAC address to display</li> </ul>
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

Use the following procedure to modify the BaySecure configuration.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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. 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: <ul style="list-style-type: none"> <li>• <i>enable</i>— port is partitioned for a period of time.</li> <li>• <i>disabled</i>— port is not partitioned on detection.</li> </ul>

*Table continues...*

Variable	Value
	<ul style="list-style-type: none"> <li><i>forever</i>— port is partitioned until manually changed.</li> </ul>
intrusion-timer <0-65535>	Temporary partition time in seconds. Default value is 0.
learning {enable disable}	Specifies MAC address learning: <ul style="list-style-type: none"> <li><i>enable</i>— enables learning by ports</li> <li><i>disable</i>— disables learning by ports</li> </ul> <p><b>!</b> <b>Important:</b>                      The MAC address learning enable command must be executed to specify learning ports.</p>
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

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. Enter Global Configuration mode:


```
enable
configure terminal
```

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.   <b>Important:</b> In this command, portlist must specify only a single port.

---

## Assigning a list of ports to a security list

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
no mac-security
```

---

## Disabling MAC address auto-learning aging time

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

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

---

## Clearing the MAC address security table

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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

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

### Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface fastEthernet <port>
```

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: <ul style="list-style-type: none"> <li>• auto-learning — configures MAC Auto-Learning</li> <li>• disable — disables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is performed</li> <li>• enable — enables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is performed</li> </ul>

*Table continues...*

Variable	Value
	<ul style="list-style-type: none"> <li>learning — disables BaySecure on the specified port and adds these port to the list of ports for which MAC address learning is performed</li> </ul>

## Filtering packets from specified MAC DAs

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. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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 CLI

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

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. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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.  DEFAULT: 60 minutes  RANGE: 0 to 65535

**Disabling MAC address auto-learning aging time****Procedure**

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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**

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. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:

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

---

## Enabling or disabling block subsequent MAC authentication

**\* Note:**

Commands issued on a unit are propagated through the entire stack and any new unit added receives the global setting.

### Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

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

```
eapol multihost block-different-radius-assigned-vlan
```

**\* Note:**

By default this feature is disabled.

3. To reset (disable) the feature, enter the following command:

```
default eapol multihost block-different-radius-assigned-vlan  
OR  
no eapol multihost block-different-radius-assigned-vlan
```

---

## Viewing the current Sticky MAC address mode

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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.

```
Switch#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

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

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

### Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
2. At the command prompt, enter the following command:  

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

---

## Disabling Sticky MAC address mode

The default state is disabled.

### Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
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

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

### Procedure

1. Enter Global Configuration mode:  

```
enable  
configure terminal
```
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

### Procedure

1. Enter Interface Configuration mode:  

```
enable  
configure terminal  
interface fastEthernet <port>
```
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 <portlist>	Specifies the ports to configure for EAPOL; enter the port numbers you want to use.  <b>!</b> <b>Important:</b> If you omit this parameter, the system uses the port number that you specified when you issued the <b>interface</b> 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: <ul style="list-style-type: none"> <li>• <i>authorized</i>— Port is always authorized.</li> <li>• <i>unauthorized</i>— Port is always unauthorized.</li> <li>• <i>auto</i>— Port authorization status depends on the result of the EAP authentication.</li> </ul>
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: <ul style="list-style-type: none"> <li>• <i>in-out</i>— If EAP authentication fails, both ingressing and egressing traffic are blocked.</li> <li>• <i>in</i>— If EAP authentication fails, only ingressing traffic is blocked.</li> </ul>

---

## Setting the guest VLAN for EAPOL

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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

### Procedure

1. Enter Privileged EXEC mode:  

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

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

## Example

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

```
Switch#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
```

---

## Resetting EAP settings globally

To simplify the configuration process on the switch, you can reset all EAP-related settings using a single command.

This command resets the following EAP settings:

- EAP state
- Fail Open VLAN
- VoIP VLANs
- all multihost settings
- multiVLAN

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
default eap-all
```

---

## Resetting EAP settings at the port level

### About this task

This command resets the following settings:

- all EAP related settings
- all EAP multihost settings
- EAP Guest VLAN settings

### Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface fastEthernet <port>
```

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

```
default eap-all <port-list>
```

---

## Displaying EAPOL diagnostics

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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**.

```
Switch#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

### Procedure

1. Enter Privileged EXEC mode:  
enable
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**.

```

Switch#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

### Procedure

1. Enter Global Configuration mode:  
enable  
configure terminal

- At the command prompt, enter the following command:

```
show eapol guest-vlan
```

### Example

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

```
Switch#show eapol guest-vlan
EAPOL Guest Vlan   : Disabled
EAPOL Guest Vlan ID: 1
```

---

## Configuring advanced EAPOL features using CLI

Use the procedures in this section to configure advanced EAPOL features, which 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

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

```
eapol multihost { [adac-non-eap-enable] [allow-non-eap-enable]
[auto-non-eap-mhsa-enable] [block-different-radius-assigned-vlan]
[eap-packet-mode] [eap-protocol-enable] [non-eap-phone-enable] [non-
eap-reauthentication-enable] [non-eap-use-radius-assigned-vlan]
[radius-non-eap-enable] [use-most-recent-radius-vlan] [use-radius-
assigned-vlan] [multivlan enable] [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.

*Table continues...*



Variable	Value
auto-non-eap-mhsa-enable	Enables auto-authentication of non-EAP clients in MHSa mode.
block-different-radius-assigned-vlan	Blocks subsequent MAC authentications if the RADIUS assigned VLAN is different than the first authorized station VLAN.
eap-packet-mode	Selects the packet mode for EAP authentication. Values are: <ul style="list-style-type: none"> <li>• multicast</li> <li>• unicast</li> </ul>
eap-protocol-enable	Enables EAP protocol on ports.
non-eap-phone-enable	Enables the use of non-EAP IP phone clients.
non-eap-reauthentication-enable	Enables re-authentication for NEAP 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-most-recent-radius-vlan	Allows the use of the most recently assigned RADIUS VLAN.
use-radius-assigned-vlan	Allows the use of RADIUS-assigned VLAN IDs.
multivlan enable	Enables multivlan functionality with MHMA mode.
non-eap-pwd-fmt <i>{{[ip-addr][mac-addr][port-number]}</i>	Sets bits in RADIUS non-EAPOL password format.

## Disabling global EAPOL multihost settings

Use the following procedure to disable EAPOL multihost settings.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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] [block-different-radius-assigned-vlan]
[eap-protocol-enable] [non-eap-phone-enable] [non-eap-
reauthentication-enable] [non-eap-use-radius-assigned-vlan] [radius-
non-eap-enable] [use-most-recent-radius-vlan] [use-radius-assigned-
vlan] [multivlan enable] [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
<code>adac-non-eap-enable</code>	Disables authentication of non-EAP Phones using ADAC.
<code>allow-non-eap-enable</code>	Disables control of MAC addresses of non-EAP clients.
<code>auto-non-eap-mhsa-enable</code>	Disables auto-authentication of non-EAP clients in MHSa mode.
<code>block-different-radius-assigned-vlan</code>	Disables the blocking of subsequent MAC authentications if the RADIUS assigned VLAN is different than the first authorized station VLAN.
<code>eap-protocol-enable</code>	Disables EAP protocol.
<code>non-eap-phone-enable</code>	Disables the use of non-EAP IP phone clients.
<code>non-eap-reauthentication-enable</code>	Disables re-authentication for non-EAP clients.
<code>non-eap-use-radius-assigned-vlan</code>	Disables the use of VLAN IDs assigned by RADIUS for non-EAP clients.
<code>radius-non-eap-enable</code>	Disables RADIUS authentication of non-EAP clients.
<code>use-most-recent-radius-vlan</code>	Disables the use of the most recent RADIUS-assigned VLAN.
<code>use-radius-assigned-vlan</code>	Disables the use of RADIUS-assigned VLAN IDs.
<code>multivlan enable</code>	Disables multiple VLAN capabilities for EAP and non-EAP hosts.
<code>non-eap-pwd-fmt <i>{[ip-addr][mac-addr][port-number]}</i></code>	Clears bits in RADIUS non-EAPOL password format.

## Restoring global EAPOL multihost settings to default

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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] [block-different-radius-assigned-
vlan] [eap-packet-mode] [eap-protocol-enable] [non-eap-phone-enable]
[non-eap-reauthentication-enable] [non-eap-use-radius-assigned-vlan]
[radius-non-eap-enable] [use-most-recent-radius-vlan] [use-radius-
```

```
assigned-vlan] [multivlan enable] [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.
block-different-radius-assigned-vlan	Disables the blocking of subsequent MAC authentications if the RADIUS assigned VLAN is different than the first authorized station VLAN.
eap-packet-mode	Defaults the type of packet used for initial EAP request for IDs (multicast).
eap-protocol-enable	Resets EAP protocol to enabled (default).
non-eap-phone-enable	Disables the use of non-EAP IP phone clients
non-eap-reauthentication-enable	Disables re-authentication for non-EAP 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-most-recent-radius-vlan	Disables the use of the most recent RADIUS-assigned VLAN.
use-radius-assigned-vlan	Disables the use of RADIUS-assigned VLAN IDs.
multivlan enable	Disables multiple VLAN capabilities for EAP and non-EAP hosts.
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

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

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
```

```
configure terminal
interface Ethernet <port>
```

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

```
eapol multihost [adac-non-eap-enable] [allow-non-eap-enable] [auto-
non-eap-mhsa-enable] [block-different-radius-assigned-vlan] [eap-
mac-max <1-32>][eap-packet-mode {<multicast | unicast>}] [eap-
protocol-enable] [enable] [mac-max <1-64>] [mhsa-no-limit] [non-eap-
mac-max <1-32>] [non-eap-phone-enable] [non-eap-use-radius-assigned-
vlan] [port <portlist>] [radius-non-eap-enable] [use-most-recent-
radius-vlan] [use-radius-assigned-vlan] [non-eap-mac [port
<portlist>]{H.H.H}]
```

## 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 MHSAs mode.
block-different-radius-assigned-vlan	Blocks subsequent MAC authentication if the RADIUS-assigned VLAN is different from the first authorized station VLAN.
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.
eap-protocol-enable	Enables EAP protocol on the port.
enable	Allows EAP clients (MAC addresses).
mac-max <1-64>	Specifies the maximum number of MAC addresses allowed per port.
mhsa-no-limit	Allows an unlimited number of auto-authenticated non-EAP clients on the port.
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.

*Table continues...*

Variable	Value
radius-non-eap-enable	Enables RADIUS authentication of non-EAP clients.
use-most-recent-radius-vlan	Enables use of the most recent RADIUS-assigned VLAN.
use-radius-assigned-vlan	Allows the use of RADIUS-assigned VLAN value.
non-eap-mac [port <portlist>] {H.H.H }	Allows a non-EAPOL MAC address.

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

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

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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] [block-different-radius-assigned-vlan]
[eap-protocol-enable] [enable] [mhsa-no-limit] [non-eap-phone-
enable] [non-eap-use-radius-assigned-vlan] [port <portlist>]
[radius-non-eap-enable] [use-most-recent-radius-vlan] [use-radius-
assigned-vlan] [non-eap-mac [port <portlist>] {delete-all | H.H.H}]
```

## 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 MHSAs mode.
block-different-radius-assigned-vlan	Disables the blocking of subsequent MAC authentication if the RADIUS-assigned VLAN is different from the first authorized station VLAN.
eap-protocol-enable	Disables EAP protocol on the port.

*Table continues...*

Variable	Value
enable	Disallows EAP clients (MAC addresses).
mhsa-no-limit	Limits the number of auto-authenticated non-EAP clients.
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-most-recent-radius-vlan	Disables the use of the most recent RADIUS-assigned VLAN.
use-radius-assigned-vlan	Disallows the use of RADIUS-assigned VLAN value.
non-eap-mac [port <portlist>] {delete-all   H.H.H}	Disallows a non-EAPOL MAC address or deletes all local non-EAP clients.

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

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. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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] [block-different-radius-assigned-vlan]
[eap-mac-max] [eap-packet-mode] [eap-protocol-enable] [enable] [mac-
max] [mhsa-no-limit] [non-eap-mac-max] [non-eap-phone-enable] [non-
eap-use-radius-assigned-vlan] [port <portlist>] [radius-non-eap-
enable] [use-most-recent-radius-vlan] [use-radius-assigned-vlan]
[non-eap-mac [port <portlist>] {default-all | H.H.H}
```

### 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 (disabled).
auto-non-eap-mhsa-enable	Disables auto-authentication of non-EAP clients.
block-different-radius-assigned-vlan	Disables the blocking of subsequent MAC authentication if the RADIUS-assigned VLAN is different from the first authorized station VLAN.
eap-mac-max	Resets the maximum number of EAP-authenticated MAC addresses allowed to default (1).
eap-packet-mode	Resets the EAP packet mode to the default (multicast).
eap-protocol-enable	Enables EAP protocol on the port.
enable	Resets control of whether EAP clients (MAC addresses) are allowed to default (disabled).
mac-max	Resets the maximum number of clients allowed on the port to the default value (1).
mhsa-no-limit	Limits the number of auto-authenticated non-EAP clients.
non-eap-mac-max	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-most-recent-radius-vlan	Disables the use of the most recent RADIUS-assigned VLAN.
use-radius-assigned-vlan	Disallows the use of RADIUS-assigned VLAN value.
non-eap-mac [port <portlist>] {default-all   H.H.H}	Resets the non-EAPOL MAC addresses to default.

## Setting the maximum number of clients allowed per port

Use the `eapol multihost mac-max` command to restrict the maximum number of clients allowed per port.

You can use the `eapol multihost mac-max` command with `eap-mac-max` and `non-eap-mac-max` commands. The value set by `mac-max` takes precedence over other commands. Even if you

set **eap-mac-max** or **non-eap-mac-max** to a higher limit, the limit set using the **mac-max** command cannot be exceeded.

The default value for **eapol multihost mac-max** is 1, which restricts the maximum number of clients allowed per port to only one client, either EAP or Non-EAP.

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

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

- where **<portlist>** is the list of ports for which you are setting the maximum number of clients. You can enter a single port, a range of ports, several ranges, or all ports. If you do not specify a port parameter, the command applies to all ports on the interface.

**<num>** is an integer between 1 and 64 that specifies the maximum number of EAP and NEAP clients allowed per port. The default is 1.

Execute the **eapol multihost [port <portlist>] mac-max** command in the Interface Configuration mode.

**\* Note:**

The switch accepts clients in the order of authentication, regardless of whether they are EAP or NEAP clients.

**Example 1::**

```
(config-if)# eapol multihost port 1 eap-mac-max 32
(config-if)# eapol multihost port 1 non-eap-mac-max 32
(config-if)# eapol multihost port 1 mac-max 10
```

In this example, a maximum of ten EAP and Non-EAP clients are authenticated, in the order of authentication.

**Example 2::**

```
(config-if)# eapol multihost port 1 eap-mac-max 1
(config-if)# eapol multihost port 1 non-eap-mac-max 1
(config-if)# eapol multihost port 1 mac-max 1
```

In this example, only one EAP or Non-EAP client is authenticated, in the order of authentication.

**Example 3::**

```
(config-if)# eapol multihost port 1 eap-mac-max 5
(config-if)# eapol multihost port 1 non-eap-mac-max 10
(config-if)# eapol multihost port 1 mac-max 32
```

In this example, the switch allows up to five EAP clients and ten Non-EAP clients.

**Example 4::**

```
(config-if)# eapol multihost port 1 eap-mac-max 5
(config-if)# eapol multihost port 1 non-eap-mac-max 8
(config-if)# eapol multihost port 1 mac-max 7
```

In this example, the switch allows up to five EAP clients and up to two Non-EAP clients, or up to seven Non-EAP clients.



## Configuring non-EAPOL MAC addresses on a specific port or on all ports on an interface

### Procedure

1. Enter VLAN Interface Configuration mode:
 

```
enable
configure terminal
interface vlan <vlan ID>
```
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

### Procedure

1. Enter Privileged EXEC mode:
 

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

```
show eapol multihost
```

### Example

The following figure provides a sample of `show eapol multihost`.

```
Switch#show eapol multihost
Allow Local Non-EAP Clients           : Disabled
Non-EAP RADIUS Authentication         : Disabled
Non-EAP AutoLearned After Single Authent (MHSA) : Disabled
Non-EAP DHCP Phone Authentication     : Disabled
EAPoL Request Packet Generation Mode  : Multicast
EAP RADIUS Assigned VLANs            : Disabled
Non-EAP RADIUS Assigned VLANs        : Disabled
```

```

Non-EAP RADIUS Password Attribute Format      : IpAddr.MACAddr.PortNumber
EAP Protocol                                 : Enabled
Use Most Recent RADIUS Assigned VLAN         : Disabled
Non-EAP ReAuthentication                     : Disabled
Block Different RADIUS Assigned VLAN Authentication : Disabled
ADAC Non-EAP Phone Authentication           : Disabled
Fail Open VLAN                               : Disabled
Fail Open VLAN ID                           : 1
Fail Open VLAN Continuity Mode               : Disabled
    
```

## 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

### Procedure

1. Enter Privileged EXEC mode:  

```
enable
```
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>]`.

```

Switch#show eapol multihost interface
Unit/Port: 1/1
MultiHost Status           : Disabled
Total Maximum Nuber of Clients : 2
Maximum Number of EAP Clients : 1
Maximum Number of Non-EAP Clients : 1
Allow Local Non-EAP Clients  : Disabled
Non-EAP RADIUS Authentication : Disabled
Non-EAP AutoLearned After Single Auth (MHSA) : Disabled
Non-EAP DHCP Phone Authentication : Disabled
EAPoL Request Packet Generation Mode : Multicast
EAP RADIUS Assigned VLANs    : Disabled
Non-EAP RADIUS Assigned VLANs : Disabled
EAP Protocol                 : Enabled
Use Most Recent RADIUS Assigned VLAN : Disabled
Block Different RADIUS Assigned VLAN Authentication : Disabled
ADAC Non-EAP Phone Authentication : Disabled
MHSA No limit Non-EAP Authentication : Disabled
...
    
```

## Displaying non-EAPOL hosts information

Use the following procedure to display information about non-EAPOL hosts currently active on the switch.

### Procedure

1. Enter Privileged EXEC mode:  

```
enable
```
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**.

```
Switch#show eapol multihost non-eap-mac status
Unit/Port Client MAC Address State Vid Pri
-----
Total number of authenticated clients: 0
```

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

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 globally 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

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 CLI 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 CLI 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

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 CLI 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 CLI 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 CLI 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

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 CLI 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 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 Extreme Networks expects that the usual maximum allowed for each port be lower. Extreme Networks expects that the combined maximum will be approximately 200 per switch.

## Creating the allowed non-EAPOL MAC address list

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 CLI 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

Use the following procedure to enable or disable non-EAP (NEAP) re-authentication for the switch.

### Procedure

1. Log on to CLI 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

Use the following procedure to display the configuration status of NEAP re-authentication for the switch.

### Procedure

1. Log on to CLI 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**.

```
Switch#show eapol multihost
Allow Local Non-EAP Clients           : Disabled
Non-EAP RADIUS Authentication         : Disabled
Non-EAP AutoLearned After Single Authent (MHSA) : Disabled
Non-EAP DHCP Phone Authentication     : Disabled
EAPoL Request Packet Generation Mode  : Multicast
EAP RADIUS Assigned VLANs            : Disabled
Non-EAP RADIUS Assigned VLANs        : Disabled
Non-EAP RADIUS Password Attribute Format : IpAddr.MACAddr.PortNumber
EAP Protocol                          : Enabled
Use Most Recent RADIUS Assigned VLAN  : Disabled
Non-EAP ReAuthentication              : Disabled
Block Different RADIUS Assigned VLAN Authentication : Disabled
ADAC Non-EAP Phone Authentication     : Disabled
Fail Open VLAN                       : Disabled
Fail Open VLAN ID                    : 1
```

## Clearing non-EAP authenticated clients from ports

Use the following procedure to clear authenticated NEAP clients from a specified port.

### Procedure

1. Log on to CLI 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.  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 CLI

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

#### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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. RANGE: 1 to 5
vid <1-4094>	Specifies the VLAN ID. RANGE: 1 to 4094



## Disabling EAPOL VoIP VLAN

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
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` command.

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

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
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 multihost 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

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
show eapol multihost voip-vlan
```

---

## Configuring TACACS+ using CLI

Use the following section to configure TACACS+ to perform AAA services for system users.

---

## Configuring switch TACACS+ server settings

### Before you begin

- Configure the TACACS+ server to add to your system.

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
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

*Table continues...*

Variable	Value
	<p>as the shared secret, must be the same as the one defined on the server. You are prompted to confirm the key when you enter it.</p> <p><b>!</b> <b>Important:</b></p> <p>The key parameter is a required parameter when you create a new server entry. The parameter is optional when you modify an existing entry.</p>
port <1–65535>	<p>Specifies the TCP port for TACACS+.</p> <p>DEFAULT: 49</p>
secondary-host <A.B.C.D>	<p>Specifies the IP address of the secondary server. The secondary server is used only if the primary server does not respond.</p>

---

## Disabling switch TACACS+ server settings

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

TACACS+ authorization is disabled by default.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

Use the following procedure to configure TACACS+ authorization privilege levels to specify the privilege levels to which TACACS+ authorization applies.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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.  The default authorization level is NONE.

---

## Enabling or disabling TACACS+ accounting

### Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
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

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. Enter Global Configuration mode:  

```
enable
configure terminal
```
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

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show tacacs`

---

## Configuring IP Manager using CLI

---

### Configuring IP Manager

Use the following procedure to control Telnet, SNMP, SSH, or HTTP access.

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
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 `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

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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
<code>&lt;ipv4addr&gt;</code>	Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation.
<code>&lt;listID&gt;</code>	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.
<code>mask &lt;mask&gt;</code>	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

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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
<code>&lt;ipv6addr/prefix&gt;</code>	Specifies the source IPv6 address and prefix from which access is allowed.
<code>&lt;listID&gt;</code>	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

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. Enter Global Configuration mode:

```
enable
configure terminal
```

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
<code>&lt;listID&gt;</code>	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.  If you do not specify a <code>&lt;listID&gt;</code> , the command resets the entire list to factory defaults.

## Displaying the IP Manager configuration

### Procedure

1. Enter Privileged EXEC mode:



```
enable
```

- 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).

```
Switch(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
2 255.255.255.0 255.255.255.0
3 255.255.255.0 255.255.255.0
4 255.255.255.0 255.255.255.0
5 255.255.255.0 255.255.255.0
6 255.255.255.0 255.255.255.0
7 255.255.255.0 255.255.255.0
8 255.255.255.0 255.255.255.0
9 255.255.255.0 255.255.255.0
10 255.255.255.0 255.255.255.0
11 255.255.255.0 255.255.255.0
12 255.255.255.0 255.255.255.0
13 255.255.255.0 255.255.255.0
14 255.255.255.0 255.255.255.0
----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 CLI

---

## Configuring DHCP snooping globally

Configure 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. Enter Global Configuration mode:  

```
enable  
configure terminal
```
2. At the command prompt, enter the following command:  

```
[no] [default] ip dhcp-snooping enable
```

---

## Configuring DHCP snooping on a VLAN

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. Enter Global Configuration mode:  

```
enable  
configure terminal
```
2. At the command prompt, enter the following command:  

```
[no] ip dhcp-snooping vlan <vlanID>
```

---

## Configuring DHCP snooping port trust

Configure port-based DHCP snooping to specify whether a port or group of ports are trusted (DHCP replies are forwarded automatically) or untrusted (DHCP replies are filtered through DHCP snooping), and to assign an Option 82 subscriber ID to the port or ports.

### Procedure

1. Enter Interface Configuration mode:  

```
enable  
configure terminal  
interface Ethernet <port> or interface vlan <1-4094>
```
2. At the command prompt, enter the following command:

```
[default] [no] ip dhcp-snooping [port <portlist>] <trusted|
untrusted> option82-subscriber-id <WORD>
```

- Return DHCP snooping for all interface ports to default values.

```
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-subscriber-id <WORD>	Specifies the DHCP Option 82 subscriber Id for the port. Value is a character string between 0 and 64 characters.
<portlist>	Specifies a port or group of ports.
<trusted>	When selected, the port or ports automatically forward DHCP replies.
<untrusted>	When selected, the port or ports filter DHCP replies through DHCP snooping.

---

## Displaying global DHCP snooping configuration information

### Procedure

- Enter Global Configuration mode:

```
enable
configure terminal
```

- At the command prompt, enter the following command:

```
show ip dhcp-snooping
```

---

## Displaying VLAN DHCP snooping configuration information

### Procedure

- Enter Global Configuration mode:

```
enable
configure terminal
```

- At the command prompt, enter the following command:

```
show ip dhcp-snooping vlan
```

---

## Displaying DHCP snooping port trust information

### Procedure

1. Enter Interface Configuration mode:

```
enable  
configure terminal  
interface fastEthernet <port>
```

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
<port>	Specifies a port or list of ports.

---

## Displaying the DHCP binding table

### Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

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

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

---

## Configuring DHCP Snooping Option 82 globally

Before DHCP Snooping can function on a VLAN or port, you must enable DHCP Snooping globally. If DHCP Snooping is disabled globally, the switch forwards DHCP reply packets to all applicable ports, regardless of whether the port is trusted or untrusted.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

- 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 VLAN-based DHCP Snooping Option 82

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

- Enter Global Configuration mode:

```
enable
configure terminal
```

- 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. 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. RANGE: 1 to 4094

## Displaying DHCP Snooping

### Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
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.

```
Switch(config)#show ip dhcp-snooping
Global DHCP snooping state: Enabled
DHCP Snooping option82 is Disabled
      DHCP      DHCP Snooping
VLAN Snooping  option82
-----
1      Disabled  Disabled
```

## Displaying DHCP Snooping for an interface

### Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
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.

```
Switch#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 CLI

---

### Displaying the ARP table

**Procedure**

1. Log on to CLI to enter User EXEC 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.

```
Switch#show arp-table
Port IP Address      MAC Address
-----
2    192.0.1.2        00:0E:62:77:64:60
```

## Configuring dynamic ARP inspection on a VLAN

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.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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 `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

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. Enter Interface Configuration mode:

```
enable
configure terminal
interface fastEthernet <port>
```

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.

## Configuring dynamic ARP inspection port trust to default

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. Enter Interface Configuration mode:

```
enable
configure terminal
interface fastEthernet <port>
```

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.

## Displaying VLAN dynamic ARP inspection configuration information

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
show ip arp-inspection vlan
```

## Displaying dynamic ARP inspection port trust information

### Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port> or interface vlan <1-4094>
```

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.
<port>	Specifies a port or list of ports.

## Configuring IP Source Guard

### 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. Extreme Networks recommends that you do not enable IP Source Guard on trunk ports.

## Configuring IP Source Guard

### Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface fastEthernet <port>
```

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 **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

## Displaying IP Source Guard port configuration information

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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.

---

## Displaying IP Guard-allowed addresses

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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.

---

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

---

### Configuring use of the most recent RADIUS VLAN

#### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
[no] [default] 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 CLI 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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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.

```
Switch#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
```

---

## Configuring EAPOL Fail Open VLAN

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
[no] 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. RANGE: 1 to 4094

---

## Displaying EAPOL Fail Open VLAN

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show eapol multihost fail-open-vlan`

---

## Configuring storm control

Use the following procedures to configure storm control using CLI

### Configuring storm control globally

1. Enter the Global Configuration mode in CLI.
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 CLI.
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 Global Configuration mode in CLI.
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

```
switch(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
```

## Configuring storm control

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
[no] 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

The following table defines the parameters for the `storm-control` command.

Variable	Description
action	Specifies the storm control action: <ul style="list-style-type: none"> <li>• <b>drop</b>: Set storm control action to drop</li> <li>• <b>none</b>:</li> <li>• <b>shutdown</b>: Set storm control action to shutdown</li> </ul>

*Table continues...*

Variable	Description
high-watermark <10-100000000>	Specifies the high-watermark value in packets per second (pps). Range: 10 to 100000000 Default: 1000
low-watermark <10-100000000>	Specifies the low-watermark value in packets per second (pps). Range: 10 to 100000000 Default: 100
poll-interval <5-300>	Specifies the interval for watermark checking; the value varies in seconds. Range: 5 to 300 Default: 5
trap-interval <0-1000>	Specifies the interval for sending traps when the poll-intervals exceed. Range: 0 to 1000 <b>* Note:</b> Value 0 means disabled (high watermark traps does not repeat). Default: 0

## Displaying global storm control state

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
show storm-control [broadcast | multicast | unicast | all]
```

### Example

The following is a sample output of the `show storm-control all` command.

```
Switch(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

### Procedure

1. Enter Privileged EXEC mode:  
enable
2. At the command prompt, enter the following command:  
show rate-limit

### Example

The following figure displays sample output from the `show rate-limit` command.

```
Switch#show rate-limit
Packet Type      Limit
-----
Both             0 pps
```

## Configuring rate limiting

Configure rate limiting in packets per second for the specified traffic type: either multicast, broadcast, or both.

### Procedure

1. Enter Global Configuration mode:  
enable  
configure terminal
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: <ul style="list-style-type: none"> <li>• multicast — applies rate limiting to multicast packets</li> <li>• broadcast — applies rate limiting to broadcast packets</li> </ul>

*Table continues...*

Variable	Value
	<ul style="list-style-type: none"> <li>• both — applies rate limiting to both multicast and broadcast packets</li> </ul>
<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 6: Security configuration and management using Enterprise Device Manager

This chapter describes the methods and procedures necessary to configure security on the switch 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.   <b>Note:</b> If you configure the Web server to respond to HTTPS client browser requests only, all existing non-secure connections with the browser are terminated.

# Chapter 7: 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
DefaultEapAll	Resets all EAP settings.

*Table continues...*

Name	Description
<b>SystemAuthControl</b>	Enables or disables EAPOL for your switch. When this field is set to disabled (the default state), the Controlled Port Status for all of the switch ports is set to Authorized (no security restriction).
<b>GuestVlanEnabled</b>	Enables or disables access to the global default Guest VLAN for the switch.
<b>GuestVlanId</b>	This object specifies the ID of the global default Guest VLAN. This VLAN is used for ports that do not have a configured Guest VLAN. Access to the global default Guest VLAN is allowed for MAC addresses before EAP authentication is performed.  The GuestVlanEnabled field must be selected to provide ports with access to the global default Guest VLAN.
<b>MultiHostAllowNonEapClient (MAC addresses)</b>	This object controls whether locally authenticated non-EAP clients (MAC addresses) are allowed on the port.
<b>MultiHostSingleAuthEnabled</b>	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.
<b>MultiHostRadiusAuthNonEapClient</b>	This object controls whether non-EAP clients (MAC addresses) can be authenticated using RADIUS on the port.
<b>MultiHostAllowNonEapPhones</b>	Enables or disables IP Phone clients as another non-EAP type.
<b>MultiHostAllowRadiusAssignedVlan</b>	Enables or disables the use of RADIUS-assigned VLAN values in the Multihost mode.
<b>MultiHostAllowNonEapRadiusAssignedVlan</b>	Enables or disables the use of RADIUS-assigned VLANs in multihost-eap mode for non-EAP clients
<b>MultiHostUseMostRecentRadiusAssignedVlan</b>	Enables or disables the use of the most recent RADIUS VLAN.   <b>Note:</b> You must also enable MultiHostUseMostRecentRadiusAssignedVlan on each port to enable the feature.
<b>MultiHostMultiVlan</b>	Enables or disables the multiple VLAN capability for EAP and non-EAP hosts.  DEFAULT: disabled
<b>MultiHostEapPacketMode</b>	Specifies the packet mode, either unicast or multicast, in the Multihost mode.

*Table continues...*

Name	Description
<b>MultiHostEapProtocolEnabled</b>	Enables or disables the processing of EAP protocol packets.
<b>MultiHostFailOpenVlanEnabled</b>	Enables or disables the EAPOL multihost Fail Open VLAN. Default is disabled.
<b>MultiHostFailOpenVlanId</b>	Configure the VLAN ID of the Fail Open VLAN or accept the default of VLAN ID 1.   <b>Note:</b> 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.
<b>MultiHostFailOpenVlanContinuityModeEnabled</b>	Enables or disables the EAPOL multihost Fail Open VLAN Continuity mode.
<b>NonEAPRadiusPasswordAttributeFormat</b>	Specifies the format of the RADIUS Server password attribute for non-EAP clients; either IP address, MAC address, or port number.
<b>MultiHostNeapReauthenticationEnabled</b>	Enables or disables the non-EAP client re-authentication. Default is disabled.
<b>MultiHostAdacNonEapEnabled</b>	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.

- On the toolbar, click **Apply**.

## Configuring port based EAPOL

The following table describes the fields on the EAPOL Ports tab.

Name	Description
<b>PortNumber</b>	Indicates the port number.
<b>PortInitialize</b>	Enables and disables EAPOL authentication for the specified port.
<b>PortReauthenticateNow</b>	Enables (true) EAPOL authentication for the specified port immediately, without waiting for the Re-Authentication Period to expire.
<b>PaeState</b>	Indicates the EAPOL authorization status for the switch:
<b>BackendAuthState</b>	Indicates the current state of the Backend Authentication state for the switch.
<b>AdminControlledDirections</b>	Indicates the current EAPOL authentication for the port: <ul style="list-style-type: none"> <li><b>both</b>: Incoming and outgoing traffic</li> <li><b>in</b>: Incoming traffic only</li> </ul> <p>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.</p>
<b>OperControlledDirections</b>	Indicates the current operational value for the traffic control direction for the port (see the preceding field description).
<b>AuthControlledPortStatus</b>	Indicates the current EAPOL authorization status for the port: <ul style="list-style-type: none"> <li><b>authorized</b></li> <li><b>unauthorized</b></li> </ul>
<b>AuthControlledPortControl</b>	Indicates the EAPOL authorization status for the port: <ul style="list-style-type: none"> <li><b>Force Authorized</b>: The authorization status is always authorized</li> <li><b>Force Unauthorized</b>: The authorization status is always unauthorized</li> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• <b>Auto</b>: The authorization status depends on the EAP authentication</li> </ul>
<b>QuietPeriod</b>	Indicates the current value of the time interval between any single EAPOL authentication failure and the start of a new EAPOL authentication attempt.
<b>SupplicantTimeout</b>	Indicates the time to wait for response from supplicant for all EAP packets, except EAP Request/Identity.
<b>ServerTimeout</b>	Indicates the time to wait for a response from the RADIUS server for all EAP packets.
<b>MaximumRequests</b>	Indicates the number of times the switch attempts to resend EAP packets to a supplicant.
<b>ReAuthenticationPeriod</b>	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.
<b>ReAuthenticationEnabled</b>	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).
<b>KeyTxEnabled</b>	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.
<b>LastEapolFrameVersion</b>	Indicates the protocol version number carried in the most recently received EAPOL frame.
<b>LastEapolFrameSource</b>	Indicates the source MAC address carried in the most recently received EAPOL frame.

---

## 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
<b>PortNumber</b>	Indicates the port number.
<b>PortInitialize</b>	Enables and disables EAPOL authentication for the specified port.
<b>PortReauthenticateNow</b>	Enables (true) EAPOL authentication for the specified port immediately, without waiting for the Re-Authentication Period to expire.
<b>PaeState</b>	Indicates the EAPOL authorization status for the switch:
<b>BackendAuthState</b>	Indicates the current state of the Backend Authentication state for the switch.
<b>AdminControlledDirections</b>	Indicates the current EAPOL authentication for the port: <ul style="list-style-type: none"> <li>• <b>both</b>: Incoming and outgoing traffic</li> <li>• <b>in</b>: Incoming traffic only</li> </ul> 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.
<b>OperControlledDirections</b>	Indicates the current operational value for the traffic control direction for the port (see the preceding field description).
<b>AuthControlledPortStatus</b>	Indicates the current EAPOL authorization status for the port: <ul style="list-style-type: none"> <li>• <b>authorized</b></li> <li>• <b>unauthorized</b></li> </ul>

*Table continues...*

Name	Description
<b>AuthControlledPortControl</b>	<p>Indicates the EAPOL authorization status for the port:</p> <ul style="list-style-type: none"> <li>• <b>Force Authorized:</b> The authorization status is always authorized</li> <li>• <b>Force Unauthorized:</b> The authorization status is always unauthorized</li> <li>• <b>Auto:</b> The authorization status depends on the EAP authentication</li> </ul>
<b>QuietPeriod</b>	<p>Indicates the current value of the time interval between any single EAPOL authentication failure and the start of a new EAPOL authentication attempt.</p>
<b>SupplicantTimeout</b>	<p>Indicates the time to wait for response from supplicant for all EAP packets, except EAP Request/Identity.</p>
<b>ServerTimeout</b>	<p>Indicates the time to wait for a response from the RADIUS server for all EAP packets.</p>
<b>MaximumRequests</b>	<p>Indicates the number of times the switch attempts to resend EAP packets to a supplicant.</p>
<b>ReAuthenticationPeriod</b>	<p>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.</p>
<b>ReAuthenticationEnabled</b>	<p>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).</p>
<b>KeyTxEnabled</b>	<p>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.</p>
<b>LastEapolFrameVersion</b>	<p>Indicates the protocol version number carried in the most recently received EAPOL frame.</p>
<b>LastEapolFrameSource</b>	<p>Indicates the source MAC address carried in the most recently received EAPOL frame.</p>

## 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
<b>PortNumber</b>	Specifies the port number.
<b>DefaultEapAll</b>	Enables or disables the default EAP settings.
<b>GuestVlanEnabled</b>	Enables and disables Guest VLAN on the port.
<b>GuestVlanId</b>	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.
<b>MultiHostMaxMacs</b>	Specifies the maximum number of clients allowed on this port. The maximum number ranges between 1 and 64.
<b>MultiHostEnabled</b>	Enables or disables EAPOL multihost on the port.
<b>MultiHostEapMaxNumMacs</b>	Specifies the maximum number of allowed EAP clients on the port.
<b>MultiHostAllowNonEapClient (MAC addresses)</b>	Enables or disables support for non EAPOL clients using local authentication.
<b>MultiHostNonEapMaxNumMacs</b>	Specifies the maximum number of non EAPOL clients allowed on this port. The default is 1. The maximum number is 32.

*Table continues...*

Name	Description
<b>MultiHostSingleAuthEnabled</b>	Enables or disables Multiple Host with Single Authentication (MHSA) support for non EAPOL clients.
<b>MultiHostSingleAuthNoLimit</b>	Specifies whether there is a limit on the number of auto-authenticated non-EAPOL clients. A value of true indicates no limit, false indicates there is a limit.  DEFAULT: false
<b>MultiHostRadiusAuthNonEapClient</b>	Enables or disables support for non EAPOL clients using RADIUS authentication.
<b>MultiHostAllowNonEapPhones</b>	Enables or disables support for IP Phone clients as another non-EAP type.
<b>MultiHostAllowRadiusAssignedVlan</b>	Enables or disables support for VLAN values assigned by the RADIUS server.
<b>MultiHostAllowNonEapRadiusAssignedVlan</b>	Enables or disables support for RADIUS-assigned VLANs in multihost-EAP mode for non-EAP clients.
<b>MultiHostEapPacketMode</b>	Specifies the mode of EAPOL packet transmission (multicast or unicast).
<b>EapProtocolEnabled</b>	Enables or disables EAP protocol.
<b>MultiHostBlockDifferentVlanAuth</b>	Enables or disables the block subsequent MAC authentication feature.
<b>ProcessRadiusRequestsServerPackets (RADIUS Dynamic Authorization Server)</b>	Enables or disables the processing of RADIUS requests-server packets that are received on this port.
<b>MultiHostClearNeap</b>	Clears a specific, or all authenticated, NEAP clients from the port. To clear a specific client on a port, enter the MAC address of the client. To clear all clients on a port, enter 00:00:00:00:00:00.
<b>MultiHostAdacNonEapEnabled</b>	Enables or disables the non-EAP multihost ADAC settings.

## 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 from 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
<b>MultiHostVoipVlanIndex</b>	Indicates the multihost VoIP VLAN index, range of 1 to 5.
<b>MultiHostVoipVlanEnabled</b>	Enables (true) or disables (false) the multihost VoIP VLAN.
<b>MultiHostVoipVlanId</b>	Indicates the VLAN ID, range of 1 to 4094.

---

## 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
<b>PortNumber</b>	The port number in use.
<b>ClientMACAddr</b>	The MAC address of the client.
<b>PaeState</b>	The current state of the authenticator PAE state machine.
<b>BackendAuthState</b>	The current state of the Backend Authentication state machine.
<b>Reauthenticate</b>	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.
UserName	The user name representing the identity of the supplicant PAE.

---

## Viewing Multihost DHCP authenticated information

Use this procedure to display multiple 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.

---

## 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 Reachability section, click a **RadiusReachability** radio button.
8. In the RADIUS Reachability section, type the reachability user name in the **UserName** dialog box.
9. In the RADIUS Reachability section, type the reachability password in the **Password** dialog box.
10. In the RADIUS Reachability section, type the reachability password again to confirm in the **Confirm Password** dialog box.
11. In the RADIUS Reachability section, specify the time-out period in the **Timeout** dialog box.
12. In the RADIUS Reachability section, specify the number of retry attempts in the **Retry** dialog box.
13. In the RADIUS Reachability section, specify the interval between checks when the RADIUS server is unreachable in the **BadTimer** dialog box.
14. In the RADIUS Reachability section, specify the interval between checks when the RADIUS server is reachable in the **GoodTimer** dialog box.
15. In the RADIUS Accounting section, select the **InterimUpdates** checkbox to enable or disable RADIUS accounting interim updates for the switch.
16. In the RADIUS Accounting section, specify the time interval before RADIUS accounting interim updates times out in the **InterimUpdatesInterval** dialog box.



17. In the RADIUS Accounting section, click an **InterimUpdatesIntervalSource** radio button.
18. On the toolbar, click **Apply**.

## Globals tab field descriptions

The following table describes the fields on the Globals tab.

Name	Description
<b>UseMgmtIp</b>	When selected, RADIUS uses the system management IP address as the source address for RADIUS requests.
<b>PasswordFallbackEnabled</b>	When selected, enables RADIUS password fallback.
<b>DynAuthReplayProtection</b>	When selected, enables RADIUS replay protection.
<b>Reachability</b>	Specifies the RADIUS server reachability mode. Values include: <ul style="list-style-type: none"> <li>• <b>useRadius</b>: Uses dummy RADIUS requests to determine reachability of the RADIUS server.</li> <li>• <b>useIcmp</b>: Uses ICMP packets to determine reachability of the RADIUS server (default).</li> </ul>
UserName	Specifies the reachability username.
Password	Specifies the reachability password.
Confirm Password	Verifies the reachability password.
Timeout	Specifies the time-out period. Values range from 1-60 seconds.
Retry	Specifies the number of retry attempts. Values range from 1-5 retries.
BadTimer	Specifies the interval between checks when the RADIUS server is unreachable. Values range from 30-600 seconds.
GoodTimer	Specifies the interval between checks when the RADIUS server is reachable. Values range from 30-600 seconds.
InterimUpdates	Enables or disables RADIUS accounting interim updates for the switch.
InterimUpdatesInterval	Specifies the time interval (in seconds) before RADIUS accounting interim updates times out. Values range from 60–3600 seconds. The default is 600 seconds.

*Table continues...*

Name	Description
InterimUpdatesIntervalSource	<p>Specifies the source of the interim updates timeout interval.</p> <ul style="list-style-type: none"> <li>• configuredValue—uses the value in the RadiusAccountingInterimUpdatesInterval dialog box</li> <li>• radiusServer—uses the value applied by the RADIUS server</li> </ul>

## Track all MACs per port

This feature tracks the following information for all MACs per port:

- EAP or non EAP authenticated or non-authenticated clients
- status of the RADIUS server authentication response if the MAC is rejected or is not authenticated

Up to 64 intruders per port can be tracked. If this limit is reached the port is automatically set to Forced Unauthorized.

## Displaying all MACs

Use this procedure to track information for all MACs per port.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display information on MACs for EAP sessions:

```
show eapol sessions {[port <portmask>] | [dhcp-phones] | [[eap] |
[non-eap [radius] [local] [adac-lldp] [adac-mac-range] [held]
[mhsa]] | [[unauthenticated [intruder] [guest-vlan] [fail-open-vlan]
[mhsa-no-limit]]]}
```

3. Display the summary of authenticated clients:

```
show eapol summary [interface <portlist>][verbose]
```

### Example

The following example displays sample output for the `show eapol sessions` and `show eapol summary` commands.

```
Switch(config)#show eapol sessions
```

```
----- DHCP Phone Clients -----
```

```

Unit/Port Client MAC Address
-----
1/15      3C:B1:5B:4C:63:BA

----- EAP Clients -----
Unit/Port Client MAC Address Pae State      Backend Auth State Vid  Pri
-----
1/15      70:05:7E:D3:00:00  Authenticated Idle           201 2
1/15      70:05:7E:D3:00:01  Authenticated Idle           202 2

----- Non-EAP Clients -----
Unit/Port Client MAC Address State                               Vid  Pri
-----
1/15      00:AB:C1:0E:00:00  Authenticated By RADIUS           501 5
1/15      00:AB:C1:0E:00:01  Authenticated By RADIUS           502 4
2/87      64:A7:DD:01:23:E4  Authenticated By RADIUS           202 0

----- Unauthorized Clients -----
Unit/Port Client MAC Address Type           Radius Status
-----
1/15      1E:7C:B2:0F:00:00  Intruder           Reject
1/15      1E:7C:B2:0F:00:01  Intruder           Reject
1/15      1E:7C:B2:0F:00:02  Intruder           Reject
1/15      1E:7C:B2:0F:00:03  Intruder           Reject
1/15      1E:7C:B2:0F:00:04  Intruder           Reject
Total number of DHCP authenticated phones: 1
Total number of EAP authenticated clients: 2
Total number of non-EAP authenticated clients: 3
Total number of unauthenticated clients: 5

```

```
Switch(config)#show eapol summary
```

```

                                Unit 1 Unit 2 Unit 3 Total
                                -----
EAP Clients                    :    2    0    0    2
NEAP Clients (total)           :    2    1    0    3
DHCP Clients                    :    1    0    0    1
Unauthenticated (total)       :    5    0    0    5

```

```
Switch(config)#show eapol summary verbose
```

```

                                Unit 1 Unit 2 Unit 3 Total
                                -----
EAP Clients                    :    2    0    0    2
NEAP Clients (total)           :    2    1    0    3
  Radius Clients                :    2    1    0    3
  User config Clients           :    0    0    0    0
  Adac Clients                  :    0    0    0    0
  Adac LLdp Clients             :    0    0    0    0
  Mhsa Clients                  :    0    0    0    0
  Held Clients                  :    0    0    0    0
DHCP Clients                    :    1    0    0    1
Unauthenticated (total)       :    5    0    0    5
  Intruders                    :    5    0    0    5
  Guests                        :    0    0    0    0
  Fail Open                    :    0    0    0    0
  Mhsa no limit                 :    0    0    0    0

```

## Variable definitions

Use the data in the following table to use the `show eapol sessions` and `show eapol summary` commands.

Variable	Value
port <portmask>	Specifies the numeric slot/port format. Range: 1/1 to 8/50 or ALL  If no port is specified, the default is ALL. If no parameter is specified, the default is show everything. If "non-eap" is without other parameters, all types of non-eap authenticated macs are shown, except when MHSA under no-limit flag is enabled. When "unauthenticated" is not followed by parameters, all unauthenticated macs are shown.
dhcp-phones	Displays MACs of DHCP Phones.
eap	Displays authenticated EAPOL sessions.
non-eap	Displays authenticated non-EAPOL clients.
radius	Displays non-EAPOL clients authenticated by RADIUS.
local	Displays locally authenticated non-EAPOL clients.
adac-ldp	Displays non-EAPOL clients authenticated through ADAC.
adac-mac-range	Displays neap sessions with macs in the adac mac range list.
held	Displays unauthenticated clients held by RADIUS.
mhsa	Displays non-EAP sessions for MHSA.
unauthenticated	Displays unauthenticated EAPOL and non-EAPOL clients.
intruder	Displays intruder MACs.
guest-vlan	Displays unauthenticated clients in Guest VLAN.
fail-open-vlan	Displays MACs of clients in Fail Open VLAN.
mhsa-no-limit	Displays non-EAP sessions for MHSA when no-limit is enabled.
interface <portlist>	Specifies the interfaces for which to display information. Select a port or a list of ports for which to display information.
verbose	Displays detailed output.

---

## 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
<b>PortNumber</b>	The port number in use.
<b>ClientMACAddr</b>	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: <ul style="list-style-type: none"> <li>• <b>rejected</b>: the MAC address cannot be authenticated on this port.</li> <li>• <b>locallyAuthenticated</b>: the MAC address was authenticated using the local table of allowed clients.</li> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• <b>radiusPending</b>: the MAC address is awaiting authentication by a RADIUS server.</li> <li>• <b>radiusAuthenticated</b>: the MAC address was authenticated by a RADIUS server.</li> <li>• <b>adacAuthenticated</b>: the MAC address was authenticated using ADAC configuration tables.</li> <li>• <b>mhsaAuthenticated</b>: the MAC address was auto-authenticated on a port following a successful authentication of an EAP client.</li> </ul>
<b>Reauthenticate</b>	The value used to reauthenticate the MAC address of the client on the port.
<b>Vid</b>	Indicates the VLAN assigned to the client.
<b>Pri</b>	Indicates the priority of the client.

---

## 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
<b>EapolFramesRx</b>	The number of valid EAPOL frames of any type that are received by this authenticator.
<b>EapolFramesTx</b>	The number of EAPOL frame types of any type that are transmitted by this authenticator.
<b>EapolStartFramesRx</b>	The number of EAPOL start frames that are received by this authenticator.

*Table continues...*

Name	Description
<b>EapolLogoffFramesRx</b>	The number of EAPOL Logoff frames that are received by this authenticator.
<b>EapolRespIdFramesRx</b>	The number of EAPOL Resp/Id frames that are received by this authenticator.
<b>EapolRespFramesRx</b>	The number of valid EAP Response frames (Other than Resp/Id frames) that are received by this authenticator.
<b>EapolReqIdFramesTx</b>	The number of EAPOL Req/Id frames that are transmitted by this authenticator.
<b>EapolReqFramesTx</b>	The number of EAP Req/Id frames (Other than Req/Id frames) that are transmitted by this authenticator.
<b>InvalidEapolFramesRx</b>	The number of EAPOL frames that are received by this authenticator in which the frame type is not recognized.
<b>EapLengthErrorFramesRx</b>	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
<b>EntersConnecting</b>	Counts the number of times that the state machine transitions to the connecting state from any other state.
<b>EapLogoffsWhileConnecting</b>	Counts the number of times that the state machine transitions from connecting to disconnecting because of receiving an EAPOL-Logoff message.
<b>EntersAuthenticating</b>	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.
<b>AuthSuccessWhileAuthenticating</b>	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.
<b>AuthTimeoutsWhileAuthenticating</b>	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.
<b>AuthFailWhileAuthenticating</b>	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.
<b>AuthReauthsWhileAuthenticating</b>	Counts the number of times that the state machine transitions from authenticating to aborting, because of a reauthentication request.
<b>AuthEapStartsWhileAuthenticating</b>	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.
<b>AuthEapLogoffWhileAuthenticating</b>	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.
<b>AuthReauthsWhileAuthenticated</b>	Counts the number of times that the state machine transitions from authenticated to connecting, because of a reauthentication request.
<b>AuthEapStartsWhileAuthenticated</b>	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.
<b>AuthEapLogoffWhileAuthenticated</b>	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.
<b>BackendResponses</b>	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.
<b>BackendAccessChallenges</b>	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.
<b>BackendOtherRequestsTo Supplicant</b>	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.
<b>BackendNonNakResponsesFromSupplicant</b>	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.
<b>BackendAuthSuccesses</b>	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.
<b>BackendAuthFails</b>	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.

# Chapter 8: Configuring and managing security using EDM

---

## 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
<b>Accounting</b>	Enables or disables accounting: <ul style="list-style-type: none"><li>• Select the checkbox to enable accounting</li><li>• Deselect the checkbox to disable accounting</li></ul>

---

## 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
<b>AuthorizationEnabled</b>	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
<b>AuthorizationLevels &lt;0-15&gt;</b>	This object controls which CLI 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
<b>AddressType</b>	Specifies the type of IP address used on the TACACS+ server.
<b>Address</b>	The IP address of the TACACS+ server referred to in this table entry.
<b>PortNumber</b>	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.
<b>Key</b>	Secret key to be shared with this TACACS+ server.
<b>Priority</b>	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
<b>AuthSecurityLock</b>	<p>If this parameter is listed as <i>locked</i>, the agent refuses all requests to modify the security configuration. Entries also include:</p> <ul style="list-style-type: none"> <li>• <b>other</b></li> <li>• <b>notlocked</b></li> </ul>
<b>AuthCtlPartTime</b>	<p>This value indicates the duration of the time for port partitioning in seconds. The default is zero. When the value is zero, the port remains partitioned until it is manually enabled.</p>
<b>SecurityStatus</b>	<p>Indicates whether or not the switch security feature is enabled.</p>
<b>SecurityMode</b>	<p>Mode of switch security. Entries include:</p> <ul style="list-style-type: none"> <li>• <b>macList</b>: Indicates that the switch is in the MAC-list mode. You can configure more than one MAC address for each port.</li> <li>• <b>autoLearn</b>: Indicates that the switch learns the first MAC address on each port as an allowed address of that port.</li> </ul>
<b>SecurityAction</b>	<p>Actions performed by the software when a violation occurs (when SecurityStatus is enabled). The security action specified here applies to all ports of the switch.</p> <p>A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include:</p> <ul style="list-style-type: none"> <li>• <b>noAction</b>: Port does not have any security assigned to it, or the security feature is turned off.</li> <li>• <b>trap</b>: Listed trap.</li> <li>• <b>partitionPort</b>: Port is partitioned.</li> <li>• <b>partitionPortAndsendTrap</b>: Port is partitioned, and traps are sent to the trap receiver.</li> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• <b>daFiltering</b>: Port filters out the frames where the destination address field is the MAC address of the unauthorized station.</li> <li>• <b>daFilteringAndsendTrap</b>: Port filters out the frames where the destination address field is the MAC address of unauthorized station. Traps are sent to trap receivers.</li> <li>• <b>partitionPortAnddaFiltering</b>: Port is partitioned and filters out the frames with the destination address field is the MAC address of unauthorized station.</li> <li>• <b>partitionPortdaFilteringAndsendTrap</b>: Port is partitioned and filters out the frames where the destination address field is the MAC address of the unauthorized station. Traps are sent to trap receivers.</li> </ul>
<b>CurrNodesAllowed</b>	Current number of entries of the nodes allowed in the AuthConfig tab.
<b>MaxNodesAllowed</b>	Maximum number of entries of the nodes allowed in the AuthConfig tab.
<b>PortSecurityStatus</b>	Set of ports for which security is enabled.
<b>PortLearnStatus</b>	Set of ports where autolearning is enabled.
<b>CurrSecurityLists</b>	Current number of entries of the Security listed in the SecurityList tab.
<b>MaxSecurityLists</b>	Maximum entries of the Security listed in the SecurityList tab.
<b>AutoLearningAgingTime</b>	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.
<b>AutoLearningSticky (sticky-mac)</b>	<p>When selected, the learning mechanism used is the same as when auto-learning is enabled, with the exception that:</p> <ul style="list-style-type: none"> <li>• when the Sticky MAC feature is enabled, migration and auto-deletion on link-down are blocked and the addresses are not aged out</li> <li>• when Sticky mode is enabled, the aging timer is automatically set to zero</li> <li>• Sticky MAC addresses are saved into NVRAM config file and ASCII files</li> <li>• administrative removal of sticky addresses is possible</li> </ul>

**! 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 **SecurityListIdx** box, accept the default sequential security list number provided by the switch.
  - Enter a number for the security list.
6. Click the ellipsis (...) for **SecurityListMembers** and do one of the following:
  - 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
<b>SecurityListIdx</b>	An index of the security list. This corresponds to the SecurityList field into AuthConfig tab.
<b>SecurityListMembers</b>	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
<b>SecurityListIdx</b>	A numerical identifier for a security list. Values range from 1 to 32.
<b>SecurityListMembers</b>	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:**

Extreme Networks 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
<b>BrdIndx</b>	Index of the slot that contains the board on which the port is located. If you specify SecureList, this field must be zero.
<b>PortIndx</b>	Index of the port on the board. If you specify SecureList, this field must be zero.
<b>MACIndx</b>	An index of MAC addresses that are designated as allowed (station).
<b>AutoLearningSticky (sticky-mac)</b>	Enables or disables Sticky MAC. Sticky MAC can store automatically learned MAC addresses across switch reboots and secure MAC addresses to a specified port.  <div style="display: flex; align-items: center;"> <div style="margin-right: 5px;"><b>* Note:</b></div> <div>If AutoLearningSticky is enabled, you cannot modify AccessCtrlType and SecureList.</div> </div>
<b>AccessCtrlType</b>	Displays the node entry as node allowed. A MAC address can be allowed on multiple ports.
<b>SecureList</b>	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.

*Table continues...*

Name	Description
	The corresponding MAC Address of this entry is allowed or blocked on all ports of this port list.
<b>Source</b>	Indicates the source MAC address.
<b>Lifetime</b>	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
<b>Brd</b>	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.
<b>Port</b>	Identifies the switch port number.
<b>Enabled</b>	Enables or disables the automatic learning of MAC addresses on the port. Values are true (enabled) and false (disabled).
<b>MaxMacs</b>	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
<b>AuthStatusBrdIndx</b>	The index of the board. This corresponds to the index of the slot that contains the board if the index is greater than zero.

*Table continues...*

Name	Description
<b>AuthStatusPortIndx</b>	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.
<b>AuthStatusMACIndx</b>	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.
<b>CurrentAccessCtrlType</b>	Displays whether the node entry is the <code>node allowed</code> or <code>node blocked</code> type.
<b>CurrentActionMode</b>	<p>A value representing the type of information contained, including:</p> <ul style="list-style-type: none"> <li>• <b>noAction</b>: Port does not have any security assigned to it, or the security feature is turned off..</li> <li>• <b>partitionPort</b>: Port is partitioned.</li> <li>• <b>partitionPortAndsendTrap</b>: Port is partitioned and traps are sent to the trap receiver.</li> <li>• <b>Filtering</b>: Port filters out the frames where the destination address field is the MAC address of the unauthorized station.</li> <li>• <b>FilteringAndsendTrap</b>: 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.</li> <li>• <b>sendTrap</b>: A trap is sent to the trap receiver(s).</li> <li>• <b>partitionPortAnddaFiltering</b>: Port is partitioned and filters out the frames where the destination address field is the MAC address of the unauthorized station</li> <li>• <b>partitionPortdaFilteringAndsendTrap</b>: 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).</li> </ul>
<b>CurrentPortSecurStatus</b>	<p>Displays the security status of the current port, including:</p> <ul style="list-style-type: none"> <li>• If the port is disabled, <code>notApplicable</code> is returned.</li> <li>• If the port is in a normal state, <code>portSecure</code> is returned.</li> <li>• If the port is partitioned, <code>portPartition</code> is returned.</li> </ul>

## 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
<b>BrdIndx</b>	The index of the board. This corresponds to the unit containing the board. The index will be 1 where it is not applicable.
<b>PortIndx</b>	The index of the port on the board. This corresponds to the port on that a security violation was seen.
<b>MACAddress</b>	The MAC address of the device attempting unauthorized network access (MAC address-based security).

## 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
<b>Web/Telnet Switch Password Type</b>	Specifies the password type. Values include: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Local Password</b></li> <li>• <b>RADIUS Authentication</b></li> </ul> 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
<b>Console Password Type</b>	<p>Specifies the password type. Values include:</p> <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Local Password</b></li> <li>• <b>RADIUS Authentication</b></li> </ul> <p>Default is None.</p>

## 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
<b>Enable</b>	<p>Indicates the SSH status. Values include:</p> <ul style="list-style-type: none"> <li>• <b>false</b>: Disabled</li> <li>• <b>true</b>: Enabled</li> <li>• <b>secure</b>: SSH enabled, turns off all remote access, takes effect after a reboot</li> </ul> <p>Default is false.</p>
<b>Version</b>	Indicates the SSH version. The default is v2only.
<b>Port</b>	Indicates the SSH connection port. Value range of 1 to 65535, default is 22.
<b>Timeout</b>	Indicates the SSH connection timeout in seconds. Value range of 1 to 120, default is 60.

*Table continues...*



Name	Description
<b>KeyAction</b>	Indicates the SSH key action. Values include: <ul style="list-style-type: none"> <li>• <b>generateDsa</b></li> <li>• <b>generateRsa</b></li> <li>• <b>deleteDsa</b></li> <li>• <b>deleteRsa</b></li> </ul>
<b>DsaAuth</b>	Enables or disables SSH with DSA public key authentication. The default is enabled.
<b>PassAuth</b>	Enables or disables SSH with password authentication. The default is enabled.
<b>DsaHostKeyStatus</b>	Indicates the current status of the SSH DSA host key: <ul style="list-style-type: none"> <li>• <b>notGenerated</b>: DSA host key has not yet been generated.</li> <li>• <b>generated</b>: DSA host key is generated.</li> <li>• <b>generating</b>: DSA host key is currently being generated.</li> </ul>
<b>RsaAuth</b>	Enables or disables SSH with RSA public key authentication. The default is enabled.
<b>RsaHostKeyStatus</b>	Indicates the current status of the SSH DSA host key: <ul style="list-style-type: none"> <li>• <b>notGenerated</b>: RSA host key has not yet been generated.</li> <li>• <b>generated</b>: RSA host key is generated.</li> <li>• <b>generating</b>: RSA host key is currently being generated.</li> </ul>
<b>TftpServerInetAddressType</b>	Indicates the type of address stored in the TFTP server. Values include: <ul style="list-style-type: none"> <li>• <b>IPv4</b></li> <li>• <b>IPv6</b></li> </ul> The default is IPv4.
<b>TftpServerInetAddress</b>	Specifies the IP address of TFTP server for all TFTP operations.
<b>TftpFile</b>	Indicates the name of the file for the TFTP transfer.
<b>TftpAction</b>	Indicates the SSH public keys that are set to initiate a TFTP download. Values include: <ul style="list-style-type: none"> <li>• <b>none</b></li> <li>• <b>downloadSshDsaPublicKeys</b></li> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• <b>deleteSshDsaAuthKey</b></li> <li>• <b>downloadSshRsaPublicKeys</b></li> <li>• <b>deleteSshRsaAuthKey</b></li> </ul> The default is none
<b>TftpResult</b>	Indicates the retrieved value of the TFTP transfer. Values include: <ul style="list-style-type: none"> <li>• <b>none</b></li> <li>• <b>success</b></li> <li>• <b>transferError</b></li> </ul>

---

## 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
<b>SshSessionInetAddressType</b>	Indicates the type of IP address of the SSH client that opened the SSH session.
<b>SshSessionInetAddress</b>	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
<b>KeyAction</b>	Specifies the action to take for the SSH Client host key. Values include: <ul style="list-style-type: none"> <li>• <b>none</b>: take no host key action</li> <li>• <b>generateDsa</b>: generates a DSA host key for the SSH Client</li> <li>• <b>generateRsa</b>: generates an RSA host key for the SSH Client</li> <li>• <b>deleteDsa</b>: deletes the SSH Client DSA host key.</li> <li>• <b>deleteRsa</b>: deletes the SSH Client DSA host key.</li> <li>• <b>generateDsaForce</b>: generates a new, active DSA key, even in the presence of an existing DSA key.</li> <li>• <b>generateRsaForce</b>: generates a new, active RSA key, even in the presence of an existing RSA key.</li> </ul>
<b>KeyFileName</b>	Specifies the SSH Client host key file name.
<b>TftpAction</b>	Specifies the type of SSH Client authentication key to upload using TFTP. Values include: <ul style="list-style-type: none"> <li>• <b>none</b>: do not upload an SSH Client authentication key using TFTP</li> <li>• <b>uploadSshcDsaAuthKey</b>: uploads a DSA SSH Client authentication key using TFTP</li> <li>• <b>uploadSshcRsaAuthKey</b>: uploads an RSA SSH Client authentication key using TFTP</li> </ul>
<b>TftpServerIpAddressType</b>	Specifies whether the IP address is IPv4 or IPv6.
<b>TftpServerIpAddress</b>	Specifies the IP address of the TFTP server.
<b>DsaKeySize</b>	Specifies the DSA key size. Values range from 512 to 1024. Default value: 512.
<b>RsaKeySize</b>	Specifies the RSA key size. Values range from 1024 to 2048. Default value: 1024.

*Table continues...*

Name	Description
<b>DSAGhostKeyStatus</b>	Indicates the current status of the SSH Client DSA host key. Values include: <ul style="list-style-type: none"> <li>• notGenerated</li> <li>• generated</li> <li>• generating</li> </ul>
<b>RsaHostKeyStatus</b>	Indicates the current status of the SSH Client RSA host key. Values include: <ul style="list-style-type: none"> <li>• notGenerated</li> <li>• generated</li> <li>• generating</li> </ul>
<b>SFTP</b>	
<b>Port</b>	Specifies the TCP port number for the SFTP file transfer. Values range from 1 to 65535. Default value: 22.
<b>DsaAuthentication</b>	When selected, enables SFTP DSA authentication for SSH Client (default).
<b>RsaAuthentication</b>	When selected, enables SFTP password authentication for SSH Client.
<b>PasswordAuthentication</b>	When selected, enables SFTP RSA authentication for SSH Client.
<b>SftpServerInetAddressType</b>	Specifies whether the IP address is IPv4 or IPv6.
<b>SftpServerInetAddress</b>	Specifies the IP address of the SFTP server.
<b>UserName</b>	Specifies the user name.
<b>SftpServerPassword</b>	Specifies the password for the SFTP server.
<b>Confirm SftpServerPassword</b>	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.

- On the toolbar, click **Apply**.

## SSL tab field descriptions

The following table describes the fields on the SSL tab.

Name	Description
<b>Enabled</b>	Enables or disables SSL.
<b>CertificateControl</b>	Enables the creation and deletion of SSL certificates. <ul style="list-style-type: none"> <li><b>create</b>: creates an SSL certificate</li> <li><b>delete</b>: deletes an SSL certificate.</li> <li><b>other</b>: results in a wrongValue error</li> </ul>
<b>CertificateExists</b>	Indicates if a valid SSL certificate is created. <ul style="list-style-type: none"> <li><b>true</b>: a valid SSL certificate is created</li> <li><b>false</b>: a valid SSL certificate is not created or the certificate has been deleted</li> </ul>
<b>CertificateControlStatus</b>	Indicates the status of the most recent attempt to create or delete a certificate. <ul style="list-style-type: none"> <li><b>inProgress</b>: the operation is not yet completed</li> <li><b>success</b>: the operation is complete</li> <li><b>failure</b>: the operation failed</li> <li><b>other</b>: the s5AgSslCertificateControl object was never set</li> </ul>
<b>ServerControl</b>	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 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.

### Note:


If Global RADIUS server is same as the EAP and NEAP RADIUS, only Global RADIUS server must be configured.

## 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
<b>PrimaryRadiusServerAddressType</b>	Specifies the IP address type for the primary Global RADIUS server. Values include unknown, IPv4, and IPv6.
<b>PrimaryRadiusServer</b>	Specifies the IPv4 or IPv6 address of the primary Global RADIUS server (default: 0.0.0.0).   <b>Important:</b> 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.
<b>SecondaryRadiusServerAddressType</b>	Specifies the IP address type for the secondary Global RADIUS server. Values include unknown, IPv4, and IPv6.
<b>SecondaryRadiusServer</b>	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

*Table continues...*

Name	Description
	<p>primary Global RADIUS server is unavailable or unreachable.</p> <p> <b>Important:</b></p> <p>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.</p>
<b>RadiusServerUdpPort</b>	<p>Specifies the UDP port number clients use to contact the Global RADIUS Server at the Global RADIUS Server IP address.</p> <p>RANGE: 1 to 65535</p> <p>DEFAULT: 1812</p>
<b>RadiusServerTimeout</b>	<p>Specifies the timeout interval between each retry for service requests to the Global RADIUS server.</p> <p>DEFAULT: 2 seconds</p> <p>RANGE: 1 to 60 seconds</p>
<b>SharedSecret(key)</b>	<p>Specifies the value for the Global RADIUS Server shared secret key.</p> <p> <b>Important:</b></p> <p>The shared secret key has a maximum of 16 characters.</p>
<b>ConfirmedSharedSecret(key)</b>	<p>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).</p>
<b>RetryLimit</b>	<p>Specifies the number of RADIUS retry attempts for a Global RADIUS Server instance.</p> <p>RANGE: 1 to 5</p>

## 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
<b>PrimaryRadiusServerAddressType</b>	Specifies the IP address type for the primary EAP RADIUS server. Values include IPv4 and IPv6.
<b>PrimaryRadiusServer</b>	Specifies the IPv4 or IPv6 address of the primary EAP RADIUS server (default: 0.0.0.0).   <b>Important:</b> 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.
<b>SecondaryRadiusServerAddressType</b>	Specifies the IP address type for the secondary EAP RADIUS server. Values include IPv4 and IPv6.
<b>SecondaryRadiusServer</b>	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.

*Table continues...*



Name	Description
	<p> <b>Important:</b></p> <p>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.</p>
<b>RadiusServerUdpPort</b>	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.
<b>RadiusServerTimeout</b>	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.
<b>SharedSecret(key)</b>	<p>Specifies the value for the EAP RADIUS Server shared secret key.</p> <p> <b>Important:</b></p> <p>The shared secret key has a maximum of 16 characters.</p>
<b>ConfirmedSharedSecret(key)</b>	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).
<b>AccountingEnabled</b>	Enables or disables RADIUS accounting for a Global RADIUS Server instance.
<b>AccountingPort</b>	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.
<b>RetryLimit</b>	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
<b>PrimaryRadiusServerAddressType</b>	Specifies the IP address type for the primary NEAP RADIUS server. Values include IPv4 and IPv6.
<b>PrimaryRadiusServer</b>	<p>Specifies the IPv4 or IPv6 address of the primary NEAP RADIUS server (default: 0.0.0.0).</p> <p> <b>Important:</b></p> <p>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.</p>
<b>SecondaryRadiusServerAddressType</b>	Specifies the IP address type for the secondary NEAP RADIUS server. Values include IPv4 and IPv6.
<b>SecondaryRadiusServer</b>	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.

*Table continues...*

Name	Description
	<p> <b>Important:</b></p> <p>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.</p>
<b>RadiusServerUdpPort</b>	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.
<b>RadiusServerTimeout</b>	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.
<b>SharedSecret(key)</b>	<p>Specifies the value for the NEAP RADIUS Server shared secret key.</p> <p> <b>Important:</b></p> <p>The shared secret key has a maximum of 16 characters.</p>
<b>ConfirmedSharedSecret(key)</b>	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).
<b>AccountingEnabled</b>	Enables or disables RADIUS accounting for a Global RADIUS Server instance.
<b>AccountingPort</b>	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.
<b>RetryLimit</b>	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
<b>Identifier</b>	Indicates the Network Access Server (NAS) identifier of the RADIUS Dynamic Authorization Server.
<b>DisconInvalidClientAddresses</b>	Indicates the number of Disconnect-Request packets received from unknown addresses.
<b>CoAInvalidClientAddresses</b>	Indicates the number of CoA-Request packets received from unknown addresses.

---

## Configuring RADIUS parameters

Use the following procedures to configure the RADIUS parameters on the Globals tab.

### Related links

[Configuring RADIUS globally using EDM](#) on page 244

---

## 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**.

## Global RADIUS Server tab field descriptions

The following table describes the fields on the Global RADIUS Server tab.

Name	Description
<b>PrimaryRadiusServerAddressType</b>	Specifies the IP address type for the primary Global RADIUS server. Values include unknown, IPv4, and IPv6.
<b>PrimaryRadiusServer</b>	Specifies the IPv4 or IPv6 address of the primary Global RADIUS server (default: 0.0.0.0).   <b>Important:</b> 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.
<b>SecondaryRadiusServerAddressType</b>	Specifies the IP address type for the secondary Global RADIUS server. Values include unknown, IPv4, and IPv6.
<b>SecondaryRadiusServer</b>	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.   <b>Important:</b> 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.
<b>RadiusServerUdpPort</b>	Specifies the UDP port number clients use to contact the Global RADIUS Server at the Global RADIUS Server IP address.  RANGE: 1 to 65535

*Table continues...*

Name	Description
	DEFAULT: 1812
<b>RadiusServerTimeout</b>	Specifies the timeout interval between each retry for service requests to the Global RADIUS server.  DEFAULT: 2 seconds  RANGE: 1 to 60 seconds
<b>SharedSecret(key)</b>	Specifies the value for the Global RADIUS Server shared secret key.   <b>Important:</b> The shared secret key has a maximum of 16 characters.
<b>ConfirmedSharedSecret(key)</b>	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).
<b>RetryLimit</b>	Specifies the number of RADIUS retry attempts for a Global RADIUS Server instance.  RANGE: 1 to 5

---

## 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
<b>AddressType</b>	Defines the IP address type of the RADIUS Dynamic Authorization Client.
<b>Address</b>	Defines the IP address of the RADIUS Dynamic Authorization Client.
<b>Enabled</b>	Enables or disables packet receiving from the RADIUS Dynamic Authorization Client.
<b>UdpPort</b>	Configures the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1025 to 65535.
<b>ProcessCoARequests</b>	Enables change-of-authorization (CoA) request processing.
<b>ProcessDisconnectRequests</b>	Enables disconnect request processing.
<b>Secret</b>	Configures the RADIUS Dynamic Authorization Client secret word.
<b>ConfirmedSecret</b>	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
<b>AddressType</b>	Indicates the IP address type for the RADIUS Dynamic Authorization Client. This is a read-only cell.
<b>Address</b>	Indicates the IP address of the RADIUS Dynamic Authorization Client. This is a read-only cell.
<b>Enabled</b>	Enables or disables packet receiving from the RADIUS Dynamic Authorization Client. <ul style="list-style-type: none"> <li>• <b>enable</b>: True</li> <li>• <b>disable</b>: False</li> </ul>
<b>UdpPort</b>	Defines the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1024 to 65535.
<b>ProcessCoARequests</b>	Enables or disables change of authorization (CoA) request processing.
<b>ProcessDisconnectRequests</b>	Enables or disables disconnect request processing.
<b>Secret</b>	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
<b>AddressType</b>	Indicates the IP address type for the RADIUS Dynamic Authorization Client.

*Table continues...*

Name	Description
<b>Address</b>	Indicates the IP address of the RADIUS Dynamic Authorization Client.
<b>Enabled</b>	Indicates whether packet receiving from the RADIUS Dynamic Authorization Client is enabled (true) or disabled (false).
<b>UdpPort</b>	Indicates the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1024–65535.
<b>ProcessCoARequests</b>	Indicates whether change of authorization (CoA) request processing is enabled or disabled.
<b>ProcessDisconnectRequests</b>	Indicates whether disconnect request processing is enabled or disabled.
<b>Secret</b>	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
<b>ClientIndex</b>	Indicates the RADIUS Dynamic Server client index.
<b>ClientAddressType</b>	Indicates the type of RADIUS Dynamic Server address. Values are ipv4 or ipv6.
<b>ClientAddress</b>	Indicates the IP address of the RADIUS Dynamic Server.
<b>ServerCounterDiscontinuity</b>	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
<b>VlanId</b>	Identifies the VLANs configured on the switch.
<b>DhcpSnoopingEnabled</b>	Enables or disables DHCP snooping on a VLAN.
<b>VlanOption82Enabled</b>	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
<b>Port</b>	Identifies the ports on the switch.
<b>DhcpSnoopingIfTrusted</b>	Specifies if the port is trusted or untrusted. Default is false.
<b>DhcpSnoopingIfOption82Subscribed</b>	Specifies the DHCP Option 82 subscriber ID for the port.  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
<b>VlanId</b>	Identifies the VLAN on the switch.
<b>MacAddress</b>	Indicates the MAC address of the DHCP client.
<b>AddressType</b>	Indicates the MAC address type of the DHCP client.
<b>Address</b>	Indicates IP address of the DHCP client.
<b>Interface</b>	Indicates the interface to which the DHCP client is connected.
<b>LeaseTime(sec)</b>	Indicates the lease time (in seconds) of the DHCP client binding.
<b>TimeToExpiry(sec)</b>	Indicates the time (in seconds) before a DHCP client binding expires.
<b>Source</b>	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 252
- 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:

Extreme Networks 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
<b>Port</b>	Identifies the port number.
<b>Mode</b>	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
<b>Condition</b>	Defines the search condition.

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• <b>AND</b>: Includes keywords specified in both the Port and Address fields while filtering results</li> <li>• <b>OR</b>: Includes either one of the keywords specified in the Port and Address fields while filtering results</li> </ul>
<b>Ignore Case</b>	Ignores the letter case while searching.
<b>Column</b>	Specifies the content of the column search. <ul style="list-style-type: none"> <li>• <b>Contains</b></li> <li>• <b>Does not contain</b></li> <li>• <b>Equals to</b></li> </ul>
<b>All records</b>	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
<b>LastUnauthenticatedInetAddressType</b>	The type of IP address that was not authenticated by the device last.
<b>LastUnauthenticatedInetAddress</b>	The last IP address that is not authenticated by the device.
<b>LastUnauthenticatedCommunityString</b>	The last community string that is not authenticated by the device.
<b>RemoteLoginInetAddressType</b>	Specifies either IPv4 or IPv6.
<b>RemoteLoginInetAddress</b>	Specifies the remote login IP address.
<b>TrpRcvrMaxEnt</b>	The maximum number of trap receiver entries.
<b>TrpRcvrCurEnt</b>	The current number of trap receiver entries.
<b>TrpRcvrNext</b>	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
<b>ViewName</b>	Specifies a name for the new entry in a range from 1 to 32 characters.
<b>Subtree</b>	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.
<b>Type</b>	To determine whether access to a MIB object is granted or denied, select one of the following: <ul style="list-style-type: none"> <li>• <b>included</b>: Granted</li> <li>• <b>excluded</b>: Denied</li> </ul>
<b>Storage Type</b>	Select one of the following: <ul style="list-style-type: none"> <li>• <b>volatile</b>: Entry does not persist if switch loses power</li> <li>• <b>nonVolatile</b>: Entry persists if switch loses power</li> </ul>

## 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
<b>Engine ID</b>	Indicates the administratively-unique identifier of the SNMP engine.
<b>Name</b>	Indicates the name of the user in usmUser.

*Table continues...*

Name	Description
<b>Auth Protocol</b>	Select an authentication protocol from the following list: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>MD5</b></li> <li>• <b>SHA</b></li> </ul>
<b>AuthPassword</b>	Specifies the current authorization password.
<b>ConfirmPassword</b>	Reenter the password to confirm.
<b>Priv Protocol</b>	To assign a privacy protocol, select one of the following from the list: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>DES</b></li> <li>• <b>3DES</b></li> <li>• <b>AES</b></li> </ul>
<b>PrivacyPassword</b>	Specifies the current privacy password.
<b>ConfirmPassword</b>	Reenter the password to confirm.
<b>ReadViewName</b>	Specifies the name of the MIB View to which the user is assigned read access.
<b>WriteViewName</b>	Specifies the name of the MIB View to which the user is assigned write access.
<b>NotifyViewName</b>	Specifies the name of the MIB View from which the user receives notifications.
<b>Storage Type</b>	Specifies whether this table entry is stored in one of the following memory types: <ul style="list-style-type: none"> <li>• <b>volatile</b>: Entry does not persist if switch loses power</li> <li>• <b>nonVolatile</b>: Entry persists if switch loses power</li> </ul>

---

## 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 **Sntp Server**.
3. In the Sntp 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
<b>Index</b>	Specifies the unique index value of a row in the community table.
<b>Name</b>	Specifies the community string: a row in the Community table represents a configuration.
<b>ContextEngineId</b>	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.
<b>CommunityString</b>	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.
<b>ReadView Name</b>	Specifies the name of the MIB View to which the user is assigned read access.
<b>WriteViewName</b>	Specifies the name of the MIB View to which the user is assigned write access.
<b>NotifyViewName</b>	Specifies the name of the MIB View from which the user receives notifications.

*Table continues...*

Name	Description
<b>Storage Type</b>	If you need to describe a series of choices for the field, use an unordered list as follows: <ul style="list-style-type: none"> <li>• <b>volatile</b>: Entry does not persist if switch loses power</li> <li>• <b>nonVolatile</b>: Entry persists if switch loses power</li> </ul>

---

## 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
<b>Domain</b>	Select one of the following: <ul style="list-style-type: none"> <li>• <b>IPv4</b></li> <li>• <b>IPv6</b></li> </ul> The default value is IPv4.
<b>DestinationAddr (Port)</b>	Specifies the destination address, expressed in IPv4 Address : port format.
<b>Timeout</b>	Specifies the timeout interval, expressed in 1/100 of a second. The default value is 1500.
<b>RetryCount</b>	Specifies the number of retries the system attempts; expressed as an integer from 0 to 255. The default value is 3.
<b>Type</b>	Specifies the type as one of the following: <ul style="list-style-type: none"> <li>• <b>trap</b></li> <li>• <b>inform</b></li> </ul>
<b>Version</b>	Specifies the SNMP version as one of the following: <ul style="list-style-type: none"> <li>• <b>SNMPv1</b></li> <li>• <b>SNMPv2c</b></li> <li>• <b>SNMPv3/USM</b></li> </ul>
<b>SecurityName</b>	Specifies security name used for generating SNMP messages.
<b>SecurityLevel</b>	Specifies the security level for SNMP messages as one of the following: <ul style="list-style-type: none"> <li>• <b>noAuthNoPriv</b></li> <li>• <b>authNoPriv</b></li> <li>• <b>authPriv</b></li> </ul>
<b>Storage Type</b>	Select one of the following: <ul style="list-style-type: none"> <li>• <b>volatile</b>: Entry does not persist if switch loses power</li> <li>• <b>nonVolatile</b>: Entry persists if switch loses power</li> </ul>

---

## 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 **Sntp 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
<b>Domain</b>	Indicates the address transport type; either IPv4 or IPv6.
<b>DestinationAddr : Port</b>	Indicates the transport address (in IPv4 Address : port format).
<b>Timeout</b>	Indicates the time interval that an application waits for a response in 1/100 second intervals from 0 to 2147483647.
<b>RetryCount</b>	Indicates the number of retries to be attempted when a response is not received for a generated message from 0 to 255.
<b>Type</b>	Indicates the type of the message; either trap or information.
<b>Version</b>	Indicates the SNMP version; either SNMPv1, SNMPv2c or SNMPv3/USM.
<b>SecurityName</b>	Enter the community string.
<b>SecurityLevel</b>	Indicates the security level; either no authorization and no privileges, authorization and no privileges, or authorization and privileges.
<b>StorageType</b>	Select one of the following: <ul style="list-style-type: none"> <li>• <b>volatile</b>: Entry does not persist if switch loses power</li> <li>• <b>nonVolatile</b>: Entry persists if switch loses power</li> </ul>

## 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
<b>NotifyControlType</b>	Lists the SNMP trap names.
<b>Notify Control Type (oid)</b>	Lists the object identifiers for the SNMP traps.
<b>NotifyControlEnabled</b>	Specifies whether traps are enabled or disabled.
<b>NotifyControlPortListEnabled</b>	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 Storm Control using EDM

Use the procedures in this section to configure Storm Control globally and for specific traffic type.

---

### 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
<b>TrafficType</b>	<p>Indicates the different types of traffic for Storm Control Settings.</p> <ul style="list-style-type: none"> <li>• <b>unicast</b>: Indicates the unicast storm control settings</li> <li>• <b>broadcast</b>: Indicates the broadcast Storm Control settings</li> <li>• <b>multicast</b>: Indicates the multicast Storm Control settings</li> </ul>
<b>Enabled</b>	<p>Indicates the current setting for the port. Values include:</p> <ul style="list-style-type: none"> <li>• <b>true</b>: enables Storm Control on the port</li> <li>• <b>false</b>: disables Storm Control on the port</li> </ul>
<b>LowWatermark(pps)</b>	<p>Indicates the low-watermark value for the port in packets per second (pps).</p> <p>RANGE: 10 to 100000000</p>
<b>HighWatermark(pps)</b>	<p>Indicates the high-watermark value for the port in packets per second (pps).</p> <p>RANGE: 10 to 100000000</p>
<b>PollInterval(secs)</b>	<p>Indicates the interval for watermark checking, the value varies in seconds.</p> <p>RANGE: 5 to 300</p>
<b>TrapInterval</b>	<p>Indicates the interval for sending traps when the poll-intervals exceed.</p> <p>RANGE: 0 to 1000</p> <p> <b>Note:</b> Value 0 means disabled (high watermark traps will not be repeated)</p>
<b>ActionType</b>	<p>Indicates the Storm Control action for the specified port.</p> <ul style="list-style-type: none"> <li>• <b>drop</b>: Set Storm Control action to drop</li> <li>• <b>none</b></li> <li>• <b>shutdown</b>: Set Storm Control action to shutdown</li> </ul>

## 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
<b>Index</b>	Indicates the port number.
<b>Enabled</b>	Indicates the current setting for the port. Values include: <ul style="list-style-type: none"> <li>• <b>true</b>: enables Storm Control on the port</li> <li>• <b>false</b>: disables Storm Control on the port</li> </ul>

*Table continues...*

Name	Description
<b>LowWatermark(pps)</b>	Indicates the low-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
<b>HighWatermark(pps)</b>	Indicates the high-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
<b>PollInterval(secs)</b>	Indicates the interval for watermark checking, the value varies in seconds. RANGE: 5 to 300
<b>TrapInterval</b>	Indicates the interval for sending traps when the poll-intervals exceed. RANGE: 0 to 1000  * <b>Note:</b> Value 0 means disabled (high watermark traps will not be repeated)
<b>ActionType</b>	Indicates the Storm Control action for the specified port.  <ul style="list-style-type: none"> <li>• <b>drop</b>: Set Storm Control action to drop</li> <li>• <b>none</b>:</li> <li>• <b>shutdown</b>: Set Storm Control action to shutdown</li> </ul>

## 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 **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**.

### Multicast Storm Control field descriptions

Name	Description
<b>Index</b>	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
<b>Enabled</b>	Indicates the current setting for the port. Values include: <ul style="list-style-type: none"> <li>• <b>true</b>: enables Storm Control on the port</li> <li>• <b>false</b>: disables Storm Control on the port</li> </ul>
<b>LowWatermark(pps)</b>	Indicates the low-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
<b>HighWatermark(pps)</b>	Indicates the high-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
<b>PollInterval(secs)</b>	Indicates the interval for watermark checking, the value varies in seconds. RANGE: 5 to 300
<b>TrapInterval</b>	Indicates the interval for sending traps when the poll-intervals exceed. RANGE: 0 to 1000  <div style="display: flex; align-items: center;"> <span style="color: green; font-weight: bold; margin-right: 5px;">*</span> <b>Note:</b>                      Value 0 means disabled (high watermark traps will not be repeated)                 </div>

*Table continues...*

Name	Description
<b>ActionType</b>	Indicates the Storm Control action for the specified port. <ul style="list-style-type: none"> <li>• <b>drop</b>: Set Storm Control action to drop</li> <li>• <b>none</b>:</li> <li>• <b>shutdown</b>: Set Storm Control action to shutdown</li> </ul>

## 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
<b>Index</b>	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
<b>Enabled</b>	Indicates the current setting for the port. Values include: <ul style="list-style-type: none"> <li>• <b>true</b>: enables Storm Control on the port</li> <li>• <b>false</b>: disables Storm Control on the port</li> </ul>
<b>LowWatermark(pps)</b>	Indicates the low-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
<b>HighWatermark(pps)</b>	Indicates the high-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
<b>PollInterval(secs)</b>	Indicates the interval for watermark checking, the value varies in seconds. RANGE: 5 to 300
<b>TrapInterval</b>	Indicates the interval for sending traps when the poll-intervals exceed. RANGE: 0 to 1000  * <b>Note:</b> Value 0 means disabled (high watermark traps will not be repeated)
<b>ActionType</b>	Indicates the Storm Control action for the specified port. <ul style="list-style-type: none"> <li>• <b>drop</b>: Set Storm Control action to drop</li> <li>• <b>none</b>:</li> <li>• <b>shutdown</b>: Set Storm Control action to shutdown</li> </ul>

## Configuring port-based storm control

### About this task

Use the following procedure to configure Storm Control on an individual port or multiple ports.


### Procedure

1. From the Device Physical View, click one or more ports.
2. From the navigation tree, double-click **Edit**.



3. In the Edit tree, double-click **Chassis**.
4. In the Chassis tree, click **Ports**.
5. In the work area, click the **Storm Control** tab.

## Unicast Storm Control field descriptions

Name	Description
<b>Index</b>	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
<b>Enabled</b>	Indicates the current setting for the port. Values include: <ul style="list-style-type: none"> <li>• <b>true</b>: enables Storm Control on the port</li> <li>• <b>false</b>: disables Storm Control on the port</li> </ul>
<b>LowWatermark(pps)</b>	Indicates the low-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
<b>HighWatermark(pps)</b>	Indicates the high-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
<b>PollInterval(secs)</b>	Indicates the interval for watermark checking, the value varies in seconds. RANGE: 5 to 300
<b>TrapInterval</b>	Indicates the interval for sending traps when the poll-intervals exceed. RANGE: 0 to 1000   <b>Note:</b> Value 0 means disabled (high watermark traps will not be repeated)
<b>ActionType</b>	Indicates the Storm Control action for the specified port. <ul style="list-style-type: none"> <li>• <b>drop</b>: Set Storm Control action to drop</li> <li>• <b>none</b>:</li> <li>• <b>shutdown</b>: Set Storm Control action to shutdown</li> </ul>

---

## 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
<b>Traffic Type</b>	Specifies the traffic type.
<b>AllowedRatePps</b>	Allowed traffic rate packets/second. It is in the range of 0–262143.   <b>Important:</b> Rate Limiting feature is disabled when AllowedRatePps is set to 0.
<b>Enable</b>	When Enable is set to True, the TrafficType can either be multicast, broadcast, or both.   <b>Important:</b> You cannot set the Enabled field for both multicast and broadcast TrafficType to False at the same time. This is an illegal configuration.

# Chapter 9: Configuration examples

---

## TACACS+ server configuration examples

This section describes basic configuration examples of the TACACS+ server.

---

### Extreme Networks Identity Engine Ignition Server TACACS+ configuration example

The following section shows the steps required to configure TACACS+ on Extreme Networks Identity Engines Ignition Server, Release 8.0. Use the preceding information to configure the switch.

A TACACS+ server responds to and audits network access requests. In an installation, the Identity Engines Ignition Server is the TACACS+ server.

The example displays how to do the following:

- Enable TACACS+
- Configure a user
- Create a command set
- Configure the authentication protocol policy
- Create the authorization policy
- Configure TACACS+ authenticators

For more information on the Ignition Server, see *Extreme Networks Ignition Server Administration*, NN47280–600.

#### Before you begin

- Configure the Ignition Server appliance and set up its network settings. For more information, see *Extreme Networks Ignition Server Getting Started*, NN47280–300.
- Install the Ignition Dashboard on your Windows OS.
- Configure each authenticator (switch) to recognize the Ignition Server appliance as its TACACS+ server.
- Configure your switch to send packets to the Ignition Server appliance with the appropriate IP address and port.
- Ensure licenses are up-to-date.

## Procedure

1. If the Ignition Server Dashboard is not connected to your Ignition Server, select **Administration: Login** to connect.
  - a. The default login credentials for **User Name** and **Password** are `admin/admin`. You are recommended to change the default values.
  - b. In the **Connect to** field enter the IP address of the Ignition Server for TACACS+. In this example, the IP address for the TACACS+ server is 192.0.2.8.
2. Enable TACACS+.
  - a. In the Ignition Server Dashboard, select **Site 0**.
  - b. In the Sites window, select the **Services** tab.
  - c. Under the Services tab, select the **TACACS+** tab.
  - d. Click the **Edit** button in the TACACS+ tab.
  - e. In the **Edit TACACS+ Configuration** dialog box, select the **Protocol is enabled** box.
  - f. In the **Bound Interface** field, select **Admin Port**.
  - g. In the **Port** field, enter `49`.
  - h. Select **Accept Requests from Any Authenticator**.

Select this option if you want to create a global TACACS+ authenticator that sets policy for all authenticators that do not match a specific TACACS+-enabled authentication in your Ignition Server configuration.
  - i. In the **Access Policy** field, select **default-tacacs-admin**.

Use this configuration in the case of a global TACACS+ authenticator. Choose your global TACACS+ policy that you want applied if the device finds no better matching authenticator.
  - j. In **TACACS+ Shared Secret** field, enter the secret that the switch and TACACS+ Ignition Server share. In this example, the shared secret is `secret`.
  - k. Click **OK**.
3. Configure a user recognized by the TACACS + server.
  - a. In the Ignition Server Dashboard, expand the following in the Configuration tree: **Site Configuration > Directories > Internal Store > Internal Users**.
  - b. Click **New**.
  - c. Fill in the appropriate fields.

As an example:

User Name: `jsmith`

First Name: `John`

Last Name: `Smith`

Password: test

Confirm password: test

4. If your TACACS+ policy uses per-command authorization, create a command set.
  - a. In the Ignition Server Dashboard, expand the following in the Configuration tree: **Site Configuration > Access Policies > TACACS+**.
  - b. Click **Define Command Sets**.
  - c. Click **New**.
  - d. In the New Device Command Set window, type a **Name** and **Description** for the command set; for instance, level5.
 

In this window you build your command set by adding commands to the list. You can build the command list manually or you can import a list. For more information on importing a command list, see *Extreme Networks Ignition Server Administration*, NN47280–600.
  - e. To manually add the commands, click **Add** in the New/Edit Device Command Set window.
  - f. Click the **Simple Command Using Keywords and Arguments** box.
  - g. In the **Command** field, type the command, and optionally its arguments.
  - h. To allow the command to be used with any argument, select the **Allow** box.
  - i. To allow only the specific command and arguments you have types, tick the **Deny** box.
  - j. Click **OK** to add the command to the list.
  - k. Continue to add the commands that you want.

5. If your TACACS+ policy uses privilege-level authorization, create the TACACS+ access policy to allow the TACACS+ Ignition Server to communicate with the switch.
  - a. In the Ignition Server Dashboard, expand the following in the Configuration tree: **Site Configuration > Access Policies > TACACS+**.
  - b. Select **default-tacacs-admin**.
  - c. Click on the **Authorization Policy** tab and select the name of the policy you want to edit.
  - d. Click **Edit** and the **Edit Authorization Policy** window appears.
  - e. In the **Rules** section, select the rule you want to edit. In this case select level5, to which you have already added commands.
 

The **Rules** list at the left lets you browse and sort the rules in your policy. Use the up and down arrow buttons at the right to set the rule sequence, and click a rule name in the list to edit that rule. The Selected Rule Details section lets you edit the rule you have selected.
  - f. In the Selected Rule Details section, under **Rule Name**, for this example, it reads level5.

- g. Select **Rule Enabled**.
- h. With level5 selected in the Rules list, go to the buttons to the right of the **Constraint** list and click **New**.
- i. In the Action section, select **Allow**.
- j. Select the **Command Sets** tab, in the Action section. Allow Commands in Set should read level-5, in this example, and under All Command Sets all the commands that are accessible under level5 should be listed.
- k. Click **OK**.

For this example to function properly, the summary window must display:

IF User: user-id = level5 THEN Allow

Permit commands in Command Set: level-5

6. Configure the Ignition Server to connect to authenticators, which is the switch:
  - a. In the Ignition Server Dashboard, expand the following folders: **Site Configuration > Authenticators > default** and the Authenticator Summary window appears.
  - b. Click **New**, and the Authenticator Details window appears.
  - c. For this example, type `VSPswitch` under name.
  - d. To the right select **Enable Authenticator**.
  - e. Type the IP address for the switch, which is the authenticator. Use the primary CPU address or the management virtual address.
  - f. In the **Vendor** field, select **Nortel**.
  - g. In the **Device template** field, select **ers-switches-nortel**.
  - h. Select the **TACACS+ Settings** tab.
  - i. Select **Enable TACACS+ Access**.
  - j. In the **TACACS+ Shared Secret** field, type the key value you entered into the switch. In this example, the key is the word `secret`.

To connect using TACACS+, you must use the shared secret for each device. In your switch documentation, the shared secret can also be referred to as a specific key string or an encryption string.
  - k. Under **Access Policy**, select **default-tacacs-user**.
  - l. Click **OK**.

---

## Configuration example: Linux freeware server

1. After TACACS+ is installed on the Linux server, change the directory to

```
$cd /etc/tacacs
```

2. Open the configuration file `tac_plus.cfg`:

```
$vi tac_plus.cfg
```

3. Comment out all the existing lines in the configuration file. Add new lines similar to the following:

```
# Enter your NAS key and user name
key = <secret key>
user = <user name> {
default service = permit
service = exec {
priv-lvl = <Privilege level 1 to 15>
}
login = <Password type> <password>
}
# Set the location to store the accounting records
```

- where

<secret key> is the key that is to be configured on the switch when creating the TACACS+ server entry

<user name> is the user name used to log on to the switch

<Privilege level> specifies the privilege level (for example `rwa = 6`; `rw = 5`; `ro = 1`)

<Password type> specifies the type of password -- for example, the password can be clear text or from the Linux password file, and so on

<Password> if the password type is clear text, the password itself

The following is a sample config file.

```
$vi tac_plus.cfg

# Created by Joe SMITH(jsmit@isp.net)
# Read user_guide and tacacs+ FAQ for more information
#
# Enter your NAS key
key = secretkey u
user = smithJ {

default service = permit
service = exec {
priv-lvl = 15
}
login = cleartext M5xyH8
```

4. Save the changes to the `tac_plus.cfg` file.
5. Run the TACACS+ daemon using the following command:

```
$/usr/local/sbin/tac_plus -C /etc/tacacs/tac_plus.cfg &
```

where

- `tac_plus` is stored under `/usr/local/sbin`
- the configuration file you just edited is stored at `/etc/tacacs/`

The TACACS+ server on Linux is ready to authenticate users.

## SNMP MIB support

The SNMP agent with industry standard Management Information Bases (MIB) and private MIB extensions ensures ompatibility 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 3: SNMP MIB support**

Application	Standard MIBs	Proprietary MIBs
<b>S5 Chassis MIB</b>		s5cha127.mib
<b>S5Agent MIB</b>		s5age140.mib
<b>RMON</b>	rfc1757.mib	
<b>MLT</b>		rcMLT
<b>SNMPv3 MIBs</b>	RFCs 2571, 2572, 2573, 2574, 2575, 2576	
<b>MIB2</b>	rfc1213.mib	
<b>IF-MIB</b>	rfc2233.mib	
<b>Etherlike MIB</b>	rfc1643.mib	
<b>Interface Extension MIB</b>		s5ifx100.mib
<b>Switch Bay Secure</b>		s5sbs102.mib
<b>System Log MIB</b>		bnlog.mib
<b>S5 Autotopology MIB</b>		s5emt104.mib
<b>VLAN</b>		rcVlan
<b>Entity MIB</b>	RFC 2037	
<b>Spanning Tree</b>	RFC1493 Bridge MIB	
<b>LLDP-MIB</b>	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 SNMP agent with industry standard SNMPv1 traps and private SNMPv1 trap extensions are supported.

Trap name	MIB	Sent when
<b>IldpRemTablesChange</b>	LLDP-MIB	Changes in IldpStatsRemTableLastChangeTime occur.
<b>risingAlarm</b>	s5CtrMIB	A rising alarm is fired.
<b>fallingAlarm</b>	s5CtrMIB	A falling alarm is fired.
<b>pethPsePortOnOffNotification</b>	rfc3621MIB	Pse Port is delivering or is not delivering power to the PD.
<b>pethMainPowerUsageOnNotification</b>	rfc3621MIB	The usage power is above the threshold.
<b>pethMainPowerUsageOffNotification</b>	rfc3621MIB	The usage power is below the threshold.
<b>entConfigChange</b>	rfc4133MIB	A change in either of these tables occurred: entPhysicalTable, entLogicalTable, entLPMappingTable, entAliasMappingTable.
<b>coldStart</b>	rfc3418MIB	The system is powered on.
<b>warmStart</b>	rfc3418MIB	The system restarts due to a management reset.
<b>linkDown</b>	rfc2863MIB	The link state changes to down on a port.
<b>linkUp</b>	rfc2863MIB	The link state changes to up on a port.
<b>authenticationFailure</b>	rfc3418MIB	SNMP authentication failure occurs.
<b>IldpXMedTopologyChangeDetected</b>	IldpExtMedMIB	A new remote device is attached to a local port, or a remote device is disconnected.
<b>bsAdacPortConfigNotification</b>	bayStackAdacMIB	The maximum number of devices supported per port is reached.
<b>bsDhcpSnoopingBindingTableFull</b>	bayStackDhcpSnoopingMIB	An attempt is made to add a new DHCP binding entry when the binding table is full.
<b>bsDhcpSnoopingTrap</b>	bayStackDhcpSnoopingMIB	A DHCP packet is dropped.
<b>bsaiArpPacketDroppedOnUntrustedPort</b>	bayStackArpInspectionMIB	An ARP packet is dropped on an untrusted port due to an invalid IP/MAC binding.
<b>bsSourceGuardReachedMaxIpEntries</b>	bayStackSourceGuardMIB	The maximum number of IP entries on a port has been reached.

*Table continues...*

Trap name	MIB	Sent when
<b>bsSourceGuardCannotEnablePort</b>	bayStackSourceGuardMIB	There are insufficient resources available to enable IP source guard checking on a port.
<b>rcnBpduReceived</b>	rcTrapsMIB	A BPDU is received on a port which has BPDU filtering enabled.
<b>bsnConfigurationSavedToNvram</b>	bsnMIB	All switch configuration is saved to NVRAM.
<b>bsnEapAccessViolation</b>	bsnMIB	An EAP access violation occurs.
<b>bsnLacTrunkUnavailable</b>	bsnMIB	An attempt is made to form an 802.3ad LAG trunk, but there are no available resources to create a new trunk.
<b>bsnLoginFailure</b>	bsnMIB	An attempt to login to the system fails as a result of an incorrect password.
<b>bsnLacPortDisabledDueToLossOfVLACPDU</b>	bsnMIB	A port is disabled due to the loss of a VLACP PDU.
<b>bsnLacPortEnabledDueToReceiptOfVLACPDU</b>	bsnMIB	A port is enabled due to receipt of a VLACP PDU.
<b>bsnEapRAVErrror</b>	bsnMIB	An Eap client MAC address was authorized on a port, but the port could not be moved to the Radius-Assigned VLAN.
<b>s5EtrNewSbsMacAccessViolation</b>	s5CtrMIB	A MAC address violation is detected.
<b>s5CtrFanDirectionError</b>	s5CtrMIB	A fan component's direction is incorrect
<b>s5CtrHighTemperatureError</b>	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:**

Extreme Networks 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.

```
Switch(config)#mac-security auto-learning sticky
Extreme Networks recommends disabling autosave when sticky mac is enabled
Switch(config)#mac-security enable
Switch(config)#no autosave enable
Switch(config)#copy config nvram
```

2. Enable MAC security and auto-learning on ports 1/6-14.

```
Switch(config)#interface Ethernet 1/6-14
Switch(config-if)#mac-security enable
Switch(config-if)#mac-security auto-learning enable
Switch(config-if)#mac-security auto-learning max-addr <1-25>
Switch(config-if)#mac-security enable
Switch(config-if)#exit
```

3. Verify the MAC security configuration for the interfaces.

```
Switch(config)#show mac-security port 1/6-14
```

Port	Trunk	Security	Auto-Learning	MAC Number
6		Disabled	Disabled	2
7		Disabled	Disabled	2
8		Disabled	Disabled	2
9		Disabled	Disabled	2
10		Disabled	Disabled	2
11		Disabled	Disabled	2
12		Disabled	Disabled	2
13		Disabled	Disabled	2
14		Disabled	Disabled	2

4. Connect a PC to port 1/8 and verify the configuration by displaying the MAC security MAC address table.

```
Switch#show mac-security mac-address-table
Number of addresses: 1
Port Allowed MAC Address Type
-----
8      00-02-A5-E9-00-28     Sticky

Security List Allowed MAC Address Type
-----

Trunk Allowed      MAC Address      Type
-----
```

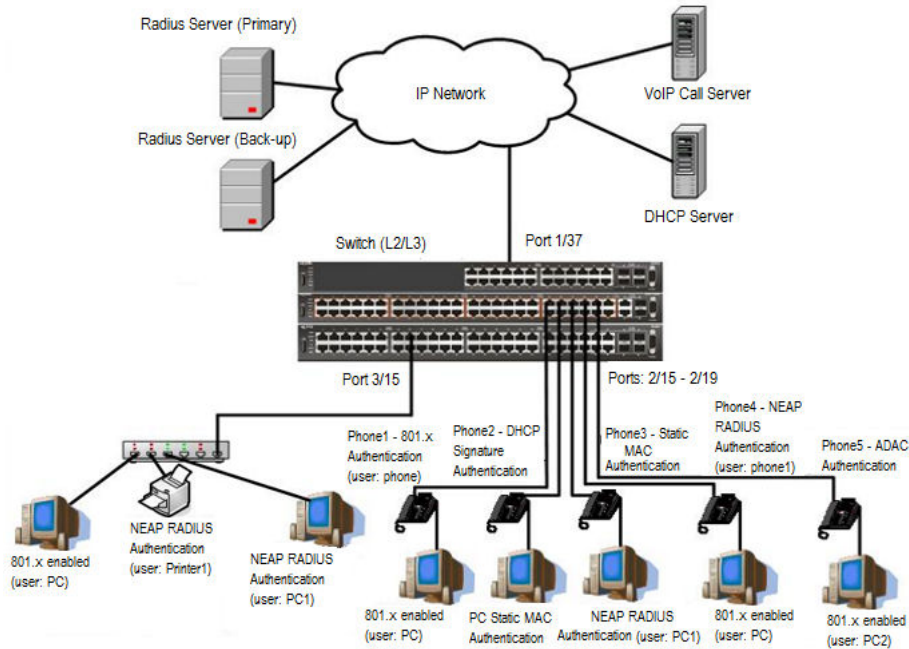
---

## MHMA authentication mode (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes

When you operate in MHMA mode with MHMV support activated each client can have its own VLAN ID and PVID. MAC type VLANs are used to achieve this new functionality.

For this EAP operational mode, the port and client will have the following settings:

- when 802.1X is disabled on the port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs
- when 802.1X is enabled on the port:
  - an unauthenticated client is on the port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs
  - an 801.x authenticated client is on the port
    - the port is added to an initial VLAN and the port PVID is the initial VLAN PVID - the client uses the initial VLAN PVIDs (client traffic can be sent in multiple initial VLANs). In this case no RADIUS attribute is received, or an invalid RADIUS attribute is received for the 801.x client.
    - the port is added to RADIUS VLAN and the port PVID is the initial VLAN PVID - the client PVID is set to RADIUS VLAN PVID (Valid RADIUS attributes received for 801.x client)
  - an authenticated non-801.x radius client is on the port with Guest VLAN enabled
    - the port is added to an initial VLAN, and the port PVID is the initial VLAN PVID - the client uses the initial VLAN PVIDs (client traffic can be sent in multiple INITIAL VLANs). In this case no RADIUS attribute is received, or an invalid RADIUS attribute is received for the non-801.x radius client.
    - the port is added to the RADIUS VLAN and the port PVID is the initial VLAN PVID - the client PVID is set to RADIUS VLAN PVID (Valid RADIUS attributes received for non-801.x radius client)
  - an authenticated non-801.x static MAC client is on the port (client MAC was learned in the MAC address table). In this case the port is added to an initial VLAN, and the port PVID is the initial VLAN PVID - the client uses the initial VLAN PVIDs (client traffic can be sent in multiple initial VLANs)
  - an authenticated non-801.x DHCP client is on the port and using a DHCP signature—the port remains in the initial VLAN, and the port uses the initial VLAN PVID - the DHCP client uses tagged traffic, with the VOIP VLANs (DHCP client traffic can be sent desired VOIP VLAN is tagged traffic is used for the IP phone)



**Figure 4: MHMA authentication mode (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes**

## Scenario

Assume the following settings:

1. RADIUS server configuration.
  - A primary server is mandatory. If a back-up server is used, the back-up server configuration must be the same as for primary server configuration.
2. Configure all IP Phones to send tag traffic with proper VoIP VLAN ID.
3. Clients settings:
  - Port 2/15:
    - 801.x authenticated user Phone1 connected
    - 801.x enabled user PC connected
    - Initial VLAN ID = 50, 200
    - PC RADIUS VLAN ID = 300
    - Phone RADIUS VLAN ID = none
  - Port 2/16:
    - DHCP signature authenticated user Phone2 connected

- Static MAC authenticated user PC connected
  - Initial VLAN ID = 50, 300
  - Phone EAP VOIP VLAN ID = 200
  - Port 2/17:
    - Static MAC authenticated user Phone3 connected
    - NEAP RADIUS authenticated user PC1 connected
    - Initial VLAN ID = 50, 200
    - PC RADIUS VLAN ID = 300
  - Port 2/18:
    - NEAP RADIUS authenticated user Phone1 connected
    - 801.x enabled user PC connected
    - Initial VLAN ID = 50, 200
    - PC RADIUS VLAN ID = 300
    - Phone RADIUS VLAN ID = none
  - Port 2/19:
    - ADAC authenticated user Phone5 connected
    - 801.x enabled user PC2 connected
    - Initial VLAN ID = 50, 300
    - PC RADIUS VLAN ID = none
    - Phone ADAC VLAN ID = 201
  - Port 3/15:
    - 801.x enabled user PC connected
    - NEAP RADIUS authenticated user Printer1 connected
    - NEAP RADIUS authenticated user PC1 connected
    - Initial VLAN ID = 50
    - RADIUS VLAN ID = 300
4. Port settings:
- VLAN ID/PVID port settings for 2/15:
    - 801.x disabled - VLAN ID/PVID = 50,200/50
    - Unauthenticated client with 801.x enabled - VLAN ID/PVID = 50,200/50
    - Authenticated (user phone authenticated, user PC unauthenticated):
      - VLAN ID/PVID = 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)

- EAP port vid for phone client: 50
  - Authenticated (user phone authenticated, user PC authenticated):
    - VLAN ID/PVID = 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
    - VLAN ID/PVID = 50, 200, 300/ 50 (Valid RADIUS attributes received)
    - EAP port vid for PC client: 300
    - EAP port vid for phone client: 50
  - VLAN ID/PVID port settings for 2/16:
    - 801.x disabled - VLAN ID/PVID = 50,300/300
    - Unauthenticated client with 801.x enabled - VLAN ID/PVID = 50,300/300
    - Authenticated (Phone DHCP signature OK, EAP VOIP VLAN ID 200 assigned):
      - VLAN ID/PVID = 50,200,300/300
    - Authenticated (PC MAC defined in static list, PC MAC learned in MAC address table, Phone DHCP signature OK):
      - VLAN ID/PVID = 50,200,300/300
      - EAP port vid for PC client: 300
      - EAP port vid for phone client: 200
  - VLAN ID/PVID port settings for 2/17:
    - 801.x disabled - VLAN ID/PVID = 50,200/50
    - Unauthenticated client with 801.x enabled - VLAN ID/PVID = 50,200/50
    - Authenticated (Phone MAC defined in static list, Phone MAC learned in MAC address table):
      - VLAN ID/PVID = 50, 200/ 50
      - EAP port vid for phone client: 50
    - Authenticated (user PC1 authenticated; Phone MAC defined in static list, Phone MAC learned in MAC address table):
      - VLAN ID/PVID = 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
      - VLAN ID/PVID = 50, 200, 300/ 300 (Valid RADIUS attributes received)
      - EAP port vid for PC client: 300
      - EAP port vid for phone client: 50
- VLAN ID/PVID port settings for 2/18:
- 801.x disabled - VLAN ID/PVID = 50,200/50
  - Unauthenticated client with 801.x enabled - VLAN ID/PVID = 50,200/50



- Authenticated (user phone1 authenticated, user PC unauthenticated):
  - VLAN ID/PVID = 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
  - EAP port vid for phone client: 50
- Authenticated (user PC authenticated, user phone1 authenticated):
  - VLAN ID/PVID = 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
  - VLAN ID/PVID = 50, 200, 300/ 300 (Valid RADIUS attributes received)
  - EAP port vid for PC client: 300
  - EAP port vid for phone client: 50

VLAN ID/PVID port settings for 2/19:

- 801.x disabled - VLAN ID/PVID = 50,300/300
- Unauthenticated client with 801.x enabled - VLAN ID/PVID = 50,300/300
- Authenticated (phone is ADAC authenticated, user PC unauthenticated):
  - VLAN ID/PVID = 50, 300, 201/ 300 (No RADIUS attribute received/Invalid RADIUS attributes received)
  - EAP port vid for phone client: NA
- Authenticated (user PC2 authenticated, phone is ADAC authenticated):
  - VLAN ID/PVID = 50, 300, 201/ 300 (No RADIUS attribute received/Invalid RADIUS attributes received)
  - EAP port vid for PC client: 300
  - EAP port vid for phone client: NA

VLAN ID/PVID port settings for 3/15:

- 801.x disabled - VLAN ID/PVID = 50/50
- Unauthenticated client with 801.x enabled - VLAN ID/PVID = 50/50
- Authenticated (at least one user authenticated from : PC, PC1, Printer1):
  - VLAN ID/PVID = 50/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
  - VLAN ID/PVID = 300/ 300 (Valid RADIUS attributes received)
  - EAP port vid for PC client: 300
  - EAP port vid for printer NEAP client: 300
  - EAP port vid for NEAP PC client: 300

## Configuration example

### 1. Configure the RADIUS servers and VLAN settings

```
Switch(config)#ip address 10.100.68.254 netmask 255.255.255.0 default-gateway 10.100.68.1
Switch(config)#radius-server host 10.100.68.2
Switch(config)#radius-server secondary-host 10.100.68.3
Switch(config)#radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
Switch(config)#vlan configcontrol automatic
Switch(config)#vlan create 50 type port
Switch(config)#vlan create 200 type port
Switch(config)#vlan create 300 type port
Switch(config)#vlan members add 50 2/15-19,3/15
```

### 2. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 2/15-19,3/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	50	0	UntagAll	Unit 2, Port 15
2/16	No	Yes	50	0	UntagAll	Unit 2, Port 16
2/17	No	Yes	50	0	UntagAll	Unit 2, Port 17
2/18	No	Yes	50	0	UntagAll	Unit 2, Port 18
2/19	No	Yes	50	0	UntagAll	Unit 2, Port 19
3/15	No	Yes	50	0	UntagAll	Unit 3, Port 15

### 3. Confirm the VLAN interface VLANs.

```
Switch(config)#show vlan interface vids 2/15-19,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	50	VLAN #50				
2/16	50	VLAN #50				
2/17	50	VLAN #50				
2/18	50	VLAN #50				
2/19	50	VLAN #50				
3/15	50	VLAN #50				

MHMA authentication mode (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes

#### 4. Change VLAN config control mode to flexible mode in order to add same port in multiple initial VLANs.

```
Switch(config)#vlan configcontrol flexible
```

#### 5. Add IP phone ports to the voice vlan, VLAN ID 200.

```
Switch(config)#vlan members add 200 2/15,2/17,2/18  
Switch(config)#vlan members add 300 2/16  
Switch(config)#vlan members add 300 2/19  
Switch(config)#vlan port 2/16 pvid 300  
Switch(config)#vlan port 2/19 pvid 300
```

#### 6. Confirm the VLAN interface settings.

```
Switch(config)#sho vlan interface info 2/15-19
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	50	0	UntagAll	Unit 2, Port 15
2/16	No	Yes	300	0	UntagAll	Unit 2, Port 16
2/17	No	Yes	50	0	UntagAll	Unit 2, Port 17
2/18	No	Yes	50	0	UntagAll	Unit 2, Port 18
2/19	No	Yes	300	0	UntagAll	Unit 2, Port 19

#### 7. Confirm the VLAN interface VIDs.

```
Switch(config)#show vlan interface vid 2/15-19
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	50	VLAN #50	200	VLAN #200		
2/16	50	VLAN #50	300	VLAN #300		
2/17	50	VLAN #50	200	VLAN #200		
2/18	50	VLAN #50	200	VLAN #200		
2/19	50	VLAN #50	300	VLAN #300		

#### 8. Since all IP Phones will be sending tagged traffic and only the PC will need to receive untagged traffic, set the port to untagpvidOnly.

```
Switch(config)#vlan ports 2/15,2/16,2/17,2/18,2/19 tagging untagpvidOnly
```

#### 9. Confirm the VLAN interface settings.

```
Switch(config)#sho vlan interface info 2/15,2/16,2/17,2/18,2/19
```

## Configuration examples

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	50	0	UntagPvid Only	Unit 2, Port 15
2/16	No	Yes	50	0	UntagPvid Only	Unit 2, Port 16
2/17	No	Yes	50	0	UntagPvid Only	Unit 2, Port 17
2/18	No	Yes	50	0	UntagPvid Only	Unit 2, Port 18
2/19	No	Yes	300	0	UntagPvid Only	Unit 2, Port 19

### 10. Confirm the VLAN interface VIDs.

```
Switch(config)#show vlan interface vids 2/15,2/16,2/17,2/18,2/19
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	50	VLAN #50	200	VLAN #200	-----	-----
2/16	50	VLAN #50	300	VLAN #300	-----	-----
2/17	50	VLAN #50	200	VLAN #200	-----	-----
2/18	50	VLAN #50	200	VLAN #200	-----	-----
2/19	50	VLAN #50	300	VLAN #300	-----	-----

### 11. Configure the uplink port 1/37 to transport traffic from all VLANs (1,50,200,300). VLAN 201 is automatically added by ADAC.

```
Switch(config)#vlan members add 50,200,300 1/37
Switch(config)#vlan ports 1/37 tagging tagall
```

### 12. Confirm the VLAN interface settings for uplink port 1/37.

```
Switch(config)#sho vlan interface info 1/37
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/37	No	Yes	1	0	TagAll	Unit 1, Port 37

### 13. Confirm the VLAN interface VIDs for uplink port 1/37.

```
Switch(config)#show vlan interface vid 1/37
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/37	1	VLAN #1	50	VLAN #50	200	VLAN #200
	300	VLAN #300				

#### 14. Configure ADAC.

```
Switch(config)#interface Ethernet 2/19
Switch(config-if)#adac detection mac lldp
Switch(config-if)#adac enable
Switch(config-if)#exit
Switch(config)#adac uplink-port 1/37
Switch(config)#adac voice-vlan 201
```

#### Important:

Select only the ADAC mode that allows multiple MACs (clients) on a port. ADAC modes untagged-frames-basic and untagged-frames-advanced, support only one MAC per port (the IP phone MAC).

```
Switch(config)#adac op-mode tagged-frames
```

#### 15. Add the MAC address of the IP phone connected on port 2/19 if the IP phone does not support the LLDP protocol.

```
Switch(config)#adac mac-range-table low-end 00-1C-9C-4A-BC-01 high-end 00-1C-9C-4A-BC-02
```

#### 16. Verify connectivity with the Primary RADIUS server and back-up RADIUS server (if back-up server is used). Firewalls may filter ICMP packets. In this case it is recommended to verify RADIUS server logs for authentication request sent by device.

```
Switch(config)#ping 10.100.68.2
(Host is reachable)

Switch(config)#ping 10.100.68.3
(Host is reachable)
```

#### 17. Set the EAPOL status for port 2/15.

```
Switch(config)#interface Ethernet all
Switch(config-if)#eapol multihost port 2/15 enable
Switch(config-if)#eapol port 2/15 status auto
Switch(config-if)#eapol multihost port 2/15 eap-mac-max 2
Switch(config-if)#eapol multihost port 2/15 use-radius-assigned-vlan
Switch(config-if)#exit
```

#### 18. Set the EAPOL status for port 2/16.

```
Switch(config)#interface Ethernet all
Switch(config-if)#eapol multihost port 2/16 enable
Switch(config-if)#eapol port 2/16 status auto
Switch(config-if)#eapol multihost port 2/16 non-eap-mac-max 2
Switch(config-if)#eapol multihost port 2/16 allow-non-eap-enable
Switch(config-if)#eapol multihost port 2/16 non-eap-phone-enable
Switch(config-if)#eapol multihost non-eap-mac port 2/16 00-19-E1-A2-4D-36
Switch(config-if)#exit
```

#### 19. Set the EAPOL status for port 2/17.

```
Switch(config)#interface Ethernet all
Switch(config-if)#eapol multihost port 2/17 enable
```

## Configuration examples

```
Switch(config-if)#eapol port 2/17 status auto
Switch(config-if)#eapol multihost port 2/17 non-eap-mac-max 2
Switch(config-if)#eapol multihost port 2/17 allow-non-eap-enable
Switch(config-if)#eapol multihost port 2/17 radius-non-eap-enable
Switch(config-if)#eapol multihost port 2/17 non-eap-use-radius-assigned- vlan
Switch(config-if)#eapol multihost non-eap-mac port 2/17 00-19-E1-E5-52-4A
Switch(config-if)#exit
```

### 20. Set the EAPOL status for port 2/18.

```
Switch(config)#interface Ethernet all
Switch(config-if)#eapol multihost port 2/18 enable
Switch(config-if)#eapol port 2/18 status auto
Switch(config-if)#eapol multihost port 2/18 eap-mac-max 1
Switch(config-if)#eapol multihost port 2/18 non-eap-mac-max 1
Switch(config-if)#eapol multihost port 2/18 allow-non-eap-enable
Switch(config-if)#eapol multihost port 2/18 radius-non-eap-enable
Switch(config-if)#eapol multihost port 2/18 use-radius-assigned-vlan
Switch(config-if)#exit
```

### 21. Set the EAPOL status for port 2/19.

```
Switch(config)#interface Ethernet all
Switch(config-if)#eapol multihost port 2/19 enable
Switch(config-if)#eapol port 2/19 status auto
Switch(config-if)#eapol multihost port 2/19 eap-mac-max 1
Switch(config-if)#eapol multihost port 2/19 non-eap-mac-max 1
Switch(config-if)#eapol multihost port 2/19 allow-non-eap-enable
```

### 22. To confirm that VLAN modifications are not performed by EAP on ADAC enabled ports, disable the VLAN assignment on port 2/19 for EAP and NON-EAP clients.

```
Switch(config-if)#no eapol multihost port 2/19 use-radius-assigned-vlan
Switch(config-if)#no eapol multihost port 2/19 non-eap-use-radius-assigned-vlan
Switch(config-if)#exit
```

### 23. Set the EAPOL status for port 3/15.

```
Switch(config)#interface Ethernet all
Switch(config-if)#eapol multihost port 3/15 enable
Switch(config-if)#eapol port 3/15 status auto
Switch(config-if)#eapol multihost port 3/15 eap-mac-max 1
Switch(config-if)#eapol multihost port 3/15 non-eap-mac-max 2
Switch(config-if)#eapol multihost port 3/15 allow-non-eap-enable
Switch(config-if)#eapol multihost port 3/15 use-radius-assigned-vlan
Switch(config-if)#eapol multihost port 3/15 radius-non-eap-enable
Switch(config-if)#eapol multihost port 3/15 non-eap-use-radius-assigned- vlan
Switch(config-if)#exit
```

### 24. Set the EAPOL MultiHost status.

```
Switch(config)#eapol multihost voip-vlan 1 vid 200
Switch(config)#eapol multihost voip-vlan 1 enable
Switch(config)#eapol multihost allow-non-eap-enable
Switch(config)#eapol multihost non-eap-phone-enable
Switch(config)#eapol multihost non-eap-use-radius-assigned-vlan
Switch(config)#eapol multihost use-radius-assigned-vlan
Switch(config)#eapol multihost radius-non-eap-enable
```

#### Important:

You can enable the MutiVlan option only when EAPOL is globally disabled and Fail Open VLAN is not used. The use-most-recent-radius-vlan option is mutually exclusive with the MutiVlan

MHMA authentication mode (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes

option because the MultiVlan option provides multiple VLAN support on one EAPOL enabled port.

```
Switch(config)#eapol multihost multivlan enable
Switch(config)#eapol enable
```

### 25. Enable ADAC.

```
Switch(config)#adac enable
```

After ADAC is enabled (for tagged-frames and untagged-frames-advanced modes), the ADAC voice VLAN is automatically created and the uplink port, and telephony ports (detected IP phones) are added to the ADAC voice VLAN.

### 26. Confirm the ADAC interface status for port 2/19.

```
Switch(config)#show adac interface 2/19
```

Unit/Port	Type	Auto Detection	Oper State	Auto Configuration	T-F PVID	T-F Tagging
2/19	T	Enabled	Enabled	Applied	No Change	Untag PVID Only

### 27. Confirm the VLAN status.

```
Switch(config)#show vlan
```

Id	Name	Type	Protocol	User PID	Active	IVL/SVL	Mgmt
1	VLAN #1	Port	None	0x0000	Yes	IVL	Yes
Port Members: 1/2-34,1/39-50,2/1-14,2/20-26,3/1-14,3/16-26							
50	VLAN #50	Port	None	0x0000	Yes	IVL	No
Port Members: 1/1,1/35,2/15-19,3/15							
200	VLAN #200	Port	None	0x0000	Yes	IVL	No
Port Members: 1/36,2/15-18							
201	Voice_VLAN	Port	None	0x0000	Yes	IVL	No
Port Members: 1/37,2/19							
300	VLAN #300	Port	None	0x0000	Yes	IVL	No
Port Members: 1/37-38,2/15-19,3/15							

28. Confirm the EAPOL MultiHost status.

```
Switch(config)#sho eapol multihost non-eap-mac status
```

Unit/Port	Client MAC Address	State	Vid	Pri
2/16	00:19:E1:A2:4D:36	Authenticated Locally	50	0
2/17	00:19:E1:E5:52:4A	Authenticated Locally	50	0
2/17	00:AB:CD:02:00:20	Authenticated By RADIUS	300	0
2/18	00:19:E1:E2:40:46	Authenticated By RADIUS	50	0
2/19	00:1E:CA:FF:C2:94	Authenticated For IP Telephony	N/A	N/A
3/15	00:AB:CD:01:00:20	Authenticated By RADIUS	300	0
3/15	00:AB:CD:01:00:21	Authenticated By RADIUS	300	0
Total number of authenticated clients: 7				

```
Switch(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
2/15	00:19:E1:E5:52:92	Authenticated	Idle	50	0
2/15	00:50:BF:B8:09:AF	Authenticated	Idle	300	0
2/18	00:AB:CD:03:00:12		Idle	3000	N/A
2/19	00:AB:CD:04:00:13	Authenticated	Idle	300	0
3/15	00:AB:CD:01:00:10	Authenticated	Idle	300	0
===== Neap Phones =====					
2/16	00:19:E1:E6:09:B1				
Total number of authenticated clients: 6					

29. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 2/15-19,3/15
```



MHMA authentication mode (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	50	0	UntagPvid Only	Unit 2, Port 15
2/16	No	Yes	300	0	UntagPvid Only	Unit 2, Port 16
2/17	No	Yes	50	0	UntagPvid Only	Unit 2, Port 17
2/18	No	Yes	50	0	UntagPvid Only	Unit 2, Port 18
2/19	No	Yes	300	0	UntagPvid Only	Unit 2, Port 19
3/15	No	Yes	50	0	UntagAll	Unit 3, Port 15

### 30. Confirm the VLAN interface VIDs.

```
Switch(config)#show vlan interface vids 2/15-19,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	50	VLAN #50	200	VLAN #200	300	VLAN #300
2/16	50	VLAN #50	200	VLAN #200	300	VLAN #300
2/17	50	VLAN #50	200	VLAN #200	300	VLAN #300
2/18	50	VLAN #50	200	VLAN #200	300	VLAN #300
2/19	50	VLAN #50	201	Voice_VLAN	300	VLAN #300
3/15	50	VLAN #50	300	VLAN #300	-----	-----

### Alternate configuration

The following operation applies to **MHMA authentication mode (Multihost MultiVLAN option enabled) without valid additional RADIUS attributes**, when the RADIUS server has no special attributes configured or the RADIUS server uses misconfigured attributes (not matching the device configuration).

This configuration example modifies EAP and NEAP client attributes on the RADIUS server, replacing VLAN ID 300 with VLAN ID 124, which is not configured on the device.

#### 1. Enable EAPOL.

```
Switch(config)#eapol disable
Switch(config)#eapol enable
```

#### 2. Confirm EAPOL MultiHost status.

```
Switch(config)#sho eapol multihost non-eap-mac status
```

## Configuration examples

Unit/Port	Client MAC Address	State	Vid	Pri
2/16	00:19:E1:A2:4D:36	Authenticated Locally	50	0
2/17	00:19:E1:E5:52:4A	Authenticated Locally	50	0
2/17	00:AB:CD:02:00:20	Authenticated By RADIUS	50	0
2/18	00:19:E1:E2:40:46	Authenticated By RADIUS	50	0
2/19	00:1E:CA:FF:C2:94	Authenticated For IP Telephony	N/A	N/A
3/15	00:AB:CD:01:00:20	Authenticated By RADIUS	50	0
3/15	00:AB:CD:01:00:21	Authenticated By RADIUS	50	0

Total number of authenticated clients: 7

```
Switch(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
2/15	00:19:E1:E5:52:92	Authenticated	Idle	50	0
2/15	00:50:BF:B8:09:AF	Authenticated	Idle	50	0
2/18	00:AB:CD:03:00:12	Authenticated	Idle	50	0
2/19	00:AB:CD:04:00:13	Authenticated	Idle	300	0
3/15	00:AB:CD:01:00:10	Authenticated	Idle	50	0

=====  
Neap Phones  
=====  
2/16 00:19:E1:E6:09:B1

Total number of authenticated clients: 6

### 3. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 2/15-19,3/15
```

MHMA authentication mode (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	50	0	UntagPvid Only	Unit 2, Port 15
2/16	No	Yes	300	0	UntagPvid Only	Unit 2, Port 16
2/17	No	Yes	50	0	UntagPvid Only	Unit 2, Port 17
2/18	No	Yes	50	0	UntagPvid Only	Unit 2, Port 18
2/19	No	Yes	300	0	UntagPvid Only	Unit 2, Port 19
3/15	No	Yes	50	0	UntagAll	Unit 3, Port 15

#### 4. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 2/15-19,3/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	50	0	UntagPvid Only	Unit 2, Port 15
2/16	No	Yes	50	0	UntagPvid Only	Unit 2, Port 16
2/17	No	Yes	50	0	UntagPvid Only	Unit 2, Port 17
2/18	No	Yes	50	0	UntagPvid Only	Unit 2, Port 18
2/19	No	Yes	300	0	UntagPvid Only	Unit 2, Port 19
3/15	No	Yes	50	0	UntagAll	Unit 3, Port 15

#### 5. Confirm the VLAN interface VLANs.

```
Switch(config)#show vlan interface vids 2/15-19,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	50	VLAN #50	200	VLAN #200		
2/16	50	VLAN #50	200	VLAN #200	300	VLAN #300
2/17	50	VLAN #50	200	VLAN #200		
2/18	50	VLAN #50	200	VLAN #200		
2/19	50	VLAN #50	201	Voice_VLAN	300	VLAN #300
3/15	50	VLAN #50				