



Configuring Security on Avaya Ethernet Routing Switch 4000 Series

Release 5.7
NN47205-505
Issue 09.01
November 2013

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A

BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

Licence types

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that 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"). 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 Documentation or on Avaya's website at: <http://support.avaya.com/Copyright>. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your

company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com>.

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction	17
Purpose.....	17
Related resources.....	17
Support.....	19
Chapter 2: New in this release	21
Features.....	21
802.1X-2004 support.....	21
Block subsequent MAC authentication.....	21
Change RADIUS Password.....	21
Default all EAP settings command.....	22
EAP-MD5 authentication.....	22
EAP and NEAP separation.....	22
eapol multihost mac-max command.....	23
Fail Open VLAN Continuity mode.....	23
MAC Security Port Lockout.....	23
NEAP Not Member of VLAN.....	24
Password change through EDM.....	24
RADIUS NEAP password configurable key.....	24
RO User access to SSH.....	24
SFTP DHCP external save file support.....	24
Syslog Support for 802.1X/EAP/NEAP/UBP.....	25
Trace feature.....	25
User Based Policies.....	25
Other Changes.....	26
Chapter 3: Security fundamentals	29
ACL command modes.....	29
Hardware-based security.....	30
HTTP/HTTPS port configuration.....	31
MAC address-based security.....	31
MAC address-based security autolearning.....	32
MAC Security Port Lockout.....	33
Block subsequent MAC authentication.....	33
Sticky MAC address.....	35
RADIUS-based network security.....	35
How RADIUS works.....	35
RADIUS server configuration.....	36
Change the RADIUS Password.....	36
RADIUS server reachability.....	37
RADIUS EAP or non-EAP requests from different servers.....	37
RADIUS password fallback.....	44
Configuring RADIUS authentication.....	44
RADIUS Request use Management IP.....	44
RADIUS Management Accounting.....	45
RADIUS interim accounting updates.....	46

Campus security example.....	47
EAPOL-based security.....	48
EAPOL dynamic VLAN assignment.....	50
System requirements.....	51
EAPOL-based security configuration rules.....	51
Advanced EAPOL features.....	52
Client reauthentication.....	52
Single Host with Single Authentication and Guest VLAN.....	53
Guest VLAN.....	53
802.1X or non-EAP and Guest VLAN on the same port.....	54
802.1X or non-EAP with Fail Open VLAN.....	54
Fail Open VLAN Continuity Mode.....	56
Multiple Host with Multiple Authentication.....	57
RADIUS-assigned VLAN use in MHMA mode.....	58
Multiple Hosts with Multiple VLANs.....	61
802.1X or non-EAP Last Assigned RADIUS VLAN.....	62
802.1X or non-EAP with VLAN names.....	62
Non EAP hosts on EAP-enabled ports.....	63
Non-EAPOL MAC RADIUS authentication.....	64
Multiple Host with Single Authentication.....	65
Non-EAP client re-authentication.....	66
NEAP Not Member of VLAN.....	67
Summary of multiple host access on EAPOL-enabled ports.....	67
802.1X authentication and Wake on LAN.....	68
EAP (802.1X) accounting.....	69
Non-EAP accounting.....	69
Feature operation.....	69
EAP and NEAP separation.....	71
802.1X dynamic authorization extension (RFC 3576).....	72
TACACS+.....	74
TACACS+ architecture.....	75
Feature operation.....	75
TACACS+ authentication.....	76
TACACS+ authorization.....	76
Changing privilege levels at runtime.....	77
TACACS+ server configuration example.....	77
TACACS+ accounting.....	78
TACACS+ configuration.....	79
IP Manager.....	79
Password security.....	80
Password length and valid characters.....	80
Password retry.....	81
Password history.....	81
Password display.....	81
Password verification.....	81
Password aging time.....	81
Read-Only and Read-Write passwords.....	81

Default password and default password security.....	82
Password security enabled or disabled.....	82
Password security commands.....	82
Password security features and requirements.....	82
ACL audit.....	83
Erasable ACLI audit log.....	84
Simple Network Management Protocol.....	84
SNMP Version 1 (SNMPv1).....	84
SNMP Version 2 (SNMPv2).....	85
SNMP Version 3 (SNMPv3).....	85
Avaya Ethernet Routing Switch 4000 Series support for SNMP.....	85
SNMP MIB support.....	85
SNMP trap support.....	86
Secure Socket Layer protocol.....	90
Secure versus Non-secure mode.....	90
SSL Certificate Authority.....	91
SSL configuration and management.....	91
Secure Shell protocol.....	92
Components of SSH2.....	92
SSH service configuration.....	92
SSH clients.....	93
SSH and SSH Client.....	94
SSH Client known hosts.....	95
SSH Client known hosts in stacks.....	95
Switch capacity to learn keys.....	95
Standards and Compliance.....	95
Feature Interactions.....	96
DHCP snooping.....	96
DHCP binding table.....	97
Static DHCP binding table entries.....	97
Externally saving the DHCP Snooping binding table file.....	97
DHCP snooping configuration and management.....	98
DHCP snooping Global Configuration.....	98
DHCP Option 82.....	98
Dynamic ARP inspection.....	99
IP Source Guard.....	99
Avaya Identity Engines Ignition Server.....	101
Trace feature.....	102
Syslog events for 802.1x/NEAP.....	102
Summary of security features.....	103
Chapter 4: Security configuration and management using ACLI.....	109
Setting user access limitations.....	109
USB port and serial console port control using ACLI.....	109
Disabling serial console ports using ACLI.....	109
Enabling serial console ports using ACLI.....	110
Viewing serial console port status using ACLI.....	111
Disabling USB ports using ACLI.....	112

Enabling USB ports using ACLI.....	113
Viewing USB port status using ACLI.....	114
HTTP/HTTPS port configuration using ACLI.....	114
Setting the switch HTTP port using ACLI.....	115
Restoring the switch HTTP port to default using ACLI.....	115
Displaying the switch HTTP port value using ACLI.....	116
Restoring the switch HTTPS port to default using ACLI.....	116
Restoring the switch HTTPS port to default using ACLI.....	117
Displaying the switch HTTP port value using ACLI.....	117
Configuring MAC address-based security.....	117
ACLI commands for MAC address security.....	118
ACLI commands for MAC address autolearning.....	124
RADIUS authentication configuration using ACLI.....	127
Configuring switch RADIUS server settings using ACLI.....	127
Enabling or disabling RADIUS password fallback using ACLI.....	129
Viewing RADIUS information using ACLI.....	130
Configuring RADIUS server reachability using ACLI.....	130
Viewing the RADIUS server reachability method using ACLI.....	131
Configuring EAPOL security.....	132
eapol command.....	132
eapol command for modifying parameters.....	132
show eapol command.....	134
show eapol multihost status command.....	134
Resetting all EAP settings.....	135
Enabling or disabling Non-EAP client re-authentication using ACLI.....	136
Viewing the non-EAP client re-authentication status using ACLI.....	136
Clearing non-EAP authenticated clients from ports using ACLI.....	137
Configuring features.....	138
no eapol multihost use radius-assigned-vlan command.....	138
802.1X or non-EAP Last Assigned RADIUS VLAN configuration using ACLI.....	139
Enabling use-most-recent-RADIUS assigned VLAN.....	140
Disabling use-most-recent-RADIUS assigned VLAN.....	140
Restoring use-most-recent-RADIUS assigned VLAN.....	141
Selecting the packet mode for EAP requests.....	141
EAPOL User Based Policy Configuration using ACLI.....	143
Enabling EAPOL User Based Policy.....	144
Disabling EAPOL User Based Policies.....	144
Setting EAPOL User Based Policy as Default.....	145
Configuring guest VLANs.....	145
eapol guest-vlan command.....	145
no eapol guest-vlan command.....	146
default eapol guest-vlan command.....	146
802.1X or non-EAP and Guest VLAN on the same port configuration using ACLI.....	147
Enabling EAPOL VoIP VLAN.....	147
Disabling EAPOL VoIP VLAN.....	147
Configuring EAPOL VoIP VLAN as the default VLAN.....	148
Displaying EAPOL VoIP VLAN.....	149

Multihost Non-EAP User Based Policy Configuration using ACLI.....	149
802.1X or non-EAP with Fail Open VLAN configuration using ACLI.....	151
Enabling EAPOL Fail Open VLAN.....	151
Disabling EAPOL Fail Open VLAN.....	152
Setting EAPOL Fail Open VLAN as the default.....	153
Displaying EAPOL Fail Open VLAN.....	153
Fail Open VLAN Continuity mode configuration using ACLI.....	154
Enabling EAPOL Fail Open VLAN Continuity mode.....	154
Disabling EAPOL Fail Open VLAN Continuity mode.....	154
Displaying EAPOL Fail Open VLAN Continuity mode.....	155
Configuring multihost support.....	155
eapol multihost command.....	155
no eapol multihost command.....	157
default eapol multihost command.....	157
eapol multihost enable command.....	158
no eapol multihost enable command.....	159
eapol multihost eap-mac-max command.....	160
Setting the maximum number of clients allowed per port.....	160
eapol multihost use radius-assigned-vlan command.....	161
Configuring support for non-EAPOL hosts on EAPOL-enabled ports.....	162
Enabling local authentication of non EAPOL hosts on EAPOL-enabled ports.....	163
Enabling RADIUS authentication of non EAPOL hosts on EAPOL-enabled ports.....	163
Configuring the format of the RADIUS password attribute when authenticating non-EAP MAC addresses using RADIUS.....	164
Setting the configurable key for RADIUS NEAP password.....	165
Related RADIUS NEAP password commands.....	166
Enabling RADIUS-assigned VLAN for non-EAP MACs.....	166
Disabling RADIUS-assigned VLAN for non-EAP MACs.....	167
Specifying the maximum number of non EAPOL hosts allowed.....	168
Creating the allowed non EAPOL MAC address list.....	168
Viewing non EAPOL host settings and activity.....	169
Configuring EAP and non-EAP multiple VLAN capability.....	171
Viewing EAP and non-EAP multiple VLAN capability status.....	171
Using the EAP and NEAP separation command.....	172
802.1X dynamic authorization extension (RFC 3576) configuration using ACLI.....	172
Configuring 802.1X dynamic authorization extension (RFC 3576) using ACLI.....	172
Disabling 802.1X dynamic authorization extension (RFC 3576) using ACLI.....	174
Viewing 802.1X dynamic authorization extension (RFC 3576) configuration using ACLI.....	174
Viewing 802.1X dynamic authorization extension (RFC 3576) statistics using ACLI.....	175
Enabling 802.1X dynamic authorization extension (RFC 3576) on EAP ports using ACLI.....	176
Disabling 802.1X dynamic authorization extension (RFC 3576) on EAP ports using ACLI.....	177
Enabling 802.1X dynamic authorization extension (RFC 3576) default on EAP ports using ACLI..	177
Configuring Wake on LAN with simultaneous 802.1X Authentication using ACLI.....	178
Enabling Avaya IP Phone clients on an EAP-enabled port.....	180
Globally enabling Avaya IP Phone clients as a non-EAP type.....	180
Enabling Avaya IP Phone clients in the interface mode.....	181
Configuring MHSA.....	182
Globally enabling support for MHSA.....	183

Configuring interface and port settings for MHSAs.....	183
Viewing MHSAs settings and activity.....	184
Setting SNMP v1, v2c, v3 Parameters.....	184
SNMPv3 table entries stored in NVRAM.....	185
Configuring SNMP using ACLI.....	185
show snmp-server command.....	186
snmp-server authentication-trap command.....	187
no snmp-server authentication-trap command.....	187
default snmp-server authentication-trap command.....	187
snmp-server community for read or write command.....	188
snmp-server community command.....	188
no snmp-server community command.....	189
default snmp-server community command.....	190
snmp-server contact command.....	191
no snmp-server contact command.....	191
default snmp-server contact command.....	191
snmp-server command.....	192
no snmp-server command.....	192
snmp-server host command.....	192
no snmp-server host command.....	194
default snmp-server host command.....	195
default snmp-server port.....	195
snmp-server location command.....	196
no snmp-server location command.....	196
default snmp-server location command.....	196
snmp-server name command.....	197
no snmp-server name command.....	197
default snmp-server name command.....	197
Enabling SNMP server notification control using ACLI.....	198
Disabling SNMP server notification control using ACLI.....	198
Setting SNMP server notification control to default using ACLI.....	199
Viewing the SNMP server notification control table using ACLI.....	199
snmp-server user command.....	200
no snmp-server user command.....	202
snmp-server view command.....	202
no snmp-server view command.....	203
snmp-server host for old-style table command.....	204
snmp-server host for new-style table command.....	204
snmp-server bootstrap command.....	205
RADIUS accounting configuration using ACLI.....	206
Enabling RADIUS server accounting using ACLI.....	207
Disabling RADIUS server accounting using ACLI.....	207
Configuring RADIUS interim accounting updates using ACLI.....	209
Disabling RADIUS interim accounting updates using ACLI.....	210
Configuring RADIUS interim accounting updates to default using ACLI.....	210
Viewing RADIUS interim accounting updates information using ACLI.....	211
TACACS+ configuration using ACLI.....	212

Configuring switch TACACS+ server settings using ACLI.....	212
Disabling switch TACACS+ server settings using ACLI.....	213
Enabling remote TACACS+ services using ACLI.....	214
Enabling or disabling TACACS+ authorization using ACLI.....	215
Configuring TACACS+ authorization privilege levels using ACLI.....	215
Enabling or disabling TACACS+ accounting using ACLI.....	216
Configuring the switch TACACS+ level using ACLI.....	216
Viewing TACACS+ information using ACLI.....	217
Configuring IP Manager.....	218
Enabling IP Manager.....	218
Configuring the IP Manager list.....	218
Removing IP Manager list entries.....	219
Viewing IP Manager settings.....	219
Setting the user name and password.....	220
username command.....	220
Setting the system user to default using ACLI.....	221
Setting ACLI password.....	221
cli password command.....	221
Viewing the user name and password configuration using ACLI.....	223
Configuring password security.....	224
password security command.....	224
no password security command.....	224
Configuring the number of retries.....	224
Password history configuration using ACLI.....	225
Configuring password history using ACLI.....	225
Configuring password history to default using ACLI.....	225
Viewing password history using ACLI.....	226
ACLI Audit log configuration.....	226
Displaying ACLI audit log.....	226
Enabling and disabling ACLI audit log.....	227
Configuring ACLI audit log to default.....	228
Clearing the ACLI audit log.....	228
Preventing erasure of the ACLI audit log.....	229
Secure Socket Layer services.....	230
Configuring the Web server for client browser requests using ACLI.....	231
Viewing the Web server client browser request configuration using ACLI.....	232
Secure Shell protocol configuration using ACLI.....	232
Displaying SSH information using ACLI.....	232
Enabling SSH using ACLI.....	234
Disabling SSH using ACLI.....	234
Generating a new SSH DSA host key using ACLI.....	235
Deleting the SSH DSA host key using ACLI.....	235
Generating a new SSH RSA host key using ACLI.....	235
Deleting the SSH RSA host key using ACLI.....	235
Downloading DSA or RSA authentication keys using ACLI.....	236
Deleting the SSH DSA authentication key using ACLI.....	236
Deleting the SSH RSA authentication key using ACLI.....	237

Enabling user log-on with an SSH DSA key using ACLI.....	237
Disabling user log-on with an SSH DSA key using ACLI.....	237
Enabling user log-on with an SSH RSA key using ACLI.....	238
Disabling user log-on with an SSH RSA key using ACLI.....	238
Enabling user log-on with SSH password authentication using ACLI.....	238
Disabling user log-on with SSH password authentication using ACLI.....	239
Disabling SNMP and Telnet With SSH using ACLI.....	239
Setting the TCP port for SSH daemon using ACLI.....	240
Setting the default TCP port for the SSH daemon using ACLI.....	240
Setting the SSH timeout using ACLI.....	240
Setting the SSH timeout to default using ACLI.....	241
Secure Shell Client configuration using ACLI.....	241
Configuring SFTP authentication for SSH Client using ACLI.....	242
Setting SFTP authentication for SSH Client to default using ACLI.....	242
Closing an SSH Client session using ACLI.....	243
Generating an SSH client DSA host key using ACLI.....	243
Deleting DSA host keys using ACLI.....	244
Generating an SSH client RSA host key using ACLI.....	244
Deleting RSA host keys using ACLI.....	245
Connecting SSH to a host using ACLI.....	245
Displaying current SSH client sessions.....	246
Displaying SSH client known hosts.....	247
Clearing SSH Client known hosts using ACLI.....	247
Configuration examples for configuring Secure Shell connections.....	248
DHCP snooping configuration using ACLI.....	249
Configuring DHCP snooping globally using ACLI.....	249
Viewing the global DHCP snooping configuration ACLI.....	250
Configuring VLAN-based DHCP snooping using ACLI.....	251
Viewing the VLAN-based DHCP snooping configuration using ACLI.....	252
Configuring port-based DHCP snooping using ACLI.....	252
Viewing the port-based DHCP snooping configuration using ACLI.....	253
Adding static entries to the DHCP binding table using ACLI.....	254
Deleting static entries from the DHCP binding table using ACLI.....	255
Viewing the DHCP binding table using ACLI.....	255
Configuring DHCP Snooping external save using ACLI.....	256
Configuring DHCP Snooping external save to an SFTP server.....	257
Disabling DHCP Snooping external save using ACLI.....	258
Restoring the externally saved DHCP Snooping database using ACLI.....	258
Restoring the externally saved DHCP Snooping database from an SFTP server.....	258
Viewing DHCP Snooping external save information using ACLI.....	259
DHCP Snooping layer 2 configuration using ACLI example.....	259
Configuring dynamic ARP inspection.....	262
Enabling dynamic ARP inspection on the VLANs.....	263
Configuring trusted and untrusted ports.....	263
Viewing dynamic ARP inspection settings.....	264
Dynamic ARP inspection layer 2 configuration example.....	264
IP Source Guard configuration using ACLI.....	267

Enabling IP Source Guard using ACLI.....	268
Viewing IP Source Guard port configuration information using ACLI.....	268
Viewing IP Source Guard-allowed addresses using ACLI.....	269
Disabling IP Source Guard using ACLI.....	270
Configuring the trace feature using ACLI.....	271
Displaying trace information using ACLI.....	271
Configuring trace using ACLI.....	271
Disabling trace using ACLI.....	272
RADIUS Request use Management IP configuration using ACLI.....	273
Enabling the RADIUS Request use Management IP.....	273
Disabling the RADIUS Request use Management IP.....	273
Setting the RADIUS Request use Management IP to default mode.....	274
Chapter 5: Ignition Server configuration using ACLI.....	275
Configuring Ignition Server as a RADIUS server using ACLI.....	275
Configuring Ignition Server as an EAP RADIUS server using ACLI.....	278
Configuring Ignition Server as a non-EAP RADIUS server using ACLI.....	280
Configuring Ignition Server as a TACACS+ server using ACLI.....	283
Chapter 6: Security configuration and management using Enterprise Device Manager	285
EAPOL configuration using EDM.....	285
Configuring EAPOL globally using EDM.....	285
Configuring port-based EAPOL using EDM.....	288
Configuring advanced port-based EAPOL using EDM.....	289
Graphing port EAPOL statistics using EDM.....	292
Graphing port EAPOL diagnostics using EDM.....	293
Viewing Multihost status information using EDM.....	295
Viewing Multihost session information using EDM.....	296
Allowed non-EAP MAC address list configuration using EDM.....	297
Viewing port non-EAP host support status using EDM.....	299
Enabling VoIP VLAN using EDM.....	300
Setting the switch HTTP/HTTPS port using EDM.....	301
Configuring general switch security using EDM.....	302
Security list configuration using EDM.....	304
AuthConfig list configuration using EDM.....	307
Configuring MAC Address AutoLearn using EDM.....	309
Viewing AuthStatus information using EDM.....	310
Viewing AuthViolation information using EDM.....	312
Viewing MacViolation information using EDM.....	313
Configuring Secure Shell protocol using EDM.....	314
Viewing SSH Sessions information using EDM.....	316
Configuring an SSH Client using EDM.....	317
Configuring SSL using EDM.....	319
Configuring RADIUS globally using EDM.....	320
Configuring the Global RADIUS Server using EDM.....	323
Configuring the EAP RADIUS server using EDM.....	325
Configuring the NEAP RADIUS server using EDM.....	327
Viewing RADIUS Dynamic Authorization server information using EDM.....	329
Creating an 802.1X dynamic authorization extension (RFC 3576) client using EDM.....	330

Viewing RADIUS Dynamic Server statistics using EDM.....	334
Graphing RADIUS Dynamic Server statistics using EDM.....	335
DHCP snooping configuration using EDM.....	336
Configuring global DHCP snooping using EDM.....	336
Configuring DHCP snooping on a VLAN using EDM.....	339
Configuring DHCP snooping on a port using EDM.....	340
DHCP binding configuration using EDM.....	341
Viewing DHCP binding information using EDM.....	341
Creating static DHCP binding table entries using EDM.....	342
Deleting DHCP binding table entries using EDM.....	343
Configuring dynamic ARP inspection on VLANs using EDM.....	344
Configuring dynamic ARP inspection on ports using EDM.....	345
IP Source Guard configuration using EDM.....	345
Configuring IP Source Guard on a port using EDM.....	346
Configuring IP Source Guard on multiple ports using EDM.....	347
Filtering IP Source Guard addresses using EDM.....	348
Viewing IP Source Guard port statistics using EDM.....	349
TACACS+ configuration using EDM.....	350
Configuring the Web and Telnet password using EDM.....	352
Configuring the console password using EDM.....	353
SNMP configuration using EDM.....	355
Viewing the SNMP configuration using EDM.....	355
Creating a user using EDM.....	356
Viewing the user details using EDM.....	357
Viewing MIBs assigned to an object using EDM.....	358
Creating a community using EDM.....	359
Viewing the details of a community using EDM.....	360
Configuring an SNMP host using EDM.....	360
Configuring notifications (traps) from the list using EDM.....	361
Configuring SNMP notification control using EDM.....	362
Graphing SNMP statistics using EDM.....	363
Chapter 7: Ignition Server configuration using Enterprise Device Manager.....	367
Configuring Ignition Servers as a RADIUS server using EDM.....	367
Configuring Ignition Server as an EAP RADIUS server using EDM.....	371
Configuring Ignition Server as a non-EAP RADIUS server using EDM.....	375
Configuring Ignition Server as a TACACS+ server using EDM.....	379
Appendix A: TACACS+ server configuration examples and supported SNMP MIBs...	381
TACACS+ server configuration examples.....	381
Configuration example: Cisco ACS (version 3.2) server.....	381
Configuration example: ClearBox server.....	386
Configuration example: Linux freeware server.....	392
Supported SNMP MIBs and traps.....	393
Supported MIBs.....	393
Supported traps.....	396
Appendix B: Supported EAP modes and configuration examples.....	399
SHSA authentication mode with or without RADIUS additional attributes with or without Multihost MultiVLAN.....	399

SHSA authentication mode (with Guest VLAN enabled) with or without RADIUS additional attributes, with or without Multihost MultiVLAN.....	405
SHSA authentication mode (with Guest VLAN and Fail Open VLAN enabled) with or without RADIUS additional attributes with or without Multihost MultiVLAN.....	412
MHSA authentication mode (with or without RADIUS VLAN and with or without Multihost MultiVLAN enabled).....	421
MHSA authentication mode (Guest VLAN option enabled) with or without RADIUS additional attributes with or without Multihost MultiVLAN.....	427
MHSA authentication mode (Guest VLAN and Fail Open VLAN options enabled) with or without RADIUS additional attributes and with or without Multihost MultiVLAN option.....	434
MHMA authentication mode (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes.....	443
MHMA authentication mode (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes.....	457
MHMA authentication mode with Guest VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes.....	472
MHMA authentication mode with Guest VLAN (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes.....	486
MHMA authentication mode with Guest VLAN and Fail Open VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes.....	500
Appendix C: Sticky MAC address configuration examples.....	519
Glossary.....	523

Chapter 1: Introduction

Purpose

This document describes security features and how to configure security services for the Avaya Ethernet Routing Switch 4000.

Related resources

Documentation

For a list of the documentation for this product, see *Documentation Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205–101.

Training

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

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

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

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to <http://www.youtube.com/AvayaMentor> and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Searching a document collection

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

Before you begin

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

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named *<product_name_release>.pdx*, for example, *ers4000_5.7x.pdx*.
3. In the Search dialog box, select the option **In the index named *<product_name_release>.pdx***.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
 - Whole words only
 - Case-Sensitive
 - Include Bookmarks
 - Include Comments
6. Click **Search**.

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

Support

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

Chapter 2: New in this release

The following section details what is new in *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505 for Release 5.7.

Features

See the following sections for information about feature changes.

802.1X-2004 support

With the 802.1x-2004 standard the switch can authenticate both EAPOL version 1 and EAPOL version 2 supplicants.

For more information, see [Advanced EAPOL features](#) on page 52

Block subsequent MAC authentication

Prior to Release 5.7, in Multiple Host with Multiple Authentication (MHMA) mode, if a station successfully authenticates, the switch places the port in the RADIUS-assigned VLAN that corresponds to the login credentials of that station. If a second station properly authenticates on that same port, the switch ignores the RADIUS-assigned VLAN and the user is placed in the same VLAN as the first successfully authenticated station, creating a potential security risk. This feature enhancement gives the administrator the option of either using the current implementation or a separate option that blocks subsequent MAC authentications if the RADIUS-assigned VLAN is different than the first authorized station VLAN.

For more information, see

- [Block subsequent MAC authentication](#) on page 33
- [Enabling or disabling block subsequent MAC authentication using ACLI](#) on page 123
- [Configuring EAPOL globally using EDM](#) on page 285

Change RADIUS Password

You can allow the users to change RADIUS account passwords when they expire.

 **Note:**

Change RADIUS password is available only in secure software builds.

You can enable or disable the Change RADIUS password feature. By default, this feature is disabled. When Change RADIUS password feature is enabled, the server reports the password expiry and system prompts you to create a new password.

For more information about the Change RADIUS password, see the following:

- [Change RADIUS password](#) on page 36
- [Configuring switch RADIUS server settings using ACLI](#) on page 127
- [Configuring RADIUS globally using EDM](#) on page 320

Default all EAP settings command

Use the default eap-all command to reset all EAP settings.

For more information, see

- [Resetting all EAP settings](#) on page 135
- [Configuring EAPOL globally using EDM](#) on page 285

EAP-MD5 authentication

With EAP-MD5 authentication, the RADIUS NEAP password is set with MD5 based encryption.

For more information, see [Non-EAPOL MAC RADIUS authentication](#) on page 64

EAP and NEAP separation

Use the EAP/ NEAP separation command to disable EAP clients without disabling NEAP clients.

For more information, see

- [Using the EAP and NEAP separation command](#) on page 172
- [Configuring EAPOL globally using EDM](#) on page 285

eapol multihost mac-max command

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

For more information, see

- [eapol multihost command](#) on page 155
- [Setting the maximum number of clients allowed per port](#) on page 160
- [Configuring advanced port-based EAPOL using EDM](#) on page 289

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(s) become unreachable.

For more information, see

- [Fail Open VLAN Continuity mode configuration using ACLI](#) on page 154
- [Enabling EAPOL Fail Open VLAN Continuity mode](#) on page 154
- [Disabling EAPOL Fail Open VLAN Continuity mode](#) on page 154
- [Displaying EAPOL Fail Open VLAN](#) on page 153
- [Configuring EAPOL globally using EDM](#) on page 285

MAC Security Port Lockout

Use the MAC Security Port Lockout feature to exclude specific ports from MAC-based security. Use this feature to simplify switch operations and prevent accidental loss of network connectivity caused by improper MAC security settings.

For more information, see

- [mac-security command for specific ports](#) on page 122
- [show mac-security port command](#) on page 122
- [Configuring general switch security using EDM](#) on page 302

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.

For more information, see [NEAP Not Member of VLAN](#) on page 67

Password change through EDM

This feature provides the ability to change the switch password through EDM. This capability must be enabled if the switch is running on HTTPS or secure image.

For more information, see [Configuring the Web and Telnet password using EDM](#) on page 352.

RADIUS NEAP password configurable key

From release 5.7 onwards, the RADIUS NEAP password includes a configurable key string in addition to IP address, MAC address, and port number.

For more information, see

- [Setting the configurable key for RADIUS NEAP password](#) on page 165
- [Related RADIUS NEAP password commands](#) on page 166
- [Configuring EAPOL globally using EDM](#) on page 285

RO User access to SSH

You can access SSH commands with read-only permissions. In previous software releases you could access SSH commands only with read-write permissions.

For more information, see [Connecting SSH to a host using ACLI](#) on page 245

SFTP DHCP external save file support

Use the SFTP DHCP external save file support feature to transfer DHCP external save files to switch or from switch using SFTP.

For more information, see

- [Configuring DHCP Snooping external save to a SFTP server using ACLI](#) on page 257
- [Restoring the externally saved DHCP Snooping database from an SFTP server](#) on page 258

Syslog Support for 802.1X/EAP/NEAP/UBP

Syslog messages for the various states of 802.1X/EAP/NEAP/UBP authentications are introduced to allow more thorough troubleshooting.

Logged messages include:

- time of authentication
- MAC authentication success/failure
- IP address associated with MAC authentication
- VLAN and UBP policy assignment

For more information, see [Syslog events for 802.1x NEAP](#) on page 102

Trace feature

The trace feature is a troubleshooting feature that provides detailed information about errors and events on the device. Use this feature to understand the cause of an error and take action to resolve it.

For more information, see

- [Trace feature](#) on page 102
- [Configuring the trace feature using ACLI](#) on page 271
- [Displaying trace information using ACLI](#) on page 271
- [Configuring trace using ACLI](#) on page 271
- [Disabling trace using ACLI](#) on page 272

User Based Policies

You can configure the Ethernet Routing Switch 4000 Series to manage access with User Based Policies (UBP). UBP revolves around the User Policy Table supporting multiple users for each interface. User data is provided through interaction with Extensible Authentication Protocol (EAP) and is maintained in the User Policy Table.

UBP processing occurs only during the authentication phase when the EAP sends the user information to the configured RADIUS server. Clients that do not support EAP can be authenticated based on their MAC address.

For more information about the ACLI and EDM configurations, see the following:

- [EAPOL User Based Policy Configuration using ACLI](#) on page 143
- [Configuring advanced port-based EAPOL using EDM](#) on page 289
- [Configuring EAPOL globally using EDM](#) on page 285

Other Changes

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

New Introduction chapter

The Introduction chapter replaces the Purpose of this document and Customer service chapters.

SNMP Traps

The following traps are updated:

- s5EtrMacAddressTablesThresholdReached
- s5CtrFanDirectionError
- s5CtrHighTemperatureError
- bspelpPhonePowerLimitNotification
- bspelpPhonePowerPriorityNotification
- bsveVrrpTrapStateTransition
- bsDhcpSnoopingExtSaveEntryInvalidVlan
- bsRadiusReachabilityServerDown
- bsRadiusReachabilityServerUp
- bsnesGloballyEnabled
- bsnesGloballyDisabled
- bsnesManuallyActivated
- bsnesManuallyDeactivated
- bsnesScheduleNotApplied
- bsnesScheduleApplied
- bsnesActivated
- bsnesDeactivated

- bsLstInterfaceStatusChanged
- bsLstGroupOperStateChanged
- bsnStackConfigurationError
- bsnSystemUp365Days
- bsnUSBInsertion
- bsnUSBRemoval
- bsnSFPInsertion
- bsnSFPRemoval
- bsnROPASSWORDExpired
- bsnRWPASSWORDExpired
- vrrpTrapNewMaster
- ntnQosPolicyEvolLocalUbpSessionFailure
- slaMonitorAgentExceptionDetected
- rcnBpduReceived
- rcnIIsisPlsbMetricMismatchTrap
- rcnIIsisPlsbDuplicateSysidTrap
- rcnIIsisPlsbLsdbUpdateTrap
- rcnIIsisPlsbBvidMismatchTrap
- rcnIIsisPlsbAdjStateTrap
- rcnIIsisPlsbDuplicateNnameTrap
- rcnIIsisPlsbMultiLinkAdjTrap
- rcnSlppGuardHoldDownExpired
- rcnSlppGuardPacketReceived
- ubpEAPSessionStart
- ubpEAPSessionEnd

HTTP/HTTPS Port Configuration

The HTTP/HTTPS port configuration information is documented in this release.

New in this release

Chapter 3: Security fundamentals

This chapter describes the hardware-based and software-based security features supported by the Avaya Ethernet Routing Switch 4000.

ACL I command modes

ACL I provides the following command modes:

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

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

If no password is set, you can enter ACL I 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: ACL I command modes

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC 4548GT-PWR>	No entrance command, default mode	exit or logout
Privileged EXEC 4548GT-PWR#	enable	exit or logout
Global Configuration 4548GT-PWR(config)#	configure terminal	mode, enter: end

Command mode and sample prompt	Entrance commands	Exit commands
		or exit To exit ACLI completely, enter: logout
Interface Configuration 4548GT-PWR(config-if)# You can configure the following interfaces: <ul style="list-style-type: none"> • Ethernet • VLAN 	From Global Configuration mode: To configure a port, enter: interface ethernet <port number> To configure a VLAN, enter: interface vlan <vlan number>	To return to Global Configuration mode, enter: Exit To return to Privileged EXEC mode, enter: end To exit ACLI completely, enter: logout
Router Configuration 4548GT-(configrouter)# You can configure the following routers: <ul style="list-style-type: none"> • RIP • OSPF • VRRP • ISIS 	From Global or Interface Configuration mode: To configure RIP, enter router rip. To configure OSPF, enter router ospf. To configure VRRP, enter router vrrp. To configure IS-IS, enter router isis.	To return to Global Configuration mode, enter exit. To return to Privileged EXEC mode, enter end. To exit ACLI completely, enter logout.
Application Configuration 4850GT-(config-app)	From Global, Interface or Router Configuration mode, enter application.	To return to Global Configuration mode, enter exit. To return to Privileged EXEC mode, enter end. To exit ACLI completely, enter logout.

Hardware-based security

Network administrators enable or disable the USB or serial console ports on the Avaya Ethernet Routing Switch 4000 to control access to an operational switch. To prevent unauthorized access and configuration, the network administrators disable the USB or serial console ports.

HTTP/HTTPS port configuration

The Web server can operate in either HTTPS (secure) mode or HTTP (non-secure) mode, with HTTPS as the default mode. You can select the Web server mode with the ACLI and SNMP management interfaces. The SSL Management Library interacts with the Web server in selecting these modes.

In secure mode, you can use the **SecureOnly** option to configure the Web server to respond to HTTPS only, or both HTTPS and HTTP client browser requests. If you configure the Web server to respond to HTTPS client browser requests only, all existing non-secure connections with the browser are terminated.

By default, the Web server listens on TCP port 443 for HTTPS client browser requests, and listens on TCP port 80 for HTTP client browser requests. You can designate alternate TCP ports, ranging in value from 1024 to 65535, for HTTPS and HTTP client browser requests.

 **Note:**

The TCP port for HTTPS client browser requests and the TCP port for HTTP client browser requests cannot be the same value.

In non-secure mode, the Web server responds to HTTP client browser requests only. All existing secure connections with the browser are terminated.

MAC address-based security

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

You can use the MAC-address-based security feature to set up network access control based on source MAC addresses of authorized stations.

You can use MAC-address-based security to perform the following activities:

- Create a list of up to 10 MAC addresses to filter
 - as destination addresses (DA)—all packets with one of the specified MAC addresses as the DAs are dropped regardless of the ingress port, source address intrusion, or virtual local area network (VLAN) membership
 - as source addresses (SA)—all packets with one of the specified MAC addresses as the SAs are dropped

! Important:

Ensure that you do not enter the MAC address of units in the stack using MAC security. This can impact operation of switch management or the stack.

- Create a list of up to 448 MAC SAs and specify SAs that are authorized to connect to the switch or stack configuration.

You can configure the 448 MAC SAs within a single stand-alone or distribute them in any order among the units in a single stack configuration.

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

- Switch ports that can be controlled for each MAC address security association.

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

- Optional actions that the switch can perform if the software detects a source MAC address security violation.

The options are to send an SNMP trap, turn on DA filtering for the specified source MAC address, disable the specific port, or a combination of these three options.

Use either the Avaya Command Line Interface (ACLI) or Enterprise Device Manager (EDM) to configure MAC-address based security features.

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 has the following features:

- You can specify the number of addresses that can be learned 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. They are dynamically learned by the switch.
- You can reset the MAC address table for a port by disabling the security on the port and then 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 is or is not 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.

MAC Security Port Lockout

Use the MAC Security Port Lockout feature to exclude specific ports from MAC-based security. Use this feature to simplify switch operations and prevent accidental loss of network connectivity caused by improper MAC security settings.

For more information, see

- [mac-security command for specific ports](#) on page 122
- [show mac-security port command](#) on page 122
- [Configuring general switch security using EDM](#) on page 302

Block subsequent MAC authentication

Prior to Release 5.7, in MHMA mode, if a station successfully authenticates, the switch places the port in the RADIUS-assigned VLAN that corresponds to that station's login credentials. If a second station properly authenticates on that same port, the switch ignores the RADIUS-assigned VLAN and the user is placed in the same VLAN as the first successfully authenticated station, creating a potential security risk. This feature enhancement gives the administrator the option of either using the current implementation or a separate option that will block subsequent MAC authentications if the RADIUS-assigned VLAN is different than the first authorized station's VLAN.

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.

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.

RADIUS-based network security

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

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

How RADIUS works

A RADIUS application has two components:

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

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

Avaya recommends that you configure two RADIUS servers so that if one server is unreachable, the switch will attempt authentication using the secondary server. If a specific RADIUS server does not respond to a certain request, the switch retries the request a maximum of five times, which is the retry limit. The default retry value is three times. To prevent

false retries, you can configure the interval between retries up to 60 seconds, based on network requirements. The default retry interval is 2 seconds.

RADIUS server configuration

You must set up specific user accounts on the RADIUS server before you can use RADIUS authentication in the Avaya Ethernet Routing Switch 4000 Series network. User account information about the RADIUS server contains user names, passwords, and service-type attributes.

Provide each user with the appropriate level of access.

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

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

Change the RADIUS Password

The remote users can change their account passwords when RADIUS server is configured and enabled in their network.

 **Note:**

Change RADIUS password is available only in secure software builds.

When RADIUS servers are configured in a network, they provide centralized authentication, authorization, and accounting for network access. The MS-CHAPv2 encapsulation method can be enabled to permit RADIUS password change for the user accounts.

Change RADIUS password is disabled by default.

When the RADIUS encapsulation MS-CHAPv2 is enabled and if an account password expires, the RADIUS server reports the password expiry during the next log on attempt and the system prompts you to create a new password. You can also change the password before the password expire using ACLI.

The following configurations are required to change RADIUS password:

- at least one configured and reachable RADIUS server in your network
- configured RADIUS encapsulation MS-CHAPv2

Change RADIUS password is compatible with RADIUS password fallback.

Settings for the change RADIUS password feature are saved in both the binary and ASCII configuration files.

Effects of software upgrade on RADIUS settings:

The RADIUS password settings are saved in NVRAM and are available after an upgrade.

Effects of software downgrade on RADIUS settings:

The RADIUS password setting is disabled if a release with this feature is downgraded.

RADIUS server reachability

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

If you implement internal firewalls which limit the flow of ICMP reachability messages from the switch to the RADIUS server, you can configure the switch to use dummy RADIUS requests. If the switch is configured to use dummy RADIUS requests, the switch generates a regular dummy RADIUS request with the username 'avaya'. It is recommended that you set up a dummy account with the user name **avaya** on the RADIUS server to avoid the generation of error messages indicating invalid user logins, if RADIUS server reachability is enabled.

If the `use-radius` option is configured, the username and password for the dummy RADIUS packet can also be configured via ACLI.

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

RADIUS EAP or non-EAP requests from 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 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.

 **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:**

Because SHSA and MHSA modes do not support the authentication of Non-EAP clients, ports in SHSA or MHSA mode do not use Non-EAP RADIUS servers for authentication.

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 re-authentication.
- 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 re-authentication.
- If only Global RADIUS servers are configured, all EAP clients are authenticated using a Global RADIUS server (primary or secondary). If both primary and secondary Global

RADIUS servers become unavailable, the EAP clients remain authenticated until the next re-authentication.

Non-EAP clients

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

Examples of RADIUS servers with MHMA mode

The following diagram illustrates a network that includes the following:

- an ERS 4000 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

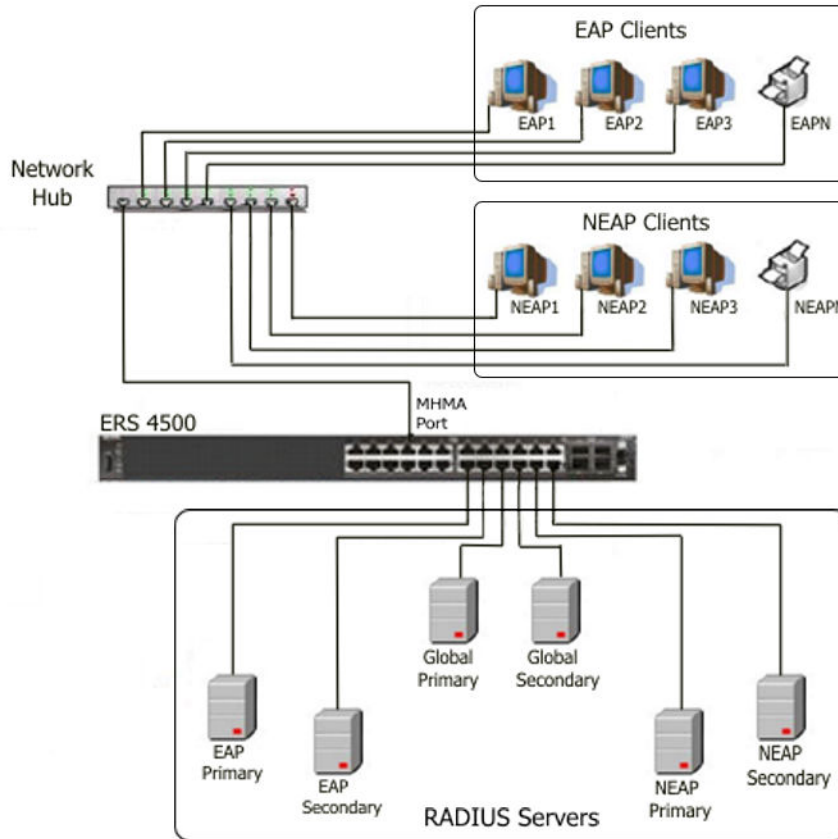


Figure 1: EAP and non-EAP RADIUS servers in MHMA mode

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 re-authenticate 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 re-authenticate 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.

Interaction with other features

The following sections describe how the RADIUS EAP or non-EAP requests from different servers feature interacts with other features.

Interaction with RADIUS server reachability

When you use the RADIUS EAP or non-EAP requests from different servers feature, the method you use to determine RADIUS server reachability, ICMP or dummy RADIUS requests, applies equally to either Global RADIUS servers, EAP RADIUS servers, or NEAP RADIUS servers.

Interaction with Fail Open VLAN and Multivlan

In software releases prior to Release 5.5, Fail Open VLAN and Multivlan were mutually exclusive when interacting with other features. With the introduction of RADIUS EAP or non-EAP requests from different servers in Release 5.5, this behavior is changed as described in this section.

When you configure Global RADIUS servers, EAP RADIUS servers, or non-EAP RADIUS servers, and a switch port cannot connect to the RADIUS servers, the system moves the port to the designated Fail Open VLAN.

When the RADIUS servers are unreachable, the different RADIUS servers feature interacts with Fail Open VLAN to provide some restricted access, independent of the Guest VLAN, when Fail Open VLAN is enabled.

EAP clients authenticate on the EAP RADIUS servers. If EAP RADIUS servers are not configured, EAP clients authenticate on the Global RADIUS server.

NEAP clients authenticate on the NEAP RADIUS servers. If NEAP RADIUS servers are not configured, NEAP clients authenticate on the Global RADIUS server.

EAP or NEAP Multivlan is disabled or not implemented

This section describes RADIUS server interaction with Fail Open VLAN when you disable or do not implement EAP or NEAP Multivlan.

- If you configure either EAP or NEAP RADIUS servers, when the RADIUS server becomes unreachable, the system moves the port to the Fail Open VLAN .
- If you configure both EAP and NEAP RADIUS servers, only when both RADIUS servers become unreachable does the port move to the Fail Open VLAN . Otherwise, port membership does not change.
- If you configure EAP and Global RADIUS servers, only when both RADIUS servers become unreachable does the port move to Fail Open VLAN .
- If you configure NEAP and Global RADIUS servers, only when both RADIUS servers become unreachable does the port move to Fail Open VLAN .
- If you configure only a Global RADIUS server, only when the RADIUS server becomes unreachable does the port move to Fail Open VLAN .
- If you configure EAP, NEAP, and Global RADIUS servers, only when both EAP and NEAP RADIUS servers become unreachable does the port move to Fail Open VLAN . If only the Global RADIUS server becomes unreachable, the port membership does not change.

EAP or NEAP Multivlan is enabled

When you enable and implement EAP or NEAP Multivlan, and the RADIUS servers are unreachable, the port can be copied to Fail Open VLAN, depending on which RADIUS servers you configured.

EAP RADIUS servers only:

If you configure only EAP RADIUS servers, when the RADIUS servers become unreachable, all EAP-enabled ports are moved to Fail Open VLAN, and no PVID or priority changes occur on those ports. Traffic from authenticated EAP clients goes to the corresponding VLAN (RADIUS assigned VLAN or the initial VLAN), and not the Fail Open Vlan.

If all new MACs learned on the EAP-enabled ports are not authenticated as NEAP clients using other authentication methods, like static MACs or DHCP signature, the new MACs are considered potential EAP clients, and traffic is forwarded to Fail Open VLAN.

If EAP re-authentication is enabled, EAP clients do not re-authenticate while ports are in Fail Open VLAN.

NEAP RADIUS servers only:

If you configure only NEAP RADIUS servers, when the RADIUS servers become unreachable, all EAP-enabled ports are moved to Fail Open VLAN, and no PVID or priority changes occur on those ports. Traffic from authenticated NEAP clients goes to the corresponding VLAN (RADIUS assigned VLAN or the initial VLAN), and not the Fail Open Vlan.

All new MACs learned on the ports are considered potential NEAP clients and traffic is forwarded to Fail Open VLAN, unless the clients are authenticated using NEAP methods that do not require connectivity to RADIUS server, like local MACs or DHCP signature.

If non-EAP re-authentication is enabled, NEAP clients do not re-authenticate while ports are in Fail Open VLAN.

EAP and NEAP RADIUS servers:

If you configure both EAP and NEAP RADIUS servers and the EAP RADIUS servers become unreachable, traffic from authenticated EAP clients goes to the corresponding VLAN. EAP-enabled ports are moved to Fail Open VLAN.

If you configure both EAP and NEAP RADIUS servers and the NEAP RADIUS servers become unreachable, traffic from authenticated NEAP clients goes to the corresponding VLAN. EAP-enabled ports are moved to Fail Open VLAN.

If EAP or non-EAP re-authentication is enabled and the corresponding RADIUS server is not reachable, EAP or NEAP clients do not re-authenticate while ports are in Fail Open VLAN.

All new MACs learned on the port are considered potential EAP or NEAP clients, depending on which RADIUS server becomes unreachable, and traffic is forwarded to Fail Open VLAN, unless the MACs are authenticated using methods like static MACs or DHCP signature. If both EAP and NEAP RADIUS servers recover, EAP-enabled ports are removed from Fail Open VLAN and all authenticated MACs, except NEAP clients authenticated based on DHCP signature, are reauthenticated. All MACs that were not authenticated are flushed from the system to be authenticated.

EAP and Global RADIUS servers:

If you configure EAP and Global RADIUS servers, Global RADIUS servers are not used to authenticate EAP clients if EAP RADIUS servers become unreachable. In this case, Global RADIUS servers are used to authenticate NEAP clients. If either EAP or Global radius servers become unreachable, the behavior is similar to when you configure both EAP and NEAP radius servers.

NEAP and Global RADIUS servers:

If you configure NEAP and Global RADIUS servers, Global RADIUS servers are not used to authenticate NEAP clients if NEAP RADIUS servers become unreachable. In this case, Global RADIUS servers are used to authenticate EAP clients. If either NEAP or Global radius servers become unreachable, the behavior is similar to when you configure both EAP and NEAP radius servers.

EAP, NEAP, and Global RADIUS servers:

If you configure EAP, NEAP, and Global RADIUS servers, the Global RADIUS server does not authenticate EAP clients when EAP RADIUS servers become unreachable, or NEAP clients when NEAP RADIUS servers become unreachable. If either EAP or NEAP radius servers become unreachable, the behavior is similar to when you only configure both EAP and NEAP radius servers.

Global RADIUS server only:

If you configure only a Global RADIUS server, both EAP and NEAP clients are authenticated using the Global RADIUS server.

If the Global RADIUS server becomes unreachable all EAP-enabled and EAP-enabled ports are moved to Fail Open VLAN.

Traffic from all authenticated EAP and NEAP clients goes to the corresponding VLAN.

All new MACs learned on the port are considered potential EAP or NEAP clients and traffic is forwarded to Fail Open VLAN, unless the MACs are authenticated using methods like static MACs or DHCP signature.

When the Global RADIUS server recovers, all EAP-enabled and EAP-enabled ports are removed from Fail Open VLAN. All authenticated clients, except those authenticated by DHCP signature, are reauthenticated. All MACs that were not authenticated are flushed from the system to be authenticated.

 **Note:**

If some MACs are forwarding traffic to a Guest VLAN when a RADIUS server becomes unreachable and the EAP-enabled ports are moved to Fail Open VLAN, those MACs continue to forward traffic to the Guest VLAN.

RADIUS password fallback

With the RADIUS password fallback feature the user can log on to the switch or stack by using the local password, if the RADIUS server is unavailable or unreachable for authentication.

RADIUS password fallback is disabled by default.

Configuring RADIUS authentication

You can configure and manage RADIUS authentication using ACLI or Enterprise Device Manager (EDM).

RADIUS Request use Management IP

When the switch is operating in Layer 2 mode, by default, all RADIUS requests generated by the switch use the stack or switch management IP address as the source address in RADIUS requests or status reports. The RADIUS Request use Management IP configuration has no impact when the switch operates in Layer 2 mode.

When the switch is operating in Layer 3 mode, by default, a RADIUS request uses one of the routing IP addresses on the switch. When the switch is operating in Layer 3 mode, the RADIUS Request use Management 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.

*** Note:**

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 (routing) and RADIUS Request Use Management IP is enabled

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

RADIUS Management Accounting

You can use the RADIUS Management Accounting feature to send radius accounting packets when management events such as user logon or logoff, or session timeout for a logged on user occur. The feature can record management logon activity to the switch. The switch generates an authentication message, to the RADIUS server, which includes basic information such as: NAS-IP-Address, Service-Type, User-Name, Client-IP-Address, and Timestamp.

The RADIUS Management accounting records are generated when the switch is accessed using the console, telnet, SSH, or when a session is disconnected either by logging out or through time-out.

The following table describes the additional information fields in the RADIUS accounting message. This information enhances the interoperability of the switch in environments where other vendors use their switches.

Table 2: RADIUS Management Accounting Records

RADIUS attribute	Definition
NAS-IP-Address	The IP address of the device generating the RADIUS accounting message (the switch or stack IP address).
NAS-IPv6-Address	The IPv6 address of the device generating the RADIUS Accounting message (the switch or stack address).
NAS-Port-Type	The type of port through which the connection is made to the switch, as defined in RFC2865. In case of logon through the console port, the port takes a value of 1, which corresponds to Async or 5 representing Virtual for the network connections.

RADIUS attribute	Definition
NAS-Port	This is equal to the unit number in a stack if the customer uses the console port. If the connection is virtual, Avaya recommends that this value be set to the protocol used to access the switch, for example, IPv4.
Service-Type	Set to Administrative-User for access to the switch or stack with read-write rights. Set to NAS-Prompt-User for access to the switch/stack with read-only rights
User-Name	The user name used to connect the current administrative session to the switch.
Acct-Status-Type	Indicates if this is an accounting Start or Stop record, used to respectively identify connection or disconnection to or from the switch.
Acct-Terminate- Cause	This is used in the accounting stop records that the switch generates after a session is disconnected from the switch. Possible values includes the following options. <ul style="list-style-type: none"> • User-Request - used when user signs off • Idle-Timeout - used when timeout occurs • Lost-Carrier - used when a serial login was performed and the serial cable is unplugged (works with serial security enabled)
Client-IP-Address	Indicates the end client IP address, if the customer connects through IP. If the customer connects through the console, this is the same as the switch or stack address.
Timestamp	The timestamp of the RADIUS accounting record.

RADIUS Management accounting mode can be configured using ACLI and EDM.

RADIUS interim accounting updates

With RADIUS interim accounting updates, the RADIUS server can make policy decisions based on real-time network attributes sent by the switch. The Framed-IP-Address attribute can help compare Layer 2 and Layer 3 IP addresses in the RADIUS server session database and with support for Dynamic Authorization Extensions to RADIUS (RFC 5176), enable integration

with applications that operate with Layer 3 IP addresses only. The Framed-IP-Address attribute will only be populated by the switch if DHCP snooping is enabled.

RADIUS interim accounting updates are disabled by default.

Campus security example

The following figure shows a typical campus configuration using the RADIUS-based and MAC-address-based security features for the Avaya Ethernet Routing Switch 4000.

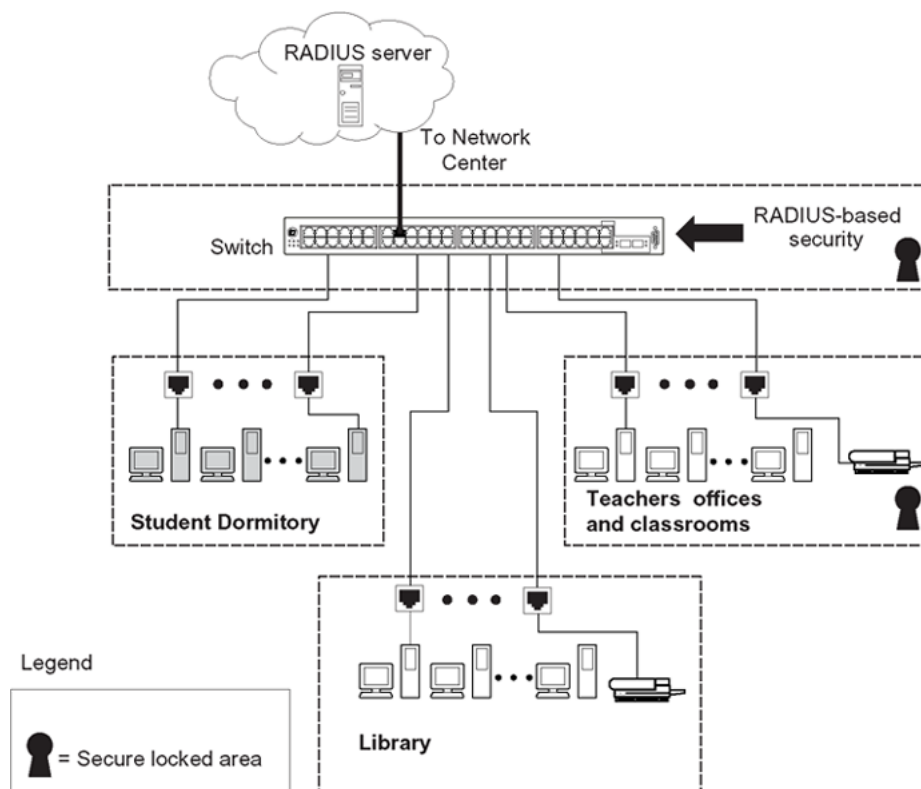


Figure 2: Avaya Ethernet Routing Switch 4000 Series security features

This example is based on the assumption that 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, as follows:

- The switch

RADIUS-based security limits administrative access to the switch through user authentication. For more information, see [RADIUS-based network security](#) on page 35.

MAC address-based security permits up to 448 authorized stations access to one or more switch ports. For more information, see [MAC address-based security](#) on page 31.

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 prewired with two RJ-45 jacks.

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

- Teachers' offices and classrooms

The PCs that are in the teachers' offices and in the classrooms are assigned MAC address-based security, which is specific for each classroom and office location.

The security feature logically locks each wall jack to the specified station, thereby preventing unauthorized access to the switch.

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

This scenario is based on the assumption that all PCs are password protected and that the classrooms and offices are physically secured.

- Library

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

This scenario is based on the assumption that all PCs are password protected and that access to the library is physically secured.

EAPOL-based security

The switch uses an encapsulation mechanism, Extensible Authentication Protocol over LAN (EAPOL), to provide security. This concept uses the Extensible Authentication Protocol (EAP) as described in the IEEE 802.1X so you can set up network access control on internal LANs. EAPOL filters traffic based on source MAC address. An unauthorized client, whether EAPOL or NonEAPOL, can receive traffic from authorized clients.

With EAP, the exchange of authentication information can occur between end stations or servers connected to the switch and an authentication server, such as a RADIUS server. The EAPOL-based security feature operates in conjunction with a RADIUS-based server to extend the benefits of remote authentication to internal LAN clients.

The following example illustrates how the Avaya Ethernet Routing Switch 4000 Series, configured with the EAPOL-based security feature, reacts to a new network connection:

- The switch detects a new connection on a port.
 - The switch requests a user ID from the new client.
 - EAPOL encapsulates the user ID and forwards it to the RADIUS server.
 - The RADIUS server responds with a request for the user's password.
- The new client forwards a password to the switch within the EAPOL packet.
 - The switch relays the EAPOL packet to the RADIUS server.
 - If the RADIUS server validates the password, the new client can access the switch and the network.

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

- **Supplicant:** The device that applies for access to the network.
- **Authenticator:** The software that authorizes a supplicant attached to the other end of a LAN segment. For SHSA mode, the authenticator sends the EAP Request Identity to the supplicant using the MAC destination address—the EAP MAC address (01:80:C2:00:00:03). For MHMA mode, the authenticator sends the EAP Request Identity to the supplicant using the MAC destination address—the supplicant MAC address.
- **Authentication Server:** The RADIUS server that provides authorization services to the Authenticator.
- **Port Access Entity (PAE):** The software entity that is associated with each port that supports the Authenticator or Supplicant functionality.
- **Controlled Port:** A switch port with EAPOL-based security enabled.

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

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

The Authenticator PAE functionality is implemented for each controlled port on the switch. At system initialization, or when a supplicant is initially connected to the switch controlled port, the controlled port state is set to Unauthorized. During this time, the authenticator processes EAP packets.

When the Authentication server returns a success or failure message, the controlled port state changes accordingly. If the authorization succeeds, the controlled port operational state is Authorized. The blocked traffic direction on the controlled port depends on the Operational Traffic Control field value in the EAPOL Security Configuration screen.

The Operational Traffic Control field can have one of the following two values:

- Incoming and Outgoing: If the controlled port is unauthorized, frames are not transmitted through the port. All frames received on the controlled port are discarded.
- Incoming: If the controlled port is unauthorized, frames received on the port are discarded, but the transmit frames are forwarded through the port.

EAPOL dynamic VLAN assignment

If you allow EAPOL-based security on an authorized port, the EAPOL feature dynamically changes the port VLAN configuration and assigns a new VLAN. The new VLAN configuration values apply according to previously stored parameters in the Authentication server.

The following VLAN configuration values are affected:

- port membership
- PVID
- port priority

When you disable EAPOL-based security on a port that was previously authorized, the port VLAN configuration values are restored directly from the switch nonvolatile random access memory (NVRAM).

The following exceptions apply to dynamic VLAN assignments:

- The dynamic VLAN configuration values assigned by EAPOL are not stored in the switch NVRAM.
- If an EAPOL connection is active on a port, then changes to the port membership, PVID, or port priority are not saved to NVRAM.
- When you enable EAPOL on a port, and you configure values other than VLAN configuration values, these values are applied and stored in NVRAM.

You can set up your Authentication server (RADIUS server) for EAPOL dynamic VLAN assignments. With the Authentication server, you can configure user-specific settings for VLAN memberships and port priority.

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

To set up the Authentication server, set the following return list attributes for all user configurations. For more information, see your Authentication server documentation.

- VLAN membership attributes (automatically configures PVID)
 - Tunnel-Type: value 13, Tunnel-Type-VLAN

- Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
- Tunnel-Private-Group-ID: ASCII value 1 to 4094 or an ASCII string starting with a non-numeric character (this value identifies the specified VLAN)
- Port priority (vendor-specific) attributes
 - Vendor Id: value 562, Avaya vendor ID
 - Attribute Number: value 1, Port Priority
 - Attribute Value: value 0 (zero) to 7 (this value indicates the port priority value assigned to the specified user)

System requirements

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

- at least one switch
- RADIUS server (Microsoft Windows 2003 Server or other RADIUS server with EAPOL support)
- client software that supports EAPOL (Microsoft Windows XP Client)

You must configure the Avaya devices with the RADIUS server IP address for the Primary RADIUS server.

EAPOL-based security configuration rules

The following configuration rules apply to the Avaya Ethernet Routing Switch 4000 Series when you use EAPOL-based security:

- Before configuring your you must configure the Primary RADIUS Server and Shared Secret fields.
- You cannot configure EAPOL-based security on ports that are currently configured for
 - shared segments
 - MultiLink Trunking
 - MAC-address-based security
 - IGMP (Static Router Ports)
 - port mirroring
- With EAPOL SHSA (the simplest EAPOL port operating mode), you can connect only one client on each port that is configured for EAPOL-based security. If you attempt to add additional clients to a port, that port state changes to Unauthorized.

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

Advanced EAPOL features

EAPOL supports the following advanced features:

- Single Host with Single Authentication (SHSA) and Guest VLAN.
- Multihost (MH) support:
 - Multiple Host with Multiple Authentication (MHMA).
 - Non EAP hosts on EAP-enabled ports.
 - Multiple Host with Single Authentication (MHSA).
- 802.1X or non-EAP and Guest VLAN on the same port.
- 802.1X or non-EAP with Fail Open VLAN.
- 802.1X or non-EAP Last Assigned RADIUS VLAN.
- 802.1X or non-EAP with VLAN names.

 **Important:**

Support exists only for untagged traffic when you use the multihost features.

 **Note:**

With the 802.1x-2004 standard, the switch can authenticate EAPOL version 1 and EAPOL version 2 supplicants. In multihost mode, the switch can communicate with EAPOL version 1 and EAPOL version 2 supplicants in the same time.

Client reauthentication

If your system is configured for SHSA and MHSA, when clients are reauthenticated the system moves them into the new RADIUS-assigned VLAN, if the new RADIUS-assigned VLAN differs from the current VLAN.

If you use RADIUS-assigned VLAN in multi-host mode and, if the RADIUS-assigned VLAN of the first authenticated clients is invalid, the switch ignores those RADIUS VLAN assignments and assigns the port to the first valid RADIUS VLAN assignment if Last RADIUS Assigned VLAN is disabled. If Last RADIUS Assigned VLAN is enabled, the port remains assigned to the last valid RADIUS Assigned VLAN. If your system is configured for MHMA, when clients are reauthenticated the system does not move them into the new RADIUS-assigned VLAN.

Single Host with Single Authentication and Guest VLAN

Single Host with Single Authentication (SHSA) support is the default configuration for an EAP-enabled port. At any time, only one MAC user can be authenticated on a port, and the port assigned to only one port-based VLAN.

If you configure no guest VLAN, only the particular device or user that completes EAP negotiations on the port can access that port for traffic. Tagged ingress packets are sent to the PVID of that port. The only exceptions are reserved addresses.

You can configure a guest VLAN for non authenticated users to access the port. Any active VLAN can be a guest VLAN.

The following rules apply for SHSA:

- When the port is EAP enabled
 - If Guest VLAN is enabled, the port is placed on a Guest VLAN.
PVID of the port = Guest VLAN ID
 - If Guest VLAN is not enabled, the port handles EAPOL packets only until successful authentication.
- During EAP authentication
 - If Guest VLAN is enabled, the port is placed on a Guest VLAN.
 - If Guest VLAN is not enabled, the port handles EAPOL packets only.
- If authentication succeeds
 - The port is placed on a preconfigured VLAN or a RADIUS-assigned VLAN. Only packets with the authenticated MAC (authMAC) can be on that port. Other packets are dropped.
- If authentication fails
 - If Guest VLAN is enabled, the port is placed on a Guest VLAN.
 - If Guest VLAN is not enabled, the port handles EAPOL packets only.
- Reauthentication can be enabled for the authenticated MAC address. If reauthentication fails, the port is placed back in the Guest VLAN.

The EAP-enabled port belongs to the Guest VLAN, RADIUS-assigned VLAN, or configured VLANs.

Guest VLAN

You can configure a global default Guest VLAN ID for the stack or the switch. Set the VLAN ID as Valid when you configure the switch or the stack.

Guest VLAN support contains the following features:

- Guest VLAN support is available for each port. Guest VLANs can have a valid Guest VLAN ID on each port. If a Guest VLAN ID is not specified for a port, the global default value is used. You cannot enable this feature on a particular port if the global default value or the local Guest VLAN ID is invalid.
- The Guest VLAN chosen must be an active VLAN configured on the switch. EAP registers with the VLAN module, so that it can be recovered if you delete a VLAN.

When a VLAN that is in use by EAP is deleted, the following actions are performed:

- A message is sent to the syslog.
- The port is blocked.
- When an authentication failure occurs, a port is placed back in the Guest VLAN.
- This feature affects ports that have EAP-Auto enabled. Therefore, the port must always be in a forwarding mode. It does not affect ports with administrative state, force-authorized, or force-unauthorized.
- This feature uses Enterprise Specific Management Information Bases (MIB).
- The Guest VLAN configuration settings are saved across resets.

! **Important:**

The EAP enabled port is not moved to the Guest VLAN, if the Guest VLAN and original VLAN are associated with different Spanning Tree Groups. The EAP port does not forward traffic in the guest VLAN or the original VLAN. If EAP authentication succeeds, packets are transmitted properly in the original VLAN.

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

802.1X or non-EAP and Guest VLAN on the same port removes the previous restrictions on configuring the 802.1X and non-EAP function on the same port simultaneously. In the current release, 802.1X functionality supports multiple modes simultaneously on the port allowing Guest VLAN to function along with non-EAP and various 802.1X operational modes.

For example, the switch supports authenticating an 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 that port is appropriately authenticated using 802.1X and optionally placed in the appropriate RADIUS assigned VLAN.

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 whether 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.

All authenticated devices move into the configured Fail Open VLAN, when the switch declares the RADIUS servers unreachable. This prevents the clients from being disconnected when the reauthentication timer expires and provides the devices some form of network connectivity. To provide the level of connectivity as required by corporate security policies, configure the Fail Open VLAN within the customer network. For example, the Fail Open VLAN configured to provide access to corporate IT services can be restricted from access to financial and other critical systems. In these situations clients receive a limited level of network connectivity when the RADIUS servers are unreachable rather than receiving no access.

When a switch is operating in the Fail Open mode, which means that the RADIUS servers are unreachable, the switch regularly verifies the connectivity. When the RADIUS servers become reachable, the clients are reauthenticated and, as appropriate, moved to the assigned VLANs, allowing normal network connectivity to resume.

When a client operates in the Fail Open VLAN, because RADIUS servers are unreachable, any 802.1X logoff messages received from the EAP supplicant are not processed by the switch.

For an EAP or non-EAP enabled port, by default, the Fail Open VLAN feature is disabled. When the RADIUS servers are unreachable, if the Fail Open VLAN is defined, then

- the port becomes a member of both the EAP Fail Open VLAN and EAP Fail Open VoIP VLAN
- the switch sets the PVID of the switch port to EAP Fail Open VLAN
- all the 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.

! Important:

When the port transitions from normal EAP operation to Fail Open, the end client is not aware that the port has transitioned to a different VLAN. Depending upon the association of the IP addressing scheme to VLANs, it is necessary for the client to obtain a new IP address when transitioning to or from the Fail Open VLAN. An enhancement calls for the port to be administratively turned off, and then back on again when the port transitions between Fail Open VLAN. If the PC is directly connected to the switch, this results in the client automatically refreshing the IP address. If the PC is located behind an IP handset, another switch, or a hub, the client must perform a manual renewal of the IP address.

After the switch accesses the RADIUS server and authentication succeeds, 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 there is at least one authenticated MAC address on the port, it

blocks all other unauthenticated MAC addresses on the port. You must turn on the debug counters to track server reachability 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(s) 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.

In previous releases, if EAP/NEAP reauthentication is enabled and an EAP/NEAP client tries to reauthenticate in this interval, the client is removed from port.

From Release 5.7 onwards, when Fail Open VLAN Continuity Mode is enabled, 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:**

With MHMV option enabled, 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.

In MHMA mode with the multihost multiVLAN option disabled, when a new EAP or NEAP client cannot be re-authenticated because the RADIUS server is not reachable, the client is placed into the configured Fail Open VLAN.

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 are allowed on the port.

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

RADIUS-assigned VLAN values are allowed in the MHMA mode. For more information about RADIUS-assigned VLANs in the MHMA mode, see [RADIUS-assigned VLAN use in MHMA mode](#) on page 58

MHMA support is available for an EAP-enabled port.

The following are some of the concepts associated with MHMA:

- Logical and physical ports

Each unique port and MAC address combination is treated as a logical port. MAX_MAC_PER_PORT defines the maximum number of MAC addresses that can perform EAP authentication on a port. Each logical port is treated as if it is in the SHSA mode.

- Indexing for MIBs

Logical ports are indexed by a port and source MAC address (src-mac) combination. Enterprise-specific MIBs are defined for state machine-related MIB information for individual MACs.

- Transmitting EAPOL packets

Only unicast packets are sent to a specific port so that the packets reach the correct destination.

- Receiving EAPOL packets

The EAPOL packets are directed to the correct logical port for state machine action.

- Traffic on an authorized port

Only a set of authorized MAC addresses is allowed access to a port.

MHMA support for EAP clients contains the following features:

- A port remains on the Guest VLAN when no authenticated hosts exist on it. Until the first authenticated host, both EAP and non-EAP clients are allowed on the port.
- After the first successful authentication, only EAPOL packets and data from the authenticated MAC addresses are allowed on a particular port.

- Only a predefined number of authenticated MAC users are allowed on a port.
- RADIUS VLAN assignment is 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 for each user session. However, the timers are used by the individual sessions on the port.
- Reauthenticate Now, when enabled, causes all sessions on the port to reauthenticate.
- Reauthentication timers are used to determine when a MAC is disconnected so as to enable another MAC to log on to the port.
- Configuration settings are saved across resets.

EAP and non-EAP MultiVLAN capability

With the EAP and non-EAP MultiVLAN capability, you can assign multiple EAP and non-EAP hosts to different VLANs on the same port. Before you can enable or disable the MultiVLAN capability, you must disable EAP globally on the switch.

The support of multiple VLAN functionality is an important option for when you want to configure Guest VLAN in MHMA mode and have multiple devices connected to the port. Using multiple VLANs simultaneously with EAP or non-EAP, you can assign the port to VLANs based on client returned attributes, and unauthenticated clients can remain in the Guest VLAN when other clients on the port (for example an IP Phone) are authenticated.

When you enable the MultiVLAN feature, the use of 802.1X or non-EAP Last Assigned RADIUS VLAN functionality is redundant and the switch does not permit Last Assigned VLAN to be enabled.

The advantages of the MultiVLAN capability are seen only when you use the `use-radius-assigned-vlan` option for EAP clients. If you perform Non-EAP MAC RADIUS authentication, then you should use `non-eap-use-radius-assigned-vlan`. When you use the MultiVLAN capability on a switch, each authenticated client can access the VLAN corresponding to the VLAN RADIUS attribute. If no attribute is received from the RADIUS server, the untagged frames from the authenticated clients will be forwarded in the initial VLAN.

! Important:

Avaya recommends that you do not change the MultiVLAN status while Fail Open VLAN is enabled.

RADIUS-assigned VLAN use in MHMA mode

RADIUS-assigned VLAN use in the MHMA mode gives you greater flexibility and a more centralized assignment. This feature is useful in an IP Phone set up also, where the phone traffic is directed to the Voice over IP (VoIP) VLAN and the PC Data traffic is directed to the assigned VLAN. When RADIUS-assigned VLAN values are allowed for the port, the first authenticated EAP MAC address cannot 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) receives 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.

In the 5.3 Release, you can use the 802.1X or non-EAP Last Assigned RADIUS VLAN functionality to configure the switch such that the last received radius-vlan assignment is always honoured on a port. For more information, see [802.1X or non-EAP Last Assigned RADIUS VLAN](#) on page 62.

! Important:

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

Consider the following setup in [Figure 3: RADIUS-assigned VLAN in MHMA mode](#) on page 59:

- Ethernet Routing Switch 4550T stand-alone switch with default settings
- IP Phone connected to the switch in port 1
- PC connected to the PC port of the IP Phone
- RADIUS server connected to switch port 24 (directly or through a network)

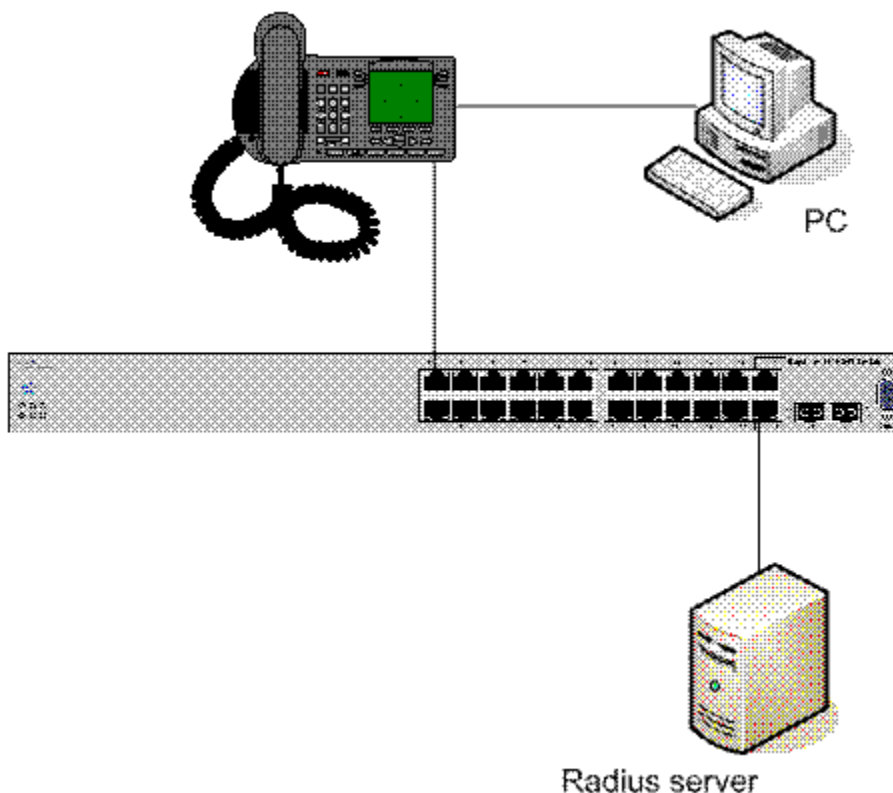


Figure 3: RADIUS-assigned VLAN in MHMA mode

EAP multihost mode needs to be configured on the switch (global settings and local settings for switch port 1/1):

1. Put a valid IP address on the switch.
2. Configure at least the Primary RADIUS server IP address (you can also fill the IP address of the Secondary one).
3. Enable EAP globally.
4. Enable EAP (status Auto) for switch port 1.
5. Enable EAP multihost mode for switch port 1.

The EAP clients will authenticate using MD5 credentials, but you can use other available types of authentication (such as TLS, PEAP-MSCHAPv2, PEAP-TLS, TTLS). The RADIUS server can be properly configured to authenticate the EAP users with at least MD5 authentication.

Non-EAP IP Phone authentication:

This enhancement is useful mainly for the IP Phones that cannot authenticate themselves with EAP. On an EAP capable IP Phone, EAP must be disabled if the user specifically wants to use the 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.

Following are the steps to enable the enhancement:

1. Enable non-EAP IP Phone authentication in the Global Configuration mode

```
4550T(config)#eapol multihost non-eap-phone-enable
```

2. Enable non-EAP IP Phone authentication in the interface mode for switch port 1

```
4550T(config-if)#eapol multihost port 1 non-eap-phone-enable
```

The switch waits for DHCP Discover packets on port 1. After a DHCP Discover packet is received on port 1, the switch looks for the phone signature (for example, Avaya-i2004-A), which can be enclosed in the DHCP Discover packet. If the proper signature is found, the switch registers the MAC address of the IP Phone as an authenticated MAC address and lets the phone traffic pass through the port.

By default, the non-EAP IP Phone authentication enhancement is disabled in both Global Configuration and Interface Configuration modes, for all switch ports.

Unicast EAP Requests in MHMA

When you enable this enhancement, the switch no longer periodically queries the connected MAC addresses to a port with EAP Request Identity packets. The clients can initiate for themselves the EAP authentication sessions (send EAP Start packets to the switch). Not all EAP supplicants can support this operating mode.

Following are the steps to enable the enhancement:

1. enable unicast EAP requests in the Global Configuration mode:


```
4550T(config)#eapol multihost eap-packet-mode unicast
```

2. enable Unicast EAP Requests in the interface mode for switch port 1:

```
4550T(config-if)#eapol multihost port 1 eap-packet-mode unicast
```

By default, multicast mode is selected in both Global Configuration and Interface Configuration modes, for all switch ports. You must set the EAP packet mode to Unicast in both global and Interface Configuration modes for a switch port, to enable this feature. Other combinations (for example, multicast in global, unicast in the interface mode) will select the multicast operating mode.

RADIUS Assigned VLANs in MHMA

This enhancement is basically an extension of the RADIUS assigned VLANs feature in SHSA mode; you can move a port to a specific VLAN even if that switch port operates in EAP MHMA mode.

This enhancement has one restriction. If you have multiple EAP clients authenticating on a 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, you can avoid a permanent bounce between different VLANs of the switch port.

Enable the enhancement by following these steps:

1. Enable RADIUS assigned VLANs in the Global Configuration mode:

```
4550T(config)#eapol multihost use-radius-assigned-vlan
```

2. Enable RADIUS assigned VLANs in the interface mode for switch port 1:

```
4550T(config-if)#eapol multihost port 1 use-radius-assigned-vlan
```

By default, the RADIUS assigned VLANs in the MHMA enhancement is disabled in the Global Configuration and Interface Configuration modes, for all switch ports.

Multiple Hosts with Multiple VLANs

With the Multiple Hosts with Multiple VLANs (MHMV) feature, you can assign multiple authenticated devices to different VLANs on the same EAP-enabled or non-EAP-enabled port, using device MAC addresses.

Benefits of using MHMV are:

- Using RADIUS VLAN attributes, different clients can access different VLANs.
- Unauthenticated clients can retain Guest VLAN access.

*** Note:**

MHVM is supported only on EAP-enabled or non-EAP-enabled ports configured for Multiple Host with Multiple Authentication (MHMA).

*** Note:**

With software releases prior to Release 5.5, the functions of MHMV and Fail Open VLAN were mutually exclusive of each other.

802.1X or non-EAP Last Assigned RADIUS VLAN

You can use 802.1X or non-EAP Last Assigned RADIUS VLAN functionality to configure the switch such that the last received RADIUS VLAN assignment is always honoured on a port. In the previous release, if you enable the use-radius-assigned-vlan option only the first valid RADIUS-assigned VLAN (by EAP or non-EAP authentication) on that port is honoured. The subsequent RADIUS VLAN assignments are ignored for any user on that port. The last 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 functional examples are as follows:

- Multiple EAP and non-EAP clients authenticate on a port.
- The EAP clients can reauthenticate; the non-EAP clients age out and reauthenticate. The Last Assigned VLAN setting for either EAP or non-EAP clients is always applied to the port when you enable the Last Assigned VLAN. This can result in the port moving unexpectedly between VLANs.

The feature supports ACLI, SNMP, and ACG interfaces. WebUI is not available for this function.

ACLI commands

For more information on the commands and procedures for configuring the most recent RADIUS-VLAN assignments on a port, see [802.1X or non-EAP Last Assigned RADIUS VLAN configuration using ACLI](#) on page 139.

802.1X or non-EAP with VLAN names

The 802.1X or non-EAP with VLAN names functionality enhances the Avaya Ethernet Routing Switch 4000 to match RADIUS assigned VLANs based on either the VLAN number or a VLAN name. Prior to this release, a match occurred based on the VLAN number of the Tunnel-Private-Group-Id attribute returned by the RADIUS server. Now you can use the VLAN number or names for configuring 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. If the first character in the attribute is a number,

the switch processes it as a VLAN number. In other cases, the attribute is taken as a VLAN and matched on the full string. The maximum length of a VLAN name can be 16 characters. You do not have to configure this feature as this mode is always 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.

Allow the following types of non-EAPOL users:

- 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 detected using LLDP Protocol.
- Avaya IP Phones.

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

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

- EAPOL and authenticated non-EAPOL clients are allowed on the port at the same time. Authenticated non-EAPOL clients are hosts that satisfy one of the following criteria:
 - Host MAC address matches an entry in an allowed list preconfigured for the port.
 - Host MAC address is authenticated by RADIUS.
- Non-EAPOL hosts are allowed even if no authenticated EAPOL hosts exist on the port.
- When a new host is seen on the port, non-EAPOL authentication is performed as follows:
 - If the MAC address matches an entry in the preconfigured allowed MAC list, the host is allowed.
 - If the MAC address does not match an entry in the preconfigured allowed MAC list, the switch generates a <username, password> pair, which it forwards to the network RADIUS server for authentication. For more information about the generated credentials, see [Non-EAPOL MAC RADIUS authentication](#) on page 64.
 - If RADIUS authenticates the MAC address, the host is allowed.
 - If the MAC address does not match an entry in the preconfigured allowed MAC list and 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 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. You can configure the maximum number of non-EAPOL hosts allowed.
- After the maximum number of allowed non-EAPOL hosts has been reached, data packets received from additional non-EAPOL hosts are dropped. The additional non-EAPOL hosts are counted as intruders. New EAPOL hosts can continue to negotiate EAPOL authentication.
- On a single port are allowed a number of EAP-MAC-MAX + 32 intruders. After this limits is reached, the system generates a SNMP trap. The port shuts down, and you must reset the port administrative status (from force-unauthorized to auto) to allow new EAPOL and non-EAPOL negotiations on the port. The intruder counter is reset to zero.
- The feature uses enterprise-specific MIBs.
- Configuration settings are saved across resets.

For more information about configuring non-EAPOL host support, see [Configuring support for non-EAPOL hosts on EAPOL-enabled ports](#) on page 162.

Non-EAPOL MAC RADIUS authentication

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

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

To increase security, the RADIUS NEAP password is set with MD5 based encryption.

Important:

Follow these Global Configuration examples to select a password format that combines one or more of these three elements:

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

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

password= 000011220001 (when only the user's MAC address is used).

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

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

- username = 00C0C1C2C3C4
- password = 010010011253.00C0C1C2C3C4.0325

Multiple Host with Single Authentication

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

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

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

MHSA support is on a port by port basis for an EAPOL-enabled port.

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

- The port remains unauthorized when no authenticated hosts exist on it. Before the first successful authentication occurs, both EAPOL and non-EAPOL clients are allowed on the port to negotiate access, but only one host can negotiate EAPOL authentication.
- After the first EAPOL client successfully authenticates, EAPOL packets and data from that client are allowed on the port. No other clients are allowed to negotiate EAPOL authentication. The port is set to preconfigured VLAN assignments and priority values or to values obtained from RADIUS for the authenticated user.
- After the first successful authentication, new hosts, up to a configured maximum number, are automatically allowed on the port, without authentication.
- After the maximum number of allowed non-EAPOL hosts has been reached, data packets received from additional non-EAPOL hosts are dropped. The additional non-EAPOL hosts are counted as intruders.
- As a general rule, the switch allows a number of EAP-MAC-MAX + 32 intruders on a port. With MHSA, only one EAP client can authenticate, meaning that the switch limits the number of intruders to 33. After this limit is reached, a SNMP trap and system message are generated. The port is set to force-unauthorized and you must reset the port to auto to allow new EAPOL negotiations on the port. The intruder counter is reset to zero.
- If the EAPOL-authenticated user logs off, the port returns to an unauthorized state and non-EAPOL hosts are not allowed.
- This feature uses enterprise-specific MIBs.

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

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 re-authentication, 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
- `eapol` command for modifying parameters

Except 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 when MAC ages out. 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 MAC ages out.

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 preceding 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 authentication globally and at the port level

Summary of multiple host access on EAPOL-enabled ports

The following table summarizes the order of the checks performed by the switch when a new host is seen on an EAPOL multihost port. If all the checks fail, the new host is counted as an intruder.

Table 3: EAPOL Multihost access

Scenario	Action
<ul style="list-style-type: none"> • No authenticated hosts on the port. • Guest VLAN is enabled. 	Allow
<ul style="list-style-type: none"> • New host MAC address is authenticated. 	Allow
<ul style="list-style-type: none"> • Port is configured for MHSA. • One EAPOL-authenticated host exists on the port. • The number of existing non-EAPOL hosts on the port is less than the configured maximum number allowed. 	Allow

Scenario	Action
<ul style="list-style-type: none"> • Host is an IP Phone. • Port is configured for ADAC (allowed PhoneMac, not callSvr, not Uplink). 	Allow
<ul style="list-style-type: none"> • Port is configured for non-EAPOL host support. • Host MAC address is in a preconfigured list of allowed MAC addresses. • The number of existing non-EAPOL hosts on the port is less than the configured maximum number allowed. 	Allow
<ul style="list-style-type: none"> • Port is configured for non-EAPOL host support. • Host MAC address is authenticated by RADIUS. • The number of existing non-EAPOL hosts on the port is less than the configured maximum number allowed. 	Disallow pending RADIUS authentication; allow when authentication succeeds.

802.1X authentication and Wake on LAN

WoL networking standard enables remotely powering-up a shutdown computer from a sleeping state. In this process, the computer is shutdown with power reserved for the network card. A packet known as Magic Packet is broadcast on the local LAN or subnet. The network card on receiving the Magic Packet verifies the information. If the information is valid, the network card powers-up the shutdown computer.

The WoL Magic Packet is a broadcast frame sent over a variety of connectionless protocols like UDP and IPX. The most commonly used connectionless protocol is UDP. The Magic Packet contains data that is a defined constant represented in hexadecimal as FF:FF:FF:FF:FF:FF, followed by 16 repetitions of the target computer MAC address and possibly by a four or six byte password.

If you implement enhanced network security using 802.1X, the transmission of Magic Packets to sleeping or unauthorized network devices is blocked. An interface specific 802.1X feature known as traffic-control can be used to address this requirement of supporting both WoL and 802.1X Authentication simultaneously. The default mode of traffic-control operation blocks both ingress and egress unauthenticated traffic on an 802.1X port. Setting the traffic control mode to in enables the transmission of Magic Packets to sleeping or unauthenticated devices. This mode allows any network control traffic, such as a WoL Magic Packet to be sent to a workstation irrespective of the authentication or sleep status.

Important:

If a PC client is assigned to a VLAN based on a previous RADIUS Assigned VLAN, when the client goes into sleep or hibernation mode it reverts to either the default port-based VLAN or Guest VLAN configured for that port. So, the WoL Magic Packet must be sent to the default VLAN or Guest VLAN.

EAP (802.1X) accounting

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

The RADIUS accounting protocol is defined in RFC 2866.

RADIUS accounting in the current Avaya Ethernet Routing Switch 4000 Series implementation utilizes the same RADIUS server used for RADIUS authentication.

By default, the RADIUS accounting UDP port is the RADIUS authentication port + 1. Beginning with Release 5.5, you can configure RADIUS accounting separately.

Non-EAP accounting

Beginning with Release 5.5, 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).

The maximum number of clients for NEAP accounting permitted on a standalone switch or a stack is 384.

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 authentication
- MHSA NEAP authentication
- RADIUS authentication

Feature operation

RADIUS accounting logs all of the activity, of each remote user in a session on the centralized RADIUS accounting server.

Session IDs for each RADIUS account are generated as 12-character strings. The first four characters in the string form a random number in hexadecimal format. The last eight characters in the string indicate, in hexadecimal format, the number of user sessions started since reboot.

The Network Access Server (NAS) IP address for a session is the IP address of the switch management VLAN.

The following table summarizes the events and associated accounting information logged at the RADIUS accounting server.

Table 4: Accounting events and logged information

Event	Accounting information logged at server
Accounting is turned on at the router	Accounting on request: NAS IP address
Accounting is turned off at the router	Accounting off request: NAS IP address
User logs on	Account start request: <ul style="list-style-type: none"> • NAS IP address • NAS port • Account session ID • Account status type • User name
User logs off or port is forced to unauthorized state	Account stop request: <ul style="list-style-type: none"> • NAS IP address • NAS port • Account session ID • Account status type • User name • Account session time • Account terminate cause • Input octet count for the session* • Output octet count for the session* • Input packet count for the session* • Output packet count for the session* <p>* Note: Octet and packet counts are by port and therefore provide useful information only when ports operate in the SHSA mode.</p>

The following table summarizes the accounting termination causes supported.

Table 5: Supported Account Terminate causes

Cause	Cause ID	When logged at server
ACCT_TERM_USER_REQUEST	1	on User LogOff
ACCT_TERM_LOST_CARRIER	2	on Port Link Down/Failure
ACCT_TERM_ADMIN_RESET	6	on Authorised to ForceUnAuthorised
ACCT_TERM_SUPP_RESTART	19	on EapStart on Authenticated Port
ACCT_TERM_REAUTH_FAIL	20	on ReAuth Failure
ACCT_TERM_PORT_INIT	21	on Port ReInitialization
ACCT_TERM_PORT_ADMIN_DISABLE	22	on Port Administratively Shutdown

EAP and NEAP separation

Use the EAP/ NEAP separation command to disable EAP clients without disabling NEAP clients.

The separation command is:

```
no eap multihost eap-protocol-enable
```

To re-enable EAP authentication, use the following command:

```
eap multihost eap-protocol-enable
```

You can issue the command to disable authentication for EAPOL clients both globally or per port. For EAPOL authentication to be possible, you must enable the EAPOL protocol both globally and per port.

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 is not 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.

Table 6: EAP per port features

Feature	Behavior
Single-Host	When Single Host is enabled (multihost is disabled) this setting has no effect on the EAP packets. This setting is a multihost specific setting.
Multihost	This setting is applied to the port only when multihost is enabled per 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 you 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).

For more information on the EAP and NEAP separation command, see [Using the EAP and NEAP separation command](#) on page 172

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 devices include the following:

- Network Access Server (NAS) — the Avaya Ethernet Routing Switch 4000 that authenticates each 802.1X client at a RADIUS server.
- RADIUS server sends disconnect and Change of Authorization (CoA) requests to the NAS. A CoA command modifies user session authorization attributes, and a disconnect command ends a user session.

! Important:

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

- 802.1X client — the device that requires authentication and uses the Avaya Ethernet Routing Switch 4000 services.

! Important:

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

An Avaya Ethernet Routing Switch 4000 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 (port VLAN ID (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 impact 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 either of the RADIUS VLAN assignment features are active on a port.

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

The following authorization considerations apply:

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

To enable the 802.1X dynamic authorization extension feature on the Avaya Ethernet Routing Switch 4000, you must do the following:

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

 **Important:**

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

While listening for request traffic from the DAC, the NAS can copy and send a UDP packet, which can disconnect a user. Avaya recommends that you implement reply protection by including the Event Timestamp attribute in both the request and response. To correctly process the Event Timestamp attribute, you must synchronize the DAC and the NAS (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 a proxy forwards RADIUS requests, the NAS-IP-Address or NAS-IPv6-Address attributes do not match the source IP address observed by the DAC. The DAC cannot resolve the NAS-Identifier attribute, whether a proxy is present or not. The authenticity check performed by the DAC does not verify the NAS identification attributes, and an unauthorized NAS can forge identification attributes and impersonate an authorized NAS in your network.

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

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

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

TACACS+

The Avaya Ethernet Routing Switch 4000 supports the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ is a security application implemented as a

client/server based protocol that provides centralized validation of users attempting to gain access to a router or network access server.

TACACS+ differs from RADIUS in two important ways:

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

! Important:

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

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

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

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

For more information about TACACS+, see the Microsoft Web site: <http://www.microsoft.com>

! Important:

TACACS+ is not compatible with previous versions of TACACS.

TACACS+ architecture

You can configure TACACS+ on the Avaya Ethernet Routing Switch 4000 using the following methods:

- Connect the TACACS+ server through a local interface. Management PCs can reside on an out-of-band management port or serial port, or on the corporate network. The TACACS+ server is placed on the corporate network so that it can be routed to the Avaya Ethernet Routing Switch 4000.
- Connect the TACACS+ server through the management interface using an out-of-band management network.

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

Feature operation

During the log on process, the TACACS+ client initiates the TACACS+ authentication session with the server. After successful authentication, if TACACS+ authorization enables, the TACACS+ client initiates the TACACS+ authorization session with the server. After successful

authentication, if TACACS+ accounting enables, the TACACS+ client sends accounting information to the TACACS+ server.

 **Note:**

TACACS+ packets are not generated if Management VLAN is not operational.

TACACS+ authentication

TACACS + authentication offers complete control of authentication through log on 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 different interfaces; for example, RADIUS on the serial connection and TACACS+ on the Telnet connection.

 **Important:**

Prompts for log on and password occur prior to the authentication process. If TACACS+ fails because there are no valid servers, 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 enables, the NAS uses information retrieved from the user profile, which is located either in the local user database or on the security server, to configure the user 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.

After the NAS requests authorization, the entire command is sent to the TACACS+ daemon for authorization. You preconfigure command authorization on the TACACS+ server by specifying a list of regular expressions that match command arguments, and associating each command with an action to deny or permit. For more information about the configuration required on the TACACS+ server, see [TACACS+ server configuration example](#) on page 77.

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 you authorize each group 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 a privilege level is not defined for a user but the user can execute at least one command, the user defaults to privilege level 0. If all commands are explicitly denied for a user, the user cannot access the switch at all.

Changing privilege levels at runtime

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

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

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

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 on the switch:

```
tacacs switch back
```

To support runtime switching of users to a particular privilege level, you must preconfigure a dummy user for that level on the daemon. The format of the user name for the dummy user is \$enab<n>\$. The privilege level to which you want to allow access is <n>.

For more information about the configuration required on the TACACS+ server, see [TACACS+ server configuration example](#) on page 77.

TACACS+ server configuration example

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

```

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

```

Figure 4: Example: TACACS+ server configuration

TACACS+ accounting

TACACS+ accounting allows you to track

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

When you enable TACACS+ 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. The accounting data can be analyzed for network management and auditing.

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

The accounting record includes the following information:

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

You cannot customize the set of events that are monitored and logged by TACACS+ accounting. TACACS+ accounting logs the following events:

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

TACACS+ configuration

You can use ACLI to configure TACACS+ on the Avaya Ethernet Routing Switch 4000. You cannot configure TACACS+ using Enterprise Device Manager.

For more information about configuring TACACS+ server information and TACACS+ authentication, authorization, and accounting using ACLI, see [TACACS+ configuration using ACLI](#) on page 212.

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

IP Manager

You can limit access to the management features of the Avaya Ethernet Routing Switch 4000 by defining the IP addresses that are allowed access to the switch.

You can use the IP Manager to do the following:

- Define up to 50 Ipv4 and 50 Ipv6 addresses and masks that can 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.

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

 **Important:**

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

Changes you make to the IP Manager list are applied immediately.

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.

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

Password length and valid characters

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

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

The password is case-sensitive.

Password retry

If the user fails to provide the correct password after a number of consecutive retries, the switch resets the log-on process. You can configure the number of retries, using ACLI. The default is three. For more information, see [Configuring the number of retries](#) on page 224.

Password history

You can configure the Avaya Ethernet Routing Switch 4000 to keep a maximum history of the last ten 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 display

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

Password verification

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

Password aging time

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

Read-Only and Read-Write passwords

The RO and RW passwords cannot be the same.

Default password and default password security

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

Password security enabled or disabled

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

You can enable password security from ACLI only. When it is enabled, the following happens:

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

You can enable password security from ACLI only. When it is disabled, the following happens:

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

Password security commands

For more information about ACLI commands to enable or disable password security, see [Configuring password security](#) on page 224.

Password security features and requirements

The following table describes the password security features and requirements in place when you enable password security.

Table 7: Password security features and requirements summary

Feature requirement	Description
Password composition	The password must contain a minimum of two of each of the following types of characters: lowercase letters,

Feature requirement	Description
	capital letters, numbers, and special symbols such as ! @#\$%^&*().
Password length	The password must consist of between 10 and 15 characters.
Login attempts	The switch allows only a specified maximum number of consecutive failed log on attempts. The number of allowed retries is configurable. The default is three.
Password history	The previous three passwords used are saved on the switch and cannot be reused until they pass out of the history table.
Password update verification	Password change must be verified by typing the new password twice.
Password aging time	Passwords expire after a specified period. The aging time is configurable. The default is 180 days.
Password display masking	When a password appears or is entered in ACLI, each character of the password is displayed as an asterisk (*).
Password security factory default	By default, password security is enabled on the SSH software image and disabled on the non-SSH software image.

ACLI audit

ACLI audit provides a means for tracking ACLI commands.

A special area of flash memory reserved for ACLI audit stores the command history. Access to this area is read-only. When you enable remote logging, the audit message is also forwarded to a remote syslog server, no matter the logging level.

Every time you issue a ACLI command, the switch generates an audit message. Each log entry consists of the following information:

- timestamp
- fixed priority setting of 30 (= informational message)
- command source
 - serial console and the unit connected
 - Telnet or SSH connection and the IP address
- command status (success or failure)
- ACLI command itself

By default ACLI audit is enabled. You can disable the audit log that stops log messages from being written to the FLASH memory and the syslog server, if configured.

Erasable ACLI audit log

You can erase the contents of the CLI audit log on a switch running the standard software image, should circumstances arise that require the log contents to be cleared. For example, you can clear the CLI audit log contents on switches that are being decommissioned or moved to another company location.

Because the CLI audit log is an important security feature, the audit log cannot be erased on switches running the secure software image or on switches that have the no-erase audit log flag enabled. Enabling the no-erase audit log function when using the standard software image is a one-time configuration option. After the audit log flag has been set to non-erasable, you cannot reverse this configuration action and you will not be able to clear the audit log, even if the switch is re-configured to factory defaults.

Simple Network Management Protocol

The Avaya Ethernet Routing Switch 4000 supports Simple Network Management Protocol (SNMP).

SNMP is traditionally used to monitor devices running software that allows the retrieval of SNMP information (for example, UNIX systems, Windows systems, printers, modem racks, switches, routers, power supplies, Web servers, and databases).

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

SNMP Version 1 (SNMPv1)

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

SNMPv1 security is based on communities, which are passwords (plain text strings allowing SNMP-based applications, which know the strings, to gain access to device management information). SNMPv1 typically has three communities: read-only, read-write, and trap.

SNMP Version 2 (SNMPv2)

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

SNMP Version 3 (SNMPv3)

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

Avaya Ethernet Routing Switch 4000 Series support for SNMP

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

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

You to configure SNMPv3 using EDM, or ACLI.

SNMP MIB support

The Avaya Ethernet Routing Switch 4000 supports an SNMP agent with industry-standard Management Information Bases (MIB) as well as private MIB extensions, which ensures compatibility with existing network management tools.

The IETF standard MIBs supported on the switch include MIB-II (originally published as RFC 1213; then split into separate MIBs as described in RFCs 4293, 4022, and 4113), Bridge MIB (RFC 4188), and the RMON MIB (RFC2819), which provides access to detailed management statistics.

For more information about the MIBs supported by the Avaya Ethernet Routing Switch 4000, see [Supported SNMP MIBs and traps](#) on page 393.

SNMP trap support

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

SNMP trap notification-control defines traps, such as **bsnConfigurationSavedToNvram**, on a global basis (per bridge). You can also use SNMP trap notification-control to configure supported notifications, such as **linkDown** or **linkup**, to be enabled or disabled on individual interfaces as well as globally.

All notifications are enabled on individual interfaces by default.

The Avaya Ethernet Routing Switch 4000 supports both industry-standard SNMP traps, as well as private Avaya enterprise traps. SNMP trap notification-control provides a generic mechanism for the trap generation control that works with any trap type.

For more information about the MIBs and traps supported by the Avaya Ethernet Routing Switch 4000, see *Supported SNMP MIBs and traps*.

You can use ACLI or EDM to enable or disable SNMP traps for the following features:

- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- IP Source Guard (IPSG)
- Auto-Detection and Auto-Configuration (ADAC)

You can use ACLI or EDM to generate the following SNMP traps for operational conditions and errors:

- IldpRemTablesChange
- risingAlarm
- fallingAlarm
- vrrpTrapNewMaster
- pethPsePortOnOffNotification
- pethMainPowerUsageOnNotification
- pethMainPowerUsageOffNotification
- ospfVirtIfStateChange
- ospfNbrStateChange
- ospfVirtNbrStateChange
- ospfIfConfigError
- ospfVirtIfConfigError

- ospflfAuthFailure
- ospfvirtlfAuthFailure
- ospflfStateChange
- entConfigChange
- coldStart
- warmStart
- linkDown
- linkUp
- authenticationFailure
- lldpXMedTopologyChangeDetected
- ntnQosPolicyEvolLocalUbpSessionFailure
- slaMonitorAgentExceptionDetected
- bspelpPhonePowerLimitNotification
- bspelpPhonePowerPriorityNotification
- bsAdacPortConfigNotification
- bsAdacPortOperDisabledNotification
- bsveVrrpTrapStateTransition
- bsDhcpSnoopingBindingTableFull
- bsDhcpSnoopingTrap
- bsDhcpOption82MaxLengthExceeded
- bsDhcpSnoopingExtSaveEntryMACConflict
- bsDhcpSnoopingExtSaveEntryInvalidInterface
- bsDhcpSnoopingExtSaveEntryLeaseExpired
- bsDhcpSnoopingExtSaveEntryParsingFailure
- bsDhcpSnoopingExtSaveNTP
- bsDhcpSnoopingExtSaveUSBSyncSuccess
- bsDhcpSnoopingExtSaveTFTPSyncSuccess
- bsDhcpSnoopingExtSaveUSBSyncFailure
- bsDhcpSnoopingExtSaveTFTPSyncFailure
- bsDhcpSnoopingExtSaveUSBRestoreSuccess
- bsDhcpSnoopingExtSaveTFTPRestoreSuccess
- bsDhcpSnoopingExtSaveUSBRestoreFailure

- bsDhcpSnoopingExtSaveTFTPRestoreFailure
- bsDhcpSnoopingExtSaveEntryInvalidVlan
- bsaiArpPacketDroppedOnUntrustedPort
- bsSourceGuardReachedMaxIpEntries
- bsSourceGuardCannotEnablePort
- bsRadiusReachabilityServerDown
- bsRadiusReachabilityServerUp
- bsnesGloballyEnabled
- bsnesGloballyDisabled
- bsnesManuallyActivated
- bsnesManuallyDeactivated
- bsnesScheduleNotApplied
- bsnesScheduleApplied
- bsnesActivated
- bsnesDeactivated
- bsLstInterfaceStatusChanged
- bsLstGroupOperStateChanged
- rcnBpduReceived
- rcnIisPlsbMetricMismatchTrap
- rcnIisPlsbDuplicateSysidTrap
- rcnIisPlsbLsdbUpdateTrap
- rcnIisPlsbBvidMismatchTrap
- rcnIisPlsbAdjStateTrap
- rcnIisPlsbDuplicateNnameTrap
- rcnIisPlsbMultiLinkAdjTrap
- bsnConfigurationSavedToNvram
- bsnEapAccessViolation
- bsnStackManagerReconfiguration
- bsnLacTrunkUnavailable
- bsnLoginFailure
- bsnTrunkPortDisabledToPreventBroadcastStorm
- bsnTrunkPortEnabledToPreventBroadcastStorm

- bsnLacPortDisabledDueToLossOfVLACPDU
- bsnLacPortEnabledDueToReceiptOfVLACPDU
- bsnStackConfigurationError
- bsnTrialLicenseExpiration
- bsnEnteredForcedStackMode
- bsnEapRAVError
- bsnSystemUp365Days
- bsnUSBInsertion
- bsnUSBRemoval
- bsnSFPInsertion
- bsnSFPRemoval
- bsnROPasswordExpired
- bsnRWPPasswordExpired
- rcnSlppGuardHoldDownExpired
- rcnSlppGuardPacketReceived
- s5EtrSbsMacTableFull
- s5EtrSbsMacTableClearedForPort
- s5EtrSbsMacTableCleared
- s5EtrSbsMacRemoved
- s5EtrNewSbsMacAccessViolation
- s5EtrMacAddressTablesThresholdReached
- s5CtrNewHotSwap
- s5CtrNewProblem
- s5CtrNewUnitUp
- s5CtrNewUnitDown
- s5CtrFanDirectionError
- s5CtrHighTemperatureError
- ubpEAPSessionStart
- ubpEAPSessionEnd

 **Important:**

When you use SNMPv1, trap receivers can mistakenly interpret the **s5EtrSbsMacRemoved** SNMP trap as **s5EtrRedBadRemCfgDetected**.

! Important:

When you use SNMPv1, trap receivers can mistakenly interpret the **s5EtrSbsMacTableClearedForPort** SNMP trap as **5EtrPortDteJabbering**.

! Important:

When you use SNMPv1, trap receivers can mistakenly interpret the **s5EtrNewSbsMacAccessViolation** SNMP trap as **s5EtrSbsMacAccessViolation**.

! Important:

Trap receivers may not display the correct TFTP server IP address in SNMP trap text related to DHCP Snooping External Save.

***** Note:

You can only use SFTP server when you are running the secure software image on the switch.

Secure Socket Layer protocol

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

The SSL server has the following features:

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

Generally, an SSL certificate is generated when

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

Secure versus Non-secure mode

The management interfaces (ACLI and SNMP) can configure the Web server to operate in a secure or nonsecure mode. The SSL Management Library interacts with the Web server to this effect.

In secure mode, the Web server listens on TCP port 443 for client browser requests. You can use the `https-only` command to configure the Web server to respond to both HTTPS and HTTP requests, or HTTPS requests only, from client browsers when the Web server is in secure mode. By default, the Web server is configured to respond to HTTPS client browser requests only.

In the nonsecure 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. You can designate this TCP port as a value between 1024 and 65535.

! Important:

If the TCP port is set to a number other than 80, you must configure the `HttpPort` attribute for the device properties to match the switch configuration to access the device home page using EDM.

SSL Certificate Authority

SSL certificates are issued and signed by a Certificate Authority (CA) such as VeriSign. Because the management and cost of purchasing a certificate from a CA is a client concern, Avaya issues and signs the SSL certificate with the understanding that it is not a recognized CA.

The SSL certificate contains the following information. The first three items (Issuer, Start Date, End Date) are constant. The remaining items are derived from the RSA host key associated with the certificate.

```
Issuer      : Avaya
Start Date  : May 26 2003, 00:01:26
End Date    : May 24 2033, 23:01:26
SHA1 Finger Print:
d6:b3:31:0b:ed:e2:6e:75:80:02:f2:fd:77:cf:a5:fe:9d:6d:6b:e0
MD5 Finger Print:
fe:a8:41:11:f7:26:69:e2:5b:16:8b:d9:fc:56:ff:cc
RSA Host Key (length= 1024 bits):
40e04e564bcfe8b7febf1f7139b0fde9f5289f01020d5a59b66ce7207895545f
b3abd694f836a9243651fd8cee502f665f47de8da44786e0ef292a3309862273
d36644561472bb8eac4d1db9047c35ad40c930961b343dd03f77cd88e8ddd3dd
a02ae29189b4690a1f47a5fa71b75ffcac305fae37c56ca87696dd9986aa7d19
```

SSL configuration and management

For more information about configuring and managing SSL services, see [Secure Socket Layer services](#) on page 230

Secure Shell protocol

Secure Shell (SSH) protocol replaces Telnet to provide secure access to ACLI interface.

The SSH protocol includes two versions: SSH1 and SSH2. The SSH implementation in the Avaya Ethernet Routing Switch 4000 series supports SSH2.

Components of SSH2

You can use SSH2 for secure remote log on and other secure network services over an insecure network. SSH2 consists of three major components:

- The Transport Layer Protocol (SSH-TRANS): SSH-TRANS is one of the fundamental building blocks, providing initial connection, packet protocol, server authentication, and basic encryption, and integrity services. The protocol can also provide compression. The transport layer is used over a TCP/IP connection and can be used on top of other reliable data streams.
- The User Authentication Protocol (SSH-USERAUTH) authenticates the client-side user to the server. It runs over the transport layer protocol. SSH-AUTH supports two methods: public key and password authentication. To authenticate, an SSH2 client tries a sequence of authentication methods chosen from the set allowed by the server (for example, public key, password) until one succeeds or all fail.
- The Connection Protocol (SSH-CONNECT) multiplexes the encrypted tunnel into several logical channels. This protocol runs over the user authentication protocol.

SSH service configuration

The SSH service engine allows you to configure the SSH service. You can configure SSH through ACLI interface and the SNMP interface.

! **Important:**

If you enable SSH on the switch and you load an ASCII configuration file containing SSH related commands, those commands will fail. You must disable SSH on the switch before you load an ASCII configuration file containing SSH related commands.

The management objects are:

- SSH enable or disable

When SSH is enabled, you can configure the SSH server to disable other non-secured interfaces. This is referred to as the SSH secured mode. Otherwise, when you enable SSH, it operates in unsecured mode.

- DSA authentication enable or disable

You can configure the SSH server to allow or disallow DSA authentication.

- RSA authentication enable or disable

You can configure the SSH server to allow or disallow RSA authentication.

-  **Note:**

If SSH is enabled on the switch and you load an ASCII configuration file containing SSH related commands, those commands will fail. You must disable SSH on the switch before you load an ASCII configuration file containing SSH related commands.

- Password authentication enable or disable

If password authentication is not enabled, you can only connect by the public key authentication method, and only if you have the correct authentication key (DSA or RSA). You cannot disable both public key and password authentication. If you disable password authentication, you must ensure that at least one of RSA and DSA authentication is enabled.

- DSA public key upload and download
- RSA public key upload and download
- SSH information dump: shows all the SSH-related information

SSH clients

The following SSH clients are supported by the switch:

- Putty SSH (Windows 2000)
- F-secure SSH, v5.3 (Windows 2000)
- SSH Secure Shell 3.2.9 (Windows 2000)
- SecureCRT 4.1
- Cygwin OpenSSH (Windows 2000)
- AxeSSH (Windows 2000)
- SSHPro (Windows 2000)
- Solaris SSH (Solaris)
- Mac OS X OpenSSH (Mac OS X)

SSH and SSH Client

Secure Shell (SSH), a network protocol, uses a secure channel to exchange data between two network devices. Remote login to execute commands is a typical use of SSH. SSH also supports file transfer (using SFTP or SCP protocols), tunneling, forwarding TCP ports and X11 connections. SSH uses the client-server model to provide confidentiality and integrity of data over an unsecured / public network, such as the Internet. The SSH Client is a secure shell protocol for connecting to an SSH Server device in the network that is accepting remote connections. SSH Client is present only on switches with SSH images and is available only through the ACLI.

The Avaya-implemented SSH Client uses SSH version 2 protocol (SSH-2) to provide an SSH Client session.

The SSH Client authenticates to a SSH server using (in order):

1. DSA public key authentication
 - —the system performs this authentication only if DSA Auth Key exists, using the DSA key for authentication.
2. RSA public key authentication
 - —the system performs this authentication only if the previous authentication method fails, and if RSA Auth Key existss, using the RSA key for authentication.
3. password authentication
 - —the system performs this authentication only if previous authentication methods fail. You can enter a username and password.

*** Note:**

If public key authentication fails and SSH server does not support password authentication, password authentication will be tried only one time.

If any authentication method succeeds, the methods following in order are not performed.

SSH Client connection can be performed from serial console, or from a SSH connection to the switch or stack. You cannot initiate the SSH connection from a telnet connection. When the Console session terminates, the inner SSH Client also terminates.

To end the SSH session and return to ACLI, enter a '~' followed by a period (~.). You can also use the ACLI command 'ssh close-session' from a different ACLI console.

*** Note:**

With software release 5.7, you can open only one SSH Client session. Multiple SSH Client sessions are not supported.

SSH Client known hosts

To support public key authentication, the switch saves a list of SSH Client known hosts—Host IP, public key entries—in NVRAM. The switch identifies a host as known when the host's public key matches the NVRAM saved public key. Only administrators, users with read-write access, have access to known hosts.

During SSH connection to a host, on receipt of the host public key the switch accepts the host if the Host IP/received public key pair matches the Host IP/public key entry of known hosts. If keys do not match, the SSH Client ends the connection.

If the Host IP does not have an entry in the known-hosts list for read-write access, you can accept or decline the Host IP/received public key association. If you accept the host, then the switch updates the known-hosts list and the switch accepts the connection.

You can delete known hosts from the ACLI, by host IP address—you require read-write access. You do not affect an existing connection if you delete the Host IP entry of an active SSH session. You do not affect the running sessions if you modify known hosts. The switch only consults known hosts during SSH connection time. After you reset the switch to default, the switch empties the SSH known-hosts list.

SSH Client known hosts in stacks

In switch stacks, the system saves and updates known hosts in the NVRAM of all units. Therefore, if the base unit leaves the stack, or the stack breaks, the rest of the units retain the learned hosts from the stack configuration.

During stack formation, the switch synchronizes the known-hosts list on all stack units and removes deleted known hosts from all units in the stack. When the stack forms, the starting known-hosts list contains the base unit known hosts. SSH Client initialization overrides known hosts on the rest of the units in the stack with known hosts from the base unit. During stack configuration, the known-hosts list updates on all units in the stack.

Switch capacity to learn keys

At 32 Bytes NVRAM per saved key, a switch should be able to save the public keys of at least twenty different hosts, and more if there is available NVRAM.

Standards and Compliance

The SSH Client complies with SSH version 2 protocol, described in these RFCs:

- RFC 4251 (Protocol Architecture) describes the overall design of SSH-2.
- RFC 4253 (Transport Layer Protocol) provides a single, full-duplex, byte-oriented connection between client and server, with privacy, integrity, server authentication, and man-in-the-middle protection.
- RFC 4252 (Authentication Protocol) identifies the client to the server.
- RFC 4254 (Connection Protocol) provides richer, application-support services over the transport pipe, such as channel multiplexing, flow control, remote program execution, signal propagation, connection forwarding, and so on.
- RFC 4250 (Assigned Numbers) gathers together and lists various constant assignments made in the other drafts.

Feature Interactions

The SSH Client interacts with the SFTP Client application. They share the same DSA and RSA keys and key sizes.

DHCP snooping

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

DHCP snooping classifies ports into two types:

- Untrusted—ports that are configured to receive messages from outside the network or firewall. Only DHCP requests are allowed.
- Trusted—ports that are configured to receive messages only from within the network, such as switch-to-switch and DHCP server ports. In the switch-to-switch scenario, in the path from switch B to switch A to the DHCP server: the outgoing port of B to A is trusted, the incoming port from A to B is untrusted, and the outgoing port from A to the server is trusted. All types of DHCP messages are allowed.

DHCP snooping operates as follows to eliminate the 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
- time to expiry
- VLAN ID
- port

The maximum size of the DHCP binding table is 1024 entries.

The DHCP binding table is stored in RAM, and therefore is not saved across restarts. You can take a back up of the DHCP binding table using *DHCP snooping external save* feature and automatically restore after it restarts. See [Externally saving the DHCP Snooping binding table file](#) on page 97 for more information.

Static DHCP binding table entries

You can manually add static entries in the DHCP binding table to protect IP devices using applications such as DAI and IPSG, that on DHCP snooping table entries. When the protection of these statically configured IP devices is no longer required, you can manually delete entries from the DHCP binding table.

Static DHCP binding table entries are stored in NVRAM and will be saved across restarts.

Externally saving the DHCP Snooping binding table file

You can use DHCP Snooping external save to store the DHCP Snooping database at predefined, 5 minute intervals, to an external TFTP or SFTP server, or to a USB drive.

When the DHCP Snooping external save feature is enabled, the switch monitors changes to the DHCP Snooping database. If a change is detected, the sync flag is set to true, and when the five minute interval is reached, the binding database is saved to the selected TFTP server or USB drive. If a reboot occurs, the switch attempts to restore the DHCP Snooping database with the externally saved file. If the switch learns duplicate DHCP addresses or processes duplicate DHCP requests between the completion of the reboot process and when the DHCP

Snooping database is restored from the externally saved file, the new information takes precedence over the information from the restored file.

Any DHCP Snooping database entries that you manually configure, or that the switch learns between the time of the last initiated external save and the beginning of the reboot process are lost and not available when the switch is again operational.

Enabling SNTP and synchronization is mandatory. The DHCP snooping external save uses the clock time as it is supported by SNTP and NTP. The lease expiry time the switch writes to the externally saved DHCP Snooping database is the absolute lease expiry time, which can be accurately restored from the externally saved file when you reboot the switch .

DHCP snooping configuration and management

DHCP snooping is configured on a VLAN to VLAN basis.

Configure and manage DHCP snooping using the Avaya Command Line Interface (ACLI), Enterprise Device Manager (EDM), and SNMP. For more information about configuring DHCP snooping through ACLI see [DHCP snooping configuration using ACLI](#) on page 249. For more information about configuring DHCP snooping through EDM, see [DHCP snooping configuration using EDM](#) on page 336.

DHCP snooping Global Configuration

This configuration enables or disables DHCP snooping for the entire unit or stack. If you enable DHCP snooping globally, the agent determines whether the DHCP reply packets will be forwarded, based on the DHCP snooping mode (enable or disable) of the VLAN and the untrusted or trusted state of the port. You must enable DHCP snooping globally before using DHCP snooping on a VLAN. If you disable DHCP snooping globally, the switch or stack will forward DHCP reply packets to all required ports, irregardless of whether the port is configured as trusted or untrusted.

DHCP Option 82

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

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

DHCP Option 82 functions with DHCP snooping (Layer 2 mode) or DHCP relay (Layer 3 mode) and cannot function independent of either of these features. To use DHCP snooping with DHCP Option 82 enable both features globally and for each client VLAN.

To use DHCP Option 82 with DHCP relay, you must enable DHCP relay globally on the switch and client VLANs. For more information about DHCP Option 82 with DHCP relay, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4000 Series*, NN47205-506.

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 attack. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings.

The address binding table is dynamically built from information gathered in the DHCP request and reply when DHCP snooping is enabled. The MAC address from the DHCP request is paired with the IP address from the DHCP reply to create an entry in the DHCP binding table. For more information about the DHCP binding table, see [DHCP binding table](#) on page 97.

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

For dynamic ARP inspection to function, DHCP snooping must be globally enabled.

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

Configure and manage dynamic ARP inspection using ACLI or Enterprise Device Manager (EDM). For more information about configuring this feature with ACLI, see [Configuring dynamic ARP inspection](#) on page 262. For more information about configuring this feature with EDM, see [Configuring dynamic ARP inspection on VLANs using EDM](#) on page 344 and [Configuring dynamic ARP inspection on ports using EDM](#) on page 345.

IP Source Guard

IP Source Guard provides security to the network by filtering clients with invalid IP addresses. IP Source Guard is a Layer 2 (L2), port-to-port basis feature that works closely with information in the Dynamic Host Control Protocol (DHCP) snooping binding table. For more information about DHCP snooping, see [DHCP snooping](#) on page 96. When you enable IP Source Guard 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 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 more filters are set up and traffic is dropped.

IP Source Guard is available to the Avaya Ethernet Routing Switch 4000 utilizing Broadcom 569x ASICs, and is implemented with the facility provided by the port ContentAware Processor (CAE) in the ASIC.

! Important:

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

Avaya recommends that you do not enable IPSG on MLT, DMLT and LAG ports.

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

Table 8: IP Source Guard and DHCP snooping

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

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

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

Avaya Identity Engines Ignition Server

Avaya Identity Engines Ignition Server (Ignition Server) is an 802.1X-capable RADIUS authentication server and TACACS+ server that grants or denies users access to your network based on your policies. When you use Ignition Server you can create a single set of policies that control access for all user connection methods: over a wired Ethernet jack, wireless, or VPN.

Ignition Server also authenticates devices and you can configure an 802.1X authentication bypass for older devices on your network that cannot perform an 802.1X authentication.

While you store access policies on the Ignition Server, user accounts remain in your traditional user store(s) such as LDAP and Active Directory servers

To reduce security risks and task duplication, and maintain clear lines of responsibility, Ignition Server acts as a single policy decision point that makes and logs access decisions but leaves the management of user account data in your enterprise directories. Your user account data can remain in your enterprise directories because you can specify a search order that directs Ignition Server identity routing to direct the Ignition Server to search one or more user directories to find the correct user account.

Consolidating access decisions provides:

- consistent policy enforcement of your network access policies across wired, wireless, VPN, and remote access
- streamlined security and compliance audits because users can access the network through any allowed switch or access point, but wherever they connect, the log entry resolves to the user account in the appropriate enterprise user directory
- faster network extension and new network services deployment, since you can add a new access point or network with just a few steps in Ignition Server.

Ignition Server includes a policy engine that lets you make network access decisions based on, but not limited to, the following criteria:

- user identity
- account details and group memberships
- the location of the login attempt
- the time of day

For example, you can create an Ignition Server policy that grants network access to a user based on identity, point of access - which network switch or wireless access point the user connects through, and the user's laptop security state - ensuring that the laptop is a company-owned laptop as recorded in the corporate Active Directory store and ensuring that it has up-to-date anti-virus profiles installed.

Ignition Server network access tool can check whether the workstation has passed MAC authentication, Windows machine authentication, and/or a security posture check and you can combine many policy elements to enforce a single rule. For example, you can create a rule to authenticate the user with PEAP/MSCHAPv2, check that the user device has been authenticated, and, if those checks are successful, assign the user to the appropriate VLAN based on role.

For more information about Ignition server, see <http://support.avaya.com>.

Trace feature

The trace feature is a troubleshooting feature that provides detailed information about errors and events on the device. Use this feature to understand the cause of an error and take action to resolve it. The trace feature provides more detailed, real time information than a `show` command.

Syslog events for 802.1x/NEAP

The syslog event feature logs any warning or error related to EAP that affects usability of the device. Use this feature to view a message that describes the EAP feature issue and the origins of the issue.

Summary of security features

For more information about some of the security features available on the Avaya Ethernet Routing Switch 4000, see [Table 9: MAC security](#) on page 103 through [Table 13: SNMPv3 security](#) on page 105.

Table 9: MAC security

MAC security	Description
Description	Use the MAC address-based security feature to set up network access control based on source MAC addresses of authorized stations.
What is being secured	Access to the network or specific subnets or hosts.
For each port or each switch	Each port.
Layer	Layer 2.
Level of security	Forwarding.
Violations	SA filtering, DA filtering, Port Partitioning, SNMP Trap.
Requirements for setup	Not applicable.
Configuring using interfaces	ACLI, ASCII configuration file, SNMP, and EDM.
Restrictions and limitations	—
Reference	s5sbs MIB (S5-SWITCH-BAYSECURE-MIB)
Comments	—

Table 10: Password Authentication security

Password authentication	Description
Description	Security feature.
What is being secured	User access to a switch or stack.
Port to port or switch to switch	For RADIUS authentication. <ul style="list-style-type: none"> • The RADIUS server needs to be accessible from switch. • The RADIUS client from the switch must be provided with the RADIUS server IP and UDP Port and a shared secret.
Layer	Not applicable.

Password authentication	Description
Level of security	Provides Read Only and Read Write access. The access rights are checked against Local Password and RADIUS Server.
Violations	Not applicable.
Requirements for setup	For RADIUS authentication. <ul style="list-style-type: none"> • The RADIUS server needs to be accessible from the switch. • The RADIUS client from the switch must be provisioned with the RADIUS server IP, the UDP Port, and a shared secret.
Configuring using interfaces	EDM, ACLI, ASCII configuration file.
Restrictions and limitations	Not applicable.

Table 11: EAPOL security

EAPOL	Description
Description	Extensible Authentication Protocol Over LAN (Ethernet)—you can use this to set up network access control on internal LANs.
What is being secured	User access to the network.
Port to port or switch to switch	User authentication by port.
Layer	Layer 2.
Level of security	Network access encryption.
Violations	The switch blocks a port if intruder is seen on that port. Administration has to reenale port.
Requirements for setup	RADIUS Server configuration on the switch. EAP-RADIUS server needs to be accessible from the switch.
Configuring using interfaces	Enterprise Device Manger (EDM) and Avaya Command Line (ACLI).
Restrictions and limitations	Not allowed: shared segments and ports configured for MultiLink Trunking, MAC address-based security, IGMP (static router ports), or port mirroring.
Reference	IEEE802.1X, RFC 2284.

Table 12: IP Manager security

IP Manager	Description
Description	IP Manager is an extension of Telnet. It provides an option to enable or disable access for TELNET (Telnet On or Off), SNMP (SNMP On or Off) and Web Page Access (Web On or Off) with or without a list of 50 IP Addresses and masks.
What is being secured	User access to the switch through Telnet, SNMP, or Web.
Port to port or switch to switch	By switch.
Layer	IP.
Level of security	Access.
Violations	User is not allowed to access the switch.
Requirements for setup	Optional IP Addresses or Masks, Individual Access (enable or disable) for Telnet, SNMP or Web page.
Configuring using interfaces	Web and ACLI.
Restrictions and limitations	Not applicable.

Table 13: SNMPv3 security

SNMPv3	Description
Description	The latest version of SNMP provides strong authentication and privacy for Simple Network Management Protocol (SNMP)—using hash message authentication codes message digest 5 (HMAC-MD5), HMAC-secure hash algorithm (SHA), cipher block chaining Data Encryption Standard (CSCDES), Advanced Encryption Standard (AES), and Triple DES (3DES)—plus access control of Management Information Base (MIB) objects based on user names.
What is being secured	Access to MIBs using SNMPv3 is secured. Access to MIBs using SNMPv1 or v2c can be restricted.
Port to port or switch to switch	By switch.
Layer	SNMP Port 161, 162.
Level of security	Access and Encryption.
Violations	Received SNMPv3 packets that cannot be authenticated are discarded. For authenticated packets that try to access MIB objects in an unauthorized manner, an error is returned to the sender. Various MIB counters are incremented when a violation occurs. (These can be monitored to detect intrusions, for example, by using RMON alarms.)

SNMPv3	Description
Requirements for setup	For maximum security, initial configuration of views, users, and keys must be done through the console port or over a physical network connection. Subsequent secure configuration changes can be accomplished using SNMPv3 using a secure SHA or DES connection.
Configuring using interfaces	Enterprise Device Manger (EDM), Avaya Command Line Interface (ACLI), ASCII configuration file, and SNMP Set requests.

Table 14: DHCP Snooping security

DHCP Snooping	Description
Description	Use the Dynamic Host Control Protocol (DHCP) snooping security feature to provide security to the network by filtering untrusted DHCP messages to prevent DHCP spoofing.
What is being secured	Access to the network.
Port to port or switch to switch	Per port.
Layer	Layer 2 and 3.
Level of security	Forwarding.
Violations	Allows only DHCP requests from untrusted ports. DHCP replies and all other types of DHCP messages are dropped. If the source MAC address and the DHCP client hardware address do not match, the switch drops the packet.
Requirements for setup	Not applicable.
Configuring using interfaces	Avaya Command Line Interface (ACLI) and Enterprise Device Manager (EDM).

Table 15: Dynamic ARP Inspection security

Dynamic ARP Inspection	Description
Description	Use the dynamic Address Resolution Protocol (ARP) Inspection to validate ARP packets in a network.
What is being secured	Access to the network.
Per port or per switch	Per port.
Layer	Layer 2 and 3.

Level of security	Forwarding.
Violations	Dynamic ARP Inspection intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings.
Requirements for setup	DHCP snooping must be globally enabled.
Configuring using interfaces	Avaya Command Line Interface (ACLI) and Enterprise Device Manager (EDM).

Chapter 4: Security configuration and management using ACLI

This chapter describes the methods and procedures necessary to configure security on the Avaya Ethernet Routing Switch 4000 using the Avaya Command Line Interface (ACLI).

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

Setting user access limitations

For more information about the configuration and management of user access limitations using ACLI, see the *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205–500.

USB port and serial console port control using ACLI

This section describes how you can control access to the Avaya Ethernet Routing Switch 4000 by enabling or disabling the USB port or serial console port. All serial console ports on the Avaya Ethernet Routing Switch 4000 are enabled by default.

Disabling serial console ports using ACLI

Disable serial console ports to deny users console access to the Avaya Ethernet Routing Switch 4000 uses the following procedure.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Disable serial console ports on all Avaya Ethernet Routing Switch 4000s in a stack by using the following command:

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

2. Disable the serial console port on a specific Avaya Ethernet Routing Switch 4000 unit in a stack by using the following command:

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

Variable definitions

The following table defines optional parameters that you enter with the `no serial-console [unit <1-8>] <enable>` command.

Variable	Value
[unit <1-8>]	Identifies the unit number of an Avaya Ethernet Routing Switch 4000 in a stack. Values range from 1 to 8.

Enabling serial console ports using ACLI

Enable serial console ports to grant users console access to the Avaya Ethernet Routing Switch 4000 by following this procedure.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Enable serial console ports on all Ethernet Routing Switch 4000s in a stack by using either of the following commands:

```
serial-console <enable>
```

OR

```
default serial-console <enable>
```

2. Enable the serial console port on a specific Ethernet Routing Switch 4000 unit in a stack by using the following command:

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

OR

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

Variable definitions

The following table defines variables that you enter with the **serial-console [unit <1-8>] <enable>** command.

Variable	Value
[unit <1-8>]	Identifies the unit number of a Ethernet Routing Switch 4000 in a stack. Values range from 1 to 8.

Viewing serial console port status using ACLI

View serial console port status to display the operational status of serial console ports on all Avaya Ethernet Routing Switch 4000s in a stack or on a stand-alone Avaya Ethernet Routing Switch 4000 by following this procedure.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

1. View the status of all serial console ports on the switch by using the following command:

```
show serial-console
```

2. View the status of a specific serial console port on the switch by using the following command:

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

Variable definitions

The following table defines variables that you enter with the `show serial-console [unit <1-8>]` command.

Variable	Value
[unit <1-8>]	Identifies the serial console port unit number. Values range from 1 to 8.

Disabling USB ports using ACLI

Disable USB ports to deny users console access to USB ports on the Avaya Ethernet Routing Switch 4000.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Disable USB ports on all Avaya Ethernet Routing Switch 4000s in a stack by using the following command:

```
no usb-host-port [unit <1-8>] <enable>
```

2. Disable the USB port on a stand-alone Avaya Ethernet Routing Switch 4000 by using the following command:

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

Variable definitions

The following table defines variables that you enter with the `usb-host-port [unit <1-8>] <enable>` command.

Variable	Value
[unit <1-8>]	Identifies the unit number of an Avaya Ethernet Routing Switch 4000 in a stack. Values range from 1 to 8.

Enabling USB ports using ACLI

Enable USB ports to grant users console access to the Avaya Ethernet Routing Switch 4000 by following this procedure.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Enable USB ports on all Avaya Ethernet Routing Switch 4000s in a stack by using either of the following commands:

```
usb-host-port [unit <1-8>] <enable>
```

OR

```
default usb-host-port [unit <1-8>] <enable>
```

2. Enable the USB port on a stand-alone Avaya Ethernet Routing Switch 4000 by using either of the following commands:

```
usb-host-port <enable>
```

OR

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

Variable definitions

The following table defines variables that you enter with the `usb-host-port [unit <1-8>] <enable>` command.

Variable	Value
[unit <1-8>]	Identifies the unit number of an Avaya Ethernet Routing Switch 4000 in a stack. Values range from 1 to 8.

Viewing USB port status using ACLI

View USB port status to display the operational status of USB ports on all Avaya Ethernet Routing Switch 4000s in a stack or on a stand-alone Avaya Ethernet Routing Switch 4000 by following this procedure.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

1. View the status of USB ports on all Avaya Ethernet Routing Switch 4000s in a stack by using the following command:

```
show usb-host-port [unit <1-8>]
```

2. View the status of the USB port on a stand-alone Avaya Ethernet Routing Switch 4000 by using the following command:

```
show usb-host-port
```

Variable definitions

The following table defines variables that you enter with the `show serial-console [unit <1-8>]` command.

Variable	Value
[unit <1-8>]	Identifies the unit number of an Avaya Ethernet Routing Switch 4000 in a stack. Values range from 1 to 8.

HTTP/HTTPS port configuration using ACLI

This section describes HTTP/HTTPS port configuration.

Setting the switch HTTP port using ACLI

Use this procedure to set the value for the HTTP port that the switch uses for client Web browser requests.

Before you begin

If the switch is running a secure image, disable SSL.

About this task

Procedure

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

```
http-port {1024-65535}
```
-

Variable definitions

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

Variable	Value
<code>{1024-65535}</code>	Specifies a value for the switch HTTP port, ranging from 1024 to 65535. DEFAULT: 80

Restoring the switch HTTP port to default using ACLI

Use this procedure to restore the value for the HTTP port that the switch uses for client Web browser requests to the default value of 80.

About this task

Procedure

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

```
default http-port
```
-

Displaying the switch HTTP port value using ACLI

Use this procedure to display the value for the HTTP port that the switch uses for client Web browser requests.

About this task

Procedure

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

```
show http-port
```

Restoring the switch HTTPS port to default using ACLI

Use this procedure to set the value for the HTTPS port that the switch uses for secure client Web browser requests.

Before you begin

If the switch is running a secure image, disable SSL.

Procedure

1. Enter Global Configuration mode.
2. At the command prompt, enter the following command:

```
https-port {1024-65535}
```

Variable definitions

The following table describes the parameters for the `https-port` command.

Variable	Value
<code>{1024-65535}</code>	Specifies a value for the switch HTTPS port, ranging from 1024 to 65535. DEFAULT: 443

Restoring the switch HTTPS port to default using ACLI

Use this procedure to restore the value for the HTTPS port that the switch uses for secure client Web browser requests to the default value of 443.

Procedure

1. Enter Global Configuration mode.
2. At the command prompt, enter the following command:

```
default https-port
```

Displaying the switch HTTP port value using ACLI

Use this procedure to display the value for the HTTPS port that the switch uses for secure client Web browser requests.

About this task

Procedure

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

```
show https-port
```

Configuring MAC address-based security

The following ACLI commands allow for the configuration of the BaySecure application using Media Access Control (MAC) addresses.

Important:

The MAC Security feature shares resources with QoS. Precedence values for non QoS features are allocated dynamically in descending order of availability. Therefore, the precedence value used depends on the order in which features are configured. With DHCP Relay enabled by default and assigned the highest precedence value (15), a QoS policy with a precedence value of 15 cannot be installed. If the MAC Security feature is also enabled, it is assigned a precedence value of 14. Therefore, a QoS policy with a precedence value of 14 cannot be installed.

For more information about QoS policies, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4000 Series*, NN47205-504.

ACLI commands for MAC address security

You can use ACLI commands in this section to configure and manage MAC address security.

show mac-security command

The `show mac-security` command displays configuration information for the BaySecure application.

The syntax for the `show mac-security` command is

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

The following table outlines the parameters for this command.

Table 16: show mac-security parameters

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

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

show mac-security mac-da-filter command

The `show mac-security mac-da-filter` command displays configuration information for filtering MAC destination addresses (DA). Packets can be filtered from up to 10 MAC DAs or MAC SAs.

The syntax for the `show mac-security mac-da-filter` command is

```
show mac-security mac-da-filter
```

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

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

mac-security command

The `mac-security` command modifies the BaySecure configuration.

The syntax for the `mac-security` command is

```
mac-security [disable|enable] [filtering {enable|disable}]
[intrusion-detect {enable|disable|forever}] [intrusion-timer
<1-65535>] [auto-learning][learning-ports <portlist>] [learning
{enable|disable}][mac-adress-table] [mac-da-filter {add|delete}]
[security-list][snmp-lock {enable|disable}] [snmp-trap {enable|
disable}]
```

The following table outlines the parameters for this command.

Table 17: mac-security parameters

Parameter	Description
disable enable	Disables or enables MAC address-based security.
filtering {enable disable}	Enables or disables destination address (DA) filtering on intrusion detected.
intrusion-detect {enable disable forever}	Specifies partitioning of a port when an intrusion is detected: <ul style="list-style-type: none"> • enable — port is partitioned for a period of time • disabled — port is not partitioned on detection • forever — port is partitioned until manually changed
intrusion-timer <1-65535>	Specifies, in seconds, length of time a port is partitioned when an intrusion is detected; enter the number of seconds desired.
auto-learning	Configures MAC Autolearning.
learning-ports <portlist>	Specifies MAC address learning. Learned addresses are added to the table of allowed MAC addresses. Enter the ports to learn; a single port, a range of ports, several ranges, all ports, or no ports can be entered.
learning {enable disable}	Specifies MAC address learning: <ul style="list-style-type: none"> • enable — enables learning by ports • disable — disables learning by ports

Parameter	Description
mac-address-table	Specifies MAC address to be added.
mac-da-filter {add delete}	Add or delete MAC DA filtering addresses.
security-list	Specifies the security list number from 1 to 32.
snmp-lock {enable disable}	Enables or disables a lock on SNMP write-access to the BaySecure MIBs.
snmp-trap {enable disable}	Enables or disables trap generation upon intrusion detection.

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

mac-security mac-address-table address command

The `mac-security mac-address-table address` command assigns a specific trunk, a specific port or a security list to the MAC address. This removes previous assignments to the specified MAC address and creates an entry in the table of allowed MAC addresses.

The syntax for the `mac-security mac-address-table address` command is

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

The following table outlines the parameters for this command.

Table 18: mac-security mac-address-table address parameters

Parameter	Description
<H.H.H.>	Enter the MAC address in the form of H.H.H.
mlt-id <1-32> port <portlist> security-list <1-32>	Enter the trunk ID, the port number or the security list number. In this command the port list must be a single port.

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

no mac-security mac-address-table command

The `no mac-security mac-address-table` command clears static entries from the MAC address security table. MAC addresses autolearned on ports are not deleted.

The syntax for the `no mac-security mac-address-table` command is

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

The following table outlines the parameters for this command.

Table 19: no mac-security mac-address-table parameters

Parameter	Description
address <H.H.H>	Enter the MAC address in the form of H.H.H.
port <portlist>	Enter the port number.
security-list <1-32>	Enter the security list number.

The `no mac-security mac-address-table` command is executed in the Global Configuration command mode.

show mac-security mac-address-table command

The `show mac-security mac-address-table` command displays the current global MAC Address security table. The syntax for this command is

```
show mac-security mac-address-table.
```

This command is executed in the Privileged EXEC command mode.

mac-security security-list command

The `mac-security security-list` command assigns a list of ports to a security list.

The syntax for the `mac-security security-list` command is

```
mac-security security-list <1-32> <portlist>
```

The following table outlines the parameters for this command.

Table 20: mac-security security-list parameters

Parameter	Description
<1-32>	Enter the number of the security list you want to use.
<portlist>	Enter the port number.

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

no mac-security security-list command

The `no mac-security security-list` command clears the port membership of a security list.

The syntax for the `no mac-security security-list` command is

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

Substitute the `<1-32>` with the number of the security list to be cleared.

The `no mac-security security-list` command is executed in the Global Configuration command mode.

mac-security command for specific ports

The `mac-security` command for specific ports configures the BaySecure status of specific ports.

The syntax for the `mac-security` command for specific ports is:

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

The following table outlines the parameters for this command.

Table 21: mac-security parameters

Parameter	Description
port <portlist>	Enter the port numbers.
disable enable learning lock-out	<p>Directs the specific port:</p> <ul style="list-style-type: none"> • <code>disable</code> - disables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is being performed • <code>enable</code> — enables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is being performed • <code>learning</code> — disables BaySecure on the specified port and adds this port to the list of ports for which MAC address learning is being performed • <code>lock-out</code> — locks out ports from mac-security

The `mac-security` command for specific ports is executed in the Interface Configuration command mode.

show mac-security port command

The `show mac-security port` command shows the current state of security, auto-learning, auto-learning max-addresses, and the security lock out.

The syntax for the command is:

```
show mac-security port [<LINE>]
```

- where *<LINE>* specifies a port or group of ports. You can enter a single port, a range of ports, several ranges, or all ports.

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

mac-security mac-da-filter command

The `mac-security mac-da-filter` command allows packets to be filtered from up to ten specified MAC DAs or MAC SAs. You can also use this command to delete such a filter, and then receive packets from the specified MAC DA.

The syntax for the `mac-security mac-da-filter` command is

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

Substitute the `{add|delete} <H.H.H.>` with either the command to add or delete a MAC address and the MAC address in the form of H.H.H.

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

Enabling or disabling block subsequent MAC authentication using ACLI

Use this procedure to enable block subsequent MAC authentication.

Procedure steps

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

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

*** Note:**

By default this feature is disabled.

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
```

*** Note:**

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

ACLI commands for MAC address autolearning

You can use ACLI commands in this section to configure and manage MAC autolearning.

mac-security auto-learning aging-time command

The **mac-security auto-learning aging-time** command sets the aging time for the autolearned addresses in the MAC Security Table.

The syntax for the command is

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

Substitute **<0-65535>** with the aging time in minutes. An aging time of 0 means that the learned addresses never age out. The default is 60 minutes.

The **mac-security auto-learning aging-time** command is executed in the Global Configuration command mode.

no mac-security auto-learning aging-time command

The **no mac-security auto-learning aging-time** command sets the aging time for the autolearned addresses in the MAC Security Table to 0. In this way, it disables the removal of autolearned MAC addresses.

The syntax for the command is

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

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

default mac-security auto-learning aging-time command

The default **mac-security auto-learning aging-time** command sets the aging time for the autolearned addresses in the MAC Security Table to the default of 60 minutes.

The syntax for the command is

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

The **default mac-security auto-learning aging-time** command is executed in the Global Configuration command mode.

mac-security auto-learning sticky command

The **mac-security auto-learning sticky** command enables the storing of automatically learned MAC addresses across switch reboots.

The syntax for the command is

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

The **mac-security auto-learning sticky** command is executed in the Global Configuration command mode.

Important:

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

To view the current Sticky MAC address mode, use the [show mac-security command](#) on page 118 with the **config** variable.

no mac-security auto-learning sticky command

The **no mac-security auto-learning sticky** command disables the storing of the automatically learned MAC addresses across switch reboots.

The syntax for the command is

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

The **no mac-security auto-learning sticky** command is executed in the Global Configuration command mode.

To view the current Sticky MAC address mode, use the [show mac-security command](#) on page 118 with the **config** variable.

default mac-security auto-learning sticky command

The **default mac-security auto-learning sticky** command sets the storing of the automatically learned MAC addresses across switch reboots to the default state (disabled).

The syntax for the command is

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

The **default mac-security auto-learning sticky** command is executed in the Global Configuration command mode.

To view the current Sticky MAC address mode, use the [show mac-security command](#) on page 118 with the `config` variable.

mac-security lock-out command

The `mac-security lock-out` command enables the lockout of specific ports from MAC-based security.

The syntax for the command is:

```
mac-security lock-out
```

The `mac-security lock-out` command is executed in the Interface ethernet mode. When you access this mode, use the command `interface ethernet <portlist>` where `<portlist>` is the list of ports that you want to add to the MAC security lockout.

no mac-security lock-out command

The `no mac-security lock-out` command disables the lockout of specific ports from MAC-based security.

The syntax for the command is:

```
no mac-security lock-out
```

The `no mac-security lock-out` command is executed in the Interface ethernet mode. When you access this mode, use the command `interface ethernet <portlist>` where `<portlist>` is the list of ports that you want to remove from the MAC security lockout.

default mac-security lock-out command

The `default mac-security lock-out` command disables the lockout of specific ports from MAC-based security.

The syntax for the command is:

```
default mac-security lock-out
```

The `default mac-security lock-out` command is executed in the Interface ethernet mode. When you access this mode, use the command `interface ethernet <portlist>` where `<portlist>` is the list of ports that you want to remove from the MAC security lockout.

RADIUS authentication configuration using ACLI

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

Configuring switch RADIUS server settings using ACLI

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

Prerequisites

- Configure at least one RADIUS server.
- Physically connect the RADIUS server to your network.
- Log on to the Global Configuration mode in ACLI

Procedure steps

1. Configure RADIUS server account information on the switch by using the following command:

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

2. To configure the RADIUS server authentication type, enter the following command:

```
[no][default] radius-server encapsulation ms-chap-v2
```

Variable definitions

Variable	Value
<ipaddr>	<p>Specifies the IPv4 address of the primary server you want to add or configure.</p> <p>! Important: A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.</p>
<ipv6addr>	<p>Specifies the IPv6 address of the primary server you want to add or configure.</p> <p>! Important: A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.</p>

Variable	Value
acct-enable	Enables RADIUS accounting for a RADIUS server instance.
acct-port <port>	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.
default	Restores the switch RADIUS server settings to default values. To delete a RADIUS server and restore default RADIUS settings, use one of the following commands in the Global or Interface Command mode: <ul style="list-style-type: none"> • default radius server host • default radius server host secondary • default radius server host used-by eapol • default radius server host secondary used-by eapol • default radius server host used-by non-eapol • default radius server host secondary used-by non-eapol
key <key>	Specifies the secret authentication and encryption key used for all communications between the NAS and the RADIUS server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to enter and confirm the key.
no	Deletes switch RADIUS server settings.
port <port>	Specifies the UDP port number for clients to use when trying to contact the RADIUS server at the corresponding RADIUS server IP address. Values range from 1 to 65535. The default port number is 1812.
retry <1–5>	Specifies the number of RADIUS retry attempts for a RADIUS Server instance. Values range from 1 to 5.
secondary	Specifies the RADIUS server you are configuring as the secondary server. The system uses the secondary server only if the primary server is not configured or is not reachable.
timeout <timeout>	Specifies the timeout interval between each retry for service requests to the RADIUS server. Values range from 1 to 60 seconds. The default value is 2 seconds.

Variable	Value
used-by <eapol non-eapol>	<p>Specifies the RADIUS server as an EAP RADIUS Server or a Non-EAP (NEAP) RADIUS Server.</p> <ul style="list-style-type: none"> • eapol—configures the RADIUS server to process EAP client requests only . • non-eapol—configures the RADIUS server to process Non-EAP client requests only. <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>
encapsulation <MS-CHAP-V2>	<p>Specifies to enable or disable Microsoft Challenge-Handshake Authentication Protocol version 2 (MS-CHAP-V2). MSCHAP-V2 provides an authenticator controlled password change mechanism also known as the change RADIUS password function. The default value is disabled.</p> <p>* Note:</p> <p>When you disable MS-CHAP-V2, RADIUS encapsulation is set to password authentication protocol (PAP) by default. PAP is not considered a secure encapsulation. Change RADIUS password is available only in secure software builds.</p>

Enabling or disabling RADIUS password fallback using ACLI

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

Prerequisites

- Log on to the Global or Interface Configuration mode in ACLI

Procedure steps

1. Enable RADIUS password fallback by using the following command:


```
radius-server password fallback
```
2. Disable RADIUS password fallback by using either of the following commands:


```
no radius-server password fallback
```

```
default radius-server password fallback
```

Viewing RADIUS information using ACLI

Use this procedure to display RADIUS server configuration information.

Prerequisites

- Log on to the Privileged EXEC command mode in ACLI.

Procedure steps

To display RADIUS configuration status, enter the following command:

```
show radius-server
```

Job aid: show radius-server command output

The following figure displays sample output for the `show radius-server` command.

```
4524GT-PWR#show radius-server
RADIUS Global Server
-----
Primary Host       : 0.0.0.0
Secondary Host    : ::
Port              : 1812
Time-out          : 2
Key               :
Radius Accounting  : Disabled
Radius Accounting Port : 1813
Radius Retry Limit : 4

RADIUS EAP Server
-----
Primary Host       : 0.0.0.0
Secondary Host    : 0.0.0.0
Port              : 1812
Time-out          : 2
Key               :
Radius Accounting  : Disabled
Radius Accounting Port : 1813
Radius Retry Limit : 3

RADIUS Non-EAP Server
-----
Primary Host       : 0.0.0.0
Secondary Host    : 0.0.0.0
Port              : 1812
Time-out          : 2
Key               :
Radius Accounting  : Disabled
Radius Accounting Port : 1813
Radius Retry Limit : 3

Other Settings
-----
Password Fallback : Disabled
4524GT-PWR#
```

Configuring RADIUS server reachability using ACLI

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

Prerequisites

- Log on to the Global Configuration mode in ACLI

Procedure steps

Select and configure the method by which to determine the reachability of the RADIUS server by using the following command:

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

Variable definitions

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

Viewing the RADIUS server reachability method using ACLI

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

Prerequisites

- Log on to the User EXEC mode in ACLI

Procedure steps

Display the configured RADIUS server reachability method by using the following command:

```
show radius reachability
```

Job aid

The following table shows sample output for the `show radius reachability` command.

```
4524GT-PWR>show radius reachability
RADIUS reachability: USE ICMP
4524GT-PWR>
```

Configuring EAPOL security

Use the following ACLI commands to configure and manage Extensible Authentication Protocol over LAN (EAPOL) security. EAPOL filters traffic based on the source MAC address.

 **Important:**

You must enable EAPOL before you enable UDP Forwarding, IP Source Guard, and other features that use QoS policies.

eapol command

The **eapol** command enables or disables EAPOL-based security.

The syntax for the eapol command is

```
eapol {disable|enable}
```

Use either **disable** or **enable** to enable or disable EAPOL-based security.

The **eapol** command is executed in the Global Configuration command mode.

eapol command for modifying parameters

The **eapol** command for modifying parameters modifies EAPOL-based security parameters for a specific port.

The syntax for the **eapol** command for modifying parameters is:

```
eapol [port <portlist>] [init] [status {authorized|unauthorized|
auto}] [traffic-control {in-out|in}] [reauthentication {enable|
disable}] [reauthentication-period <1-604800>] [re-authenticate]
[quiet-interval <num>] [transmit-interval <num>] [supplicant-timeout
<num>] [server-timeout <num>] [max-request <num>]
```

The following table outlines the parameters for this command.

Table 22: eapol parameters

Parameter	Description
port <portlist>	Specifies the ports to configure for EAPOL; enter the desired port numbers ! Important: If this parameter is omitted, the system uses the port number specified when the interface command was issued.
init	Reinitiates EAP authentication.
status {authorized unauthorized auto}	Specifies the EAP status of the port: <ul style="list-style-type: none"> • authorized — port is always authorized • unauthorized — port is always unauthorized • auto — port authorization status depends on the result of the EAP authentication
traffic-control {in-out in}	Sets the level of traffic control: <ul style="list-style-type: none"> • in-out — if EAP authentication fails, both ingressing and egressing traffic are blocked • in — if EAP authentication fails, only ingressing traffic is blocked EAPOL filters traffic based on the source MAC address. An unauthorized client, whether EAPOL or NonEAPOL, can receive traffic from authorized clients.
reauthentication enable disable	Enables or disables reauthentication for EAPOL clients.
reauthentication-period <1-604800>	Enter the desired number of seconds between reauthentication attempts.
re-authenticate	Specifies an immediate reauthentication. NonEAP clients are not reauthenticated even if reauthentication is enabled on the port.
quiet-interval <num>	Enter the desired number of seconds between an authentication failure and the start of a new authentication attempt; range is 1 to 65535.
transmit-interval <num>	Specifies a waiting period for response from supplicant for EAP Request/Identity packets. Enter the number of seconds to wait; range is 1 to 65535.
supplicant-timeout <num>	Specifies a waiting period for response from supplicant for all EAP packets except EAP Request/

Parameter	Description
	Identity packets. Enter the number of seconds to wait; range is 1 to 65535.
server-timeout <num>	Specifies a waiting period for response from the server. Enter the number of seconds to wait; range is 1 to 65535.
max-request <num>	Enter the number of times to retry sending packets to supplicant; range is 1 to 10.

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

show eapol command

The `show eapol` command displays the EAPOL-based security.

The syntax for the `show eapol` command is

```
show eapol [<portlist>] [multihost {interface|status}] [guest-vlan
{interface}][auth-diags {interface}] [auth-stats {interface}]
```

The following table outlines the parameters for this command.

Table 23: show eapol parameters

Parameter	Description
port	The list of ports for which EAPOL security is to appear.
multihost {interface status }	Displays EAPOL multihost configuration. Select interface to display multihost port configuration and status to display multihost port status.
guest-vlan {interface}	Displays EAPOL port Guest VLAN settings.
auth-diags {interface}	Displays the EAPOL authentication diagnostics interface.
auth-stats {interface}	Displays the authentication statistics interface.

The `show eapol` command is executed in the Privileged EXEC command mode.

show eapol multihost status command

The `show eapol multihost status` command displays the multihost status of eapol clients on EAPOL-enabled ports.

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

```
show eapol multihost status [<port_list>] [verbose]
```

! Important:

If you apply the `show eapol multihost status` command on a large stack with complex configuration, you can experience slow output if this command is executed within 4-5 minutes of the stack being booted or power-cycled. If you wait 5 minutes after the stack is booted or power-cycled before executing this show command, the normal response times will be observed.

The following table outlines the parameters for this command.

Table 24: show eapol multihost status parameters

Parameter	Description
<port_list>	Specifies an individual port or list of ports for which to display the EAPOL multihost status.
<verbose>	Displays detailed EAPOL multihost port status.

The `show eapol multihost status` command is executed in the Privileged Exec command mode.

Resetting all EAP settings

To simplify the configuration process on the switch, you can reset all EAP-related settings using a single command. You can reset the EAP settings globally or at the port level.

To reset all EAP/NEAP settings globally, enter the following command in Global Configuration mode:

```
default eap-all
```

This command resets the following EAP settings:

- EAP state
- fail open VLAN
- VoIP VLANs
- allow port mirroring
- multihost
- multiVLAN
- user-based policies
- NEAP user-based policies

To reset all EAP settings at the port level, enter the following command in Interface mode:

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

- where

<port-list> is the list of ports to which you want the setting to apply. You can enter a single port, a range of ports, or all ports.

This command resets the following:

- all EAP related settings
- all EAP multihost settings
- EAP guest VLAN settings

Enabling or disabling Non-EAP client re-authentication using ACLI

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

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Enable Non-EAP re-authentication by using the following command:

```
eapol multihost non-eap-reauthentication-enable
```
2. Disable Non-EAP re-authentication by using either of the following commands:

```
no eapol multihost non-eap-reauthentication-enable
```



```
default eapol multihost non-eap-reauthentication-enable
```

Viewing the non-EAP client re-authentication status using ACLI

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

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Display the configuration status of NEAP re-authentication by using the following command:

```
show eapol multihost
```

Job aid: show eapol multihost command output

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

```
ERS-4524GT(config)#show eapol multihost
Allow Non-EAPOL Clients: Disabled
Use RADIUS To Authenticate Non-EAPOL Clients: Disabled
Allow Non-EAPOL Clients After Single Auth (MHSAA): Disabled
Allow Non-EAPOL VoIP Phone Clients: Disabled
EAPOL Request Packet Generation Mode: Multicast
Allow Use of RADIUS Assigned ULANs: Disabled
Allow Use of Non-Eapol RADIUS Assigned ULANs: Disabled
EAPOL Reauthentication Security Mode: Fail on RADIUS Timeout
Non-EAPOL RADIUS Password Attribute Format: IpAddr.MACAddr.PortNumber
Use most recent RADIUS ULAN: Disabled
Non-EAP re-authentication: Disabled
ERS-4524GT(config)#
```

Clearing non-EAP authenticated clients from ports using ACLI

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

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Clear authenticated NEAP clients from a specified port by using the following command:

```
clear eapol non-eap [<portList>] [address <H.H.H>]
```

Variable definitions

Variable	Value
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.

Variable	Value
<portList>	Specifies an individual port or list of ports from which to clear authenticated NEAP clients.

Configuring features

The Avaya Ethernet Routing Switch 4000 supports advanced EAPOL features that allow multiple hosts on a port. For more information about the advanced EAPOL features, see [Advanced EAPOL features](#) on page 52.

This section provides information about configuring the following features:

- Single Host with Single Authentication (SHSA) and Guest VLAN. For more information, see [Configuring guest VLANs](#) on page 145.
- Multiple Host with Multiple Authentication (MHMA). For more information, see [Multiple Host with Multiple Authentication](#) on page 57.
- Multiple Host with Single Authentication (MHSA). For more information, see [Multiple Host with Single Authentication](#) on page 65.
- Non EAP hosts on EAP-enabled ports. For more information, see [Non EAP hosts on EAP-enabled ports](#) on page 63.

SHSA is the default configuration.

no eapol multihost use radius-assigned-vlan command

To globally disable RADIUS-assigned VLAN use in MHMA mode, use one of the following commands in the Global Configuration mode:

```
no eapol multihost [use-radius-assigned-vlan]
```

or

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

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

Table 25: no eapol multihost [use-radius-assigned-vlan] parameters

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

Table 26: default eapol multihost [use-radius-assigned-vlan] parameters

Parameter	Description
use-radius-assigned-vlan	globally sets the default (disable) for RADIUS-assigned VLAN use in the MHMA mode.

To disable RADIUS-assigned VLAN use in the MHMA mode for the desired interface, use one of the following commands:

```
no eapol multihost [port <portlist>] [use-radius-assigned-vlan]
```

or

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

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

Table 27: no eapol multihost [use-radius-assigned-vlan] parameters: Interface mode

Parameter	Description
<portlist>	specifies the port on which you want RADIUS-assigned VLAN use disabled in the MHMA mode. You can enter a port, several ports or a range of ports.
use-radius-assigned-vlan	disables RADIUS-assigned VLAN use in the MHMA mode, on the desired interface.

Table 28: default eapol multihost [use-radius-assigned-vlan] parameters: Interface mode

Parameter	Description
<portlist>	specifies the port on which you want RADIUS-assigned VLAN use disabled in the MHMA mode. You can enter a port, several ports or a range of ports.
use-radius-assigned-vlan	sets the default (disable) for RADIUS-assigned VLAN use in the MHMA mode, on the desired port.

802.1X or non-EAP Last Assigned RADIUS VLAN configuration using ACLI

This section describes the procedures for the configuration of 802.1X non-EAP Last Assigned RADIUS VLAN using ACLI.

Enabling use-most-recent-RADIUS assigned VLAN

Perform this procedure to allow the system to use the most recently assigned RADIUS VLAN.

Prerequisites

- Log on to the Global configuration mode using ACLI.

Procedure steps

Enable the most recent RADIUS VLAN by using the following command:

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

Variable Definitions

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

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

Disabling use-most-recent-RADIUS assigned VLAN

Perform this procedure to prevent the system from using the most recently assigned RADIUS VLAN.

Prerequisites

- Log on to the Global configuration mode using ACLI.

Procedure steps

Disable the use of most recent RADIUS VLAN by using the following command:


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

Variable Definitions

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

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

Restoring use-most-recent-RADIUS assigned VLAN

Perform this procedure to restore the default EAPoL multihost settings.

Prerequisites

- Log on to the Global configuration mode using ACLI.

Procedure steps

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

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

Variable Definitions

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

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

Selecting the packet mode for EAP requests

This feature prevents repeated EAP responses from an EAP-capable device that has already been authenticated.

Use the following command to globally select the packet mode for EAP requests:

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

The following table outlines the parameters for this command.

Table 29: eapol multihost [eap-packet-mode {multicast | unicast}] parameters

Parameter	Description
[eap-packet-mode {multicast unicast}]	globally enables the desired packet mode (multicast or unicast) for EAP requests.

Use the following command to select the packet mode on the desired interface or on specific ports:

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

The following table outlines the parameters for this command.

Table 30: eapol multihost [eap-packet-mode {multicast | unicast}] parameters: Interface mode

Parameter	Description
<portlist>	the port or ports for which you want to select the packet mode. You can enter a single port, several ports or a range of ports.
[eap-packet-mode {multicast unicast}]	enables the desired packet mode (multicast or unicast) on the desired port or ports.

Use one of the following commands to globally disable the selection of packet mode:

```
no eapol multihost [eap-packet-mode {multicast | unicast}]
```

or

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

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

Table 31: no eapol multihost [eap-packet-mode {multicast | unicast}] parameters

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

Table 32: default eapol multihost [eap-packet-mode {multicast | unicast}] parameters

Parameter	Description
[eap-packet-mode {multicast unicast}]	globally sets the default (disable) for the selection of packet mode.

Use one of the following commands to disable the selection of packet mode on the desired interface:

```
no eapol multihost [port <portlist>][[eap-packet-mode {multicast | unicast}]
```

or

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

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

Table 33: no eapol multihost [eap-packet-mode {multicast | unicast}] command parameters

Parameter	Description
[eap-packet-mode {multicast unicast}]	disables selection of packet mode on the desired interface.

Table 34: default eapol multihost [eap-packet-mode {multicast | unicast}] command parameters

Parameter	Description
[eap-packet-mode {multicast unicast}]	sets the default (disable) for the selection of packet mode on the desired interface.

EAPOL User Based Policy Configuration using ACLI

To process the User Based Policy (UBP) attributes, UBP support must be enabled on the EAPOL Security Configuration. Also, the RADIUS server must be configured for retrieving the user information during EAP Authentication.

Use the following procedure to configure EAPOL User Based Policy.

Enabling EAPOL User Based Policy

Perform the following procedure to enable 802.1x (RADIUS server accounting) User Based Policy settings.

Prerequisite

- RADIUS server must be configured before enabling EAPOL User Based Policies.

Note:

If the RADIUS server is not configured, an error appears while loading the ASCII file.

Procedure step

Enable 802.1x (RADIUS server accounting) User Based Policy settings using the following command in the Global Configuration mode:

```
eapol user-based-policies { [enable] [filter-on-mac enable] }
```

The following table outlines the parameters for this command.

Table 35: eapol user-based-policies parameters

Parameter	Description
enable	Configures 802.1x User Based Policies settings.
filter-on-mac enable	Enables filtering on MAC addresses.

Disabling EAPOL User Based Policies

Perform the following procedure to disable 802.1x (RADIUS server accounting) User Based Policy settings.

Procedure steps

Disable 802.1x (RADIUS server accounting) User Based Policy settings using the following command in the Global Configuration mode:

```
no eapol user-based-policies { [enable] [filter-on-mac enable] }
```

The following table outlines the parameters for this command:

Table 36: no eapol user-based-policies parameters

Parameter	Description
enable	Disables 802.1x (RADIUS server accounting) User Based Policy settings.

Parameter	Description
filter-on-mac enable	Disables filtering on MAC addresses.

Setting EAPOL User Based Policy as Default

Perform the following procedure to set EAPOL User Based Policy as the default.

Procedure steps

Set the EAPOL User Based Policy as the default by using the following command in the Global Configuration mode:

```
default eapol user-based-policies { [enable] [filter-on-mac enable] }
```

The following table outlines the parameters for this command:

Table 37: default eapol user-based-policies

Parameter	Description
enable	Sets the default configuration for 802.1x User Based Policies.
filter-on-mac enable	Sets the default configuration for filtering on MAC addresses.

Configuring guest VLANs

To configure guest VLAN support, do the following:

1. Enable guest VLAN globally, and set the guest VLAN ID.
2. Enable guest VLAN on specific ports on an interface.

eapol guest-vlan command

The `eapol guest-vlan` command sets the guest VLAN for EAP-controlled ports.

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

```
eapol guest-vlan enable vid <1-4094>
```

The following table outlines the parameters for this command.

Table 38: eapol guest-vlan parameters

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

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

no eapol guest-vlan command

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

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

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

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

default eapol guest-vlan command

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

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

```
default eapol guest-vlan [enable] [vid]
```

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

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

Important:

EAP enabled port is not moved to guest VLAN, if guest VLAN and original VLAN are associated with different STGs. EAP port does not forward traffic in guest VLAN or original VLAN; if EAP authentication succeeds packets are transmitted properly in the original VLAN.

802.1X or non-EAP and Guest VLAN on the same port configuration using ACLI

Use the commands in this section to allow a non-EAP phone to function with the Guest VLAN enabled.

Enabling EAPOL VoIP VLAN

Perform this procedure to enable the EAPOL multihost VoIP VLAN.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enable the EAPOL multihost VoIP VLAN by using the following command:

```
eapol multihost voip-vlan <1-5> {[enable] [vid <1-4094>]}
```

Variable definitions

The following table defines variables you can use with the `eapol multihost voip-vlan <1-5> {[enable] [vid <1-4094>]}` command.

Variable	Value
enable	Enables VoIP VLAN.
voip-vlan <1-5>	Sets number of VoIP VLAN from 1 to 5.
vid <1-4094>	Sets VLAN ID, which ranges from 1 to 4094.

Disabling EAPOL VoIP VLAN

Perform this procedure to disable the EAPOL multihost VoIP VLAN.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Disable the EAPOL multihost VoIP VLAN by using the following command:

```
no eapol multihost voip-vlan <1-5> [enable]
```

Variable Definitions

The following table defines variables you can use with the `no eapol multihost voip-vlan <1-5> [enable]` command.

Variable	Value
enable	Disables VoIP VLAN.
voip-vlan <1-5>	Sets number of VoIP VLAN from 1 to 5.

Configuring EAPOL VoIP VLAN as the default VLAN

Perform this procedure to configure the EAPOL multihost VoIP VLAN as the default setting.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Configure the EAPOL multihost VoIP VLAN by using the following command:

```
default eapol multihost voip-vlan <1-5> [enable] [vid]
```

Variable Definitions

The following table defines variables you can use with the `default eapol multihost voip-vlan <1-5> [enable] [vid]` command.

Variable	Value
enable	Disables VoIP VLAN.
vid	Default VoIP VLAN ID.
voip-vlan <1-5>	Sets number of VoIP VLAN from 1 to 5.

Displaying EAPOL VoIP VLAN

Perform this procedure to display information related to the EAPOL multihost VoIP VLAN.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Display information related to the EAPOL multihost VoIP VLAN by using the following command:

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

Multihost Non-EAP User Based Policy Configuration using ACLI

Clients that do not support EAP can be authenticated based on their MAC address. RADIUS authenticates the Non-EAP users and sends their information similar to the EAP users. Also, the User Based Policy support for Non-EAP users is similar to EAP users.

Use the following procedures to configure 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy.

Enabling Multihost Non-EAP User Based Policy

Perform the following procedure to enable 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy settings.

Prerequisite

RADIUS server must be configured.

Note:

If the RADIUS server is not configured, an error appears while loading the ASCII file.

Procedure step

Enable 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy settings using the following command in the Global Configuration mode:

```
eapol multihost non-eap-user-based-policies { [enable][filter-on-mac enable] }
```

The following table outlines the parameters for this command.

Table 39: apol multihost non-eap-user-based-policies parameters

Parameter	Description
enable	Configures the Multihost Non-EAP User Based Policies settings.
filter-on-mac enable	Configures settings for the Multihost Non-EAP filtering on MAC addresses.

Disabling Multihost Non-EAP User Based Policy

Perform the following procedure to disable 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy settings.

Procedure step

Disable 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy settings using the following command in the Global Configuration mode:

```
no eapol multihost non-eap-user-based-policies { [enable][filter-on-mac enable] }
```

The following table outlines the parameters for this command.

Table 40: no eapol multihost non-eap-user-based-policies parameters

Parameter	Description
enable	Disables the Multihost Non-EAP User Based Policies settings.
filter-on-mac enable	Disables settings for the Multihost Non-EAP filtering on MAC addresses.

Setting Multihost Non-EAP User Based Policy as Default Configuration

Perform the following procedure to set 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy as the default configuration.

Procedure steps

Set 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy settings as default configuration using the following command in the Global Configuration mode:

```
default eapol multihost non-eap-user-based-policies { [enable]
[filter-on-mac enable] }
```

The following table outlines the parameters for the command.

Table 41: default eapol multihost non-eap-user-based-policies parameters

Parameter	Description
enable	Sets the default Multihost Non-EAP User Based Policies settings.
filter-on-mac enable	Sets the default Multihost Non-EAP settings for filtering on MAC addresses.

802.1X or non-EAP with Fail Open VLAN configuration using ACLI

Use the procedures in this section to configure the 802.1X non-EAP with Fail Open VLAN using ACLI.

Note:

The switch does not validate that RADIUS Assigned VLAN attribute is not the same as the Fail_Open VLAN. This means that if you configure the Fail_Open VLAN name or ID the same as one of the VLAN names or IDs which can be returned from the RADIUS server, then EAP or NEAP clients is assigned to the Fail_Open VLAN even though no failure to connect to the RADIUS server has occurred.

Enabling EAPOL Fail Open VLAN

Perform this procedure to enable the EAPOL Fail Open VLAN.

Prerequisites

- Log on to the Global configuration mode using ACLI.

Procedure steps

Enable the EAPOL Fail Open VLAN by using the following command:

```
eapol multihost fail-open-vlan {[enable] [vid <1-4094>]}
```

Variable Definitions

The following table defines variables you can use with the `eapol multihost fail-open-vlan {[enable] [vid <1-4094>]}` command.

Variable	Value
Enable	Enables fail-open-vlan.
Vid <1-4094>	Specifies a guest VLAN ID in a range from <1-4094>.

Disabling EAPOL Fail Open VLAN

Perform this procedure to disable the EAPOL Fail Open VLAN.

Prerequisites

- Log on to the Global configuration mode using ACLI.

Procedure steps

Disable the EAPOL Fail Open VLAN by using the following command:

```
no eapol multihost fail-open-vlan [enable]
```

Variable Definitions

The following table defines variables you can use with the `no eapol multihost fail-open-vlan [enable]` command.

Variable	Value
Enable	Disables the Fail Open VLAN.

Setting EAPOL Fail Open VLAN as the default

Perform this procedure to set the EAPOL Fail Open VLAN as the default.

Prerequisites

- Log on to the Global configuration mode using ACLI.

Procedure steps

Set the EAPOL Fail Open VLAN as the default by using the following command:

```
default eapol multihost fail-open-vlan [enable] [vid]
```

Variable Definitions

The following table defines variables you can use with the `default eapol multihost fail-open-vlan [enable] [vid]` command.

Variable	Value
Enable	Disables the Fail Open VLAN.
Vid	Sets the default Fail Open VLAN ID.

Displaying EAPOL Fail Open VLAN

Perform this procedure to display information related to the EAPOL Fail Open VLAN.

Prerequisites

- Log on to the privileged exec mode and configuration mode using ACLI.

Procedure steps

Display the status of the fail-open VLAN by using the following command:

```
show eapol multihost fail-open-vlan
```

Fail Open VLAN Continuity mode configuration using ACLI

Use the procedures in this section to configure Fail Open VLAN Continuity mode using ACLI.

Enabling EAPOL Fail Open VLAN Continuity mode

Perform this procedure to enable the EAPOL Fail Open VLAN Continuity mode.

Before you begin

Enable EAPOL Fail Open VLAN.

Procedure

1. Enter Global configuration mode.
2. Use the following command to enable EAPOL Fail Open VLAN Continuity mode:

```
eapol multihost fail-open-vlan continuity-mode enable
```

Disabling EAPOL Fail Open VLAN Continuity mode

Perform this procedure to disable EAPOL Fail Open VLAN continuity mode.

Procedure

1. Enter Global configuration mode.
2. Use the following command to disable EAPOL Fail Open VLAN continuity mode:

```
no eapol multihost fail-open-vlan continuity-mode enable
```

Displaying EAPOL Fail Open VLAN Continuity mode

Perform this procedure to display information related to EAPOL Fail Open VLAN Continuity mode.

Procedure

1. Enter Global configuration mode.
 2. Use one of the following commands to display the status of EAPOL Fail Open VLAN mode:


```
show eapol multihost fail-open-vlan
```

OR

```
show eapol multihost
```
-

Configuring multihost support

Configure multihost support by completing the following steps:

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

eapol multihost command

This command is executed in the Interface Configuration mode.

The syntax for the **eapol multihost** command is

```
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>] [non-eap-mac-max <1-32>]
```

```
[non-eap-phone-enable] [non-eap-use-radius-assigned-vlan] [port]
[radius-non-eap-enable] [use-most-recent-radius-vlan] [use-radius-
assigned-vlan]}
```

The following table outlines the parameters for this command.

Table 42: eapol multihost parameters

Parameter	Description
adac-non-eap-enable	Allow authentication of Non-EAP Phones using ADAC.
allow-non-eap-enable	Enables MAC addresses of non-EAP clients.
auto-non-eap-mhsa-enable	Enables autoauthentication of non-EAP clients in the Multiple Host with Single Authentication (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-mac-max	Specifies the maximum number of EAP MAC addresses allowed per port.
eap-packet-mode {multicast unicast}	Enables the packet mode (multicast or unicast) for EAP requests.
eap-protocol-enable	Enables EAP protocol on port
enable	Globally enables EAPOL.
mac-max	Specifies the maximum number of MAC addresses allowed per port.
non-eap-mac-max	Specifies the maximum number of non-EAP MAC addresses allowed per port.
non-eap-phone-enable	Enables Avaya IP Phone clients as another non-EAP type.
non-eap-use-radius-assigned-vlan	Allows the use of VLAN IDs assigned by RADIUS for non-EAP clients.
port	The port number on which to apply EAPOL settings.
radius-non-eap-enable	Enables RADIUS authentication of non-EAP clients.
use-most-recent-radius-vlan	Allows the use of most recent RADIUS VLAN.
use-radius-assigned-vlan	Enables use of RADIUS-assigned VLAN values in the multihost mode.

no eapol multihost command

The `no eapol multihost` command disables EAPOL multihost. This command is executed in the Interface Configuration mode.

The syntax for the `no eapol multihost` command is

```
no eapol multihost [enable] [port] [allow-non-eap-enable] [radius-
non-eap-enable] [auto-non-eap-mhsa-enable] [non-eap-phone-enable]
[use-radius-assigned-vlan] [non-eap-use-radius-assigned-vlan] [use-
most-recent-radius-vlan]
```

The following table outlines the parameters for this command. If you do not specify parameters, the command resets all EAPOL multihost settings to the defaults.

Table 43: no eapol multihost parameters

Parameter	Description
allow-non-eap-enable	disables MAC addresses of non-EAP clients.
auto-non-eap-mhsa-enable	disables auto-authentication of non-EAP clients.
enable	disables EAP multihost mode.
non-eap-mac-max	specifies the maximum number of non-EAP authenticated MAC addresses allowed.
non-eap-mac	disables allowing a non-EAPOL MAC address.
non-eap-phone-enable	disables authentication of Avaya IP Phone clients as another non-EAP type.
non-eap-use-radius-assigned-vlan	disables the use of VLAN IDs assigned by RADIUS for non-EAP clients.
port	the port number on which to disable EAPOL.
radius-non-eap-enable	disables RADIUS authentication of non-EAP clients.
use-most-recent-radius-vlan	disables the use of VLAN IDs assigned by RADIUS.
use-radius-assigned-vlan	disables use of RADIUS-assigned VLAN values in the MHMA mode.

default eapol multihost command

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

The syntax for the default EAPOL multihost command is

```
default eapol multihost [enable] [port] [mac-max] [eap-mac-max] [non-
eap-mac-max] [allow-non-eap-enable] [radius-non-eap-enable] [auto-
non-eap-mhsa-enable] [non-eap-phone-enable][use-radius assigned-
vlan] [eap-packet-mode] [use-most-recent-radius-vlan] [non-eap-use-
radius-assigned-vlan]
```

The following table outlines the parameters for this command. If you do not specify parameters, the command resets all EAPOL multihost settings to the defaults.

Table 44: default eapol multihost parameters

Parameter	Description
allow-non-eap-enable	resets control of non-EAP clients (MAC addresses) to the default (disabled).
auto-non-eap-mhsa-enable	disables auto-authentication of non-EAP clients.
mac-max	resets the maximum number of clients allowed on the port to the default value (1).
eap-mac-max	resets the maximum number of EAP clients allowed on the port to the default value (1).
eap-packet-mode	Resets the EAP packet mode to the default (multicast).
enable	restores EAPOL multihost support status to the default value (disabled).
non-eap-mac	resets the non-EAP MAC addresses to the default.
non-eap-mac-max	resets the maximum number of non-EAP authenticated MAC addresses allowed to the default value (1).
non-eap-phone-enable	disables authentication of Avaya IP Phone clients as non-EAP type.
non-eap-use-radius-assigned-vlan	disables the use of VLAN IDs assigned by RADIUS for non-EAP clients.
port	the port number on which to disable EAPOL.
radius-non-eap-enable	disables RADIUS authentication of non-EAP clients.
use-most-recent-radius-vlan	disables the use of most recent RADIUS VLAN.
use-radius-assigned-vlan	disables use of RADIUS-assigned VLAN values in the MHMA mode.

eapol multihost enable command

The `eapol multihost enable` command enables multihost support for EAPOL.

The syntax for the `eapol multihost enable` command is

```
eapol multihost [port <portlist>] enable
```

- where

<portlist> is the list of ports on which you want to enable EAPOL support. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies to all ports on the interface.

The default is disabled.

The **eapol multihost [port <portlist>] enable** command is executed in the Interface Configuration mode.

no eapol multihost enable command

The **no eapol multihost enable** command disables the EAPOL multihost.

The syntax for the **no eapol multihost enable** command is

```
no eapol multihost [<portlist>] [enable] [allow-non-eap-enable]
[radius-non-eap-enable] [auto-non-eap-mhsa-enable] [non-eap-phone-
enable] [use-radius-assigned-vlan]
```

Table 45: no eapol multihost command parameters

Variable	Description
<portlist>	is the list of ports on which you want to disable EAPOL support. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies to all ports on the interface
enable	Disables eapol on the desired ports.
radius-non-eap-enable	Disables RADIUS authentication of non-EAP clients.
allow-non-eap-enable	Disables control of non-EAP clients (MAC addresses).
auto-non-eap-mhsa-enable	Disables auto-authentication of non-EAP clients.
non-eap-phone-enable	Disables Avaya IP Phone clients.
use-radius-assigned-vlan	Disables use of RADIUS-assigned VLAN.

The **no eapol multihost enable** command is executed in the Interface Configuration mode.

eapol multihost eap-mac-max command

The `eapol multihost eap-mac-max` command sets the maximum number of EAP clients.

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

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

- where

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

`<num>` is an integer in the range 1–32 that specifies the maximum number of EAP clients allowed. The default is 1.

The `eapol multihost [port <portlist>] eap-mac-max` command is executed in the Interface Configuration mode.

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.

eapol multihost use radius-assigned-vlan command

To enable RADIUS-assigned VLAN use in the MHMA mode, use the following command in the Global Configuration mode:

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

The following table outlines the parameters for this command.

Table 46: eapol multihost [use-radius-assigned-vlan] parameters

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

To enable RADIUS-assigned VLAN use in the MHMA mode for the desired interface, use the following command:

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

The following table outlines the parameters for this command.

Table 47: eapol multihost [use-radius-assigned-vlan] parameters: Interface mode

Parameter	Description
<portlist>	the port on which you want RADIUS-assigned VLAN use configured in the MHMA mode. You can enter a single port, several ports or a range of ports.
use-radius-assigned-vlan	enables RADIUS-assigned VLAN use on the desired interface.

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

To configure support for non-EAPOL hosts on EAPOL-enabled ports, do the following:

1. Ensure that:
 - a. EAPOL is enabled globally and locally (for the desired interface ports). For more information, see [Configuring EAPOL security](#) on page 132.
 - b. the desired ports are enabled for multihost mode. For more information, see [Configuring multihost support](#) on page 155.
 - c. guest VLAN is disabled locally (for the desired interface ports). For more information, see [Configuring guest VLANs](#) on page 145.
2. Enable non EAPOL support globally on the switch and locally (for the desired interface ports), using one or both of the following authentication methods:
 - a. local authentication. For more information, see [Enabling local authentication of non EAPOL hosts on EAPOL-enabled ports](#) on page 163.

- b. RADIUS authentication. For more information, see [Enabling RADIUS authentication of non EAPOL hosts on EAPOL-enabled ports](#) on page 163.
3. Specify the maximum number of non EAPOL MAC addresses allowed on a port. For more information, see [Specifying the maximum number of non EAPOL hosts allowed](#) on page 168.
4. For local authentication only, identify the MAC addresses of non EAPOL hosts allowed on the ports. For more information, see [Creating the allowed non EAPOL MAC address list](#) on page 168.

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.

To enable local authentication of non EAPOL hosts globally on the use the following command in Global Configuration mode:

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

To enable local authentication of non EAPOL hosts for a specific port or for all ports on an interface, use the following command in Interface configuration mode:

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

- where

<portlist> is the list of ports on which you want to enable non EAPOL hosts using local authentication. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies to all ports on the interface.

To discontinue local authentication of non EAPOL hosts on EAPOL-enabled ports, use the **no** or **default** keywords at the start of the commands in both the Global and Interface configuration modes.

Enabling RADIUS authentication of non EAPOL hosts on EAPOL-enabled ports

For RADIUS authentication of non EAPOL hosts on EAPOL-enabled ports, you must enable the feature globally on the switch and locally for ports on the interface.

To enable RADIUS authentication of non EAPOL hosts globally, use the following command in Global Configuration mode:

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

The following table outlines the parameters for this command.

Table 48: eapol multihost radius-non-eap-enable command

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

To enable RADIUS authentication of non EAPOL hosts for a specific port or for all ports on an interface, use the following command in Interface configuration mode:

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

The following table outlines the parameters for this command.

Table 49: eapol multihost radius-non-eap-enable command: Interface mode

Parameter	Description
<portlist>	the port or ports on which you want RADIUS authentication enabled. You can enter a single port, several ports or a range of ports. If you do not specify a port parameter, the command enables RADIUS authentication of non-EAP hosts on all ports on the interface.
radius-non-eap-enable	enables RADIUS authentication on the desired interface or on a specific port, for non EAPOL hosts.

The default setting for this feature is: disabled.

To discontinue RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports, use the **no** or **default** keywords at the start of the commands, in both the Global and Interface configuration modes.

Configuring the format of the RADIUS password attribute when authenticating non-EAP MAC addresses using RADIUS

To configure the format of the RADIUS password when authenticating non-EAP clients using RADIUS, use the following command in Global Configuration mode:

```
eapol multihost non-eap-pwd-fmt
```

The syntax for the **eapol multihost non-eap-pwd-fmt** command is

```
eapol multihost non-eap-pwd-fmt {[ip-addr] [mac-addr] [port-number]
[key] [key-string <key-string>] [padding] [no-padding]}
```


The following table outlines the parameters for this command.

Table 50: eapol multihost non-eap-pwd-fmt parameters

Parameter	Description
ip-addr	Includes switch IP address string.
mac-addr	Includes MAC address string.
port-number	Includes port string.
key	Includes configurable key string.
key-string <key-string>	Defines the Non-EAP configurable key.
padding	The RADIUS password uses dots for every missing parameter.
no-padding	The RADIUS password uses dots only to separate fields. This is the default setting.

To exclude an attribute from the RADIUS password, use the **no** or **default** keywords at the start of the commands, in Global Configuration mode.

Setting the configurable key for RADIUS NEAP password

From release 5.7 onwards, the RADIUS NEAP password includes a configurable key string in addition to IP address, MAC address, and port number. By default the configurable key feature is disabled and the key is set to null.

Procedure

1. Enter Global Configuration mode.
2. Use the following command to include the configurable key in the RADIUS NEAP password:

```
eapol multihost non-eap-pwd-fmt key
```
3. Use the following command to define the key string:

```
eapol multihost non-eap-pwd-fmt key-string <key-string>
```

 - where <key-string> is a string of up to 32 ASCII characters.

*** Note:**

If you are using an SSH image or a non-SSH image with password security enabled you cannot enter the key immediately in clear text. Press Enter after "key-string", enter the password, and then re-enter the password to confirm.

Related RADIUS NEAP password commands

When you configure the RADIUS password, you can also use the following commands:

- `show eapol multihost non-eap-pwd-fmt`—this command shows the password fields and padding.
- `show eapol multihost non-eap-pwd-fmt key`—this command prints the key used. The password is printed in cleartext only when password security is not enabled. Otherwise, the password is printed as a string of asterisks.

Enabling RADIUS-assigned VLAN for non-EAP MACs

To enable RADIUS-assigned VLAN use for non-EAP MACs in the MHMA mode, use the following command in the Global Configuration mode:

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

RADIUS-assigned VLAN use for non-EAP MACs in the MHMA mode is disabled by default.

To enable RADIUS-assigned VLAN use for non-EAP MACs in the MHMA mode for a specific interface, use the following command in the Interface Configuration mode:

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

RADIUS-assigned VLAN use for non-EAP MACs in the MHMA mode is disabled by default.

Variable definitions

The following table outlines the parameters for the `eapol multihost [non-eap-use-radius-assigned-vlan]` command in the Global Configuration mode:

Variable	Value
[non-eap-use-radius- assigned-vlan]	Globally enables RADIUS-assigned VLAN use for non-EAP MACs in the MHMA mode.

The following table outlines the parameters for the `eapol multihost [port <portlist>] [non-eap-use-radius-assigned-vlan]` command in the Interface Configuration mode:

Variable	Value
<portlist>	Defines the port on which to enable RADIUS-assigned VLAN use for non-EAP configured in the MHMA mode. You can

Variable	Value
	enter a single port, several ports or a range of ports.
[non-eap-use-radius- assigned-vlan]	Enables RADIUS-assigned VLAN use on the interface.

Disabling RADIUS-assigned VLAN for non-EAP MACs

To disable RADIUS-assigned VLAN use for non-EAP macs in the MHMA mode, use one of the following commands in the Global Configuration mode:

```
no eapol multihost [non-eap-use-radius-assigned-vlan]
```

OR

```
default eapol multihost [non-eap-use-radius-assigned-vlan]
```

RADIUS-assigned VLAN use for non-EAP MACs in the MHMA mode is disabled by default.

To disable RADIUS-assigned VLAN use for non-EAP MACs in the MHMA mode for a specific interface, use the following command in the Interface Configuration mode:

```
no eapol multihost [port <portlist>] [non-eap-use-radius-assigned-vlan]
```

OR

```
default eapol multihost [non-eap-use-radius-assigned-vlan]
```

RADIUS-assigned VLAN use for non-EAP MACs in the MHMA mode is disabled by default.

Variable definitions

The following table outlines the parameters for the `no eapol multihost [non-eap-use-radius-assigned-vlan]` and `default eapol multihost [non-eap-use-radius-assigned-vlan]` commands in the Global Configuration mode:

Variable	Value
[non-eap-use-radius- assigned-vlan]	Globally disables RADIUS-assigned VLAN use for non-EAP MACs in the MHMA mode.

The following table outlines the parameters for the `no eapol multihost [port <portlist>] [non-eap-use-radius-assigned-vlan]` and `default eapol multihost [non-eap-use-radius-assigned-vlan]` commands in the Interface Configuration mode:

Variable	Value
<portlist>	Defines the port on which to enable RADIUS-assigned VLAN use for non-EAP configured in the MHMA mode. You can enter a single port, several ports or a range of ports.
[non-eap-use-radius- assigned-vlan]	Disables RADIUS-assigned VLAN use on the interface.

Specifying the maximum number of non EAPOL hosts allowed

To configure the maximum number of non EAPOL hosts allowed for a specific port or for all ports on an interface, use the following command in Interface configuration mode:

```
eapol multihost [port <portlist>] non-eap-mac-max <value>
```

- where

<portlist> is the list of ports to which you want the setting to apply. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command sets the value for all ports on the interface.

<value> is an integer in the range 1–32 that specifies the maximum number of non EAPOL clients allowed on the port at one time. The default is 1.

Important:

The configurable maximum number of non- EAPOL clients for each port is 32, but Avaya recommends that the maximum allowed for each port be lower. Avaya recommends that the combined maximum be approximately 200 for each box and 800 for a stack.

Creating the allowed non EAPOL MAC address list

To specify the MAC addresses of non EAPOL hosts allowed on a specific port or on all ports on an interface, for local authentication, use the following command in Interface configuration mode:

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

- where

<portlist> is the list of ports on which you want to allow the specified non EAPOL hosts. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies to all ports on the interface.

<H.H.H> is the MAC address of the allowed non EAPOL host.

Viewing non EAPOL host settings and activity

Various show commands allow you to view:

- global settings. For more information, see [Viewing global settings for non EAPOL hosts](#) on page 169.
- port settings. For more information, see [Viewing port settings for non EAPOL hosts](#) on page 169.
- allowed MAC addresses, for local authentication. For more information, see [Viewing allowed MAC addresses](#) on page 170.
- current non EAPOL hosts active on the switch. For more information, see [Viewing current non EAPOL host activity](#) on page 170.
- status in the Privilege Exec mode. For more information, see [show eapol multihost status command](#) on page 134.

Viewing global settings for non EAPOL hosts

To view global settings for non EAPOL hosts on EAPOL-enabled ports, use the following command in Privileged Exec, Global Configuration, or Interface configuration mode:

```
show eapol multihost
```

The display shows whether local and RADIUS authentication of non EAPOL clients is enabled or disabled.

Important:

If you apply the `show eapol multihost` command on a large stack with complex configuration, you can experience slow output if this command is executed within 4-5 minutes of the stack being booted or power-cycled. If you wait 5 minutes after the stack is booted or power-cycled before executing this show command, the normal response times will be observed.

Viewing port settings for non EAPOL hosts

To view non EAPOL support settings for each port, use the following command in Privileged Exec, Global Configuration, or Interface configuration mode:

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

- where

`<portlist>` is the list of ports you want to view. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command displays all ports.

For each port, the display shows whether local and RADIUS authentication of non EAPOL clients is enabled or disabled, and the maximum number of non EAPOL clients allowed at a time.

Viewing allowed MAC addresses

To view the MAC addresses of non EAPOL hosts allowed to access ports on an interface, use the following command in Privileged Exec, Global Configuration, or Interface configuration mode:

```
show eapol multihost non-eap-mac interface [<portlist>]
```

- where

`<portlist>` is the list of ports you want to view. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command displays all ports.

The display lists the ports and the associated allowed MAC addresses.

Viewing current non EAPOL host activity

To view information about non EAPOL hosts currently, use the following command in Privileged Exec, Global Configuration, or Interface configuration mode:

```
show eapol multihost non-eap-mac status [<portlist>]
```

- where

`<portlist>` is the list of ports you want to view. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command displays all ports.

Important:

If you apply the `show eapol multihost non-eap-mac status [<portlist>]` command on a large stack with complex configuration, you can experience slow output if this command is executed within 4-5 minutes of the stack being booted or power-cycled. If you wait 5 minutes after the stack is booted or power-cycled before executing this show command, the normal response times will be observed.

The following example shows sample output for the command.

```

show eapol multihost non-eap-mac status
Unit/Port Client MAC Address State
-----
1/5 00:01:00:07:00:01      Authenticated By RADIUS
1/7 00:02:B3:BC:AF:6E      Authenticated By RADIUS
1/7 00:C0:C1:C2:C3:C4      Authenticated Locally
1/7 00:C0:C1:C2:C3:C7      Authenticated Locally
2/21 00:02:00:21:00:80      Authenticated By RADIUS
3/12 00:03:12:21:00:82      Auto-Learned For MHSA
3/15 00:0A:E4:01:10:21      Authenticated For IP Telephony
3/15 00:0A:E4:01:10:22      Authenticated For IP Telephony
-----

```

Configuring EAP and non-EAP multiple VLAN capability

To enable the multiple VLAN capability for EAP and non-EAP hosts, use the following command in Global Configuration mode:

```
eapol multihost multivlan enable
```

The default setting for this feature is: -disabled.

To disable the multiple VLAN capability for EAP and non-EAP hosts, use the **no** or **default** keywords at the start of the commands, in the Global Configuration mode.

Important:

Before you can configure the multiple VLAN capability for EAP and non-EAP hosts, you must disable EAP globally on the switch.

Important:

Avaya recommends that you do not change the multiple VLAN status while Fail Open VLAN is enabled.

Important:

You cannot enable EAP and non-EAP multiple VLAN capability, and use-most-recent-RADIUS assigned VLAN at the same time.

Viewing EAP and non-EAP multiple VLAN capability status

To display the status the multiple VLAN capability for EAP and non-EAP hosts, use the following command in User EXEC mode:

```
show eapol multihost multivlan
```

Using the EAP and NEAP separation command

Use the `no eap multihost eap-protocol-enable` command to disable EAP clients without disabling NEAP clients.

Ensure eapol is enabled globally and per port.

Variables

Table 51: eap multihost eap-protocol-enable parameters

Variable	Value
eap multihost eap-protocol-enable	Global and per port: allow and process eap packets.
no eap multihost eap-protocol-enable	Global and per port: drop all eap packets.
default eap multihost eap-protocol-enable	Per port: allow and process eap packets.
show eapol multihost interface <port #>	Per port: displays the parameter.

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

You can configure 802.1X dynamic authorization extension (RFC 3576) for a third party device to dynamically change VLANs on switches or close user sessions.

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

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

Prerequisites

- 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

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Configure RADIUS dynamic authorization extension by using the following command:

```
radius dynamic-server client A.B.C.D [ secret] [ port
<1024-65535> ] [ enable ] [process-disconnect-requests]
[process-change-of-auth-requests]
```

Variable definitions

The following table defines parameters that you enter with the **radius dynamic-server client A.B.C.D [secret] [port <1024-65535>] [enable] [process-disconnect-requests] [process-change-of-auth-requests]** command.

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

Variable	Value
secret	Configures the RADIUS Dynamic Authorization Client secret word.

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

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

Procedure steps

Disable RADIUS dynamic authorization extension by using the following command:

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

Variable definitions

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

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

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

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

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

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

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

Variable definitions

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

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

Viewing 802.1X dynamic authorization extension (RFC 3576) statistics using ACLI

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

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

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

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

Variable definitions

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

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

Enabling 802.1X dynamic authorization extension (RFC 3576) on EAP ports using ACLI

Enable 802.1X dynamic authorization extension (RFC 3576) on EAP ports for the ports to process CoA and disconnect requests from the RADIUS server.

Prerequisites

- Log on to the Interface Configuration mode in ACLI.

Procedure steps

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

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

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

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

Variable definitions

The following table defines variable parameters that you enter with the `eapol port <LINE> radius-dynamic-server enable` command.

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

Disabling 802.1X dynamic authorization extension (RFC 3576) on EAP ports using ACLI

Disable 802.1X dynamic authorization extension (RFC 3576) on EAP ports to discontinue the ports from processing CoA and disconnect requests from the RADIUS server.

Prerequisites

- Log on to the Interface Configuration mode in ACLI.

Procedure steps

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

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

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

```
no eapol port <LINE> radius-dynamic-server enable
```

Variable definitions

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

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

Enabling 802.1X dynamic authorization extension (RFC 3576) default on EAP ports using ACLI

Enable 802.1X dynamic authorization extension (RFC 3576) default on EAP ports to return the ports to the default configuration for processing CoA and disconnect requests from the RADIUS server.

Prerequisites

- Log on to the Interface Configuration mode in ACLI.

Procedure steps

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

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

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

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

Variable definitions

The following table defines variable parameters that you enter with the `default eapol port <LINE> radius-dynamic-server enable` command.

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

Configuring Wake on LAN with simultaneous 802.1X Authentication using ACLI

Authenticate 802.1X and Wake on LAN simultaneously by changing the 802.1X port configuration control.

Prerequisites

- Configure the primary RADIUS server
- Configure the shared secret
- Enable EAPOL

Procedure steps

1. Enter the Interface Configuration mode.
2. Enable the EAPOL administrative state by using the following command:

```
eapol port <port_list> traffic-control in
```

Variable Definitions

Variable	Value
<port_list>	Specifies a port or list of ports.

Job aid

To verify the EAPOL administrative state, use the following command:

```
show eapol port <port_list>
```

Following is a sample show eapol port <port_list> command output:

EAPOL administrative state enabled – Wake on LAN available	EAPOL administrative state disabled – no Wake on LAN
<pre>4526FX(config-if)# show eapol port 1/1 EAPOL Administrative State: Enabled Unit/Port: 1/1 Admin Status: Auto Auth: No Admin Dir: In Oper Dir: In ReAuth Enable: No ReAuth Period: 3600 Quiet Period: 60 Xmit Period: 30 Supplic Timeout: 30 Server Timeout: 30 Max Req: 2 RDS DSE: No</pre>	<pre>4526FX(config-if)# show eapol port 1/1 EAPOL Administrative State: Disabled Unit/Port: 1/1 Admin Status: Auto Auth: Yes Admin Dir: In Oper Dir: In ReAuth Enable: No ReAuth Period: 3600 Quiet Period: 60 Xmit Period: 30 Supplic Timeout: 30 Server Timeout: 30 Max Req: 2 RDS DSE: No</pre>

Enabling Avaya IP Phone clients on an EAP-enabled port

Enable this feature to allow an Avaya IP Phone client and an EAP PC to exist together on a port. To enable Avaya IP Phone clients on an EAP-enabled port, do the following:

1. Ensure that:
 - EAP is enabled globally and locally (on the desired interface ports). (See [Configuring EAPOL security](#) on page 132).
 - Multihost is enabled on the desired ports. (See [Configuring multihost support](#) on page 155).
 - NonEAP is enabled globally and locally (on the desired interface ports). (See [Configuring support for non-EAPOL hosts on EAPOL-enabled ports](#) on page 162).
 - Filtering is enabled (to capture DHCP packets and to look for the Avaya Phone Signature).

Important:

Avaya recommends that the following two features not be enabled at the same time:

- Guest VLAN.

This is to ensure that the Call server and VoIP information packets the phone receives from the DHCP server are sent on the configured VLAN, so correct information (such as the IP address) is obtained.

- EAP at the phone.

2. Enable Avaya IP Phone clients globally on the switch. (See [Globally enabling Avaya IP Phone clients as a non-EAP type](#) on page 180).
3. Enable Avaya IP Phone clients locally or for specific ports on the interface. (See [Enabling Avaya IP Phone clients in the interface mode](#) on page 181).
4. Specify the maximum number of non EAPOL MAC addresses allowed: the maximum number allowed is 32.

Globally enabling Avaya IP Phone clients as a non-EAP type

To globally enable Avaya IP Phone clients as a non-EAP type, use the following command in the Global Configuration mode:

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

The following table outlines the parameters for this command.

Table 52: eapol multihost non-eap-phone-enable parameters

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

To globally disable Avaya IP Phone clients as a non-EAP type, use one of the following commands in the Global Configuration mode:

```
no eapol multihost {[non-eap-phone-enable]}
```

or

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

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

Table 53: no eapol multihost non-eap-phone-enable parameters

Parameter	Description
non-eap-phone-enable	globally disables Avaya IP Phone clients as a non-EAP type.

Table 54: default eapol multihost non-eap-phone-enable parameters

Parameter	Description
non-eap-phone-enable	globally sets the default (disable) for Avaya IP Phone clients as a non-EAP type.

Enabling Avaya IP Phone clients in the interface mode

To enable Avaya IP Phone clients in the interface mode, use the following command:

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

Table 55: eapol multihost non-eap-phone-enable parameters: Interface mode

Parameter	Description
<portlist>	the port or ports on which you want Avaya IP Phone clients enabled as a non-EAP type. You can enter a single port, several ports or a range of ports.
non-eap-phone-enable	enables Avaya IP Phone clients as a non-EAP type, on the desired port or ports.

To disable Avaya IP Phone clients in the interface mode, use one of the following commands:

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

or

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

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

Table 56: no eapol multihost non-eap-phone-enable parameters: Interface mode

Parameter	Description
<portlist>	the port or ports on which you want Avaya IP Phone clients disabled as a non-EAP type. You can enter a single port, several ports or a range of ports.
non-eap-phone-enable	disables Avaya IP Phone clients as a non-EAP type, on the desired port or ports.

Table 57: default eapol multihost non-eap-phone-enable parameters: Interface mode

Parameter	Description
<portlist>	the port or ports on which you want the defaults for Avaya IP Phone clients set. You can enter a single port, several ports or a range of ports.
non-eap-phone-enable	sets the default (disable) for Avaya IP Phone clients, on the desired port or ports.

Configuring MHSA

To configure MHSA support, do the following:

1. Ensure that:
 - a. EAPOL is enabled globally and locally (for the desired interface ports). For more information, see [Configuring EAPOL security](#) on page 132.
 - b. the desired ports are enabled for multihost mode. For more information, see [Configuring multihost support](#) on page 155.
 - c. guest VLAN is disabled locally (for the desired interface ports). For more information, see [Configuring guest VLANs](#) on page 145.
2. Enable MHSA globally on the switch. For more information, see [Globally enabling support for MHSA](#) on page 183.
3. Configure MHSA settings for the interface or for specific ports on the interface. For more information, see [Configuring interface and port settings for MHSA](#) on page 183.

- a. Enable MHSa support.
 - b. Specify the maximum number of non EAPOL MAC addresses allowed.
- By default, MHSa support on EAP-enabled ports is disabled.

Globally enabling support for MHSa

To enable support for MHSa globally, use the following command in Global Configuration mode:

```
eapol multihost auto-non-eap-mhsa-enable
```

To discontinue support for MHSa globally, use one of the following commands in Global Configuration mode:

```
no eapol multihost auto-non-eap-mhsa-enable
default eapol multihost auto-non-eap-mhsa-enable
```

Configuring interface and port settings for MHSa

To configure MHSa settings for a specific port or for all ports on an interface, use the following command in Interface configuration mode:

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

- where

<portlist> is the list of ports to which you want the settings to apply. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port parameter, the command applies the settings to all ports on the interface.

This command includes the following parameters for configuring MHSa:

eapol multihost [port <portlist>] followed by:	
auto-non-eap-mhsa-enable	Enables MHSa on the port. The default is disabled. To disable MHSa, use the no or default keywords at the start of the command.
non-eap-mac-max <value>	Sets the maximum number of non EAPOL clients allowed on the port at one time. <ul style="list-style-type: none"> • <value> is an integer in the range 1 to 32. The default is 1. <p>! Important: The configurable maximum number of non EAPOL clients for each port is 32, but Avaya expects that the</p>

	usual maximum allowed for each port will be lower. Avaya expects that the combined maximum will be approximately 200 for each box and 800 for a stack.
--	--

Viewing MHPA settings and activity

For more information about the commands to view MHPA settings and non EAPOL host activity, see [Viewing non EAPOL host settings and activity](#) on page 169.

Setting SNMP v1, v2c, v3 Parameters

Earlier releases of SNMP used a proprietary method for configuring SNMP communities and trap destinations for specifying SNMPv1 configuration that included up to four trap destinations and associated community strings that can be configured using SNMP Set requests on the s5AgTrpRcvrTable.

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

The also supports the previous proprietary SNMP configuration methods for backward compatibility.

All the configuration data configured in the proprietary method is mapped into the SNMPv3 tables as read-only table entries. In the new standards-based SNMPv3 method of configuring SNMP, all processes are configured and controlled through the SNMPv3 MIBs. The Command Line Interface commands change or display the single read-only community, read-write community, or four trap destinations of the proprietary method of configuring SNMP. Otherwise, the commands change or display SNMPv3 MIB data.

The software supports MD5 and SHA authentication, as well as AES DES, and 3DES encryption.

The SNMP agent supports exchanges using SNMPv1, SNMPv2c and SNMPv3. Support for SNMPv2c introduces a standards-based GetBulk retrieval capability using SNMPv1 communities. SNMPv3 support introduces high security 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. Export restrictions on SHA and DES necessitate support for domestic and non domestic executable images or defaulting to no encryption for all customers.

The traps can be configured in SNMPv1, v2, or v3 format. If you do not identify the version (v1, v2, or v3), the system formats the traps in the v1 format. A community string can be entered if the system requires one.

SNMPv3 table entries stored in NVRAM

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

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

Configuring SNMP using ACLI

Use the following commands to configure and manage SNMP:

- [show snmp-server command](#) on page 186
- [snmp-server authentication-trap command](#) on page 187
- [no snmp-server authentication-trap command](#) on page 187
- [default snmp-server authentication-trap command](#) on page 187
- [snmp-server community for read or write command](#) on page 188
- [snmp-server community command](#) on page 188
- [no snmp-server community command](#) on page 189
- [default snmp-server community command](#) on page 190
- [snmp-server contact command](#) on page 191
- [no snmp-server contact command](#) on page 191
- [default snmp-server contact command](#) on page 191
- [snmp-server command](#) on page 192
- [no snmp-server command](#) on page 192
- [snmp-server host command](#) on page 192
- [no snmp-server host command](#) on page 194

- [default snmp-server host command](#) on page 195
- [snmp-server location command](#) on page 196
- [no snmp-server location command](#) on page 196
- [default snmp-server location command](#) on page 196
- [snmp-server name command](#) on page 197
- [no snmp-server name command](#) on page 197
- [default snmp-server name command](#) on page 197
- [Enabling SNMP server notification control using ACLI](#) on page 198
- [Disabling SNMP server notification control using ACLI](#) on page 198
- [Setting SNMP server notification control to default using ACLI](#) on page 199
- [Viewing the SNMP server notification control table using ACLI](#) on page 199
- [snmp-server user command](#) on page 200
- [no snmp-server user command](#) on page 202
- [snmp-server view command](#) on page 202
- [no snmp-server view command](#) on page 203
- [snmp-server bootstrap command](#) on page 205

show snmp-server command

The `show snmp-server` command displays the SNMP configuration.

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

```
show snmp-server {host|notification-control|notify-filter|user|view}
```

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

[Table 58: show snmp-server command parameters and variables](#) on page 186 describes the parameters and variables for the `show snmp-server` command.

Table 58: show snmp-server command parameters and variables

Parameters and variables	Description
host	Displays the trap receivers configured in the SNMPv3 MIBs.
notification-control	Displays the notification control table
notify-filter	Displays the SNMP notify filter configuration
user	Displays the SNMP users, including views accessible to each user.

Parameters and variables	Description
view	Displays SNMP views.

snmp-server authentication-trap command

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

The syntax for the `snmp-server authentication-trap` command is

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

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

[Table 59: snmp-server authentication-trap command parameters and variables](#) on page 187 describes the parameters and variables for the `snmp-server authentication-trap` command.

Table 59: snmp-server authentication-trap command parameters and variables

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

no snmp-server authentication-trap command

The `no snmp-server authentication-trap` command disables generation of SNMP authentication failure traps.

The syntax for the `no snmp-server authentication-trap` command is

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

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

default snmp-server authentication-trap command

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

The syntax for the `default snmp-server authentication-trap` command is

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

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

snmp-server community for read or write command

This command configures a single read-only or a single read-write community. A community configured using this command does not have access to the SNMPv3 MIBs. These community strings have a fixed MIB view.

The `snmp-server community` command for read/write modifies the community strings for SNMPv1 and SNMPv2c access.


The syntax for the `snmp-server community` for read/write command is

```
snmp-server community [word{notify-view|read-view|ro|rw|write-view}]
```

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

[Table 60: snmp-server community for read/write command](#) on page 188 describes the parameters and variables for the `snmp-server community` for read/write command.

Table 60: snmp-server community for read/write command

Parameters and variables	Description
word [notify-view read-view ro rw write-view]	<p>The following list describes the snmp-server community parameters:</p> <ul style="list-style-type: none"> • notify-view specifies the notify (trap) access view name. • Read-view specifies the read access view name. • ro specifies read-only access with this community string. • rw specifies read-write access with this community string. • write-view specifies the write-access view name. <p> Important: Stations with ro access can retrieve MIB objects, and stations with rw access can retrieve and modify MIB objects. If neither ro nor rw is specified, ro is assumed (default).</p>

snmp-server community command

You can use the `snmp-server community` command to create community strings with varying levels of read, write, and notification access based on SNMPv3 views. These

community strings are separate from those created using the `snmp-server community` for read/write command.

This command affects community strings stored in the SNMPv3 `snmpCommunity` Table, which allows several community strings to be created. These community strings can have any MIB view.

The syntax for the `snmp-server community` command is

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

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

[Table 61: snmp-server community command parameters and variables](#) on page 189 describes the parameters and variables for the `snmp-server community` command.

Table 61: snmp-server community command parameters and variables

Parameters and variables	Description
read-view <view-name>	Changes the read view used by the new community string for different types of SNMP operations. view-name: specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.
write-view <view-name>	Changes the write view used by the new community string for different types of SNMP operations. view-name: specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.
notify-view <view-name>	Changes the notify view settings used by the new community string for different types of SNMP operations. view-name: specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.

no snmp-server community command

The `no snmp-server community` command clears the `snmp-server community` configuration.

The syntax for the `no snmp-server community` command is

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

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

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

If you specify read-only or read-write, then just the read-only or read-write community is removed. If you specify the name of a community string, then the community string with that name is removed.

[Table 62: no snmp-server community command parameters and variables](#) on page 190 describes the parameters and variables for the `no snmp-server community` command.

Table 62: no snmp-server community command parameters and variables

Parameters and variables	Description
ro rw <community-string>	<p>Changes the settings for SNMP:</p> <ul style="list-style-type: none"> • ro rw: sets the specified old-style community string value to NONE, thereby disabling it. • community-string: deletes the specified community string from the SNMPv3 MIBs (that is, from the new-style configuration).

default snmp-server community command

The `default snmp-server community` command restores the community string configuration to the default settings.

The syntax for the `default snmp-server community` command is

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

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

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

[Table 63: default snmp-server community command parameters and variables](#) on page 191 describes the parameters and variables for the `default snmp-server community` command.

Table 63: default snmp-server community command parameters and variables

Parameters and variables	Description
ro rw	Restores the read-only community to Public, or the read-write community to Private.

snmp-server contact command

The `snmp-server contact` command configures the SNMP sysContact value.

The syntax for the `snmp-server contact` command is

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

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

[Table 64: snmp-server contact command parameters and variables](#) on page 191 describes the parameters and variables for the `snmp-server contact` command.

Table 64: snmp-server contact command parameters and variables

Parameters and variables	Description
text	Specifies the SNMP sysContact value.

no snmp-server contact command

The `no snmp-server contact` command clears the sysContact value.

The syntax for the `no snmp-server contact` command is

```
no snmp-server contact
```

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

default snmp-server contact command

The `default snmp-server contact` command restores sysContact to the default value.

The syntax for the `default snmp-server contact` command is

```
default snmp-server contact
```

The **default snmp-server contact** command is executed in the Global Configuration command mode.

snmp-server command

The **snmp-server** command enables or disables the SNMP server.

The syntax for the **snmp-server** command is

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

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

[Table 65: snmp-server command parameters and variables](#) on page 192 describes the parameters and variables for the **snmp-server** command.

Table 65: snmp-server command parameters and variables

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

no snmp-server command

The **no snmp-server** command disables SNMP access.

The syntax for the **no snmp-server** command is

```
no snmp-server
```

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

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

 **Important:**

If you disable SNMP access you cannot use Enterprise Device Manager for the switch.

snmp-server host command

The **snmp-server host** command adds a trap receiver to the trap-receiver table.

In the proprietary method, the table has a maximum of four entries, and these entries can generate only SNMPv1 traps. This command controls the contents of the `s5AgTrpRcvrTable`.

The proprietary method syntax for the `snmp-server host` command is

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

Using the new standards-based SNMP method, you can create several entries in this table, and each can generate v1, v2c, or v3 traps.

! Important:

Before using the desired community string or user in this command, ensure that it has been configured with a `notify-view`.

The new standards-based method syntax for the `snmp-server host` command is

```
snmp-server host <host-ip> [port <trap-port>] {v1 <community-string>|
v2c <community-string> {inform [timeout <1-2147483647>] [retries
<0-255>]} |v3 {auth|no-auth|auth-priv} <username>} {inform [timeout
<1-2147483647>] [retries <0-255>]}}
```

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

[Table 66: snmp-server host command parameters and variables](#) on page 193 describes the parameters and variables for the `snmp-server host` command.

Table 66: snmp-server host command parameters and variables

Parameters and variables	Description
host-ip	Enter a dotted-decimal IP address of a host to be the trap destination.
community-string	If you are using the proprietary method for SNMP, enter a community string that works as a password and permits access to the SNMP protocol.
port <trap-port>	If you are using the new standards-based tables, enter a value from 1 to 65535 for the SNMP trap port.
v1 <community-string>	To configure the new standards-based tables, using v1 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels can be created.
v2c <community-string>	To configure the new standards-based tables, using v2c creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels can be created.

Parameters and variables	Description
v3 {auth no-auth auth-priv}	To configure the new standards-based tables, using v3 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels can be created. The variables are: <ul style="list-style-type: none"> • auth: auth specifies SNMPv3 traps are sent using authentication and no privacy; • no-auth: no-auth specifies SNMPv3 traps are sent using with no authentication and no privacy. • auth-priv: specifies traps are sent using authentication and privacy; this parameter is available only if the image has full SHA/DES support.
username	To configure the new standards-based tables; specifies the SNMPv3 user name for trap destination; enter an alphanumeric string.
{inform [timeout <1-2147483647>] [retries <0-255>]}	Generates acknowledge Inform requests.

no snmp-server host command

The **no snmp-server host** command deletes trap receivers from the table.

The proprietary method syntax for the **no snmp-server host** command is

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

Using the standards-based method of configuring SNMP, trap receivers matching the IP address and SNMP version are deleted.

The standards-based method syntax for the **no snmp-server host** command is

```
no snmp-server host <host-ip> [port <trap-port>] {v1|v2c|v3
<community-string>}
```

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

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

[Table 67: no snmp-server host command parameters and variables](#) on page 195 describes the parameters and variables for the **no snmp-server host** command.

Table 67: no snmp-server host command parameters and variables

Parameters and variables	Description
<host-ip> [<community-string>]	In the proprietary method, enter the following variables: <ul style="list-style-type: none"> • host-ip: the IP address of a trap destination host. • community-string: the community string that works as a password and permits access to the SNMP protocol. If both parameters are omitted, nothing is cleared. If a host IP is included, the community-string is required or an error is reported.
<host-ip>	Using the standards-based method, enter the IP address of a trap destination host.
port <trap-port>	Using the standards-based method, enter the SNMP trap port.
v1 v2c v3 <community-string>	Using the standards-based method, specifies trap receivers in the SNMPv3 MIBs. <community-string>: the community string that works as a password and permits access to the SNMP protocol.

default snmp-server host command

The **default snmp-server host** command restores the old-style SNMP server and the standards based tables are reset (cleared).

The syntax for the **default snmp-server host** command is

```
default snmp-server host
```

The **default snmp-server host** command is executed in the Global Configuration command mode.

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

default snmp-server port

default snmp-server port command restores all trap receivers configured ports to the default port used for listening traps. The default port is 162.

The syntax for the **default snmp-server port** command is

```
default snmp-server port
```

The **default snmp-server port** command is executed in the Global configuration command mode.

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

snmp-server location command

The **snmp-server location** command configures the SNMP sysLocation value.

The syntax for the **snmp-server location** command is

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

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

[Table 68: snmp-server location command parameters and variables](#) on page 196 describes the parameters and variables for the **snmp-server location** command.

Table 68: snmp-server location command parameters and variables

Parameters	Description
text	Specify the SNMP sysLocation value; enter an alphanumeric string of up to 255 characters.

no snmp-server location command

The **no snmp-server location** command clears the SNMP sysLocation value.

The syntax for the **no snmp-server location** command is

```
no snmp-server location
```

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

default snmp-server location command

The **default snmp-server location** command restores sysLocation to the default value.

The syntax for the **default snmp-server location** command is


```
default snmp-server location
```

The **default snmp-server location** command is executed in the Global Configuration command mode.

snmp-server name command

The **snmp-server name** command configures the SNMP sysName value.


The syntax for the **snmp-server name** command is

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

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

[Table 69: snmp-server name command parameters and variables](#) on page 197 describes the parameters and variables for the **snmp-server name** command.

Table 69: snmp-server name command parameters and variables

Parameters and variables	Description
text	Specify the SNMP sysName value; enter an alphanumeric string of up to 255 characters.  Note: On the console, the SNMP server name is truncated. On the Web interface, the full SNMP server name appears.

no snmp-server name command

The **no snmp-server name** command clears the SNMP sysName value.

The syntax for the **no snmp-server name** command is

```
no snmp-server name
```

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

default snmp-server name command

The **default snmp-server name** command restores sysName to the default value.

The syntax for the `default snmp-server name` command is

```
default snmp-server name
```

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

Enabling SNMP server notification control using ACLI

Use this procedure to enable SNMP traps for specific ports, or for all switch ports.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enable SNMP server notification control by using the following command:

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

Variable definitions

Variable	Value
<portlist>	Specifies a port or group of ports. If you do not specify a port or group of ports, notification control is enabled 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, linkDown , linkup . An example of an OID describing the notification type is, 1.3.6.1.6.3.1.1.5.3 , 1.3.6.1.6.3.1.1.5.4 .

Disabling SNMP server notification control using ACLI

Use this procedure to disable SNMP traps for specific ports, or for all switch ports.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Disable the SNMP server notification control by using the following command:

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

Variable definitions

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, linkDown , linkup . An example of an OID describing the notification type is, 1.3.6.1.6.3.1.1.5.3 , 1.3.6.1.6.3.1.1.5.4 .

Setting SNMP server notification control to default using ACLI

Use this procedure to set SNMP traps to the default value (disabled).

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Set SNMP server notification control to default by using the following command:

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

Variable definitions

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 set to default globally.
<WORD>	Specifies a character string or OID describing the notification type. An example of a character string describing the notification type is, linkDown , linkup . An example of an OID describing the notification type is, 1.3.6.1.6.3.1.1.5.3 , 1.3.6.1.6.3.1.1.5.4 .

Viewing the SNMP server notification control table using ACLI

Use this procedure to display the SNMP server notification control table.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display the SNMP server notification control table by using the following command:

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

snmp-server user command

The **snmp-server user** command creates an SNMPv3 user.

For each user, you can create three sets of read/write/notify views:

- for unauthenticated access
- for authenticated access
- for authenticated and encrypted access

The syntax for the **snmp-server user** command for unauthenticated access is:

```
snmp-server user [engine-id <engine-id>] <username> [read-view  
<view-name>] [write-view <view-name>] [notify-view <view-name>]
```

The syntax for the **snmp-server user** command for authenticated access is:

```
snmp-server user <username> [[read-view <view-name>] [write-view  
<view-name>] [notify-view <view-name>]] md5|sha <password> [read-view  
<view-name>] [write-view <view-name>] [notify-view <view-name>]
```

The syntax for the **snmp-server user** command for authenticated and encrypted access is:

```
snmp-server user <username>[[read-view <view-name>] [write-view  
<view-name>] [notify-view <view-name>]] md5|sha <password> [[read-  
view <view-name>] [write-view <view-name>] [notify-view <view-name>]]  
{3des|aes|des} <password> [read-view <view-name>] [write-view <view-  
name>] [notify-view <view-name>]
```

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

The **sha** and **3des/aes/des** parameters are only available if the switch/stack image has SSH support.

For authenticated access, you must specify the **md5** or **sha** parameter. For authenticated and encrypted access, you must also specify the **3des**, **aes**, or **des** parameter.

For each level of access, you can specify read, write, and notify views. If you do not specify view parameters for authenticated access, the user will have access to the views specified for

unauthenticated access. If you do not specify view parameters for encrypted access, the user will have access to the views specified for authenticated access or, if no authenticated views were specified, the user will have access to the views specified for unauthenticated access.

[Table 70: snmp-server user parameters](#) on page 201 describes the parameters and variables for the `snmp-server user` command.

Table 70: snmp-server user parameters

Parameters	Description
username	Specifies the user name. Enter an alphanumeric string of up to 255 characters.
md5 <password>	Specifies the use of an md5 password. <password> specifies the new user md5 password; enter an alphanumeric string. If this parameter is omitted, the user is created with only unauthenticated access rights.
read-view <view-name>	Specifies the read view to which the new user has access: <ul style="list-style-type: none"> view-name: specifies the viewname; enter an alphanumeric string of up to 32 characters.
write-view <view-name>	Specifies the write view to which the new user has access: <ul style="list-style-type: none"> view-name: specifies the viewname; enter an alphanumeric string that can contain at least some of the non alphanumeric characters.
notify-view <view-name>	Specifies the notify view to which the new user has access: <ul style="list-style-type: none"> view-name: specifies the viewname; enter an alphanumeric string that can contain at least some of the non alphanumeric characters.
SHA	Specifies SHA authentication.
3DES	Specifies 3DES privacy encryption.
AES	Specifies AES privacy encryption.
DES	Specifies DES privacy encryption.
engine-id	Specifies the SNMP engine ID of the remote SNMP entity.

! Important:

If a view parameter is omitted from the command, that view type cannot be accessed.

no snmp-server user command

The `no snmp-server user` command deletes the specified user.

The syntax for the `no snmp-server user` command is

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

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

[Table 71: no snmp-server user command parameters and variables](#) on page 202 describes the parameters and variables for the `no snmp-server user` command.

Table 71: no snmp-server user command parameters and variables

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

snmp-server view command

The `snmp-server view` command creates an SNMPv3 view. The view is a set of MIB object instances which can be accessed.

The syntax for the `snmp-server view` command is


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

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

[Table 72: snmp-server view command parameters and variables](#) on page 202 describes the parameters and variables for the `snmp-server view` command.

Table 72: snmp-server view command parameters and variables

Parameters and variables	Description
viewname	Specifies the name of the new view; enter an alphanumeric string.
OID	Specifies Object identifier. OID can be entered as a dotted form OID. Each OID must be preceded by a + or - sign (if this is omitted, a + sign is implied).

Parameters and variables	Description
	<p>The + is not optional. For the dotted form, a sub-identifier can be an asterisk, indicating a wildcard. Here are some examples of valid OID parameters:</p> <ul style="list-style-type: none"> • sysName • +sysName • -sysName • +sysName.0 • +ifIndex.1 • -ifEntry.*.1 (this matches all objects in the ifTable with an instance of 1; that is, the entry for interface #1) • 1.3.6.1.2.1.1.1.0 (the dotted form of sysDescr) <p>The + or - indicates whether the specified OID is included in or excluded from, respectively, the set of MIB objects that are accessible using this view. For example, if you create a view like this:</p> <ul style="list-style-type: none"> • snmp-server view myview +system -sysDescr <p>And you use that view for the read-view of a user, then the user can read only the system group except for sysDescr.</p> <p> Important: There are ten possible OID values.</p>

no snmp-server view command

The `no snmp-server view` command deletes the specified view.

The syntax for the `no snmp-server view` is:

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

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

[Table 73: no snmp-server view command parameters and variables](#) on page 204 describes the parameters and variables for the `no snmp-server view` command.

Table 73: no snmp-server view command parameters and variables

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

snmp-server host for old-style table command

The **snmp-server host** for old-style table command adds a trap receiver to the old-style trap-receiver table. The table has a maximum of four entries, and the entries can generate only SNMPv1 traps. This command controls the contents of the s5AGTrpRcvrTable, which is the set of trap destinations controlled by the SNMP Configuration screen in the console interface.

The syntax for the **snmp-server host** for old-style table command is

```
snmp-server host <host-ip> [port <1-65535>] <community-string>
```

Run the **snmp-server host** for old-style table command in Global Configuration command mode.

[Table 74: snmp-server host for old-style table command parameters and variables](#) on page 204 describes the parameters and variables for the **snmp-server host** for old-style table command.

Table 74: snmp-server host for old-style table command parameters and variables

Parameters and variables	Description
port <1-65535>	Assign SNMP trap port.
<host-ip>	Enter a dotted-decimal IP address of a host that is the trap destination.
<community-string>	Enter a community string that works as a password and permits access to the SNMP protocol.

snmp-server host for new-style table command

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


```
snmp-server host <host-ip> [port <1-65535>] {v1 <community-string>|
v2c <community-string>| v3 {auth|no-auth|auth-priv} <username>}
```

Run the **snmp-server host** for new-style table command in Global Configuration command mode.

[Table 75: snmp-server host for new-style table command parameters and variables](#) on page 205 describes the parameters and variables for the **snmp-server host** for new-style table command.

Table 75: snmp-server host for new-style table command parameters and variables

Parameters and variables	Description
<host-ip>	Enter a dotted-decimal IP address of a host (trap destination).
port <1-65535>	Assign SNMP trap port.
v1 <community-string>	Using v1 creates trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels.
v2c <community-string>	Using v2c creates trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels.
v3 {auth no-auth auth-priv}	Using v3 creates trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels. Enter the following variables: <ul style="list-style-type: none"> • auth no-auth: specifies whether SNMPv3 traps are authenticated • auth-priv: this parameter is available if the image has full SHA/DES support.
<username>	The SNMPv3 user name for trap destination; enter an alphanumeric string.

snmp-server bootstrap command

You can use the **snmp-server bootstrap** command to specify how you wish to secure SNMP communications, as described in the SNMPv3 standards. It creates an initial set of configuration data for SNMPv3. This configuration data follows the conventions described in the SNMPv3 standard (in RFC 3414 and 3415). This command creates a set of initial users, groups, and views.

! Important:

This command deletes all existing SNMP configurations.

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

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

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

[Table 76: snmp-server bootstrap command parameters and variables](#) on page 206 describes the parameters and variables for the `snmp-server bootstrap` command.

Table 76: snmp-server bootstrap command parameters and variables

Parameters and variables	Description
<minimum-secure>	Specifies a minimum security configuration that allows read access and notify access to all processes (or Internet views) using no authentication and no privacy; and write access to all processes using authentication and no privacy.
<semi-secure>	Specifies a partial security configuration that allows read access and notify access but no write access to a small subset of system information (or restricted views) using no authentication and no privacy; and read, write, and notify access to all processes using authentication and no privacy. (Refer to RFCs 3414 and 3415 for a list of the MIB views in the semi-secure restricted set.)
<very-secure>	Specifies a maximum security configuration that allows no access to the users.

RADIUS accounting configuration using ACLI

RADIUS accounting utilizes the same network server settings used for RADIUS authentication. For more information about the commands to configure the RADIUS server settings, see [Configuring switch RADIUS server settings using ACLI](#) on page 127.

The RADIUS accounting UDP port is the RADIUS authentication port +1. By default, the RADIUS accounting UDP port is port 1813.

By default, RADIUS accounting is disabled.

Enabling RADIUS server accounting using ACLI

Use this procedure to enable RADIUS accounting for a Global, EAPOL, or non-EAPOL RADIUS server.

Procedure steps

1. Log on to Global Configuration or Interface Command mode in ACLI.
2. To enable RADIUS accounting for a Global RADIUS server, use the following command:


```
radius server host [<ipaddr> | <ipv6addr>] acct-enable
```
3. To enable RADIUS accounting for an EAPOL RADIUS server, use the following command:


```
radius server host [<ipaddr> | <ipv6addr>] used-by eapol
acct-enable
```
4. To enable RADIUS accounting for a non-EAPOL RADIUS server, use the following command:


```
radius server host [<ipaddr> | <ipv6addr>] used-by non-eapol
acct-enable
```

Variable definitions

Variable	Value
<ipaddr>	Specifies the IPv4 address of the RADIUS server for which you want to enable accounting.
<ipv6addr>	Specifies the IPv6 address of the RADIUS server for which you want to enable accounting.

Disabling RADIUS server accounting using ACLI

Use this procedure to disable RADIUS accounting for a Global, EAPOL, or non-EAPOL RADIUS server.

Procedure steps

1. Log on to Global Configuration or Interface Command mode in ACLI.
2. To disable RADIUS accounting for a Global RADIUS server, use the following command:


```
no radius server host [<ipaddr> | <ipv6addr>] acct-enable
```

3. To disable RADIUS accounting for an EAPOL RADIUS server, use the following command:

```
no radius server host [<ipaddr> | <ipv6addr>] used-by eapol
acct-enable
```

4. To disable RADIUS accounting for a non-EAPOL RADIUS server, use the following command:

```
no radius server host [<ipaddr> | <ipv6addr>] used-by non-
eapol acct-enable
```

Variable definitions

Variable	Value
<ipaddr>	Specifies the IPv4 address of the RADIUS server for which you want to disable accounting.
<ipv6addr>	Specifies the IPv6 address of the RADIUS server for which you want to disable accounting.

Setting RADIUS server accounting to default using ACLI

Use this procedure to set RADIUS accounting for a Global, EAPOL, or non-EAPOL RADIUS server to default.

Procedure steps

1. Log on to Global Configuration or Interface Command mode in ACLI.
2. To set RADIUS accounting for a Global RADIUS server to default, use the following command:

```
default radius server host [<ipaddr> | <ipv6addr>] acct-
enable
```

3. To set RADIUS accounting for an EAPOL RADIUS server to default, use the following command:

```
default radius server host [<ipaddr> | <ipv6addr>] used-by
eapol acct-enable
```

4. To set RADIUS accounting for a non-EAPOL RADIUS server to default, use the following command:

```
default radius server host [<ipaddr> | <ipv6addr>] used-by
non-eapol acct-enable
```

Variable definitions

Variable	Value
<ipaddr>	Specifies the IPv4 address of the RADIUS server for which you want to set accounting to default.
<ipv6addr>	Specifies the IPv6 address of the RADIUS server for which you want to set accounting to default.

Configuring RADIUS interim accounting updates using ACLI

Use the following procedure to enable RADIUS interim accounting updates and configure the interval timeout period for the updates.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Configure RADIUS interim accounting updates by using the following command:

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

Variable definitions

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

Variable	Value
enable	Enables RADIUS accounting interim updates for the switch.
interval <seconds>	Specifies the time interval (in seconds) before RADIUS accounting interim updates times out.
use-server-interval	Uses the value applied by the RADIUS server for the time interval (in seconds)

Variable	Value
	before RADIUS accounting interim updates times out.

Disabling RADIUS interim accounting updates using ACLI

Use this procedure to disable RADIUS interim accounting updates for the switch or to discontinue using the RADIUS server timeout interval for the updates.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Disable RADIUS interim accounting updates by using the following command:

```
no radius accounting interim-updates [enable] [use-server-
interval]
```

Variable definitions

The following table defines parameters that you can enter with the `no radius accounting interim-updates [enable] [use-server-interval]` command.

Variable	Value
enable	Disables RADIUS accounting interim updates for the switch.
use-server-interval	Discontinues using the value applied by the RADIUS server for the time interval (in seconds) before RADIUS accounting interim updates times out.

Configuring RADIUS interim accounting updates to default using ACLI

Use this procedure to configure RADIUS interim accounting updates to default values.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Configure RADIUS interim accounting updates to default by using the following command:

```
default radius accounting interim-updates [enable] [interval]
[use-server-interval]
```

Variable definitions

The following table defines parameters that you can enter with the **default radius accounting interim-updates [enable] [interval] [use-server-interval]** command.

Variable	Value
enable	Configures the RADIUS accounting interim updates status to default (disabled).
interval	Configures the RADIUS accounting interim updates timeout interval to default (600 seconds).
use-server-interval	Configures the use of the RADIUS server applied timeout interval for interim updates to default (enabled).

Viewing RADIUS interim accounting updates information using ACLI

Use this procedure to display information about RADIUS interim accounting updates configuration information.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Configure RADIUS interim accounting updates by using the following command:

```
show radius accounting interim-updates
```

Job aid: show radius accounting interim-updates command output

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

```
ERS-4524GT(config)#show radius accounting interim-updates
RADIUS accounting interim-updates: Disabled
RADIUS accounting interim-updates interval: 600
RADIUS accounting use-server-interval: Enabled
ERS-4524GT(config)#
```

Figure 5: show radius accounting interim-updates command output

TACACS+ configuration using ACLI

This section describes how you configure TACACS+ to perform AAA services for system users.

Configuring switch TACACS+ server settings using ACLI

Configure switch TACACS+ server settings to add a TACACS+ server to your system.

Prerequisites

- Configure the TACACS+ server to be added to your system.
- Log on to the Global Configuration mode in ACLI.


Procedure steps

Configure switch TACACS+ server settings by using the following command:

```
tacacs server
```

Variable definitions

The following table describes variables that you use with the `tacacs server` command.

Variable	Value
host <IPAddr>	Specifies the IP address of the primary server you want to add or configure.
key <key>	Specifies the secret authentication and encryption key used for all communications between the NAS and the TACACS+ server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to confirm the key when you enter it.  Important: The key parameter is a required parameter when you create a new server entry. The parameter is optional when you are modifying an existing entry.
port <port>	Specifies the TCP port for TACACS+. <port> is an integer in the range of 1 to 65535. The default port number is 49.
secondary host <IPAddr>	Specifies the IP address of the secondary server. The secondary server is used only if the primary server does not respond.

Disabling switch TACACS+ server settings using ACLI

Disable switch TACACS+ server settings to discontinue using TACACS+ services in your system.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Disable switch TACACS+ server settings by using one of the following command:

```
no tacacs
```

OR

```
default tacacs
```

These commands erase settings for the TACACS+ primary and secondary servers and secret key; and restore default port settings.

Enabling remote TACACS+ services using ACLI

Enable remote TACACS+ services to provide services to remote users over serial or Telnet connections.

Prerequisites

- Log on to the Global Configuration mode in ACLI.
- Configure a TACACS+ server on the switch before you can enable remote TACACS+ services. For information see [Configuring switch TACACS+ server settings using ACLI](#) on page 212.

Procedure steps

1. Enable remote TACACS+ services for serial connections by using the following command:

```
cli password serial tacacs
```

2. Enable remote TACACS+ services for Telnet connections by using the following command:

```
cli password telnet tacacs
```

Enabling or disabling TACACS+ authorization using ACLI

You can enable or disable TACACS+ authorization globally on the switch by following this procedure.

 **Important:**

TACACS+ authorization is disabled by default.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Enable TACACS+ authorization by using the following command:

```
tacacs authorization enable
```

2. Disable TACACS+ authorization by using the following command:

```
tacacs authorization disable
```

Configuring TACACS+ authorization privilege levels using ACLI

Configure TACACS+ authorization privilege levels to specify the privilege levels to which TACACS+ authorization applies.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Configure TACACS+ authorization privilege levels by using the following command:

```
tacacs authorization level
```

Variable definitions

The following table defines the parameters, which you can enter after the **tacacs authorization level** command.

Variable	Value
ALL	Enables authorization for all privilege levels.
LINE	Enables authorization for a specific privilege level. LINE is a numerical value in the range of 0–15.
NONE	Authorization is not enabled for privilege levels. All users can execute commands available on the switch. The default authorization level is NONE

Enabling or disabling TACACS+ accounting using ACLI

Enable or disable TACACS+ accounting globally on the switch by following this procedure.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Enable TACACS+ accounting by using the following command:

```
tacacs accounting enable
```

2. Disable TACACS+ accounting by using the following command:

```
tacacs accounting disable
```

Configuring the switch TACACS+ level using ACLI

Configure the switch TACACS+ level to select a new level for a switch or use the last configured level.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Configure a new TACACS+ level for a switch by using the following command:

```
tacacs switch level
```

2. Use the last configured TACACS+ level for a switch by using the following command:

```
tacacs switch back
```

Variable definitions

The following table defines optional parameters that you enter after the `tacacs switch level` command.

Variable	Value
<cr>	Selects the default switch TACACS+ level (15).
<1-15>	Defines the new TACACS+ level for the switch. Values range from 1 to 15.

Viewing TACACS+ information using ACLI

View TACACS+ information to display TACACS+ configuration status by following this procedure.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

View TACACS+ information by using the following command:

```
show tacacs
```

Configuring IP Manager

To configure the IP Manager to control management access to the do the following:

- Enable IP Manager.
- Configure the IP Manager list.

Enabling IP Manager

To enable IP Manager to control Telnet, SNMP, or HTTP access, use the following command in Global Configuration mode:

```
ipmgr {telnet|snmp|web|ssh} [source-ip]
```

- where

telnet enables the IP Manager list check for Telnet access

snmp enables the IP Manager list check for SNMP, including Enterprise Device Manager

web enables the IP Manager list check for Web connections

ssh enables IP manager control over SSH sessions

source-ip sets the source IP address from which connections are allowed: 1-50 for address/mask pair and 51-100 for IPv6 address/prefix

To disable IP Manager for a management system, use the `no` keyword at the start of the command.

Configuring the IP Manager list

To specify the source IP addresses or address ranges that have access the switch or the stack when IP Manager is enabled, use the following command in Global Configuration mode:

```
ipmgr source-ip <list ID> <IPaddr> [mask <mask>]
```

- where

<list ID> is an integer in the range of 1 to 50 that uniquely identifies an ipv4 entry in the IP Manager list or in the range of 51 to 100 that uniquely identifies an ipv6 entry in the IP Manager list.

The `ipmgr source-ip <list ID>` command contains the following parameters for configuring the IP Manager list:

Parameter	Description
<IPAddr>	Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation.
[mask <mask>]	Specifies the subnet mask from which access is allowed. Enter the IP mask in dotted-decimal notation.

Removing IP Manager list entries

To deny access to the switch or stack for specified source IP addresses or address ranges, use the following command in Global Configuration mode:

```
no ipmgr source-ip [<list ID>]
```

- where

<list ID> is an integer in the range of 1 to 50 that uniquely identifies an ipv4 entry in the IP Manager list or in the range of 51 to 100 that uniquely identifies an ipv6 entry in the IP Manager list.

The command sets both the IP address and mask for the specified entry to 255.255.255.255. If you do not specify a <list ID> value, the command resets the whole list to factory defaults.

Viewing IP Manager settings

To view IP Manager settings, use the following command:

```
show ipmgr
```

The command displays:

- whether Telnet, SNMP, SSH, and Web access are enabled
- whether the IP Manager list is being used to control access to Telnet, SNMP, SSH, and the Web-based management system
- the current IP Manager list configuration

Setting the user name and password

The username authentication feature enhances the security level of the Avaya ERS 4000 series by adding a user name field to the existing security infrastructure. This feature integrates the local authentication methods in a general and commonly accepted user name — password framework.

username command

Use the **username** command in Global command mode to configure the system user name and password for serial console port, Telnet, and EDM access to a switch. The username command supports just one read-only and one read-write user identification on the switch or stack.

The syntax for the username command is:

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

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

Table 77: username command parameters and variables

Parameters and variables	Description
<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	Sets the read-only (ro) user name or the read-write (rw) user name. The ro rw variable is optional. If you omit this variable, the command applies to both read-only and read-write users.

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 system user to default using ACLI

Use this procedure to set the read-only and read-write user name for serial console port, Telnet, and EDM access to a switch to default values.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Set the read-only or read-write user name to default values by using the following command:

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

Variable definitions

Variable	Value
ro rw	Sets the read-only (ro) user name or the read-write (rw) user name to default. The ro rw variable is optional. If you omit this variable, the command applies to both read-only and read-write users.

Setting ACLI password

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

cli password command

The `cli password` command has two forms and performs the following functions:

- Change the read-only and read-write passwords for serial console port and Telnet access to a switch.
- Change the password authentication type for serial console port or Telnet access to a switch.

! Important:

The `cli password` command changes only the password does not effect the configured username.

The syntax for the `cli password` command is

```
cli password [serial | telnet] [local | none | radius | tacacs]
```

```
cli password {read-only | read-write} [<password>]
```

Run the `cli password` command in Global Configuration command mode.

[Table 78: cli password command parameters and variables](#) on page 222 describes the parameters and variables for the `cli password` command.

Table 78: cli password command parameters and variables

Parameters and variables	Description
read-only read-write	Modify the read only password or the read/write password.
<password>	Enter your password. ! Important: 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.
switch stack	Modify the password for a standalone switch or switches in a stack.
none local radius	Indicates the password type you are modifying: <ul style="list-style-type: none"> • none: disable the password • local: uses the locally defined password for serial console or Telnet access. • radius: uses RADIUS authentication for serial console or Telnet access. • tacacs: uses TACACS+ authentication, authorization, and accounting (AAA) services for serial console or Telnet access.

Viewing the user name and password configuration using ACLI

Use this procedure to display the current user name and password authentication configuration for a switch.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display the current user name and password authentication configuration by using the following command:

```
show cli password [type]
```

Variable definitions

Variable	Value
[type]	<p>Displays the current password type configured for serial console and Telnet access to the stack, or standalone switch. Values include:</p> <ul style="list-style-type: none"> • local—the system local password is used • none—no password is used • radius—RADIUS password authentication is used • tacacs—TACACS+ AAA services are used

Job aid: show cli password type command output

The following figure displays sample output for the show cli password type command.

```
4524GT-PWR>en
4524GT-PWR#show cli password type
Console Password Type: Local Password
Telnet Password Type: None
4524GT-PWR#
```

Configuring password security

ACLI commands detailed in this section are used to manage password security features. These commands can be used in the Global Configuration and Interface Configuration command modes.

password security command

The `password security` command enables the Password Security feature on the Avaya Ethernet Routing Switch 4000 Series.

The syntax of the `password security` command is

```
password security
```

no password security command

The `no password security` command disables the Password Security feature on the Avaya Ethernet Routing Switch 4000 Series.

The syntax for the `no password security` command is

```
no password security
```

Configuring the number of retries

To configure the number of times a user can retry a password, use the following command in Global or Interface Configuration mode:

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

- where

number is an integer in the range 1 to 100 that specifies the allowed number of failed log on attempts. The default is 3.

Password history configuration using ACLI

You can configure the Avaya Ethernet Routing Switch 4000 to keep a maximum history of ten passwords. The default password history configuration is three.

Configuring password history using ACLI

Configure password history to select the number of last-used passwords the switch keeps a record of.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Configure password history by using the following command:

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

Variable definitions

The following table defines variable parameters that you enter with the `password password-history <3-10>` command.

Variable	Value
<3-10>	Defines the number of passwords the switch records a history of. Values range from 3 to 10. The default value is 3.

Configuring password history to default using ACLI

Configure the password history to default to select the default value of 3 for the number of last-used passwords the switch keeps a record of by following this procedure.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Configure the password history to default by using the following command:

```
default password password-history
```

Viewing password history using ACLI

View password history to display the password history configuration by following this procedure.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

View password history by using the following command:

```
show password password-history
```

ACLI Audit log configuration

ACLI Audit provides a means for tracking ACLI commands.

Displaying ACLI audit log

Perform this procedure to display ACLI audit log.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

To display ACLI audit log enter the following command:

```
show audit log [asccfg | serial | telnet |config]
```

Variable definitions

The following table defines variable parameters that you enter with the `show audit log` command.

Variable	Value
asccfg	Displays the audit log for ASCII configuration.
serial	Displays the audit log for serial connections.
telnet	Displays the audit log for Telnet and SSH connections.
config	Displays the status of activation of the Audit log.

Enabling and disabling ACLI audit log

Perform this procedure to enable or disable ACLI audit log.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. To enable ACLI audit enter the following command:

```
audit log save
```

2. To disable ACLI audit enter the following command:

```
no audit log
```

3. To verify ACLI audit setting enter the following command:

```
show audit log config
```

The following response appears:

```
Audit Log Save To NVRAM:: Disabled
```

Configuring ACLI audit log to default

Perform this procedure to set ACLI audit log to default.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. To set ACLI audit log to default mode enter the following command:

```
default audit log
```

2. To verify ACLI audit settings enter the following command:

```
show audit log config
```

The following response appears:

```
Audit Log Save To NVRAM:: Enabled
```

Clearing the ACLI audit log

Perform this procedure to erase the contents of the ACLI audit log.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

To clear the ACLI audit log, enter the following command:

```
clear audit log
```

Job aid:

If the contents of the ACLI audit log is successfully erased, the following message appears:

```
% Audit log was successfully erased
```

If the no-erase audit log flag is set on the switch or your are running the secure software image, the following message appears:

```
% Clearing audit log is not authorized
```

Preventing erasure of the ACLI audit log

Perform this procedure to prevent erasure of the ACLI audit log contents when using the standard software image, by applying the no-erase flag.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

To prevent erasure of the ACLI audit log, enter the following command:

```
audit log noerase enable
```

Warning:

Applying the **audit log noerase enable** command on a switch is a one time function which is non-reversible and is only applicable when the switch is running the standard software image. After the no-erase audit log flag is set, you cannot clear the audit log, even if the switch is re-configured to factory defaults. When you enter the command for the first

time on a switch running the standard software image, the following warning message appears:

```
% WARNING: Setting the audit log noerase is a non-reversible command
Do you want to continue (y/n) ?
```

If the no-erase flag is already set on the switch, the following message appears:

```
% Audit log noerase is already enabled
```

Secure Socket Layer services

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

Table 79: SSL commands

Command	Description
[no] ssl	Enables or disables SSL. The Web server operates in a secure mode when SSL is enabled and in non secure mode when the SSL server is disabled.
[no] ssl certificate	Creates or deletes a certificate. The new certificate is used only on the next system reset or SSL server reset. The new certificate is stored in the NVRAM with the file name SSLCERT.DAT. The new certificate file replaces the existing file. On deletion, the certificate in NVRAM is also deleted. The current SSL server operation is not affected by the create or delete operation.
ssl reset	Resets the SSL server. When SSL is enabled: existing SSL connections are closed, the SSL server is restarted and initialized with the certificate that is stored in the NVRAM. When SSL is not enabled: existing non secure connections are closed, the server is restarted, and non secure operation resumes.
show ssl	Shows the SSL server configuration and SSL server state. See Table 80: Server state information on page 231 for more information.
show ssl certificate	Displays the certificate which is stored in the NVRAM and is used by the SSL server.

The following table describes the output for the **show ssl** command.

Table 80: Server state information

Field	Description
WEB Server SSL secured	Shows whether the Web server is using an SSL connection.
SSL server state	Displays one of the following states: <ul style="list-style-type: none"> • Un-initialized: The server is not running. • Certificate Initialization: The server is generating a certificate during its initialization phase. • Active: The server is initialized and running.
SSL Certificate: Generation in progress	Shows whether SSL is in the process of generating a certificate. The SSL server generates a certificate during server startup initialization, or ACLI user can regenerate a new certificate.
SSL Certificate: Saved in NVRAM	Shows whether an SSL certificate exists in the NVRAM. The SSL certificate is not present if the system is being initialized for the first time or ACLI user has deleted the certificate.

Configuring the Web server for client browser requests using ACLI

Use this procedure to configure the Web server to respond to HTTPS only, or both HTTPS and HTTP client browser requests when SSL is enabled.

Prerequisites

- Enable SSL.

Procedure steps

1. Log on to the Global Configuration mode in ACLI.
2. To configure the Web server to respond to HTTPS client browser requests only, use the following command:

```
https-only
```

3. To configure the Web server to respond to both HTTPS and HTTP client browser requests, use the following command:

```
no https-only
```

*** Note:**

`https-only` is enabled by default.

Viewing the Web server client browser request configuration using ACLI

Use this procedure to display whether the Web server is configured to respond to HTTPS only, or both HTTPS and HTTP client browser requests when SSL is enabled.

Prerequisites

- Enable SSL.

Procedure steps

1. Log on to the Privileged EXEC mode in ACLI.
2. To display whether the Web server is configured to respond to HTTPS only, or both HTTPS and HTTP client browser requests, use the following command:

```
show https-only
```

Job aid: show https-only command output

The following figure shows sample output for the `show https-only` command.

```
4524GT-PWR#show https-only
HTTPS only:disabled
```

Secure Shell protocol configuration using ACLI

Secure Shell (SSH) protocol is used to improve Telnet and provide a secure access to the ACLI interface. There are two versions of the SSH Protocol (SSH1 and SSH2). The Avaya Ethernet Routing Switch 4000 Series supports SSH2.

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

Displaying SSH information using ACLI

Use this procedure to display general SSH settings and information about all active SSH sessions.

Prerequisites

- Use this command in the Privileged Exec mode.

Procedure steps

Enter the following command:

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

Variable definitions

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

Job aid: sample SSH information display output

The following example displays sample output for the `show ssh global` command:

```
4548GT-PWR#show ssh global
Active SSH Sessions      : 0
Version                  : Version 2 only
Port                     : 22
Authentication Timeout  : 60
DSA Authentication       : False
RSA Authentication       : False
Password Authentication  : True
Auth Key TFTP Server     : 172.16.3.2
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys            : Exist
RSA Host Keys            : Exist
Enabled                  : True
```

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

```
4548GT-PWR#show ssh download-auth-key
Auth Key TFTP Server     : 172.16.3.2
DSA Auth Key File Name  :
RSA Auth Key File Name  :
Last Transfer Result    : None
```

Enabling SSH using ACLI

Use this procedure to enable SSH in a non-secure mode. If the host keys do not exist, they are generated.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
ssh
```

Disabling SSH using ACLI

Use this procedure to disable SSH for the switch.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

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

Variable definitions

Variable	Value
dsa-auth	Disables SSH DSA authentication.
dsa-auth-key	Deletes the SSH DSA authentication key.
dsa-host-key	Deletes the SSH DSA host key.
rsa-auth	Disables SSH RSA authentication.
rsa-auth-key	Deletes the SSH RSA authentication key.
rsa-host-key	Deletes the SSH RSA host key.
pass-auth	Disables SSH password authentication.

Generating a new SSH DSA host key using ACLI

Use this procedure to generate a new SSH DSA host key for the switch.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

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

Deleting the SSH DSA host key using ACLI

Use this procedure to delete the switch SSH DSA host key.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

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

Generating a new SSH RSA host key using ACLI

Use this procedure to generate a new SSH RSA host key in the switch.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

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

Deleting the SSH RSA host key using ACLI

Use this procedure to delete the SSH RSA host key in the switch.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

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

Downloading DSA or RSA authentication keys using ACLI

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

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

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

Variable	Value
address <A.B.C.D> <WORD>	Specifies the address of the TFTP server. <ul style="list-style-type: none"> • A.B.C.D—specifies the IP address • WORD—specifies the IPv6 address
dsa rsa	Specifies DSA or RSA authentication key to be downloaded.
key-name <WORD>	Specifies the TFTP or USB filename.
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 using ACLI

Use this procedure to delete the SSH DSA authentication key in the switch.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

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

Deleting the SSH RSA authentication key using ACLI

Use this procedure to delete the SSH RSA authentication key in the switch.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

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

Enabling user log-on with an SSH DSA key using ACLI

Use this procedure to enable user log-on with SSH DSA key authentication.

Prerequisites

- Use these commands in the Global Configuration mode.

Procedure steps

Enter either of the following commands:

```
ssh dsa-auth
```

OR

```
default ssh dsa-auth
```

Disabling user log-on with an SSH DSA key using ACLI

Use this procedure to disable user log-on with SSH DSA key authentication.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
no ssh dsa-auth
```

Enabling user log-on with an SSH RSA key using ACLI

Use this procedure to enable user log-on with SSH RSA key authentication.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter either of the following commands:

```
ssh rsa-auth
```

OR

```
default ssh rsa-auth
```

Disabling user log-on with an SSH RSA key using ACLI

Use this procedure to disable user log-on with SSH RSA key authentication.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
no ssh rsa-auth
```

Enabling user log-on with SSH password authentication using ACLI

Use this procedure to enable user log-on using the SSH password authentication method.

Prerequisites

- Use these commands in the Global Configuration mode.

Procedure steps

Enter either of the following commands:

```
ssh pass-auth
```

OR

```
default ssh pass-auth
```

Disabling user log-on with SSH password authentication using ACLI

Use this procedure to disable user log-on using the SSH password authentication method.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter either of the following commands:

```
no ssh pass-auth
```

Disabling SNMP and Telnet With SSH using ACLI

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

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
ssh secure [force]
```

Variable definitions

Variable	Value
force	Skips the confirmation step.

Setting the TCP port for SSH daemon using ACLI

Use this procedure to set the TCP port for the SSH daemon.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

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

Variable definitions

Variable	Value
<1-65535>	Specifies the number of the TCP port to use.

Setting the default TCP port for the SSH daemon using ACLI

Use this procedure to set the default TCP port for the SSH daemon.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
default ssh port
```

Setting the SSH timeout using ACLI

Use this procedure to set the SSH authentication timeout, in seconds.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

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

Variable definitions

Variable	Value
<1-120>	Specifies the desired timeout value in seconds.

Setting the SSH timeout to default using ACLI

Use this procedure to sets the SSH authentication timeout to the default value of 60 seconds.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
default ssh timeout
```

Secure Shell Client configuration using ACLI

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 using ACLI

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

Prerequisites

- Use the following command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
sshc authentication {dsa | password | rsa}
```

Variable definitions

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.

Setting SFTP authentication for SSH Client to default using ACLI

Use this procedure to set the SFTP authentication method SSH Client to uses for transferring files to the default value of *dsa*.

Prerequisites

- Use the following command from Global Configuration mode.

Procedure steps

Enter either of the following commands:

```
default sshc authentication
```

OR

```
no sshc authentication
```

Closing an SSH Client session using ACLI

Use this procedure to close a specific SSH Client session.

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

Enter the following command:

```
sshc close-session <0-8>
```

Variable definitions

Variable	Value
<0-8>	Specifies the SSH Client session ID.

Generating an SSH client DSA host key using ACLI

Use the following procedure to generate public and private DSA SSH client host keys for user access authentication.

Prerequisites

- Use the following command from Global Configuration mode.

Procedure steps

Enter the following command:

```
sshc dsa-host-key [force]
```

Important:

If you use the `sshc dsa-host-key` command without the *force* option you must remove the current key before you can generate the new key. If a DSA key exists and you use the command without the *force* option the system does not generate a new key. If you use the *force* option, the system generates a new, active DSA key, even in the presence of an existing DSA key. The authentication method remains unchanged.

Variable definitions

Variable	Value
force	Creates a new DSA key, even in the presence of an existing DSA key.

Deleting DSA host keys using ACLI

Use the following procedure to delete the public or private DSA host keys from NVRAM.

Prerequisites

- Use the following command from Global Configuration mode.

Procedure steps

Enter the following command:

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

The DSA authentication state remains unchanged

Generating an SSH client RSA host key using ACLI

Use the following procedure to generate public and private SSH client RSA host keys for user access authentication.

Prerequisites

- Use the following command from Global Configuration mode.

Procedure steps

Enter the following command:

```
sshc rsa-host-key [force]
```

Important:

If you use the `sshc rsa-host-key` command without the *force* option you must remove the current key before you can generate the new key. If an RSA key exists and you use the command without the *force* option the system does not generate a new key. If you use the *force* option, the system generates a new, active RSA key, even in the presence of an existing RSA key. The authentication method remains unchanged.

Variable definitions

Variable	Value
force	Creates a new RSA key, even in the presence of an existing RSA key.

Deleting RSA host keys using ACLI

Use the following procedure to delete public and private RSA host keys from the NVRAM.

Prerequisites

- Use the following command from Global Configuration mode.

Procedure steps

Enter the following command:

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

The RSA authentication state remains unchanged.

Connecting SSH to a host using ACLI

Use the following procedure to establish a SSH connection to a host.

Prerequisites

- Use the following command from User EXEC or Privileged EXEC mode .

Procedure steps

Enter the following command

```
ssh <A.B.C.D. | host_name> [username <user_name>] [port <0-65535>]
```

Important:

When the SSH client connects to a host, if the host is not known to the client, the following message is displayed on the console:

```
The authenticity of host '<host's ip>' can't be established. RSA Key
with the following SHA256 fingerprint: 4:90:56:E6:F8:9D:E3:BC:
88:10:4F:B4:9B:CD:F4:26:84:6:D6:E1:10:64: DD:2E:99:7A:93:27:3B:
15:9E:7E. Are you sure you want to continue connecting (yes/no)?
```

! Important:

The first time a user connects to a host, the console displays **fingerprint** and **yes/no** questions for read-write access only. Type `yes` only if the host IP address is reliable (no man-in-the-middle attack happens). After you type `yes`, the following message appears:

```
Warning: Permanently added '<host's IP>' (RSA) to the list of known hosts.
```

Variable definitions

Variable	Value
<A.B.C.D. host_name>	Specifies either the host IP address, or the host name.
username <user_name>	Specifies the user name.
port <0–65535>	Specifies the TCP port number. Values range from 0 to 65535.

Configuration example

This example displays sample steps for connecting an SSH Client to a host.

```
4550T#ssh 10.100.54.35
4550T#ssh 10.100.54.35 username laur
4550T#ssh 10.100.54.35 username RW port 22
```

Displaying current SSH client sessions

Use the following procedure to display current SSH client sessions.

Prerequisites

- Use the following command from Privileged Exec mode.

Procedure steps

Enter the following command:

```
show sshc sessions
```

Job aid: sample SSH session display output

The following example shows sample output for the `show sshc sessions` command.

```
4826GTS-PWR+#show sshc sessions
1 active SSH Session:
```

Session ID	Host IP Address	Connection time:
0	10.100.54.35	1 minute

Displaying SSH client known hosts

Use this procedure to display information about SSH client known hosts configuration on the switch.

Prerequisites

- Use the following command from Privileged Exec mode.

Procedure steps

Enter the following command:

```
show sshc known-hosts
```

* Note:

The `show sshc known-hosts` command is present only on terminals with Read-Write access.

Job aid: sample SSH client known hosts display output

The following example shows sample output for the `show sshc known-hosts` command.

```
4826GTS-PWR+#show sshc known-hosts
IP Address          SHA-256 Fingerprint
-----
10.100.54.200      B1:E1:C4:4D:8C:72:3:D:C:16:D6:F7:20:C1:3:C2:
                   DF:83:70:BE:42:EA:AC:6A:5:6F:59:4F:F5:B0:DF:3B
-----
10.100.54.35      98:62:1:15:90:FD:51:33:98:14:28:DF:BF:28:1B:97:
                   EA:FA:6E:2:75:E9:63:16:69:79:62:DB:8D:CC:2C:55
```

Clearing SSH Client known hosts using ACLI

Use the following procedure to clear the public key of a known host.

Prerequisites

- Use the following command from Global Configuration mode.

Procedure steps

Enter the following command:

```
clear sshc known-host {<A.B.C.D> | <host_name> | <ipv6_address>
| all}
```

Variable definitions

Variable	Value
all	Specifies the public keys of all known hosts
<A.B.C.D>	Specifies the host IP address.
<host_name>	Specifies the host name.
<ipv6_address>	Specifies the host IPv6 address.

Configuration example

The following example displays a sample step for clearing the public key of a known host.

```
4550T#clear sshc known-host 172.16.1.12
```

Configuration examples for configuring Secure Shell connections

Establishing an SSH connection to another switch using public key authentication

1. Switch #1: generate a public key using the `sshc dsa-host-key` command.
2. On Switch #1: upload the generated public key using the `sshc upload-auth-key` command.
3. On Switch #2: obtain the public key using the `ssh download-auth-key` command.
4. On Switch #2: verify that SSH DSA authentication is enabled by default by entering the `show sshc` command. If necessary, enable SSH DSA authentication by entering the `ssh dsa-auth` command. Then, enable SSH by entering the `ssh` command.
5. On Switch #1: enter the `<ssh switch two IP> username RW` command.

Establishing an SSH connection to a Linux-PC using public key authentication

1. Generate a public key using the `sshc dsa-host-key` command.
2. Upload the generated public key using the `sshc upload-auth-key` command.

3. On the remote PC, append the public key in the `~user/.ssh/authorized_keys` file.
4. On the switch, enter the following command to establish SSH on the PC: `ssh <PC IP> username <user>`

Establishing an IPv6 SSH connection to another switch

1. Configure an IPv6 address for each switch, .

For Switch #1 enter the following commands:

```
ipv6 enable
int vlan 1
ipv6 interface enable
ipv6 address 3000::1000/64
```

For Switch #2 enter the following commands:

```
ipv6 enable
int vlan 1
ipv6 interface enable
ipv6 address 3000::2000/64
```

2. Establish a SSH connecting using the IPv6 address.
 - Establish a SSH connection from Switch #1 to Switch #2.
 - On Switch #1 : **ssh 3000::2000 user RW**
 - SSH from Switch #1 to Switch #2:
 - On Switch #2: **ssh 3000::1000 user RO**

DHCP snooping configuration using ACLI

This section describes how you can configure DHCP snooping to provide security to your network by preventing DHCP spoofing, using ACLI.

Warning:

In layer 3 mode, you must enable DHCP snooping on the layer 3 VLANs spanning towards the DHCP server. DHCP-relay is also required for the correct functionality.

Configuring DHCP snooping globally using ACLI

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

Use this procedure to enable or disable DHCP snooping for the switch.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enable DHCP globally by using the following command:

```
[default] [no] ip dhcp-snooping <enable> <option82>
```

Variable definitions

The following table defines optional parameters that you can enter with the `[default] [no] ip dhcp-snooping [enable] <option82>` 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>	When selected, enables DHCP snooping with Option 82 globally on the switch.

Viewing the global DHCP snooping configuration ACLI

View the global DHCP snooping configuration to review and confirm the DHCP snooping configuration for the switch.

Prerequisites

- Log on to the User EXEC mode in ACLI.

Procedure steps

View the global DHCP snooping configuration by using the following command:

```
show ip dhcp-snooping
```

Configuring VLAN-based DHCP snooping using ACLI

You must enable DHCP snooping separately for each VLAN. If DHCP snooping is disabled on a VLAN, the switch forwards DHCP reply packets to all applicable ports, regardless of whether the port is trusted or untrusted.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enable DHCP snooping on a VLAN by using the following command:

```
[default] [no] ip dhcp-snooping vlan <vidlist> [option82]
```

Variable definitions

The following table defines parameters that you can enter with the `[default] [no] ip dhcp-snooping vlan <vidlist> [option82]` command.

Variable	Value
[default]	Configures DHCP snooping on a VLAN to the default value (disabled).
[no]	Disables DHCP snooping on a VLAN. If you do not specify a VLAN ID, DHCP snooping is disabled on all VLANs.
[option82]	When selected, enables DHCP snooping with Option 82 on a VLAN.
<vidlist>	Specifies the list of preconfigured VLANs on which you want to enable DHCP snooping. The list syntax is (<vlanID> [-<vlanID>][,...]), where each vlan ID is an integer in the range 1–4094.

Viewing the VLAN-based DHCP snooping configuration using ACLI

View the VLAN-based DHCP snooping configuration to review and confirm the DHCP snooping configuration for a VLAN.

Prerequisites

- Log on to the User EXEC mode in ACLI.

Procedure steps

View the VLAN-based DHCP snooping configuration by using the following command:

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

The output displays only the VLANs enabled for DHCP snooping.

Configuring port-based DHCP snooping using ACLI

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.

Prerequisites

- Log on to the Interface Configuration mode in ACLI.

Procedure steps

1. Configure port-based DHCP snooping by using the following command:

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

2. Return DHCP snooping for all interface ports to default values by using the following command:

```
default ip dhcp-snooping port all
```


Variable definitions

The following table defines parameters that you can enter with the `[default] [no] ip dhcp-snooping [port <portlist>] [<trusted|untrusted>] option82-subscriber-id <WORD>` 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.
<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.

Viewing the port-based DHCP snooping configuration using ACLI

View the port-based DHCP snooping configuration to review and confirm the DHCP snooping configuration for a port or group of ports.

Prerequisites

- Log on to the User EXEC mode in ACLI.

Procedure steps

View the port-based DHCP snooping configuration by using the following command:

```
show ip dhcp-snooping interface [<interface type>] [<portlist>]
```

Variable definitions

The following table defines optional parameters that you can enter with the **show ip dhcp-snooping interface [<interface type>] [<portlist>]** command.

Variable	Value
<interface type>	Specifies the interface type for the port or ports.
<portlist>	Specifies an individual port or list of ports.

Adding static entries to the DHCP binding table using ACLI

Use this procedure to add entries for devices with static IP addresses to the DHCP binding table.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Add entries to the DHCP binding table by using the following command:

```
ip dhcp-snooping binding <1-4094> <MAC_addr> [ip <IP_addr>]
[port <LINE>] [expiry <1-4294967295>]
```

Variable definitions

The following table defines parameters that you enter with the **ip dhcp-snooping binding <1-4094> <MAC_addr> [ip <IP_addr>] [port <LINE>] [expiry <1-4294967295>]** command.

Variable	Value
<1-4094>	Specifies the ID of the VLAN that the DHCP client is a member of.
expiry <1-4294967295>	Specifies the time, in seconds, before the DHCP client binding expires.

Variable	Value
ip <IP_addr>	Specifies the IP address of the DHCP client.
<MAC_addr>	Specifies the MAC address of the DHCP client.
port <LINE>	Specifies the switch port that the DHCP client is connected to.

Deleting static entries from the DHCP binding table using ACLI

Use this procedure to delete entries for devices with static IP addresses from the DHCP binding table.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Delete entries from the DHCP binding table by using the following command:

```
no ip dhcp-snooping binding <1-4094> <MAC_addr>
```

Variable definitions

The following table defines parameters that you enter with the `no ip dhcp-snooping binding <1-4094> <MAC_addr>` command.

Variable	Value
<1-4094>	Specifies the ID of the VLAN that the DHCP client is a member of.
<MAC_addr>	Specifies the MAC address of the DHCP client.

Viewing the DHCP binding table using ACLI

Use this procedure to display DHCP binding table entries.

Prerequisites

- Log on to the User EXEC mode in ACLI.

Procedure steps

View the DHCP binding table by using the following command:

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

Important:

If you apply the `show ip dhcp-snooping binding` command on a large stack with complex configuration, you can experience slow output if this command is executed within 4-5 minutes of the stack being booted or power-cycled. If you wait 5 minutes after the stack is booted or power-cycled before executing this show command, the normal response times will be observed.

Configuring DHCP Snooping external save using ACLI

Use this procedure to save the DHCP Snooping database to an external USB drive or TFTP server.

Prerequisites

- Log on to the Global Configuration mode in ACLI.
- Synchronize the switch with an NTP server.

Procedure steps

Configure DHCP Snooping external save by using the following command:

```
ip dhcp-snooping external-save [enable] {[tftp <ipv4address> | <ipv6address> | [usb <unit 1-8> ]} filename <filename>
```

Variable definitions

Variable	Value
[enable]	Enables DHCP Snooping external save.
[tftp <ipv4address> <ipv6address> { <filename>}]	Specifies an IPv4 or IPv6 address for the TFTP server on which to save the DHCP Snooping database, and the name of the file to save.

Variable	Value
[usb <1–8>]	Specifies to save the DHCP Snooping database on a USB device and the unit on which the USB drive is located.
filename <filename>	Specifies the filename to apply to the saved DHCP Snooping database.

Configuring DHCP Snooping external save to an SFTP server

Use this procedure to save the DHCP Snooping database to an SFTP server.

* Note:

You cannot save the DHCP Snooping database to an SFTP server using a password for authentication, because saving the DHCP snooping database is an automated process, and password authentication requires entering the password each time the saving occurs. Use either RSA key or DSA key authentication for DHCP Snooping external save to an SFTP server.

Prerequisites

- Synchronize the switch with an NTP/SNTP server.
- For authentication using an RSA or DSA key, the authentication key must be generated and uploaded to server.

Procedure steps

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Use the following command to save the DHCP Snooping database to an SFTP server if you use an RSA or DSA key for authentication:

```
ip dhcp-snooping external-save sftp <sftp_ip_address>
filename <filename> username <user_name>
```

Variable definitions

Variable	Value
<sftp_ip_address>	Specifies the IP address for the SFTP server.
<filename>	Specifies the name of the file to save.
<user_name>	Specifies the user name.

Disabling DHCP Snooping external save using ACLI

Use this procedure to disable DHCP Snooping external save for the switch.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Disable DHCP Snooping external save by using one of the following commands:

```
no ip dhcp-snooping external-save enable
default ip dhcp-snooping external-save
```

Restoring the externally saved DHCP Snooping database using ACLI

Use this procedure to force a restoration of the DHCP Snooping database on the switch from the file previously saved to an external USB drive or TFTP server.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Restore the externally saved DHCP Snooping database by using the following command:

```
ip dhcp-snooping external-save restore
```

Restoring the externally saved DHCP Snooping database from an SFTP server

Use this procedure to force a restoration of the DHCP Snooping database on the switch from the file previously saved to an SFTP server.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```
2. Use the following command to restore the externally saved DHCP Snooping database if you use an RSA or DSA key for authentication:

```
ip dhcp-snooping external-save restore sftp username
<user_name>
```

- where *<user-name>* specifies the user name.

3. Use the following command to restore the externally saved DHCP Snooping database if you use a password for authentication:

```
ip dhcp-snooping external-save restore sftp username
<user_name> password
```

- where *<user-name>* specifies the user name.

Viewing DHCP Snooping external save information using ACLI

Use this procedure to display DHCP Snooping external save configuration information for the switch.

Prerequisites

- Log on to the User EXEC mode in ACLI.

Procedure steps

Display DHCP Snooping external save configuration information by using the following command:

```
show ip dhcp-snooping external-save
```

Job aid: show ip dhcp-snooping external-save command output

The following figure displays sample output for the show ip dhcp-snooping external-save command.

```
4524GT-PWR>show ip dhcp-snooping external-save
DHCP Snooping external save: Disabled
DHCP Snooping external device: USB
DHCP Snooping external filename: test1
DHCP Snooping external last sync:
DHCP Snooping external sync flag: True <changes will be synchronized at next wr
ite>
4524GT-PWR>
```

DHCP Snooping layer 2 configuration using ACLI example

[Figure 6: Layer 2 configuration example](#) on page 260 depicts the network setup for this example. PC1 and PC2 act as DHCP clients. The device under test (DUT) is in layer 2 mode and must be configured with DHCP Snooping to increase network security. The DHCP server and clients must belong to the same L2 VLAN (VLAN #1 by default). You can configure the DHCP client lease time on the DHCP server.

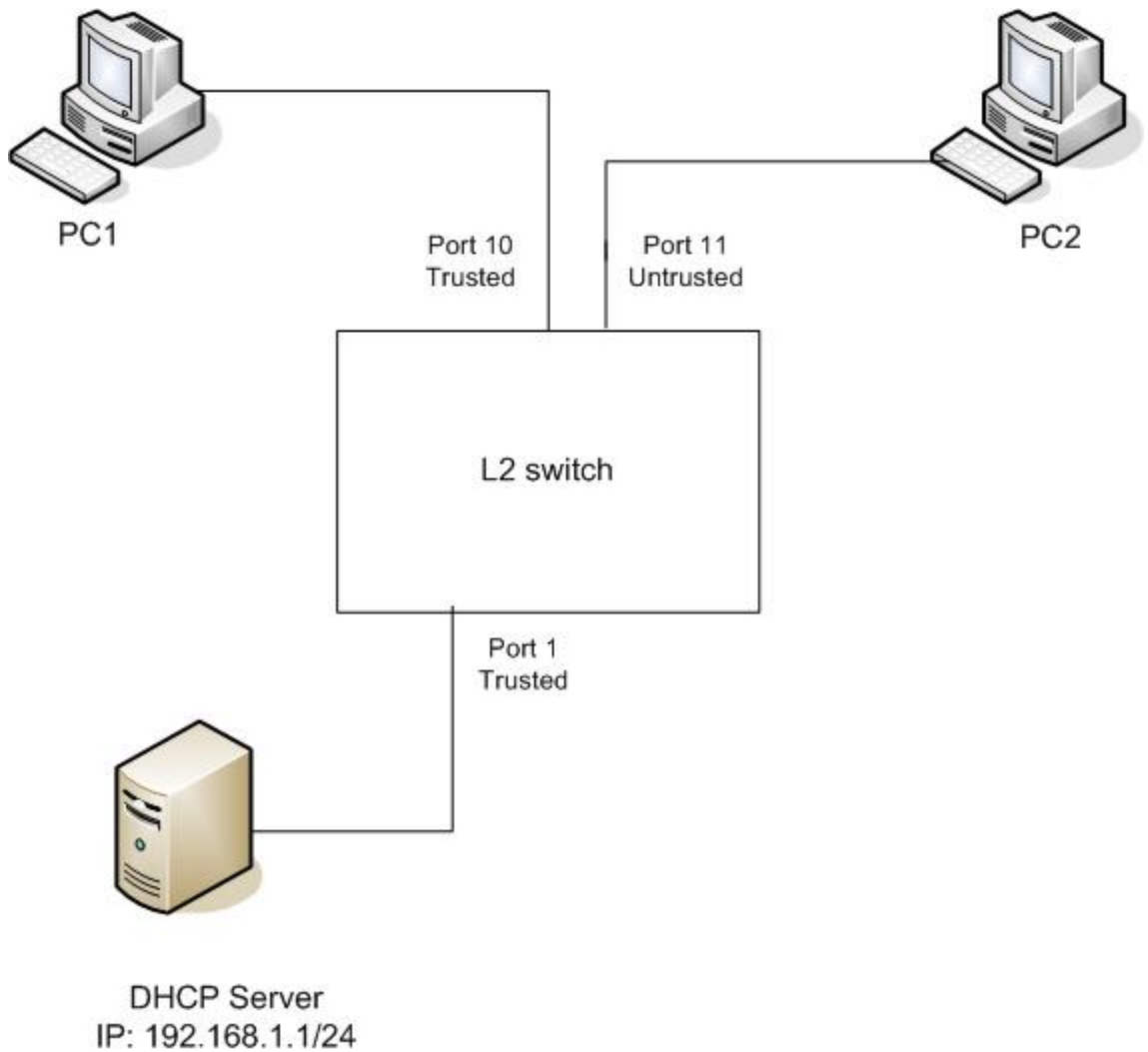


Figure 6: Layer 2 configuration example

The DHCP server port must always be Trusted, because Untrusted DHCP ports drop DHCP replies coming from the DHCP server. All ports are DHCP Untrusted by default. You must connect DHCP clients to Untrusted DHCP ports, however, PC1 is connected to a Trusted port for this configuration example case.

This configuration example illustrates a security hole that permits PC1 to install a fake DHCP Server. Port10 (DHCP Trusted) allows DHCP replies to be forwarded to PC2 in this case.

DHCP Snooping configuration commands

The following section describes the detailed ACLI commands required to configure DHCP Snooping for this example.

```
#configure terminal
(config)#ip dhcp-snooping
(config)# ip dhcp-snooping vlan 1
```



```
(config)#interface Ethernet 1,10
(config-if)#ip dhcp-snooping trusted
(config-if)#exit
```

Verifying the DHCP Snooping settings

This section describes the commands used to verify the settings and the expected response to each command.

```
(config)#show ip dhcp-snooping
```

```
Global DHCP snooping state: Enabled
DHCP
VLAN Snooping
----
1 Enabled
```

```
(config)#show ip dhcp-snooping interface 1,10,11
```

```
DHCP
Port Snooping
----
1 Trusted
10 Trusted
11 Untrusted
```

```
(config)#show ip dhcp-snooping binding
```

```
MAC IP Lease (sec) VID Port
-----
-----
Total Entries: 0
```

```
4526GTX-PWR#sho running-config
```

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 4526GTX-PWR
! Software version = v5.1.0.1
enable
configure terminal
!
! *** CORE ***
!
autosave enable
mac-address-table aging-time 300
autotopology
no radius-server
radius-server host 0.0.0.0
radius-server secondary-host 0.0.0.0
radius-server port 1812
! radius-server key *****
radius-server timeout 2
telnet-access login-timeout 1
telnet-access retry 3
```

```
telnet-access inactive-timeout 15
telnet-access logging all
cli password stack serial none
cli password stack telnet local
!....
! *** IP ***Note information in this section.
!
ip default-gateway 0.0.0.0
ip address netmask 0.0.0.0
ip address stack 0.0.0.0
ip address switch 0.0.0.0
ip bootp server disable
!....
*** DHCP SNOOPING *** Note information in this section.
!
ip dhcp-snooping
no ip dhcp-snooping vlan
ip dhcp-snooping vlan 1
interface Ethernet ALL
default ip dhcp-snooping
ip dhcp-snooping port 1,10 trusted
exit
!
! *** ARP INPSECTION *** Note information in this section
!
no ip arp-inspection vlan
interface Ethernet ALL
default ip arp-inspection
exit
! ...
```

Renew the IP addresses for PC1 and PC2. Both PCs obtain IP addresses from the DHCP server. A DHCP binding entry for PC2 appears in the DHCP binding table. No binding entry for PC1 exists because port 10 is DHCP Trusted.

```
(config)#show ip dhcp-snooping binding
```

```
MAC IP Lease (sec) VID Port -----
-----
00-02-44-ab-2d-f4 192.168.1.10 86460 1 11
Total Entries: 1
```

Configuring dynamic ARP inspection

For more information about the function and operation of dynamic Address Resolution Protocol (ARP) inspection in a network, see [Dynamic ARP inspection](#) on page 99.

To configure dynamic ARP inspection, do the following:

1. Enable dynamic ARP inspection on the VLANs. For more information, see [Enabling dynamic ARP inspection on the VLANs](#) on page 263.
2. Identify the ports as trusted (ARP traffic is not subjected to dynamic ARP inspection) or untrusted (ARP traffic is filtered through dynamic ARP inspection). For more information, see [Configuring trusted and untrusted ports](#) on page 263.

! **Important:**

For dynamic ARP inspection to function, DHCP snooping must be globally enabled. For more information about configuring DHCP snooping, see [DHCP snooping configuration using ACLI](#) on page 249 or [Configuring global DHCP snooping using EDM](#) on page 336.

Enabling dynamic ARP inspection on the VLANs

You must enable dynamic ARP inspection separately for each VLAN.

To enable dynamic ARP inspection on a VLAN, use the following command in Global Configuration mode:

```
ip arp-inspection vlan <vlanID>
```

- where

<vlanID> is an integer in the range 1–4094 that specifies the preconfigured VLAN on which you want to enable dynamic ARP inspection.

The default is disabled.

To disable dynamic ARP inspection on a VLAN, use the following command in Global Configuration mode:

```
no ip arp-inspection vlan <vlanID>
```

- where

<vlanID> is an integer in the range 1–4094 that specifies the preconfigured VLAN on which you want to disable dynamic ARP inspection.

Configuring trusted and untrusted ports

To specify whether a particular port or range of ports is trusted (ARP traffic is not subject to dynamic ARP inspection) or untrusted (ARP traffic is subject to dynamic ARP inspection), use the following command in Interface configuration mode:

```
ip arp-inspection [port <portlist>] {trusted|untrusted}
```

- where

<portlist> is the physical port number of the port you want to configure. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port number, the command applies to the ports specified upon entering the Interface configuration mode.

The default is untrusted.

To return a port or range of ports to default values, use the following command in Interface configuration mode:

```
default ip arp-inspection port <portlist>
```

- where

<portlist> is the physical port number of the port you want to configure. You can enter a single port, a range of ports, several ranges, or all. If you do not specify a port number, the command applies to the ports specified upon entering the Interface configuration mode.

To return all ports in the interface to default values, use the following command in Interface configuration mode:

```
default ip arp-inspection port ALL
```

Viewing dynamic ARP inspection settings

To view the VLANs on which dynamic ARP inspection has been enabled, use the following command in the Global or Interface Command mode:

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

The output lists only the VLANs enabled for dynamic ARP inspection.

To view port settings, use the following command in the Global or Interface Command mode:

```
show ip arp-inspection interface [<interface type>] [<port>]
```

The output lists the ports and their associated dynamic ARP inspection status (trusted or untrusted). If you specify the interface type or port as part of the command, the output includes only the ports specified. If you do not specify the interface type or port as part of the command, the output displays all ports.

Dynamic ARP inspection layer 2 configuration example

This configuration example uses the same network setup and configuration created in the [DHCP snooping configuration using ACLI](#) on page 249 section and illustrated by the [Figure 6: Layer 2 configuration example](#) on page 260. To increase security in this network, you must enable Dynamic ARP inspection. If the device under test (DUT) has no IP address assigned, BOOTP must be DISABLED in order for ARP Inspection to work. The DHCP Server port must be ARP Trusted also.

Dynamic ARP inspection configuration commands

The following section details the commands required to configure Dynamic ARP Inspection for this example. The following commands are in addition to those specified in the [DHCP snooping configuration using ACLI](#) on page 249 section.

```
configure terminal
(config)#ip bootp server disable
(config)#ip arp-inspection vlan 1
(config)#interface Ethernet 1,10
(config-if)#ip arp-inspection trusted
(config-if)#exit
```

Verifying Dynamic ARP Inspection settings

This section describes the commands used to verify settings, and the expected response to each command.

```
(config)#show ip arp-inspection
```

```
ARP
VLAN Inspection
----
1 Enabled
```

```
(config)#show ip arp-inspection interface 1,10,11
```

```
ARP
Port Inspection
----
1 Trusted
10 Trusted
11 Untrusted
```

```
4526GTX-PWR#sho running-config
```

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 4526GTX-PWR
! Software version = v5.1.0.0
enable
configure terminal
!
! *** CORE ***
!
autosave enable
mac-address-table aging-time 300
autotopology
no radius-server
radius-server host 0.0.0.0
radius-server secondary-host 0.0.0.0
```

Security configuration and management using ACLI

```
radius-server port 1812
! radius-server key *****
radius-server timeout 2
telnet-access login-timeout 1
telnet-access retry 3
telnet-access inactive-timeout 15
telnet-access logging all
cli password stack serial none
cli password stack telnet local
!
! *** IP *** Note information in this section.
!
ip default-gateway 0.0.0.0
ip address netmask 0.0.0.0
ip address stack 0.0.0.0
ip address switch 0.0.0.0
ip bootp server disable
!
! *** DHCP SNOOPING *** Note information in this section.
!
ip dhcp-snooping
no ip dhcp-snooping vlan
ip dhcp-snooping vlan 1
interface Ethernet ALL
default ip dhcp-snooping
ip dhcp-snooping port 1,10 trusted
exit
!
! *** ARP INSPECTION *** Note information in this section.
!
no ip arp-inspection vlan
ip arp-inspection vlan 1
interface Ethernet ALL
default ip arp-inspection
ip arp-inspection port 1,10 trusted
exit
!...
```

Renew the IP addresses for PC1 and PC2. Both PCs will obtain IP addresses from the DHCP server. A DHCP binding entry for PC2 appears in the DHCP binding table although it is ARP Untrusted. No binding entry for PC1 exists because port10 is DHCP Trusted even though it is ARP Trusted.

Now clear the ARP cache on both PCs.

```
>arp -a
>arp -d <IP-address>
```

Attempt to start communication (use ping) between PCs or between the PCs and the DHCP server. You can establish communication in any direction because ARPs are allowed on port10 (PC1) (that port is ARP Trusted) and on port 11 (PC2) because ARP packets coming from PC2 have an entry for ARP Untrusted port 11 that matches the IP-MAC from the DHCP binding table.

Next make a link-down/link-up for port 11 (PC2) or change PC2 IP address to a static one and set port10(PC1) as ARP Untrusted. Clear the ARP cache on both PCs and the DHCP server. Attempt to start communication (use ping) between PCs or between the PCs and the DHCP server. The PCs and DHCP server are unable to communicate with one another.

IP Source Guard configuration using ACLI

This section describes how you configure IP Source Guard using the Avaya Command Line Interface (ACLI).

! Important:

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

! Important:

Avaya recommends that you carefully manage the number of applications running on the Avaya Ethernet Routing Switch 4000 that use filters. For example, if you configure ADAC on ports and attempt to configure IP Source Guard on those same ports, the IP Source Guard configuration can fail due to the limited number of filters available.

Prerequisites

Before you can configure IP Source Guard, you must ensure the following:

- Dynamic Host Control Protocol (DHCP) snooping is globally enabled.
For information see [Configuring DHCP snooping globally using ACLI](#) on page 249.
- The port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- The port is an untrusted DHCP snooping and dynamic ARP Inspection port.
- The bsSourceGuardConfigMode MIB object exists.

This MIB object is used to control the IP Source Guard mode on an interface.

- The following applications are not enabled:
 - Baysecure
 - Extensible Authentication Protocol over LAN (EAPOL)

! Important:

Hardware resources can run out if IP Source Guard is enabled on trunk ports with a large number of VLANs that have DHCP snooping enabled. If this happens, traffic sending can

be interrupted for some clients. Avaya recommends that IP Source Guard not be enabled on trunk ports.

Enabling IP Source Guard using ACLI

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

Important:

The IP addresses are obtained from DHCP binding table entries defined automatically for the port. A maximum of 10 IP addresses from the binding table are allowed. The rest are dropped.

Prerequisites

- Log on to the Ethernet Interface Configuration mode in ACLI.

Procedure steps

Enable IP Source Guard by using the following command:

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

Variable definitions

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

Variable	Value
<interface id>	Identifies the ID of the interface on which you want IP Source Guard enabled.
<interface type>	Identifies the interface on which you want IP Source Guard enabled.

Viewing IP Source Guard port configuration information using ACLI

To view IP Source Guard port configuration information, open the Tacacs configuration screen by selecting Applications configuration settings for interfaces.

Prerequisites

- Log on to the Privileged Exec mode in ACLI.

Procedure steps

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

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

Variable definitions

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

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

Viewing IP Source Guard-allowed addresses using ACLI

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

Prerequisites

- Log on to the Privileged Exec mode in ACLI.

Procedure steps

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

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

Variable definitions

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

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

Disabling IP Source Guard using ACLI

Disable IP Source Guard to allow all IP traffic to go through without being filtered by following this procedure.

Prerequisites

- Log on to the Ethernet Interface Configuration mode in ACLI.

Procedure steps

Disable IP Source Guard by using the following command:

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

Variable definitions

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

Variable	Value
<interface id>	Identifies the ID of the interface on which you want IP Source Guard disabled.
<interface type>	Identifies the interface on which you want IP Source Guard disabled.

Configuring the trace feature using ACLI

Use the following procedures to display, set, and disable the trace level. This troubleshooting feature provides dynamic, detailed error, and event information.

Displaying trace information using ACLI

Use this procedure to show trace level information for the modules and the supported module list.

Procedure steps

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


```
show trace level
```

 to show trace level information for the modules.
 OR

```
show trace modid-list
```

 to show supported module list.

Configuring trace using ACLI

Use this procedure to configure trace level and trace output to the console.

Procedure steps

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


```
trace level <1-7> <0-4>
```

 to set the trace level
 OR

```
trace screen <enable|disable>
```

 to set trace screen on or off.

*** Note:**
Default is disable (off).

Variable definitions

The following table describes the parameters for the configuring the trace command.

Variable	Value
<1-7>	Module ID
<0-4>	<p>Enter the level you want to set for the module. There are five verbose levels for each module:</p> <ul style="list-style-type: none"> • 0 (NO_DISPLAY) to suppress displaying any information • 1 (VERY_TERSE) to display minimal information • 2 (TERSE) to display some information • 3 (VERBOSE) to display additional information • 4 (VERY_VERBOSE) to display most information <p>* Note: For Trace to display any information the trace level must be different from 0 for at least one module, and trace output must be enabled.</p>
<enable disable>	<p>Enable indicates the trace feature is on. Disable is the default and indicates the trace screen is off.</p> <p>* Note: For troubleshooting purposes the trace screen should be on (enable).</p>

Disabling trace using ACLI

Use this procedure to disable the trace for all modules.

Procedure steps

1. Enter Global Configuration mode.
2. At the command prompt, enter the following command:

```
trace shutdown
```

RADIUS Request use Management IP configuration using ACLI

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

Enabling the RADIUS Request use Management IP

Perform this procedure to enable the RADIUS requests to use the Management VLAN IP address.

Prerequisites

- Log on to the Global configuration mode.

Procedure steps

1. To enable RADIUS Request use Management IP enter the following command:

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

2. To verify the settings enter the following command:

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

Disabling the RADIUS Request use Management IP

Perform this procedure, to disable the RADIUS requests to use the Management VLAN IP address.

Prerequisites

- Log on to the Global configuration mode.

Procedure steps

1. To disable the RADIUS Request use Management IP, enter the following command:

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

2. To verify the settings enter the following command:

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

Setting the RADIUS Request use Management IP to default mode

Perform this procedure to set the RADIUS Request use Management IP to default mode.

Prerequisites

- Log on to the Global configuration mode.

Procedure steps

1. To set the RADIUS Request use Management IP to default mode, enter the following command:

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

2. To verify the settings enter the following command:

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

Chapter 5: Ignition Server configuration using ACLI

This chapter describes how to configure the Avaya Ethernet Routing Switch 4000 Series as a network access device in the Identity Engine Ignition Server solution using ACLI.

Configuring Ignition Server as a RADIUS server using ACLI

Use this procedure to configure Ignition Server to act as the RADIUS server for your switches and access points. For more information about configuring the Ignition Server for RADIUS, see Avaya Identity Engines Ignition Server Configuration, NN47280-500.

Prerequisites

- Ignition Server installed and configured in your network
- Configure the following policies for your switch on Ignition Server
 - Access
 - User Authentication
 - User Authorization
- Configure the following optional policies for your switch on Ignition Server:
 - Provisioning Polices that set network session and switch parameters for users
 - Client Posture Policies that require that laptops meet a minimum standard of system health
 - VLAN Assignments that assign each user to an appropriate VLAN
 - Windows machine authentication that checks connecting devices to ensure they are known to the Active Directory before the system permits connection
 - MAC authentication that allows operator-less devices to connect and records which device a user connected with
- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. To configure the reachability of the RADIUS server, enter:

```
radius reachability use-radius [username <username> password
<password>]
```

2. To configure RADIUS server account information on the switch enter:

```
radius server host {<A.B.C.D> | <WORD>} [acct-enable] [acct-
port <1-65535>] [key{key}] [port <1-65535>] [retry <1-5>]
[secondary] [timeout <1-60>] [used-by {eapol|non-eapol}]
```

Variable definitions

The following table describes variables that you use with the **radius reachability** command

Variable	Value
password <password>	Specifies a password for the RADIUS request.
use-radius	Uses dummy RADIUS requests to determine reachability of the RADIUS server.
username <username>	Specifies a user name for the RADIUS request.

Variable definitions

The following table describes variables that you use with the **radius server host** command

Variable	Value
<A.B.C.D>	Specifies the IPv4 address of the primary server you want to add or configure. ! Important: A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.
<WORD>	Specifies the IPv6 address of the primary server you want to add or configure. ! Important: A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.
acct-enable	Enables RADIUS accounting for a RADIUS server instance.

Variable	Value
acct-port <1–65535>	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 1 to 65535.
key <key>	Specifies the secret authentication and encryption key used for all communications between the NAS and the RADIUS server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to enter and confirm the key.
port <1–65535>	Specifies the UDP port number for clients to use when trying to contact the RADIUS server at the corresponding RADIUS server IP address. Values range from 1 to 65535. The default port number is 1812.
retry <1–5>	Specifies the number of RADIUS retry attempts for a RADIUS Server instance. Values range from 1 to 5.
secondary	Specifies the RADIUS server you are configuring as the secondary server. The system uses the secondary server only if the primary server is not configured or is not reachable.
timeout <1–60>	Specifies the timeout interval between each retry for service requests to the RADIUS server. Values range from 1 to 60 seconds. The default value is 2 seconds.
used-by <eapol non-eapol>	<p>Specifies the RADIUS server as an EAP RADIUS Server or a Non-EAP (NEAP) RADIUS Server.</p> <ul style="list-style-type: none"> • eapol—configures the RADIUS server to process EAP client requests only. • non-eapol—configures the RADIUS server to process Non-EAP client requests only.

Configuring Ignition Server as an EAP RADIUS server using ACLI

Use this procedure to configure Ignition Server to act as the EAP RADIUS server for your switches and access points. For more information about configuring the Ignition Server for RADIUS, see Avaya Identity Engines Ignition Server Configuration, NN47280-500.

Prerequisites

- Ignition Server installed and configured in your network
- Configure the following policies for your switch on Ignition Server
 - Access
 - User Authentication
 - User Authorization
- Configure the following optional policies for your switch on Ignition Server:
 - Provisioning Polices that set network session and switch parameters for users
 - Client Posture Policies that require that laptops meet a minimum standard of system health
 - VLAN Assignments that assign each user to an appropriate VLAN
 - Windows machine authentication that checks connecting devices to ensure they are known to the Active Directory before the system permits connection
 - MAC authentication that allows operator-less devices to connect and records which device a user connected with
- EAP configured on your switch.
- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. To configure the reachability of the EAP RADIUS server, enter:

```
radius reachability use-radius [username <username> password  
<password>]
```

2. To configure EAP RADIUS server account information on the switch enter:

```
radius server host {<A.B.C.D> | <WORD>} [acct-enable] [acct-  
port <1-65535>] [key{key}] [port <1-65535>] [retry <1-5>]  
[secondary] [timeout <1-60>] used-by eapol
```

Variable definitions

The following table describes variables that you use with the `radius reachability` command

Variable	Value
password <password>	Specifies a password for the RADIUS request.
use-radius	Uses dummy RADIUS requests to determine reachability of the RADIUS server.
username <username>	Specifies a user name for the RADIUS request.

Variable definitions

The following table describes variables that you use with the `radius server host` command

Variable	Value
<A.B.C.D>	Specifies the IPv4 address of the primary server you want to add or configure. ! Important: A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.
<WORD>	Specifies the IPv6 address of the primary server you want to add or configure. ! Important: A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.
acct-enable	Enables RADIUS accounting for a RADIUS server instance.
acct-port <1–65535>	Specifies the UDP accounting port number for clients to use when trying to contact the RADIUS server at the corresponding RADIUS Server IP address. Values range from 1 to 65535.
key <key>	Specifies the secret authentication and encryption key used for all communications

Variable	Value
	between the NAS and the RADIUS server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to enter and confirm the key.
port <1–65535>	Specifies the UDP port number for clients to use when trying to contact the RADIUS server at the corresponding RADIUS server IP address. Values range from 1 to 65535. The default port number is 1812.
retry <1–5>	Specifies the number of RADIUS retry attempts for a RADIUS Server instance. Values range from 1 to 5.
secondary	Specifies the RADIUS server you are configuring as the secondary server. The system uses the secondary server only if the primary server is not configured or is not reachable.
timeout <1–60>	Specifies the timeout interval between each retry for service requests to the RADIUS server. Values range from 1 to 60 seconds. The default value is 2 seconds.
used-by eapol	Specifies the RADIUS server as an EAP RADIUS Server to process EAP client request only.

Configuring Ignition Server as a non-EAP RADIUS server using ACLI

Use this procedure to configure Ignition Server to act as the non-EAP RADIUS server for your switches and access points. For more information about configuring the Ignition Server for RADIUS, see Avaya Identity Engines Ignition Server Configuration, NN47280-500.

Prerequisites

- Ignition Server installed and configured in your network
- Configure the following policies for your switch on Ignition Server
 - Access
 - User Authentication
 - User Authorization

- Configure the following optional policies for your switch on Ignition Server:
 - Provisioning Policies that set network session and switch parameters for users
 - Client Posture Policies that require that laptops meet a minimum standard of system health
 - VLAN Assignments that assign each user to an appropriate VLAN
 - Windows machine authentication that checks connecting devices to ensure they are known to the Active Directory before the system permits connection
 - MAC authentication that allows operator-less devices to connect and records which device a user connected with
- Non-EAP configured on your switch.
- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. To configure the reachability of the non-EAP RADIUS server, enter:

```
radius reachability use-radius [username <username> password
<password>]
```

2. To configure non-EAP RADIUS server account information on the switch enter:

```
radius server host {<A.B.C.D> | <WORD>} [acct-enable] [acct-
port <1-65535>] [key{key}] [port <1-65535>] [retry <1-5>]
[secondary] [timeout <1-60>] used-by non-eapol
```

Variable definitions

The following table describes variables that you use with the **radius reachability** command

Variable	Value
password <password>	Specifies a password for the RADIUS request.
use-radius	Uses dummy RADIUS requests to determine reachability of the RADIUS server.
username <username>	Specifies a user name for the RADIUS request.

Variable definitions

The following table describes variables that you use with the **radius server host** command

Variable	Value
<A.B.C.D>	<p>Specifies the IPv4 address of the primary server you want to add or configure.</p> <p>! Important: A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.</p>
<WORD>	<p>Specifies the IPv6 address of the primary server you want to add or configure.</p> <p>! Important: A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.</p>
acct-enable	<p>Enables RADIUS accounting for a RADIUS server instance.</p>
acct-port <1–66535>	<p>Specifies the UDP accounting port number for clients to use when trying to contact the RADIUS server at the corresponding RADIUS Server IP address. Values range from 1 to 65535.</p>
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>
port <1–65535>	<p>Specifies the UDP port number for clients to use when trying to contact the RADIUS server at the corresponding RADIUS server IP address. Values range from 1 to 65535. The default port number is 1812.</p>
retry <1–5>	<p>Specifies the number of RADIUS retry attempts for a RADIUS Server instance. Values range from 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 <1–60>	<p>Specifies the timeout interval between each retry for service requests to the RADIUS server. Values range from 1 to 60 seconds. The default value is 2 seconds.</p>

Variable	Value
used-by non-eapol	Specifies the RADIUS server as an non-EAP (NEAP) RADIUS Server to process Non—EAP client request only.

Configuring Ignition Server as a TACACS+ server using ACLI

You can configure Ignition Server to act as the TACACS+ authentication and authentication server, and you can use it as the TACACS+ accounting server. For more information , see *Avaya Identity Engines Ignition Server Configuration*, NN47280-600.

Prerequisites

- Ignition Server installed and configured in your network
- Configure the following policies for your switch on Ignition Server
 - Access
 - User Authentication
 - User Authorization
- Configure the following optional policies for your switch on Ignition Server:
 - Provisioning Polices that set network session and switch parameters for users
 - Client Posture Policies that require that laptops meet a minimum standard of system health
 - VLAN Assignments that assign each user to an appropriate VLAN
 - Windows machine authentication that checks connecting devices to ensure they are known to the Active Directory before the system permits connection
 - MAC authentication that allows operator-less devices to connect and records which device a user connected with
- Configure an Ignition Server authentication record with a TACACS+ policy
 - * **Note:**
If you use Ignition Server for TACACS+ authorization, you must use Ignition Server for TACACS+ authentication.
- Configure the TACACS+ server to be added to your system.
- Log on to the Global Configuration mode in ACLI.

Procedure steps

To configure switch TACACS+ server settings enter the following command:

```
tacacs server host <A.B.C.D> port <1-65535> secondary-host
<A.B.C.D> key <key>
```

Variable definitions

The following table describes variables that you use with the `tacacs server` command

Variable	Value
host <A.B.C.D>	Specifies the IP address of the primary server you want to add or configure
key <key>	<p>Specifies the secret authentication and encryption key used for all communications between the NAS and the TACACS+ server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to enter and confirm the key when you enter it.</p> <p>! Important:</p> <p>The key parameter is a required parameter when you create a new server entry. The parameter is optional when you are modifying an existing entry.</p>
port <1-65535>	Specifies the TCP port for TACACS+. <port> is an integer in the range of 1 to 65535. The default port number is 49.
secondary host <A.B.C.D>	Specifies the IP address of the secondary server. The secondary server is used only if the primary server does not respond.

Chapter 6: Security configuration and management using Enterprise Device Manager

This chapter describes the methods and procedures necessary to configure security on the Avaya Ethernet Routing Switch 4000 using Enterprise Device Manager (EDM).

EAPOL configuration using EDM

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

 **Important:**

You must enable EAPOL before you enable UDP Forwarding, IP Source Guard, and other features that use QoS policies.

Configuring EAPOL globally using EDM

Use the following procedure to configure EAPOL globally to configure EAPOL parameters for the switch.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **802.1X/EAP**.
3. On the **EAPOL** tab, configure the EAPOL parameters as required.
4. On the toolbar, click **Apply**.

Variable definitions

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

Variable	Value
DefaultEapAll	Resets all EAP settings.
SystemAuthControl	Enables or disables port access control on the switch.

Variable	Value
UserBasedPoliciesEnabled	Enables the User Based Policies.
UserBasedPoliciesFilterOnMac	Enables the User Based Policies filtering on MAC addresses.
GuestVlanEnabled	Enables or disables the Guest VLAN.
GuestVlanId	Sets the VLAN ID of the Guest VLAN.
MultiHostAllow NonEapClient	Enables or disables support for non EAPOL hosts on EAPOL-enabled ports.
MultiHostSingle AuthEnabled	Enables or disables Multiple Host Single Authentication (MHSA). When selected, non EAPOL hosts are allowed on a port if there is one authenticated EAPOL client on the port.
MultiHostRadiusAuth NonEapClient	Enables or disables RADIUS authentication of non EAPOL hosts on EAPOL-enabled ports.
MultiHostAllowNonEapPhones	Enables or disables Avaya IP Phone clients as another non-EAP type.
MultiHostAllowRadiusAssignedVlan	Enables or disables the use of RADIUS-assigned VLAN values in the Multihost mode.
MultiHostAllowNonEapRadius AssignedVlan	Enables or disables support for RADIUS-assigned VLANs in multihost-eap mode for non-EAP clients.
MultiHostUseMostRecentRadius AssignedVlan	Enables or disables the Last Assigned VLAN on a port.
MultiHostMultiVlan	Enables or disables the multiple VLAN capability for EAP and non-EAP hosts. The default is disabled.
MultiHostEapPacketMode	Enables or disables the choice of packet mode (unicast or multicast) in the Multihost mode.
MultiHostEapProtocolEnabled	Enables or disables the processing of EAP protocol packets.
MultiHostFailOpenVlanEnabled	<p>Enables or disables the EAPOL multihost Fail Open VLAN.</p> <p>! Important:</p> <p>The switch does not validate that RADIUS Assigned VLAN attribute is not the same as the Fail_Open VLAN. This means that if you configure the Fail_Open VLAN name or ID the same as one of the VLAN names or IDs which can be returned from the RADIUS server, then EAP or NEAP clients cannot be assigned to the Fail_Open VLAN even though no failure to connect to the RADIUS server has occurred.</p>

Variable	Value
MultiHostFailOpenVlanId	Sets the VLAN ID of the Fail Open VLAN.
MultiHostFailOpenVlanContinuityModeEnabled	Enables or disables the EAPOL multihost Fail Open VLAN Continuity mode.
NonEapRadiusPasswordAttributeFormat	Configures the format of the RADIUS server password attribute for Non-EAP clients.
MultiHostNonEapRadiusPasswordFreeformKey	Sets the user-configurable key for Non-EAP RADIUS password.
Confirm MultiHostNonEapRadiusPasswordFreeformKey	Confirms the user-configurable key for Non-EAP RADIUS password.
NonEapUserBasedPoliciesEnabled	Enables Non-EAP User Based Policies settings.
NonEapUserBasedPoliciesFilterOnMac	Enables Non-EAP filtering on MAC addresses.
MultiHostAdacNonEapEnabled	Enables Non-EAP Multihost ADAC settings.
MultiHostNeapReauthenticationEnabled	Enables Multihost NEAP reauthentication.
MultiHostBlockDifferentVlanAuth	Enables or disables the block subsequent MAC authentication feature.

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 steps

1. From 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. Select the **MultiHstNeapReauthenticationEnabled** checkbox to enable NEAP re-authentication.

OR

Clear the **MultiHstNeapReauthenticationEnabled** checkbox to disable NEAP re-authentication.

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

Configuring port-based EAPOL using EDM

Use the following procedure to configure port-based EAPOL to configure EAPOL security parameters for an individual port or multiple ports.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-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. You can repeat the previous two steps until you have amended all of the parameters you want to change.
7. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
PortNumber	Indicates the port number.
AdminControlledDirections	Indicates the current value of the administrative controlled directions parameter for the port.
OperControlledDirections	Indicates the current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	Indicates the current value of the controlled port status parameter for the port.
AuthControlledPortControl	Indicates the current value of the controlled port control parameter for the port.
QuietPeriod	Indicates the current value of the time interval between authentication failure, and the start of a new authentication.
TransmitPeriod	Indicates the time to wait for response from supplicant for EAP requests/Identity packets.
SupplicantTimeout	Indicates the time to wait for response from supplicant for all EAP packets except EAP Request/Identity.
ServerTimeout	Indicates the time to wait for a response from the RADIUS server

Variable	Value
MaximumRequests	Indicates the number of times to retry sending packets to the supplicant.
ReAuthenticationPeriod	Indicates the time interval between successive reauthentications.
ReAuthenticationEnabled	Indicates whether to reauthenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field.
PortProtocolVersion	Indicates the EAP Protocol version that is running on this port.
PortCapabilities	Indicates the PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable (0).
PortInitialize	Indicates whether to initialize the EAPOL state of the port. Setting this attribute to True causes this port EAPOL state to be initialized.
PortReauthenticateNow	Indicates the current reauthentication state of the machine. Setting this attribute to True causes the reauthentication of the client.
PaeState	Indicates the current authenticator PAE state machine stat value.
BackendAuthState	Indicates the current state of the Backend Authentication state machine.
KeyTxEnabled	Indicates the value of the KeyTransmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns False as key transmission is irrelevant.
LastEapolFrameVersion	Indicates the protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	Indicates the source MAC address carried in the most recently received EAPOL frame.


Configuring advanced port-based EAPOL using EDM

Use the following procedure to configure advanced EAPOL security parameters for an individual port or multiple ports.

Procedure steps

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 **EAPOL Advance** tab.

Variable definitions

Variable	Value
Portnumber	Indicates the port number.
DefaultEapAll	Enables or disables the default EAP settings.
GuestVlanEnabled	Enables or disables Guest VLAN functionality.
GuestVlanId	<p>Specifies the VLAN ID of the VLAN that acts as the Guest VLAN. The default is 0. The Guest VLAN ID can be between 0 and 4094.</p> <p> Important: Use 0 to indicate a global Guest VLAN ID.</p>
MultiHostMaxMacs	Specifies the maximum number of clients allowed on this port. The default is 1. The maximum number can be between 1 and 64.
MultiHostEnabled	Enables or disables Multiple Host/MAC support with Multiple Authentication (MHMA).
MultiHostEapMaxNumMacs	Specifies the maximum number of EAPOL-authenticated clients allowed on this port. The default is 1. The maximum number can be between 1 and 32
MultiHostAllowNonEapClient	Enables or disables support for non EAPOL clients using local authentication.
MultiHostNonEapMaxNumMacs	Specifies the maximum number of non EAPOL clients allowed on this port. The default is 1. The maximum number can be between 1 and 32.

Variable	Value
MultiHostSingleAuthEnabled	Enables or disables Multiple Host with Single Authentication (MHSA) support for non EAPOL clients.
MultiHostRadiusAuthNonEapClient	Enables or disables support for non EAPOL clients using RADIUS authentication.
MultiHostAllowNonEapPhones	Enables or disables support for Avaya IP Phone clients as another non-EAP type.
MultiHostAllowRadiusAssignedVlan	Enables or disables support for VLAN values assigned by the RADIUS server.
MultiHostAllowNonEapRadiusAssignedVlan	Enables or disables support for RADIUS-assigned VLANs in multihost-EAP mode for non-EAP clients.
MultiHostEapPacketMode	Specifies the mode of EAPOL packet transmission (multicast or unicast).
MultiHostAllowRadiusAssignedVlan	Enables or disables support for VLAN values assigned by the RADIUS server.
MultiHostAllowNonEapRadiusAssignedVlan	Enables or disables support for RADIUS assigned VLANs in multihost-EAP mode for non-EAP clients.
MultiHostEapPacketMode	Specifies the mode of EAPOL packet transmission (multicast or unicast).
EapProtocolEnabled	Enables or disables EAP protocol.
MultiHostBlockDifferentVlanAuth	Enables or disables the block subsequent MAC authentication feature.
ProcessRadiusRequestsServerPackets	Enables or disables the processing of RADIUS requests-server packets that are received on this port.
MultiHostClearNeap	Clears authenticated NEAP clients from a specified port. 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.
MultiHostAdacNonEapEnabled	Enables or disables Non-EAP Multihost ADAC settings.

Graphing port EAPOL statistics using EDM

Use this procedure to display and graph port EAPOL statistics.

Procedure steps

1. From the Device Physical View, click a port.
2. From the navigation pane, double-click **Graph** .
3. In the Graph tree, double-click **Port** .
4. In the work area, click the **EAPOL Stats** tab.
5. On the toolbar, select a **Poll Interval** from the list.
6. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
7. To select statistics to graph, click a statistic type row under a column heading.
8. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

Use the data in the following table to help you understand port EAPOL statistics.

Variable	Value
EapolFramesRx	The number of valid EAPOL frames of any type that are received by this authenticator.
EapolFramesTx	The number of EAPOL frame types of any type that are transmitted by this authenticator.
EapolStartFramesRx	The number of EAPOL start frames that are received by this authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that are received by this authenticator.
EapolRespIdFramesRx	The number of EAPOL Resp/Id frames that are received by this authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (Other than Resp/Id frames) that are received by this authenticator.
EapolReqIdFramesTx	The number of EAPOL Req/Id frames that are transmitted by this authenticator.
EapolReqFramesTx	The number of EAP Req/Id frames (Other than Req/Id frames) that are transmitted by this authenticator.

Variable	Value
InvalidEapolFramesRx	The number of EAPOL frames that are received by this authenticator in which the frame type is not recognized.
EapLengthError FramesRx	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 display and graph port EAPOL diagnostic statistics.

Procedure steps

1. From the Device Physical View, click a port.
2. From the navigation pane, double-click **Graph** .
3. In the Graph tree, double-click **Port** .
4. In the work area, click the **EAPOL Diag** tab.
5. On the toolbar, select a **Poll Interval** from the list.
6. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
7. To select statistics to graph, click a statistic type row under a column heading.
8. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

Use the data in the following table to help you understand EAPOL diagnostic statistics.

Variable	Value
EntersConnecting	Counts the number of times that the state machine transitions to the connecting state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the state machine transitions from connecting to disconnecting because of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the state machine transitions from connecting to authenticating, because of an EAP-Response or Identity message being received from the Supplicant.

Variable	Value
AuthSuccessWhile Authenticating	Counts the number of times that the state machine transitions from authenticating to authenticated, because of the Backend Authentication state machine indicating a successful authentication of the Supplicant.
AuthTimeoutsWhile Authenticating	Counts the number of times that the state machine transitions from authenticating to aborting, because of the Backend Authentication state machine indicating an authentication timeout.
AuthFailWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to held, because of the Backend Authentication state machine indicating an authentication failure.
AuthReauthsWhile Authenticating	Counts the number of times that the state machine transitions from authenticating to aborting, because of a reauthentication request.
AuthEapStartsWhile Authenticating	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.
AuthEapLogoffWhile Authenticating	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.
AuthReauthsWhile Authenticated	Counts the number of times that the state machine transitions from authenticated to connecting, because of a reauthentication request.
AuthEapStartsWhile Authenticated	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.
AuthEapLogoffWhile Authenticated	Counts the number of times that the state machine transitions from authenticated to disconnected, because of an EAPOL-Logoff message being received from the Supplicant.
BackendResponses	Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
BackendAccessChallenges	Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the

Variable	Value
	Authentication Server has communication with the Authenticator.
BackendOtherRequestsTo Supplicant	Counts the number of times that the state machine sends an EAP-Request packet, other than an Identity, Notification, Failure or Success message, to the Supplicant. Indicates that the Authenticator chooses an EAP-method.
BackendNonNakResponses FromSupplicant	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the EAP-method that the Authenticator chooses.
BackendAuthSuccesses	Counts the number of times that the state machine receives an EAP-Success message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.
BackendAuthFails	Counts the number of times that the state machine receives an EAP-Failure message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.

Viewing Multihost status information using EDM

Use the following procedure to view Multihost status information to display multiple host status for a port.

 **Important:**

The **Multi Hosts** button is not available when you select multiple ports before clicking the EAPOL Advance tab. You can select only one port to use the Multi Hosts option.

Procedure steps

1. From the navigation tree, double-click **Edit**
2. In the Edit tree, double-click **Chassis**
3. In the Chassis tree, double-click **Ports**.
4. In the work area, click the **EAPOL Advance** tab.
5. On the toolbar, click **Multi Hosts**.

Variable definitions

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

Variable	Value
PortNumber	Indicates the port number in use.
ClientMACAddr	Indicates the MAC address of the client.
PaeState	Indicates the current state of the authenticator PAE state machine.
BackendAuthState	Indicates the current state of the Backend Authentication state machine.
Reauthenticate	Indicates the current reauthentication state of the machine. When the reauthenticate attribute is set to True, the client reauthenticates.
Vid	Indicates the VLAN assigned to the client.
Pri	Indicates the priority of the client.

Viewing Multihost session information using EDM

Use the following procedure to view Multihost session information to display multiple host session information for a port.

 **Important:**

The **Multi Hosts** button is not available when you select multiple ports before clicking the EAPOL Advance tab. You can select only one port to use the Multi Hosts option.

Procedure steps

1. From the navigation tree, double-click **Edit**
2. In the Edit tree, double-click **Chassis**
3. In the Chassis tree, double-click **Ports**.
4. In the work area, click the **EAPOL Advance** tab.
5. On the toolbar, click **Multi Hosts Multi Host Session** tab.

Variable definitions

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

Variable	Value
PortNumber	Indicates the port number in use.
ClientMACAddr	Indicates the MAC address of the client.
Id	Indicates the unique identifier for the session, in the form of a printable ASCII string of at least three characters.
AuthenticMethod	Indicates the authentication method used to establish the session.
Time	Indicates the elapsed time of the session.
TerminateCause	Indicates the cause of the session termination.
UserName	Indicates the user name representing the identity of the supplicant PAE.

Allowed non-EAP MAC address list configuration using EDM

Use the following procedure to configure the allowed non-EAP MAC address list to view and configure the list of MAC addresses for non-EAPOL clients that are authorized to access the port.

Allowed non-EAP MAC address list configuration using EDM navigation

- [Adding a MAC address to the allowed non-EAP MAC address list using EDM](#) on page 297
- [Deleting a MAC address from the allowed non-EAP MAC address list using EDM](#) on page 298

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

Use the following procedure to add a MAC address to the allowed non-EAP MAC address list to insert a new MAC address to the list of MAC addresses for non-EAPOL clients that are authorized to access the port.

Procedure steps

Important:

The **Non-EAP MAC** button is not available when you select multiple ports before clicking the EAPOL Advance tab. You can select only one port to use the Non-EAP MAC option.

1. From the navigation tree, double-click **Edit**
2. In the Edit tree, double-click **Chassis**
3. In the Chassis tree, double-click **Ports**.
4. In the work area, click the **EAPOL Advance** tab.
5. In the table, click the port you want to edit.
6. In the tool bar, Click the **Non-EAP MAC** button.
7. On the Allowed non-EAP MAC table, in the ClientMACAddr column, click a client MAC Address to insert.
8. In the ClientMACAddr box, enter a MAC address to add to the list of allowed non-EAPOL clients
9. Click **Insert**.
10. On the tool bar, click **Apply** to confirm the addition..
11. On the tool bar, you can click **Refresh** to see the results of your addition.

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

Use the following procedure to remove an existing MAC address from the list of MAC addresses for non-EAPOL clients that are authorized to access the port.

Procedure steps

1. From the navigation tree, double-click **Edit**
2. In the Edit tree, double-click **Chassis**
3. In the Chassis tree, double-click **Ports**.
4. In the work area, click the **EAPOL Advance** tab.
5. In the table, click the port you want to edit.
6. In the tool bar, Click the **Non-EAP MAC** button.

Important:

The **Non-EAP MAC** button is not available when you select multiple ports before clicking the EAPOL Advance tab. You can select only one port to use the Non-EAP MAC option.

7. On the Allowed non-EAP MAC table, in the ClientMACAddr column, click a client MAC Address to insert.

8. On the toolbar, click **Delete**.
9. Click **Yes** to confirm the deletion.
10. On the tool bar, you can click **Refresh** to see the results of your addition.

Variable definitions

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

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

Viewing port non-EAP host support status using EDM

Use the following procedure to display the status of non-EAP host support on the port.

Procedure steps

1. From the navigation tree, double-click **Edit**
2. In the Edit tree, double-click **Chassis**
3. In the Chassis tree, double-click **Ports**.
4. In the work area, click the **EAPOL Advance** tab.
5. In the tool bar, click the **Non-EAP MAC** button.
6. Click the **Non-EAP Status** tab.

Variable definitions

Variable	Value
PortNumber	Indicates the port number in use.
ClientMACAddr	Indicates the MAC address of the client.
State	Indicates the authentication status. Possible values are: <ul style="list-style-type: none"> • rejected: the MAC address cannot be authenticated on this port • locallyAuthenticated: the MAC address was authenticated using the local table of allowed clients

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

Enabling VoIP VLAN using EDM

Use the following procedure to activate the VoIP VLAN.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-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 header you want to edit.
5. Select a parameter or value from the drop-down list.

You can repeat the previous two steps until you have amended all of the parameters you want to change.

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

Variable Definitions

The following table defines variables you can use to enable VoIP VLAN.

Variable	Value
MultiHostVoipVlanIndex	Indicates the multihost VoIP VLAN index. Range is 1–5.
MultiHostVoipVlanEnabled	Enables (true) or disables (false) the multihost VoIP VLAN.
MultiHostVoipVlanId	Indicates the VLAN ID; value ranges from 1–4094.

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.  Note: If you configure the Web server to respond to HTTPS client browser requests only, all existing non-secure connections with the browser are terminated.

Configuring general switch security using EDM

Use the following procedure to configure general switch security and to configure and manage general security parameters for the switch.


Procedure steps


1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. On the **MAC Security** tab, configure general switch security parameters as required.
4. On the toolbar, click **Apply**.

Variable definitions

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

Variable	Value
AuthSecurityLock	If this parameter is listed as locked, the agent refuses all requests to modify the security configuration. Entries also include: <ul style="list-style-type: none"> • other • notlocked
AuthCtlPartTime	Indicates the duration of time for port partitioning in seconds. Default: 0 (zero). When the value is zero, port remains partitioned until it is manually reenabled.
SecurityStatus	Indicates whether or not the switch security feature is enabled.
SecurityMode	Indicates the mode of switch security. Entries include: <ul style="list-style-type: none"> • macList—Indicates that the switch is in the MAC-list mode. You can configure more than one MAC address for a port. • autoLearn—Indicates that the switch learns the MAC addresses on each port as allowed addresses of that port.

Variable	Value
SecurityAction	<p>Indicates the actions performed by the software when a violation occurs (when SecurityStatus is enabled). The security action specified here applies to all ports of the switch.</p> <p>A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include:</p> <ul style="list-style-type: none"> • noAction—Port does not have security assigned to it, or the security feature is turned off. • trap—Listed trap. • partitionPort—Port is partitioned. • partitionPortAndsendTrap—Port is partitioned and traps are sent to the trap receive station. • daFiltering—Port filters out the frames where the destination address field is the MAC address of unauthorized Station. • daFilteringAndsendTrap—Port filters out the frames where the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive stations. • partitionPortAnddaFiltering— Port is partitioned and filters out the frames where the destination address field is the MAC address of unauthorized station. • partitionPortdaFilteringAndsendTrap—Port is partitioned and filters out the frames where the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive stations. <p> Important: da means destination addresses.</p>
CurrNodesAllowed	Indicates the current number of entries of the nodes allowed in the AuthConfig tab.
MaxNodesAllowed	Indicates the maximum number of entries of the nodes allowed in the AuthConfig tab.
PortSecurityStatus	Indicates the set of ports for which security is enabled.
PortLearnStatus	Indicates the set of ports where autolearning is enabled.
CurrSecurityLists	Indicates the current number of entries of the Security listed in the SecurityList tab

Variable	Value
MaxSecurityLists	Indicates the maximum entries of the Security listed in the SecurityList tab.
AutoLearningAgingTime	Indicates the MAC address age-out time, in minutes, for the autolearned MAC addresses. A value of zero (0) indicates that the address never ages out.
AutoLearningSticky (sticky-mac)	Enables or disables MAC security auto-learning sticky mode.
SecurityLockoutPortList	Controls the list of ports that are locked so they are excluded from MAC-based security.  Important: You must disable autolearning before you change the SecurityLockoutPortList .

Security list configuration using EDM

Use the procedures in this section to configure the security list to manage the port members in a security list.

Security list configuration using EDM navigation

- [Adding ports to a security list using EDM](#) on page 304
- [Deleting specific ports from a security list using EDM](#) on page 305
- [Deleting all ports from a security list using EDM](#) on page 306

Adding ports to a security list using EDM

Use the following procedure to add ports to the security list to insert new port members into a security list.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. In the work area, click the **Security List** tab.

4. On the toolbar, click the **Insert** button.

The Insert SecurityList dialog box appears.

5. Type a number for the security list in the **SecurityListIdx** box.
6. Click the SecurityListMembers ellipsis [...], and select ports to add to the security list.

OR

Click **All** to select all ports.

7. Click **Ok**.
8. Click **Insert**.

Variable definitions

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

Variable	Value
SecurityListIdx	Indicates a numerical identifier for a security list. Values range from 1–32.
SecurityListMembers	Defines the security list port members.

Deleting specific ports from a security list using EDM

Use the following procedure to delete specific ports from a security list to remove specific existing port members from a security list.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. In the work area, click the **SecurityList** tab.
4. Double-click the **SecurityListMembers** box for a security list.
5. Deselect security list port members as required.
6. Click **Ok**.
7. Click **Apply**.

Variable definitions

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

Variable	Value
SecurityListIdx	Indicates the numerical identifier for a security list. Values range from 1–32.
SecurityListMembers	Defines the security list port members.

Deleting all ports from a security list using EDM

Use the following procedure to delete all ports from a security list to remove all existing port members from a security list.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. In the work area, click the **SecurityList** tab.
4. Click the **SecurityListMembers** box for a security list.
5. Click **Delete**.
6. Click **Yes**.

Variable definitions

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

Variable	Value
SecurityListIdx	Indicates the numerical identifier for a security list. Values range from 1–32.
SecurityListMembers	Defines the security list port members.

AuthConfig list configuration using EDM

This section describes how you can add entries to or remove entries from a list of boards, ports and MAC addresses that have the security configuration.

AuthConfig list configuration using EDM navigation

- [Adding entries to the AuthConfig list using EDM](#) on page 307
- [Deleting entries from the AuthConfig list using EDM](#) on page 309

Adding entries to the AuthConfig list using EDM

Use the following procedure to add information to the list of boards, ports and MAC addresses that have the security configuration.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. In the work area, click the **AuthConfig** tab.
4. On the toolbar, click **Insert**.
The Insert AuthConfig dialog box appears.
5. Type a value in the **BrdIndx** box.
6. Type a value in the **PortIndx** box.
7. Type a value in the **MACIndx** box.
8. Select the **AutoLearningSticky** check box to enable Sticky MAC address.

OR

Clear the **AutoLearningSticky** check box, if selected, to disable Sticky MAC address.

9. Select the **AccessCtrlType** radio button to allow a MAC address on multiple ports.

OR

Clear the **AccessCtrlType** radio button to disallow a MAC address on multiple ports.

10. Type a value in the **SecureList** box.




OR


Type a value in the **Trunk** box.

11. Click **Insert**.

Variable definitions

Use the data in the following table to add entries to the list of boards, ports and MAC addresses that have the security configuration.

Variable	Value
BrdIdx	Indicates the index of the board. This corresponds to the unit.  Important: If a BrdIdx is specified, the SecureList field is 0.
PortIdx	Indicates the index of the port.  Important: If a PortIdx is specified, the SecureList field is 0.
MACIdx	Indicates the index of MAC addresses that are designated as <i>allowed</i> (station).
AutoLearningSticky (sticky-mac)	Enables or disables the storing of automatically learned MAC addresses across switch reboots.  Important: When the AutoLearningSticky check box is selected, you cannot modify AccessCtrlType and SecureList.
AccessCtrlType	Displays the node entry <i>node allowed</i> . A MAC address can be allowed on multiple ports.
SecureList	Indicates the index of the security list. This value is meaningful only if BrdIdx and PortIdx values are set to zero. For other board and port index values, this field can also have the value of zero. The corresponding MAC address of this entry is allowed or blocked on all ports of this port list.
Source	Indicates the method used by the MAC security and MAC address tables to learn MAC addresses. Values include:

Variable	Value
	<ul style="list-style-type: none"> • Static • Sticky • AutoLearn
Lifetime	Indicates the time period before the system automatically deletes an AuthConfig entry.
Trunk	Indicates the trunk ID.  Note: You cannot specify a trunk ID and a security list at the same time.

Deleting entries from the AuthConfig list using EDM

Use the following procedure to remove information from the list of boards, ports, and MAC addresses that have security configuration.

Procedure steps

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. In the work area, click the **AuthConfig** tab.
4. Select a list entry.
5. Click **Delete**.
6. Click **Yes**.

Configuring MAC Address AutoLearn using EDM

Use the following procedure to configure MAC Address AutoLearn to configure the MAC Address auto learning properties of switch ports.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. In the work area, click the **AutoLearn** tab.
4. Double-click the **Enabled** box for a port.
5. Select **true** to enable AutoLearn on the port.

OR

- Select **false** to disable AutoLearn on the port.
6. Double-click the **MaxMacs** box for a port.
 7. Type a value between 1 and 25.
 8. Click **Apply**.

Variable definitions

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

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

Viewing AuthStatus information using EDM

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

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. Click the **AuthStatus** tab to view the status information.

Variable definitions

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

Variable	Value
AuthStatusBrdIndx	Indicates the index of the board. This corresponds to the index of the slot containing the board if the index is greater than zero.
AuthStatusPortIndx	Indicates the index of the port on the board. This corresponds to the index of the last manageable port on the board if the index is greater than zero.
AuthStatusMACIndx	Indicates the index of MAC address on the port. This corresponds to the index of the MAC address on the port if the index is greater than zero.
CurrentAccessCtrlType	Displays whether the node entry is <code>node allowed</code> or <code>node blocked</code> type.
CurrentActionMode	Indicates the value representing the type of information contained, including: <ul style="list-style-type: none"> • <code>noAction</code>—Port does not have security assigned to it, or the security feature is turned off. • <code>partitionPort</code>—Port is partitioned. • <code>partitionPortAndsendTrap</code>— Port is partitioned and traps are sent to the trap receive station. • <code>Filtering</code>—Port filters out the frames, where the destination address field is the MAC address of unauthorized station. • <code>FilteringAndsendTrap</code>—Port filters out the frames, where the destination address field is the MAC address of unauthorized station. Trap are sent to trap receive station. • <code>sendTrap</code>—A trap is sent to trap receive stations.

Variable	Value
	<ul style="list-style-type: none"> • partitionPortAnddaFiltering— Port is partitioned and will filter out the frames where the destination address field is the MAC address of unauthorized station. • partitionPortdaFilteringAndsendTrap—Port is partitioned and will filter out the frames where the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive stations.
CurrentPortSecurStatus	Displays the security status of the current port, including: <ul style="list-style-type: none"> • If the port is disabled, notApplicable is returned. • If the port is in a normal state, portSecure is returned. • If the port is partitioned, portPartition is returned.

Viewing AuthViolation information using EDM

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

Procedure steps

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. Click the **AuthViolation** tab to view the AuthViolation information.

Variable definitions

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

Variable	Value
BrdIdx	Indicates the index of the board. This corresponds to the slot containing the board. The index is 1 where it is not applicable.

Variable	Value
PortIndx	Indicates the index of the port on the board. This corresponds to the port on that a security violation was seen.
MACAddress	Indicates the MAC address of the device attempting unauthorized network access (MAC address-based security).

Viewing MacViolation information using EDM

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

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. Click the **MacViolation** tab.

Variable definitions

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

Variable	Value
Address	Indicates the MAC address of the device attempting unauthorized network access (MAC address-based security).
Brd	Indicates the index of the board. This corresponds to the slot containing the board. The index is 1 when it is not applicable.
Port	Indicates the index of the port on the board. This corresponds to the port on which a security violation was seen.

Configuring Secure Shell protocol using EDM

Use the following procedure to configure the Secure Shell (SSH) protocol to replace Telnet and provide secure access to the ACLI interface.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **SSH/SSL**.
3. In the work area, click the **SSH** tab.
4. Configure SSH parameters as required.
5. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
Enable	Enables, disables, or selects secure mode for SSH authentication. <ul style="list-style-type: none"> • false • true • secure
Version	Displays the SSH version.
Port	Defines the SSH connection port. Values range from 1 to 65535.
Timeout	Defines the SSH connection timeout in seconds. Values range from 1 to 120 seconds.
KeyAction	Specifies the SSH key action. <ul style="list-style-type: none"> • generateDsa • generateRsa • deleteDsa • deleteRsa
RsaAuth	Enables or disables SSH RSA authentication

Variable	Value
DsaAuth	Enables or disables SSH DSA authentication.
PassAuth	Enables or disables SSH password authentication.
RsaHostKeyStatus	Indicates the current status of the SSH RSA host key. Values include: <ul style="list-style-type: none"> • noSuchInstance_OID • notGenerated • generated • generating
DsaHostKeyStatus	Indicates the current status of the SSH DSA host key. Values include: <ul style="list-style-type: none"> • noSuchInstance_OID • notGenerated • generated • generating
TftpServerInetAddressType	Indicates the type of address stored in the TFTP server. Values include: <ul style="list-style-type: none"> • ipv4 • 1pv6
TftpServerInetAddress	Specifies the IP address of the TFTP server for all TFTP operations.
TftpFile	Indicates the name of file for the TFTP transfer.
TftpAction	Specifies the action for the TFTP transfer. Values include: <ul style="list-style-type: none"> • none • downloadSshPublicKeys • deleteSshDsaAuthKey • downloadSshRsaPublicKeys • deleteSshRsaAuthKey
TftpResult	Displays the result of the last TFTP action request.
SshAuthKeyFilename	Specifies the SSH authentication key file to download.

Variable	Value
UsbTargetUnit	Specifies the unit number of the USB port to use for file uploads and downloads. Values range from 1 to 9. Values 1 to 8 apply to a USB port in a switch stack. Value 9 applies to a standalone switch.
Action	DnldSshAuthKeyFromUsb—when selected, specifies to download the SSH authentication key using the USB port.
Status	Indicates the status of the latest SSH authentication key download using the USB port. Values include the following: <ul style="list-style-type: none"> • other—no action taken since the switch boot up • inProgress—authentication key download is in progress • success—authentication key download completed successfully • fail—authentication key download failed

Viewing SSH Sessions information using EDM

Use the following procedure to display currently active SSH session information.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **SSH/SSL**.
3. In the work area, click the **SSH Sessions** tab.

Variable definitions

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

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

Configuring an SSH Client using EDM

Use this procedure to configure and manage a Secure Shell (SSH) Client.

Procedure steps

1. From 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**.

Variable definitions

Variable	Value
KeyAction:	<p>Specifies the action to take for the SSH Client host key. Values include:</p> <ul style="list-style-type: none"> • none—take no host key action. • generateDsa—generates a DSA host key for the SSH Client. • generateRsa—generates an RSA host key for the SSH Client. • deleteDsa—deletes the SSH Client DSA host key. • deleteRsa—deletes the SSH Client RSA host key.
KeyFileName:	Specifies the a SSH Client host key file name.

Variable	Value
TftpAction:	Specifies the type of SSH Client authentication key to upload using TFTP. Values include: <ul style="list-style-type: none"> • none—do not upload an SSH Client authentication key using TFTP. • uploadSshcDsaAuthKey—uploads a DSA SSH Client authentication key using TFTP. • uploadSshcRsaAuthKey—uploads an RSA SSH Client authentication key using TFTP.
UsbAction	Specifies the type of SSH Client authentication key to upload using USB. Values include: <ul style="list-style-type: none"> • none—do not upload an SSH Client authentication key using USB. • uploadSshcDsaAuthKey—uploads a DSA SSH Client authentication key using USB. • uploadSshcRsaAuthKey—uploads an RSA SSH Client authentication key using USB.
DsaKeySize:	Specifies the DSA key size. Values range from 512 to 1024.
RsaKeySize:	Specifies the RSA key size. Values range from 512 to 1024.
DsaHostKeyStatus:	Indicates the current status of the SSH Client DSA host key. Values include: <ul style="list-style-type: none"> • notGenerated • generated • generating
RsaHostKeyStatus:	Indicates the current status of the SSH Client RSA host key. Values include: <ul style="list-style-type: none"> • notGenerated • generated • generating
SFTP	
Port:	Specifies the TCP port number for the SFTP file transfer. Values range from 1 to 65535.
DsaAuthentication	When selected, enables SFTP DSA authentication for SSH Client (default).
RsaAuthentication	When selected, enables SFTP password authentication for SSH Client.

Variable	Value
PasswordAuthentication	When selected, enables SFTP RSA authentication for SSH Client.
UserName	Specifies the user name.
SftpServerAddress	Specifies the IP address of the SFTP server.

Configuring SSL using EDM


Use the following procedure to configure Secure Socket Layer (SSL) to provide your network with a secure Web management interface.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **SSH/SSL**.
3. In the work area, click the **SSL** tab.
4. Configure SSL parameters as required.
5. Click **Apply**.

Variable definitions

Variable	Value
Enabled	Indicates whether SSL is enabled or disabled
CertificateControl	Creates or deletes SSL certificates. The last value set is displayed until you change the selection. The default value is other , which indicates that the object was never set.
CertificateExists	Indicates whether a valid SSL certificate is created. Values include: <ul style="list-style-type: none"> • true—indicates that a valid certificate is created. • false—indicates that no valid certificate is created, or that the certificate is deleted.

Variable	Value
CertificateControlStatus	Indicates the status of the most recent attempt to create or delete a certificate. The possible status messages are as follows: <ul style="list-style-type: none"> • inProgress—the operation is not yet completed • success—the operation is complete • failure—the operation failed • other—CertificateControl was never set
ServerControl	Resets the SSL server. Values are reset and other. The default is other. <p> Important: You cannot reset the SSL server while creating the SSL certificate.</p>

Configuring RADIUS globally using EDM

Remote users can change their account passwords when RADIUS server is configured and enabled in their network.

When RADIUS servers are configured in a network, they provide centralized authentication, authorization, and accounting for network access. The MS-CHAPv2 encapsulation method can be enabled to permit RADIUS password change for the user accounts.

Use the following procedure to configure RADIUS security and encapsulation for the switch.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **RADIUS**.
3. In the work area, click the **Globals** tab.
4. In the RADIUS section, select the **UseMgmtIp** checkbox, to enable RADIUS request use management, .

OR

In the RADIUS section, clear the **UseMgmtIp** checkbox. to disable RADIUS request use management.

5. In the RADIUS section, select the **PasswordFallbackEnabled** checkbox. to enable RADIUS password fallback.

OR

In the RADIUS section, clear the **PasswordFallbackEnabled** checkbox, to disable RADIUS password fallback.

- In the RADIUS section, select the **DynAuthReplayProtection** checkbox, to enable RADIUS replay protection .

OR

In the RADIUS section, clear the **DynAuthReplayProtection** checkbox, to disable RADIUS replay protection .

- In the RADIUS section, click a **Reachability** radio button.
- In the RADIUS section, type the reachability user name in the **ReachabilityUserName** dialog box.
- In the RADIUS section, type the reachability password in the **ReachabilityPassword** dialog box.
- In the RADIUS section, type the reachability password again to confirm in the **ConfirmReachabilityPassword** dialog box.
- In the RADIUS Encapsulation section, click an **EncapsulationProtocol** radio button.
- On the toolbar, click **Apply**.

Variable definitions

Variable	Value
UseMgmtIp	When selected, RADIUS uses the system management IP address as the source address for RADIUS requests.
PasswordFallbackEnabled	When selected, enables RADIUS password fallback.
DynAuthReplayProtection	When selected, enables RADIUS replay protection.
Reachability	Specifies the RADIUS server reachability mode. Values include: <ul style="list-style-type: none"> • use-radius—uses dummy RADIUS requests to determine reachability of the RADIUS server. • use-icmp—uses ICMP packets to determine reachability of the RADIUS server (default).
ReachabilityUserName	Specifies a user identification name for RADIUS reachability.
ReachabilityPassword	Specifies a user password for RADIUS reachability.
ConfirmReachabilityPassword	Re-enter the user password for verification.

Variable	Value
EncapsulationProtocol	Specifies the type of encapsulation for the RADIUS packets. Values include: <ul style="list-style-type: none"> • pap — Password Authentication Protocol. • ms-chap-v2 — Microsoft Challenge Handshake Authentication Protocol Version 2.

Configuring RADIUS accounting using EDM

Use the following procedure to enable or disable RADIUS accounting and to configure RADIUS accounting interim updates for the switch.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **RADIUS**.
3. In the work area, click the **Globals** tab.
4. In the RADIUS Accounting section, select the **InterimUpdates** checkbox, to enable RADIUS accounting interim updates.

OR

In the RADIUS Accounting section, clear the **InterimUpdates** checkbox, to disable RADIUS accounting interim updates.

5. In the RADIUS Accounting section, type an interval value in the **InterimUpdatesInterval** dialog box.
6. In the RADIUS Accounting section, select a radio button in the **InterimUpdatesIntervalSource** section.
7. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
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.
InterimUpdatesIntervalSource	Specifies the source of the interim updates timeout interval.

Variable	Value
	<ul style="list-style-type: none"> • configuredValue—uses the value in the RadiusAccountingInterimUpdatesInterval dialog box • radiusServer—uses the value applied by the RADIUS server

Configuring the Global RADIUS Server using EDM

Use this procedure to configure a Global RADIUS Server for processing client requests without designating separate EAP or Non-EAP requests.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **RADIUS**.
3. In the work area, click the **Global RADIUS Server** tab.
4. Choose an address type in the **PrimaryRadiusServerAddressType** box.
5. Type an IP address in the **PrimaryRadiusServer** box.
6. Choose an address type in the **SecondaryRadiusServerAddressType** box.
7. Type an IP address in the **SecondaryRadiusServer** box.
8. Type a UDP port number in the **RadiusServerUdpPort** box.
9. Type a timeout value in the **RadiusServerTimeout** field.
10. To change the shared secret key, type a value in the **SharedSecret(Key)** box.
11. Confirm the new shared secret value in the **ConfirmSharedSecret(Key)** box.
12. To enable accounting, check the **AccountingEnabled** checkbox.

OR

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**.

Variable definitions

Variable	Value
PrimaryRadiusServerAddressType	Specifies the type of IP address type for the primary Global RADIUS server. Values include unknown, ipv4, and ipv6.
PrimaryRadiusServer	<p>Specifies the IPv4 or IPv6 address for the primary Global RADIUS Server. The default address is 0.0.0.0.</p> <p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a primary Global RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a primary Global RADIUS Server is not configured.</p>
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary Global RADIUS Server. Values include unknown, ipv4, and ipv6.
SecondaryRadiusServer	<p>Specifies the IP address for the secondary Global RADIUS Server. The default address is 0.0.0.0. The secondary Global RADIUS Server is used only if the primary Global RADIUS Server is unavailable or unreachable.</p> <p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a secondary Global RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a secondary Global RADIUS Server is not configured.</p>
RadiusServerUdpPort	Specifies the UDP port number for clients to use when trying to contact the Global RADIUS Server at the corresponding Global RADIUS Server IP address. Values range from 1 to 65535. The default port number is 1812.
RadiusServerTimeout	Specifies the timeout interval between each retry for service requests to the Global RADIUS Server. The default is 2 Seconds. Values range from 1 to 60 seconds.
SharedSecret(Key)	Specifies a new value for the Global RADIUS Server shared secret key, to a maximum of 16 characters.
ConfirmedSharedSecret(key)	Confirms the value typed in the shared secret key box. If you do not change the Global RADIUS Server

Variable	Value
	shared secret key, you do not have to type a value in this box.
AccountingEnabled	Enables or disables RADIUS accounting for a Global RADIUS Server instance.
AccountingPort	Specifies the UDP accounting port number for clients to use when trying to contact the RADIUS server at the corresponding Global RADIUS Server IP address. Values range from 0 to 65535.
RetryLimit	Specifies the number of RADIUS retry attempts for a Global RADIUS Server instance. Values range from 1 to 5.

Configuring the EAP RADIUS server using EDM

Use this procedure to configure an EAP RADIUS Server for processing EAP client requests only.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **RADIUS**.
3. In the work area, click the **EAP RADIUS Server** tab.
4. Choose an address type in the **PrimaryRadiusServerAddressType** box.
5. Type an IPv4 or IPv6 address in the **PrimaryRadiusServer** field.
6. Choose an address type in the **SecondaryRadiusServerAddressType** box.
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. Type a value in the **SharedSecret(Key)** box, to change the shared secret key.
11. Confirm the new shared secret value in the **ConfirmSharedSecret(Key)** box.
12. Check the **AccountingEnabled** checkbox, to enable accounting.

OR

- Clear the **AccountingEnabled** checkbox , to disable accounting.
13. Type a value in the **AccountingPort** box.
 14. Type a value in the **RetryLimit** box.
 15. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
PrimaryRadiusServerAddressType	Specifies the type of IP address type for the primary EAP RADIUS Server. Values include unknown, ipv4, and ipv6.
PrimaryRadiusServer	<p>Specifies the IPv4 or IPv6 address for the primary EAP RADIUS Server. The default address is 0.0.0.0.</p> <p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a primary EAP RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a primary EAP RADIUS Server is not configured.</p>
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary EAP RADIUS Server. Values include unknown, ipv4, and ipv6.
SecondaryRadiusServer	<p>Specifies the IP address for the secondary EAP RADIUS Server. The default address is 0.0.0.0. The secondary EAP RADIUS Server is used only if the primary EAP RADIUS Server is unavailable or unreachable.</p> <p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a secondary EAP RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a secondary EAP RADIUS Server is not configured.</p>
RadiusServerUdpPort	Specifies the UDP port number for clients to use when trying to contact the EAP RADIUS Server at the corresponding EAP RADIUS Server IP address. Values range from 1 to 65535. The default port number is 1812.
RadiusServerTimeout	Specifies the timeout interval between each retry for service requests to the EAP RADIUS Server. The default is 2 Seconds. Values range from 1 to 60 seconds.
SharedSecret(Key)	Specifies a new value for the EAP RADIUS Server shared secret key, to a maximum of 16 characters.
ConfirmedSharedSecret(key)	Confirms the value typed in the shared secret key box. If you do not change the EAP RADIUS Server

Variable	Value
	shared secret key, you do not have to type a value in this box.
AccountingEnabled	Enables or disables RADIUS accounting for an EAP RADIUS Server instance.
AccountingPort	Specifies the UDP accounting port number for clients to use when trying to contact the EAP RADIUS Server at the corresponding EAP RADIUS Server IP address. Values range from 1 to 65535.
RetryLimit	Specifies the number of RADIUS retry attempts for an EAP RADIUS Server instance. Values range from 1 to 5.

Configuring the NEAP RADIUS server using EDM

Use this procedure to configure a Non-EAP (NEAP) RADIUS Server for processing NEAP client requests only.

Procedure steps

1. From the navigation tree, double-click **Security** .
2. In the Security tree, double-click **RADIUS**.
3. In the work area, click the **NEAP RADIUS Server** tab.
4. Choose an address type in the **PrimaryRadiusServerAddressType** box.
5. Type an IPv4 or Ipv6 address in the **PrimaryRadiusServer** box.
6. Choose an address type in the **SecondaryRadiusServerAddressType** box.
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 value in the **ConfirmSharedSecret(Key)** box.
12. To enable accounting, check the **AccountingEnabled** checkbox.

OR

To disable accounting, clear the **AccountingEnabled** checkbox.

13. Type a value in the **AccountingPort** box.
14. Type a value in the box **RetryLimit**.
15. On the toolbar, click **Apply**.

Variable definition

Variable	Value
PrimaryRadiusServerAddressType	Specifies the type of IP address type for the primary NEAP RADIUS server. Values include unknown, ipv4, and ipv6.
PrimaryRadiusServer	<p>Specifies the IPv4 or IPv6 address for the primary NEAP RADIUS Server. The default address is 0.0.0.0. Important:</p> <p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a primary NEAP RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a primary NEAP RADIUS server is not configured.</p>
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary NEAP RADIUS Server. Values include unknown, ipv4, and ipv6.
SecondaryRadiusServer	<p>Specifies the IP address for the secondary NEAP RADIUS Server. The default address is 0.0.0.0. The secondary NEAP RADIUS Server is used only if the primary NEAP RADIUS Server is unavailable or unreachable.</p> <p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a secondary NEAP RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a secondary NEAP RADIUS server is not configured.</p>
RadiusServerUdpPort	Specifies the UDP port number for clients to use when trying to contact the NEAP RADIUS Server at the corresponding NEAP RADIUS Server IP address. Values range from 1 to 65535. The default port number is 1812.
RadiusServerTimeout	Specifies the timeout interval between each retry for service requests to the NEAP RADIUS Server. The default is 2 Seconds. Values range from 1 to 60 seconds.
SharedSecret(Key)	Specifies a new value for the NEAP RADIUS Server shared secret key, to a maximum of 16 characters.

Variable	Value
ConfirmedSharedSecret(key)	Confirms the value typed in the shared secret key box. If you do not change the NEAP RADIUS Server shared secret key, you do not have to type a value in this box.
AccountingEnabled	Enables or disables RADIUS accounting for a NEAP RADIUS Server instance.
AccountingPort	Specifies the UDP accounting port number for clients to use when trying to contact the NEAP RADIUS Server at the corresponding NEAP RADIUS Server IP address. Values range from 0 to 65535.
RetryLimit	Specifies the number of RADIUS retry attempts for a NEAP RADIUS Server instance. Values range from 1 to 5.

Viewing RADIUS Dynamic Authorization server information using EDM

Use the following procedure to display RADIUS Dynamic Authorization server information for the switch.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Server** tab.

Variable definitions

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

Variable	Value
Identifier	Indicates the Network Access Server (NAS) identifier of the RADIUS Dynamic Authorization Server.

Variable	Value
DisconInvalidClientAddresses	Indicates the number of Disconnect-Request packets received from unknown addresses.
CoAInvalidClientAddresses	Indicates the number of CoA-Request packets received from unknown addresses.

Creating an 802.1X dynamic authorization extension (RFC 3576) client using EDM

Use the following procedure to create an RADIUS Dynamic Authorization client for the switch.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.
4. Click **Insert**.

The Insert RADIUS Dynamic Auth. Client dialog box appears.

5. In the **AddressType** section, select a radio button.
6. In the **Address** dialog box, type an IP address.
7. To enable the RADIUS Dynamic Authorization client, select the **Enabled** checkbox.

OR

To disable the RADIUS Dynamic Authorization client, clear the **Enabled** checkbox.

8. In the **UdpPort** dialog box, type a port number.
9. To enable change of authorization request processing, select the **ProcessCoARequests** checkbox.

OR

To disable change of authorization request processing, clear the **ProcessCoARequests** checkbox.

10. To enable disconnect request processing, select the **ProcessDisconnectRequests** checkbox.

OR

To disable disconnect request processing, clear the **ProcessDisconnectRequests** checkbox.

11. In the **Secret** dialog box, type a shared secret word.
12. Click **Insert**.
13. On the toolbar, click **Apply**.

Variable definitions

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

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

Deleting an 802.1X dynamic authorization extension (RFC 3576) client configuration using EDM

Use the following procedure to delete an existing RADIUS Dynamic Authorization client configuration.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-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. Click **Delete**.

Viewing the 802.1X dynamic authorization extension (RFC 3576) client configuration using EDM

Use the following procedure to display existing RADIUS Dynamic Authorization client configurations for the switch.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.

Variable definitions

Use the data in the following table to understand the RADIUS Dynamic Authorization client display.

Variable	Value
AddressType	Indicates the IP address type for the RADIUS Dynamic Authorization Client.
Address	Indicates the IP address of the RADIUS Dynamic Authorization Client.
Enabled	Indicates whether packet receiving from the RADIUS Dynamic Authorization Client is enabled (true) or disabled (false).
UdpPort	Indicates the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1025–65535.
ProcessCoARequests	Indicates whether change of authorization (CoA) request processing is enabled or disabled.
ProcessDisconnectRequests	Indicates whether disconnect request processing is enabled or disabled.
Secret	Indicates the secret word shared between the RADIUS Dynamic Authorization Client and the RADIUS server.

Modifying the 802.1X dynamic authorization extension (RFC 3576) client configuration using EDM

Use the following procedure to edit an existing RADIUS Dynamic Authorization client configuration.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-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**.

Variable definitions

Use the data in the following table to modify an existing RADIUS Dynamic Authorization client configuration.

Variable	Value
AddressType	Indicates the IP address type for the RADIUS Dynamic Authorization Client. This is a read-only cell.
Address	Indicates the IP address of the RADIUS Dynamic Authorization Client. This is a read-only cell.
Enabled	Enables or disables packet receiving from the RADIUS Dynamic Authorization Client.

Variable	Value
	<ul style="list-style-type: none"> • enable—true • disable—false
UdpPort	Defines the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1024 to 65535.
ProcessCoARequests	Enables or disables change of authorization (CoA) request processing.
ProcessDisconnectRequests	Enables or disables disconnect request processing.
Secret	The RADIUS Dynamic Authorization Client secret word. This cell remains empty.

Changing the 802.1X dynamic authorization extension (RFC 3576) client secret word using EDM

Use the following procedure to change the existing RADIUS Dynamic Authorization client secret word.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.
4. Click **Change Secret**.
5. In the **Secret** dialog box, type a new secret word.
6. In the **Confirmed Secret** dialog box, retype the new secret word.
7. Click **Apply**.

Viewing RADIUS Dynamic Server statistics using EDM

Use the following procedure to display RADIUS Dynamic Server statistical information.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Server Stats** tab.

Variable definitions

Use the data in the following table to help you understand the RADIUS Dynamic Server statistics display.

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

Graphing RADIUS Dynamic Server statistics using EDM

Use the following procedure to graph statistics for a RADIUS Dynamic Server client.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Server Stats** tab.
4. To select a VLAN to edit, click the client row.
5. On the toolbar, click **Graph**.

6. Click and drag your cursor to highlight all RADIUS Dynamic Server statistical information to graph.
7. Click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

DHCP snooping configuration using EDM

This section describes how you can configure DHCP snooping to provide security to your network by preventing DHCP spoofing, using Enterprise EDM (EDM).

Configuring global DHCP snooping using EDM

Use the following procedure to configure global DHCP snooping to enable or disable DHCP snooping parameters for the switch.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping Globals** tab.
4. To enable DHCP snooping globally, select the **Enabled** checkbox in the DHCP Snooping section.

OR

To disable DHCP Snooping globally, clear the **Enabled** checkbox in the DHCP Snooping section.

5. To enable Option 82 for DHCP snooping, select the **Option82Enabled** checkbox in the DHCP Snooping section.

OR

To Disable Option 82 for DHCP Snooping, clear the **Option82Enabled** checkbox in the DHCP Snooping section.

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

Warning:

DHCP snooping must be enabled on Layer 3 VLANs spanning toward DHCP servers in Layer 3 mode. DHCP relay is also required for correct operation.

Configuring DHCP Snooping external save using EDM

Use the following procedures to store the DHCP Snooping database to an external TFTP or SFTP server or to a USB drive.

Configuring DHCP Snooping external save to an external TFTP server

Use this procedure to store the DHCP Snooping database to an external TFTP.

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping Globals** tab.
4. In the DHCP Snooping External Save section, select the **Enabled** checkbox, to enable DHCP Snooping external save.

OR

In the DHCP Snooping External Save section, clear the **Enabled** checkbox, to disable DHCP Snooping external save.

5. Click a **TftpServerAddressType** button.
6. Type a value in the **TftpServerAddress** box.
7. Type 0 in the **UsbTargetUnit** box.
8. Type a value in the **Filename** box.
9. To force a binding table restore, click the **ForceRestore** button.
10. On the toolbar, click **Apply**.

Configuring DHCP Snooping external save to an external SFTP server

Use the following procedure to store the DHCP Snooping database to an external SFTP server.

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping Globals** tab.
4. In the DHCP Snooping External Save section, select the **Enabled** checkbox, to enable DHCP Snooping external save.

OR

In the DHCP Snooping External Save section, clear the **Enabled** checkbox, to disable DHCP Snooping external save.

5. Click a **SftpServerAddressType** button.
6. Type a value in the **SftpServerAddress** box.
7. Type 10 in the **UsbTargetUnit** box.

8. Type a value in the **Filename** box.
9. To force a binding table restore, click the **ForceRestore** button.
10. On the toolbar, click **Apply**.

 **Note:**

To store the DHCP Snooping database to an external SFTP server, you must also make the following configurations:

- choose an authentication method
- generate a DSA/RSA key
- set the sshc user name
- set the sshc password if it is needed for restore

Configuring DHCP Snooping external save to a USB drive

Use the following procedure to store the DHCP Snooping database to a USB drive.

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping Globals** tab.
4. In the DHCP Snooping External Save section, select the **Enabled** checkbox, to enable DHCP Snooping external save.

OR

In the DHCP Snooping External Save section, clear the **Enabled** checkbox, to disable DHCP Snooping external save.

5. Type a value in the **UsbTargetUnit** box (the unit number on which the USB stick is inserted).
6. Type a value in the **Filename** box.
7. To force a binding table restore, click the **ForceRestore** button.
8. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
DHCP Snooping External Save	
Enabled	Enables or disables DHCP Snooping External Save.

Variable	Value
SyncFlag	Indicates if changes in the DHCP Snooping binding table are synchronized on the external device. Values include: <ul style="list-style-type: none"> • true—changes will be synchronized at the next write operation • false—changes will not be synchronized at the next write operation
LastSyncTime	Displays the UTC time when the switch last backed up the DHCP Snooping binding table.
TftpServerAddressType	Specifies the IP address type of the TFTP server on which to save the DHCP Snooping binding file. Values include ipv4 or ipv6.
TftpServerAddress	Specifies the IPv4 or IPv6 address of the TFTP server on which to save the DHCP Snooping binding file.
SftpServerAddressType	Specifies the IP address type of the SFTP server on which to save the DHCP Snooping binding file. Values include ipv4 or ipv6.
SftpServerAddress	Specifies the IPv4 or IPv6 address of the SFTP server on which to save the DHCP Snooping binding file.
UsbTargetUnit	Specifies the unit number of the USB port to use in file save or restore operations.
Filename	Specifies the name of the DHCP Snooping database that is saved externally.
ForceRestore	Forces the restoration of the DHCP Snooping database on the switch from the file previously saved to an external USB drive or TFTP server.

Configuring DHCP snooping on a VLAN using EDM

Use the following procedure to configure DHCP snooping on a VLAN through to enable or disable DHCP snooping and DHCP snooping with Option 82 for a VLAN.

! **Important:**

You must 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 steps

1. From the Device Physical View, select a port.
2. From the navigation tree, double-click **Security**.
3. In the Security tree, double-click **DHCP Snooping**.
4. In the work area, click the **DHCP Snooping-VLAN** tab.
5. To select a VLAN to edit, click the VLAN ID.
6. In the VLAN row, double-click the cell in the **DhcpSnoopingEnabled** column.
7. Select a value from the list—**true** to enable DHCP snooping for the VLAN, or **false** to disable DHCP snooping for the VLAN.
8. In the VLAN row, double-click the cell in the **VlanOption82Enabled** column.
9. Select a value from the list—**true** to enable DHCP snooping with Option 82 for the VLAN, or **false** to disable DHCP snooping with Option 82 for the VLAN.
10. Click **Apply**.

Configuring DHCP snooping on a port using EDM

Use the following 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. Ports are untrusted by default.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-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 list—**trusted** or **untrusted**.
7. Double-click the **DhcpSnoopingIfOption82SubscriberId** for a port.
8. Type a subscriber Id value for the port.
9. Click **Apply**.

Variable definitions

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

Variable	Value
Port	Indicates the port on the switch.
DhcpSnoopingIfTrusted	Specifies whether the port is trusted or untrusted. Default is false.
DhcpSnoopingIfOption82SubscriberId	Specifies the DHCP Option 82 subscriber Id for the port. Value is a character string between 0 and 64 characters.

DHCP binding configuration using EDM

Use the information in this section to view and manage DHCP client lease static entries.

DHCP binding configuration using EDM navigation

- [Viewing DHCP binding information using EDM](#) on page 341
- [Creating static DHCP binding table entries using EDM](#) on page 342
- [Deleting DHCP binding table entries using EDM](#) on page 343

Viewing DHCP binding information using EDM

Use the following procedure to display DHCP binding information.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security Routing tree, double-click **DHCP Snooping**.
3. In the work area, click the **DHCP Bindings** tab.

Variable definitions

Use the data in the following table to help you understand the DHCP binding information display.

Variable	Value
VlanId	Indicates the ID of the VLAN that the DHCP client is a member of.
MacAddress	Indicates the MAC address of the DHCP client.
AddressType	Indicates the MAC address type of the DHCP client.
Address	Indicates IP address of the DHCP client.
Interface	Indicates the interface to which the DHCP client is connected.
LeaseTime(sec)	Indicates the lease time (in seconds) of the DHCP client binding. Values range from 0 to 4294967295.
TimeToExpiry(sec)	Indicates the time (in seconds) before a DHCP client binding expires.
Source	Indicates the source of the binding table entry

Creating static DHCP binding table entries using EDM

Use the following procedure to add entries for devices with static IP addresses to the DHCP binding table.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **DHCP Snooping**.
3. In the work area, click the **DHCP Bindings** tab.
4. Click **Insert**.
The Insert DHCP Bindings dialog box appears.
5. Click the VlanId elipsis (...), and select the DHCP client VLAN ID.

6. Click **Ok**.
7. In the **MacAddress** dialog box, type the DHCP client MAC address.
8. In the **AddressType** section, select a radio button.
9. In the **Address** dialog box, type the DHCP client IP address.
10. Click the Interface elipsis (...).
11. From the list, select an interface port.
12. Click **Ok**.
13. In the **Lease Time(sec)** field, type a lease time.
14. Click **Insert**.
15. On the toolbar, click **Apply**.

Variable definitions

Use the data in the following table to add static entries to the DHCP binding table.

Variable	Value
VlanId	Specifies the ID of the VLAN that the DHCP client is a member of.
MacAddress	Specifies the MAC address of the DHCP client.
AddressType	Specifies the IP address type of the DHCP client.
Address	Specifies IP address of the DHCP client.
Interface	Specifies the interface to which the DHCP client is connected.
LeaseTime(sec)	Specifies the lease time (in seconds) for the DHCP client binding. Values range from 0 to 4294967295.

Deleting DHCP binding table entries using EDM

Use the following procedure to delete static IP addresses from the DHCP binding table.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **DHCP Snooping**.
3. Select the **DHCP Bindings** tab.
4. Click the VLAN ID.
5. On the toolbar, click **Delete**.
6. Click **Yes** to confirm that you want to delete the entry.

Configuring dynamic ARP inspection on VLANs using EDM

Use the following procedure to configure ARP inspection on a VLAN to enable or disable ARP inspection on one or more VLANs.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **Dynamic ARP Inspection (DAI)**.
3. In the work area, click the **ARP Inspection-VLAN** tab.
4. Double-click the **ARPInspectionEnabled** box for a VLAN.
5. Select **true** to enable ARP Inspection-VLAN.
OR
Select **false** to disable ARP Inspection-VLAN.
6. Repeat steps **3** and **4** for additional VLANs as required.
7. Click **Apply**.

Configuring dynamic ARP inspection on ports using EDM

Use this procedure to configure dynamic ARP inspection for one or more switch ports as *trusted* (ARP traffic is not subject to dynamic ARP inspection) or *untrusted* (ARP traffic is subject to dynamic ARP inspection).

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **Dynamic ARP Inspection (DAI)**.
3. In the work area, click the **ARP Inspection-Port** tab.
4. Double-click the **ARPInspectionIfTrusted** cell for a port.
5. From the list, select **trusted** or **untrusted**.
6. Repeat steps **3** and **4** for additional ports as required.
7. Click **Apply**.

IP Source Guard configuration using EDM

This section describes how to configure IP Source Guard to add a higher level of security to a port or ports by preventing IP spoofing

 **Important:**

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

 **Important:**

Avaya recommends that you carefully manage the number of applications running on the Avaya Ethernet Routing Switch 4000 that use filters. For example, if you configure ADAC on ports and attempt to configure IP Source Guard on those same ports, the IP Source Guard configuration can fail due to the limited number of filters available.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.
- Dynamic Host Control Protocol (DHCP) snooping is globally enabled.

For more information, see [DHCP snooping configuration using EDM](#) on page 336.

- The port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- The port is an untrusted DHCP snooping and dynamic ARP Inspection port.
- The bsSourceGuardConfigMode MIB object exists.

This MIB object is used to control the IP Source Guard mode on an interface.

- The following applications are not enabled:
 - Baysecure
 - Extensible Authentication Protocol over LAN (EAPOL)

Important:

Hardware resources can run out if IP Source Guard is enabled on trunk ports with a large number of VLANs, which have DHCP snooping enabled. If this happens, traffic sending can be interrupted for some clients. Avaya recommends that IP Source Guard not be enabled on trunk ports.

Configuring IP Source Guard on a port using EDM

Configure IP Source Guard to enable or disable a higher level of security on a port or ports.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **IP Source Guard (IPSG)**.
3. In the work area, click the **IP Source Guard-port** tab.
4. Double-click the **Mode** box for a port.
5. Select **ip** from the list to enable IP Source Guard.

OR

Select **disabled** from the list to disable IP Source Guard.

6. On the toolbar, click **Apply**.
7. On the toolbar, click **Refresh** to update the IP Source Guard-port dialog box display.

Variable definitions

Use the data in the following table to enable IP Source Guard on a port.

Variable	Value
Port	Identifies the port number.
Mode	Identifies the Source Guard mode for the port. The mode can be disabled or ip. The default mode is disabled.

Configuring IP Source Guard on multiple ports using EDM

Configure IP Source Guard to enable or disable a higher level of security on a port or ports.

Procedure steps

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, double click **Ports**
5. Click the **IP Source Guard** tab.
6. Double-click the **Mode** box for a port.
7. Select **ip** from the list to enable IP Source Guard.

OR

Select **disabled** from the list to disable IP Source Guard.

8. On the toolbar, click **Apply**.
9. On the toolbar, click **Refresh** to update the IP Source Guard-port dialog box display.

Variable definitions

Use the data in the following table to enable IP Source Guard on a port.

Variable	Value
Port	Identifies the port number.
Mode	Identifies the Source Guard mode for the port. The mode can be disabled or ip. The default mode is disabled.

Filtering IP Source Guard addresses using EDM

Use the following procedure to filter IP Source Guard addresses to display IP Source Guard information for specific IP addresses.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **IP Source Guard (IPSG)**.
3. In the work area, click the **IP Source Guard-addresses** tab.
4. Select an entry in the table.
5. On the toolbar, click **Filter**.
6. In the **IP Source Guard-addresses - Filter** dialog box, select the required parameters for displaying port IP Source Guard information.
7. Click **Filter**.

IP Source Guard information for the specified IP addresses appears in the IP Source Guard-addresses dialog box.

Variable definitions

Use the data in the following table to filter IP Source Guard addresses.

Variable	Value
Condition	Defines the search condition. Values are:

Variable	Value
	<ul style="list-style-type: none"> • AND: Includes keywords specified in both the Port and Address fields while filtering results. • OR: Includes either one of the keywords specified in the Port and Address fields while filtering results.
Ignore Case	Ignores the letter case while searching.
Column	Specifies the content of the column search. Values are <ul style="list-style-type: none"> • Contains • Does not contain • Equals to
All records	Displays all entries in the table.
Port	Searches for the specified port.
Address	Searches for the specified IP address.

Use the data in the following table to display IP Source Guard information for filtered addresses.

Variable	Value
Port	Indicates the port number.
Type	Indicates the internet address type.
Address	Indicates the IP address allowed by IP Source Guard.
Source	Indicates the source of the address.

Viewing IP Source Guard port statistics using EDM

View IP Source Guard port statistics to display dropped packet statistics for IP Source Guard enabled ports.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **IP Source Guard (IPSG)**.
3. In the work area, click the **IP Source Guard-stats** tab to view the IP Source Guard port statistics.

Variable definitions

Use the data in the following table to understand the IP Source Guard statistics display.

Variable	Value
IfIndex	Identifies the slot and port number of the IP Source Guard enabled ports.
DroppedPackets	Displays the number of instances of dropped packets that occur on IP Source Guard enabled ports.

TACACS+ configuration using EDM

This section describes how to configure, enable, and disable TACACS+ servers in the system.

Configuring TACACS+ services using EDM

Use the following procedure to configure a TACACS+ services.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **TACACS+** .
3. In the **Globals** tab, configure the parameters as required.
4. On the toolbar, click **Apply**.

Variable definitions

Use the data in the following table to configure TACACS+ services.

Variable	Value
Accounting	Enables or disables TACACS+ accounting.
Authentication	Indicates the authentication status.
AuthorizationEnabled	Enables or disables TACACS+ authorization.
AuthorizationLevels	Indicates the TACACS+ authorization level.

Adding a TACACS+ server using EDM

Use the following procedure to add TACACS+ server in the system.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **TACACS+**.
3. In the work area, click the **TACACS+ Server** tab.
4. On the toolbar, click **Insert**.
The Insert TACACS+ Server dialog box appears.
5. Type the address in the **Address** field.
6. Type the port number in the **PortNumber** field.
7. Type the key in the **Key** field.
8. Retype the key in the **Confirm Key** field.
9. Choose the priority in the **Priority** field.
10. Click **Insert**.

Variable definitions

Use the data in the following table to add a TACACS+ server.

Variable	Value
AddressType	Specifies the type of IP address used on the TACACS+ server.
Address	Indicates the IP address of the TACACS+ server in use.
PortNumber	Indicates the TCP port on which the client establishes a connection to the server.
Key	Indicates the secret key to be shared with this TACACS+ server. Key length zero indicates no encryption is being used.
Confirm Key	Indicates the key in use.
Priority	Determines the order in which the TACACS+ servers are used. Available options are— primary or secondary.

Deleting a TACACS+ server using EDM

Use the following procedure to delete a TACACS+ server from the system.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **TACACS+**.
3. In the work area, click the **TACACS+ Server** tab.
4. In the table, select the TACACS+ server entry you want to delete.
5. On the toolbar, click **Delete**.
6. Click **Yes** to confirm.

Configuring the Web and Telnet password using EDM

Use the following procedure to configure a password for Web and Telnet access to a stack, or standalone switch.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **Web/Telnet/Console**.

3. In the work area, click the **Web/Telnet** tab.
4. Click the arrow on the **Web/Telnet Switch Password Type** box.
5. Select a password type from the list.
6. Type the password for read-only access in the **Read-Only Stack Password** box.
7. Type the same password for read-only access in the **Re-enter to verify** box.
8. Type the password for read-write access in the **Read-Write Switch Password** box.
9. Type the same password for read-write access in the **Re-enter to verify** box.
10. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
Web/Telnet Stack Password Type	<p>Specifies the type of the password to use. Values include:</p> <ul style="list-style-type: none"> • none—disables the password • Local Password— uses the locally defined password for Web and Telnet access. • RADIUS Authentication— uses RADIUS password authentication for Web and Telnet access. • TACACS Authentication— uses TACACS + authentication, authorization, and accounting (AAA) services authentication for Web and Telnet access.
Read-Only Stack Password	<p>Specifies the read-only password for stack or switch access. The maximum length of the password is 15 characters.</p>
Read-Write Switch Password	<p>Specifies the read-write password for stack or switch access. The maximum length of the password is 15 characters.</p>

Configuring the console password using EDM

Use the following procedure to configure a password for serial console access to a stack, or standalone switch.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **Web/Telnet/Console**.
3. In the work area, click the **Console Password** tab.
4. Click the arrow on the **Console Stack Password Type** box.
5. Select a password type from the list.
6. Type the password for read-only access in the **Read-Only Stack Password** box.
7. Type the same password for read-only access in the **Re-enter to verify** box.
8. Type the password for read-write access in the **Read-Write Stack Password** box.
9. Type the same password for read-write access in the **Re-enter to verify** box.
10. On the toolbar, click **Apply**.

Variable definitions

Use the data in the following table to configure the console switch password.

Variable	Value
Console Stack Password Type	Specifies the type of password to use. Values include: <ul style="list-style-type: none"> • none—disables the password • Local Password— uses the locally defined password for serial console access. • RADIUS Authentication— uses RADIUS authentication for serial console access. • TACACS Authentication— uses TACACS + authentication, authorization, and accounting (AAA) services authentication for console access.
Read-Only Stack Password	Specifies the read-only password for stack or switch access.
Read-Write Stack Password	Specifies the read-write password for stack or switch access.

SNMP configuration using EDM

This section details the configuration options available for SNMP in EDM.

Viewing the SNMP configuration using EDM

Use the following procedure to display information about SNMP on your switch.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. In the work area, click the **SNMP** tab.

Variable definitions

The following table describes fields on the SNMP tab.

Table 81: SNMP tab fields

Field	Description
LastUnauthenticatedInetAddressType	Indicates the type of IP address that was not authenticated by the device last.
LastUnauthenticatedInetAddress	Indicates the last IP address that was not authenticated by the device.
LastUnauthenticatedCommunityString	Indicates the last community string that was not authenticated by the device.
RemoteLoginInetAddressType	Indicates the type of IP address to last remotely log on to the system.
RemoteLoginInetAddress	Indicates the last IP address to remotely log on to the system.
TrpRcvrMaxEnt	Indicates the maximum number of trap receiver entries.

Field	Description
TrpRcvrCurEnt	Indicates the current number of trap receiver entries.
TrpRcvrNext	Indicates the next trap receiver entry to be created.

Creating a user using EDM

User the following procedure to create an SNMP user.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Sntp Server**.
3. In the Sntp Server tree, double-click **User**.
4. On the toolbar, click **Insert** to open the Insert User dialog.
5. Configure the parameters as required.
6. Click **Insert**.

Variable definitions

Use the data in the following table to create an SNMP user.

Variable	Value
EngineID	Indicates the administratively-unique identifier of SNMP engine.
Name	Indicates the user name.
Auth Protocol	Indicates the registration point for standards-track authentication protocols used in SNMP Management Frameworks.
AuthPassword	Specifies the current authorization password.
ConfirmPassword	Reenter the password to confirm.
Priv Protocol	To assign a privacy protocol, select one of the following from the list: <ul style="list-style-type: none"> • None • DES

Variable	Value
	<ul style="list-style-type: none"> • 3DES • AES
PrivacyPassword	Specifies the current privacy password.
ConfirmPassword	Re-enter the password to confirm.
ReadViewName	Specifies the name of the MIB View to which the user is assigned read access.
WriteViewName	Specifies the name of the MIB View to which the user is assigned write access.
NotifyViewName	Specifies the name of the MIB View from which the user receives notifications.
Storage Type	Specifies whether this table entry is stored in one of the following memory types: <ul style="list-style-type: none"> • volatile—entry does not persist if switch loses power • nonVolatile—entry persists if switch loses power

Viewing the user details using EDM

User the following procedure to view information about an SNMP user.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snm Server**.
3. In the Snmp Server tree, double-click **User**.
4. In the table, select the user you want to view.
5. On the toolbar, click **Details** to view the details of selected user.

Variable definitions

The following table describes the fields of User Details tab.

Field	Value
Name	Indicates the user name.
ContextPrefix	Indicates the context prefix in use.

Field	Value
SecurityModel	Indicates the security model in use.
SecurityLevel	Indicates the minimum level of security in use.
ReadViewName	Indicates name of the MIB view of the SNMP context that has read access.
WriteViewName	Indicates the name of the MIB view of the SNMP context that has write access.
NotifyViewName	Indicates the name of the MIB view of the SNMP context that has access for notifications.
Storage Type	Indicates the memory storage type.

Viewing MIBs assigned to an object using EDM

Use the following procedure to view the MIBs assigned to an object.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, double-click **MIB View**.
4. On the toolbar, click **Insert** to open the Insert MIB View dialog.
5. Configure the parameter as required.
6. Click **Insert**.

Variable definitions

The following table describes the fields of MIB View tab.

Field	Value
ViewName	Indicates the name of the family of view subtrees.
Subtree	Indicates the MIB subtree.
Type	Indicates whether the subtree is included or excluded from the MIB view.
Storage Type	Indicates the storage type.

Creating a community using EDM

Use the following procedure to create an SNMP community.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, double-click **Community**.
4. On the toolbar, click **Insert**.
The Insert Community dialog box appears.
5. Configure the parameter as required.
6. Click **Insert**.

Variable definitions

The following table describes the fields of Community tab.

Field	Value
Index	Indicates the unique identifier of community.
Name	Indicates the name of the community.
ContextEngineID	Indicates the engine ID of the context.
Storage Type	Indicates the storage type.

Deleting a community using EDM

Use the following procedure to delete a community.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, double-click **Community**.
4. In the table, select the community you want to delete.
5. On the toolbar, click **Delete**.

Viewing the details of a community using EDM

Use the following procedure to view the details of a community.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, double-click **Community**.
4. In the table, select the community you want to view.
5. On the toolbar, click **Details** to view the details of the selected community.

Variable definitions

The following table describes the fields on the Community Details tab.

Field	Value
Name	Indicates the community name.
ContextPrefix	Indicates the context prefix in use.
SecurityModel	Indicates the security model in use.
SecurityLevel	Indicates the minimum level of security in use.
ReadViewName	Indicates name of the community that has read access.
WriteViewName	Indicates the name of the community that has write access.
NotifyViewName	Indicates the name of the community has access for notifications.
Storage Type	Indicates the storage type.

Configuring an SNMP host using EDM

Use the following procedure to configuring an SNMP host notification control.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, double-click **Host**.
4. On the toolbar, click **Insert** to open the Insert Host dialog.
5. Configure the parameter as required.
6. Click **Insert**.

Variable definitions

The following table describes the fields on the Community Details tab.

Field	Value
Domain	Indicates the transport type of the address in the snmpTargetAddrTAddress object.
DestinationAddr : Port	Indicates the transport address (in IPv4 Address : port format).
Timeout	Indicates the time interval that an application waits for a response.
RetryCount	Indicates the number of retries to be attempted when a response is not received for a generated message.
Type	Indicates the type of the message.
Storage Type	Indicates the storage type.

Configuring notifications (traps) from the list using EDM

Use the following procedure to enable and disable SNMP trap control.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, double-click **Host**.
4. In the table, select an entry.

5. On the toolbar, click **Notification** to display a list of traps.
6. Clear the trap that you do not want the switch to send.
By default all the traps are selected.
7. Click **Apply**.

Configuring SNMP notification control using EDM

Use the following procedure to enable or disable SNMP traps.

Notification Control is the Trap Web Page.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Snm Server**.
3. From the Snmp Server tree, double-click **Notification Control**.
4. To select an SNMP trap to edit, click a **NotifyControlType** row.
5. In the NotifyControlType row, double-click the cell in the **NotifyControlEnabled** column.
6. Select a value from the list — **true** to enable the trap, **false** to disable the trap.
7. On the toolbar, click the **Enable All** button to enable all SNMP traps available on the switch.

OR

On the toolbar, click the **Disable All** button to disable all SNMP traps available on the switch.

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

Variable definitions

Use the data in the following table to configure SNMP notification control

Variable	Value
NotifyControlType	Lists the SNMP trap names.
Notify Control Type (oid)	Lists the object identifiers for the SNMP traps.
NotifyControlEnabled	Enables (true) or disables (false) the SNMP trap.
NotifyControlPortListEnabled	Indicates the port list for which the notification is enabled or disabled. Whether or not this field is configurable depends on the NotifyControlType value.

Configuring SNMP traps for ports using EDM

Use this procedure to enable or disable SNMP traps for specific ports, or for all switch ports.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Snmp Server**.
3. From the Snmp Server tree, click **Notification Control**.
4. In the work area, click a **NotifyControlType** row for supported notifications, to select an SNMP trap.
5. Double-click the cell in the **NotifyControlPortListEnabled** column.
6. To enable or disable the trap for specific ports, select or deselect one or more port numbers.

OR

To enable or disable the trap for all switch ports, click **All**.

7. Click **Ok**.
8. On the toolbar, click **Apply**.

Variable definition

Variable	Value
NotifyControlType	Lists the SNMP trap names.
Notify Control Type (OID)	Lists the object identifiers for the SNMP traps.
NotifyControlEnabled	Enables (true) or disables (false) the SNMP trap.
NotifyControlPortListEnabled	Specifies the port list for which the SNMP trap is enabled or disabled. Whether or not this field is configurable depends on the NotifyControlType value.

Graphing SNMP statistics using EDM

Use this procedure to display and graph SNMP statistics.

Procedure steps

1. From the navigation pane, double click **Graph** to open the navigation tree.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **SNMP** tab.
4. On the toolbar, select a **Poll Interval** from the list.
5. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
6. To select statistics to graph, click a statistic type row under a column heading.
7. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

Use the data in the following table to help you understand SNMP statistics.

Variable	Value
InPkts	The total number of messages delivered to the SNMP from the transport service.
OutPkts	The total number of SNMP messages passed from the SNMP protocol to the transport service.
InTotalReqVars	The total number of MIB objects retrieved successfully by the SNMP protocol as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
InTotalSetVars	The total number of MIB objects altered successfully by the SNMP protocol as the result of receiving valid SNMP Set-Request PDUs.
InGetRequests	The total number of SNMP Get-Request PDUs that are accepted and processed by the SNMP protocol.
InGetNexts	The total number of SNMP Get-Next PDUs that are accepted and processed by the SNMP protocol.
InSetRequests	The total number of SNMP Set-Request PDUs that are accepted and processed by the SNMP protocol.
InGetResponses	The total number of SNMP Get-Response PDUs that are accepted and processed by the SNMP protocol.
OutTraps	The total number of SNMP Trap PDUs generated by the SNMP protocol.
OutTooBig	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is tooBig.

Variable	Value
OutNoSuchNames	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is noSuchName.
OutBadValues	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is badValue.
OutGenErrs	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is genErr.
InBadVersions	The total number of SNMP messages delivered to the SNMP protocol for an unsupported SNMP version.
InBadCommunity Names	The total number of SNMP messages delivered to the SNMP protocol that used an unknown SNMP community name.
InBadCommunity Uses	The total number of SNMP messages delivered to the SNMP protocol that represented an SNMP operation not allowed by the SNMP community named in the message.
InASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP protocol when decoding received SNMP messages.
InTooBigs	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is tooBig.
InNoSuchNames	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is noSuchName.
InBadValues	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is badValue.
InReadOnlys	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is readOnly. It is a protocol error to generate an SNMP PDU containing the value readOnly in the error-status field. This object is provided to detect incorrect implementations of the SNMP.
InGenErrs	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is genErr.

Chapter 7: Ignition Server configuration using Enterprise Device Manager

This chapter describes how to configure the Avaya Ethernet Routing Switch 4000 Series as a network access device in the Identity Engine Ignition Server solution using Enterprise Device Manager (EDM).

Configuring Ignition Servers as a RADIUS server using EDM

You can configure Ignition Server to act as the RADIUS server for your switches and access points. For more information about configuring the Ignition Server for RADIUS, see Avaya Identity Engines Ignition Server Configuration, NN47280-500.

Prerequisites

- Ignition Server installed and configured in your network
- Configure the following policies for your switch on Ignition Server
 - Access
 - User Authentication
 - User Authorization
- Configure the following optional policies for your switch on Ignition Server:
 - Provisioning Policies that set network session and switch parameters for users
 - Client Posture Policies that require that laptops meet a minimum standard of system health
 - VLAN Assignments that assign each user to an appropriate VLAN
 - Windows machine authentication that checks connecting devices to ensure they are known to the Active Directory before the system permits connection
 - MAC authentication that allows operator-less devices to connect and records which device a user connected with

Procedure steps

1. From the Configuration tree, double-click **Security**.
2. From the Security tree, click **RADIUS**.
3. On the work area, click the **Globals** tab.
4. In the **Reachability** box select **useRadius**.
5. Optional: in the **RADIUS Accounting** section, select values to configure RADIUS Accounting.
6. On the work area, click the **Global RADIUS Server** tab.
7. In the PrimaryRadiusServerAddressType field, select the address type
8. In the **PrimaryRadiusServer** field, enter the Ignition Server RADIUS service IP address.
9. Optional: In the **SecondaryRadiusServerAddressType** , select the address type.
10. Optional: In the **SecondaryRadiusServer** field, enter the Ignition Server secondary RADIUS service IP address.
11. In the **RadiusServerUdpPort** field, enter the port number for the UDP port.
12. In the **RadiusServerTimeout** field, enter a timeout value.
13. In the **SharedSecret(Key)** field, enter the RADIUS shared secret (also known as the *key* or *encryption key*).
14. Optional: In the **Confirm SharedSecret(Key)** field, re-enter the RADIUS shared secret from the preceding step.
15. Optional: Select the **AccountingEnabled** field to enable RADIUS Accounting.
16. Optional: In the **AccountingPort** field, enter a port number.
17. Optional: In the **RetryLimit** field, enter a value.
18. On the tool bar, click **Apply**.

Variable definitions

The following table describes the Globals tab fields.

Variable	Value
UseMgmtIp	When selected, RADIUS uses the system management IP address as the source address for RADIUS requests.
PasswordFallbackEnabled	When selected, enables RADIUS password fallback.
DynAuthReplayProtection	When selected, enables RADIUS replay protection.

Variable	Value
Reachability	Specifies the RADIUS server reachability mode. Values include: <ul style="list-style-type: none"> • use-radius — uses dummy RADIUS requests to determine reachability of the RADIUS server. • use-icmp — uses ICMP packets to determine reachability of the RADIUS server (default).
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. DEFAULT: 600 seconds.
InterimUpdatesIntervalSource	Specifies the source of the interim updates timeout interval. <ul style="list-style-type: none"> • configuredValue — uses the value in the RadiusAccountingInterimUpdatesInterval dialog box • radiusServer — uses the value applied by the RADIUS server
EncapsulationProtocol	Specifies the type of encapsulation for the RADIUS packets. Values include: <ul style="list-style-type: none"> • pap — Password Authentication Protocol. • ms-chap-v2 — Microsoft Challenge Handshake Authentication Protocol Version 2.

Variable definitions

The following table describes the Global RADIUS Server tab fields.

Variable	Value
PrimaryRadiusServerAddressType	Specifies the type of IP address type for the primary Global RADIUS server. Values include unknown, ipv4, and ipv6.
PrimaryRadiusServer	Specifies the IPv4 or IPv6 address for the primary Global RADIUS Server. The default address is 0.0.0.0.

Variable	Value
	<p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a primary Global RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a primary Global RADIUS Server is not configured.</p>
SecondaryRadiusServerAddressType	<p>Specifies the IP address type for the secondary Global RADIUS Server. Values include unknown, ipv4, and ipv6.</p>
SecondaryRadiusServer	<p>Specifies the IP address for the secondary Global RADIUS Server. The default address is 0.0.0.0. The secondary Global RADIUS Server is used only if the primary Global RADIUS Server is unavailable or unreachable.</p> <p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a secondary Global RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a secondary Global RADIUS Server is not configured.</p>
RadiusServerUdpPort	<p>Specifies the UDP port number for clients to use when trying to contact the Global RADIUS Server at the corresponding Global RADIUS Server IP address. Values range from 1 to 65535. The default port number is 1812.</p>
RadiusServerTimeout	<p>Specifies the timeout interval between each retry for service requests to the Global RADIUS Server. The default is 2 Seconds. Values range from 1 to 60 seconds.</p>
SharedSecret(Key)	<p>Specifies a new value for the Global RADIUS Server shared secret key, to a maximum of 16 characters.</p>
ConfirmedSharedSecret(key)	<p>Confirms the value typed in the shared secret key box. If you do not change the Global RADIUS Server shared secret key, you do not have to type a value in this box.</p>
AccountingEnabled	<p>Enables or disables RADIUS accounting for a Global RADIUS Server instance</p>

Variable	Value
AccountingPort	Specifies the UDP accounting port number for clients to use when trying to contact the RADIUS server at the corresponding Global RADIUS Server IP address. Values range from 0 to 65535.
RetryLimit	Specifies the number of RADIUS retry attempts for a Global RADIUS Server instance. Values range from 1 to 5

Configuring Ignition Server as an EAP RADIUS server using EDM

You can configure Ignition Server to act as the EAP RADIUS server for your switches and access points. For more information about configuring the Ignition Server for RADIUS, see Avaya Identity Engines Ignition Server Configuration, NN47280-500.

Prerequisites

- Ignition Server installed and configured in your network
- Configure the following policies for your switch on Ignition Server
 - Access
 - User Authentication
 - User Authorization
- Configure the following optional policies for your switch on Ignition Server:
 - Provisioning Policies that set network session and switch parameters for users
 - Client Posture Policies that require that laptops meet a minimum standard of system health
 - VLAN Assignments that assign each user to an appropriate VLAN
 - Windows machine authentication that checks connecting devices to ensure they are known to the Active Directory before the system permits connection
 - MAC authentication that allows operator-less devices to connect and records which device a user connected with
- EAP configured on your switch.

Procedure steps

1. From the Configuration tree, double-click **Security**.
2. From the Security tree, click **RADIUS**.

3. On the work area, click the **Globals** tab.
4. In the **Reachability** box select **useRadius**.
5. Optional: in the **RADIUS Accounting** section, select values to configure RADIUS Accounting.
6. On the work area, click the **EAP RADIUS Server** tab.
7. In the PrimaryRadiusServerAddressType field, select the address type
8. In the **PrimaryRadiusServer** field, enter the Ignition Server RADIUS service IP address.
9. Optional: In the **SecondaryRadiusServerAddressType** , select the address type.
10. Optional: In the **SecondaryRadiusServer** field, enter the Ignition Server secondary RADIUS service IP address.
11. In the **RadiusServerUdpPort** field, enter the port number for the UDP port.
12. In the **RadiusServerTimeout** field, enter a timeout value.
13. In the **SharedSecret(Key)** field, enter the RADIUS shared secret (also known as the *key* or *encryption key*).
14. Optional: In the **Confirm SharedSecret(Key)** field, re-enter the RADIUS shared secret from the preceding step.
15. Optional: Select the **AccountingEnabled** field to enable RADIUS Accounting.
16. Optional: In the **AccountingPort** field, enter a port number.
17. Optional: In the **RetryLimit** field, enter a value.
18. On the tool bar, click **Apply**.

Variable definitions

The following table describes the Globals tab fields.

Variable	Value
UseMgmtIp	When selected, RADIUS uses the system management IP address as the source address for RADIUS requests.
PasswordFallbackEnabled	When selected, enables RADIUS password fallback.
DynAuthReplayProtection	When selected, enables RADIUS replay protection.
Reachability	Specifies the RADIUS server reachability mode. Values include:

Variable	Value
	<ul style="list-style-type: none"> • use-radius — uses dummy RADIUS requests to determine reachability of the RADIUS server. • use-icmp — uses ICMP packets to determine reachability of the RADIUS server (default).
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. DEFAULT: 600 seconds.
InterimUpdatesIntervalSource	<p>Specifies the source of the interim updates timeout interval.</p> <ul style="list-style-type: none"> • configuredValue — uses the value in the RadiusAccountingInterimUpdatesInterval dialog box • radiusServer — uses the value applied by the RADIUS server
EncapsulationProtocol	<p>Specifies the type of encapsulation for the RADIUS packets. Values include:</p> <ul style="list-style-type: none"> • pap — Password Authentication Protocol. • ms-chap-v2 — Microsoft Challenge Handshake Authentication Protocol Version 2.

Variable definitions

The following table describes the EAP RADIUS Server tab fields.

Variable	Value
PrimaryRadiusServerAddressType	Specifies the type of IP address type for the primary EAP RADIUS server. Values include unknown, ipv4, and ipv6.
PrimaryRadiusServer	Specifies the IPv4 or IPv6 address for the primary EAP RADIUS Server. The default address is 0.0.0.0.

Variable	Value
	<p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a primary EAP RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a primary EAP RADIUS Server is not configured.</p>
SecondaryRadiusServerAddressType	<p>Specifies the IP address type for the secondary EAP RADIUS Server. Values include unknown, ipv4, and ipv6.</p>
SecondaryRadiusServer	<p>Specifies the IP address for the secondary EAP RADIUS Server. The default address is 0.0.0.0. The secondary EAP RADIUS Server is used only if the primary EAP RADIUS Server is unavailable or unreachable.</p> <p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a secondary EAP RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a secondary EAP RADIUS Server is not configured.</p>
RadiusServerUdpPort	<p>Specifies the UDP port number for clients to use when trying to contact the EAP RADIUS Server at the corresponding EAP RADIUS Server IP address. Values range from 1 to 65535. The default port number is 1812.</p>
RadiusServerTimeout	<p>Specifies the timeout interval between each retry for service requests to the EAP RADIUS Server. The default is 2 Seconds. Values range from 1 to 60 seconds.</p>
SharedSecret(Key)	<p>Specifies a new value for the EAP RADIUS Server shared secret key, to a maximum of 16 characters.</p>
ConfirmedSharedSecret(key)	<p>Confirms the value typed in the shared secret key box. If you do not change the EAP RADIUS Server shared secret key, you do not have to type a value in this box.</p>
AccountingEnabled	<p>Enables or disables RADIUS accounting for an EAP RADIUS Server instance</p>
AccountingPort	<p>Specifies the UDP accounting port number for clients to use when trying to contact the</p>

Variable	Value
	RADIUS server at the corresponding EAP RADIUS Server IP address. Values range from 0 to 65535.
RetryLimit	Specifies the number of RADIUS retry attempts for a EAP RADIUS Server instance. Values range from 1 to 5

Configuring Ignition Server as a non-EAP RADIUS server using EDM

You can configure Ignition Server to act as the non-EAP RADIUS server for your switches and access points. For more information about configuring the Ignition Server for RADIUS, see Avaya Identity Engines Ignition Server Configuration, NN47280-500.

Prerequisites

- Ignition Server installed and configured in your network
- Configure the following policies for your switch on Ignition Server
 - Access
 - User Authentication
 - User Authorization
- Configure the following optional policies for your switch on Ignition Server:
 - Provisioning Polices that set network session and switch parameters for users
 - Client Posture Policies that require that laptops meet a minimum standard of system health
 - VLAN Assignments that assign each user to an appropriate VLAN
 - Windows machine authentication that checks connecting devices to ensure they are known to the Active Directory before the system permits connection
 - MAC authentication that allows operator-less devices to connect and records which device a user connected with
- Non-EAP configured on your switch.

Procedure steps

1. From the Configuration tree, double-click **Security**.
2. From the Security tree, click **RADIUS**.
3. On the work area, click the **Globals** tab.
4. In the **Reachability** box select **useRadius**.

5. Optional: in the **RADIUS Accounting** section, select values to configure RADIUS Accounting.
6. On the work area, click the **NEAP RADIUS Server** tab.
7. In the PrimaryRadiusServerAddressType field, select the address type
8. In the **PrimaryRadiusServer** field, enter the Ignition Server RADIUS service IP address.
9. Optional: In the **SecondaryRadiusServerAddressType** , select the address type.
10. Optional: In the **SecondaryRadiusServer** field, enter the Ignition Server secondary RADIUS service IP address.
11. In the **RadiusServerUdpPort** field, enter the port number for the UDP port.
12. In the **RadiusServerTimeout** field, enter a timeout value.
13. In the **SharedSecret(Key)** field, enter the RADIUS shared secret (also known as the *key* or *encryption key*).
14. Optional: In the **Confirm SharedSecret(Key)** field, re-enter the RADIUS shared secret from the preceding step.
15. Optional: Select the **AccountingEnabled** field to enable RADIUS Accounting.
16. Optional: In the **AccountingPort** field, enter a port number.
17. Optional: In the **RetryLimit** field, enter a value.
18. On the tool bar, click **Apply**.

Variable definitions

The following table describes the Globals tab fields.

Variable	Value
UseMgmtIp	When selected, RADIUS uses the system management IP address as the source address for RADIUS requests.
PasswordFallbackEnabled	When selected, enables RADIUS password fallback.
DynAuthReplayProtection	When selected, enables RADIUS replay protection.
Reachability	Specifies the RADIUS server reachability mode. Values include:

Variable	Value
	<ul style="list-style-type: none"> • use-radius — uses dummy RADIUS requests to determine reachability of the RADIUS server. • use-icmp — uses ICMP packets to determine reachability of the RADIUS server (default).
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. DEFAULT: 600 seconds.
InterimUpdatesIntervalSource	<p>Specifies the source of the interim updates timeout interval.</p> <ul style="list-style-type: none"> • configuredValue — uses the value in the RadiusAccountingInterimUpdatesInterval dialog box • radiusServer — uses the value applied by the RADIUS server
EncapsulationProtocol	<p>Specifies the type of encapsulation for the RADIUS packets. Values include:</p> <ul style="list-style-type: none"> • pap — Password Authentication Protocol. • ms-chap-v2 — Microsoft Challenge Handshake Authentication Protocol Version 2.

Variable definitions

The following table describes the NEAP RADIUS Server tab fields.

Variable	Value
PrimaryRadiusServerAddressType	Specifies the type of IP address type for the primary NEAP RADIUS server. Values include unknown, ipv4, and ipv6.
PrimaryRadiusServer	Specifies the IPv4 or IPv6 address for the primary NEAP RADIUS Server. The default address is 0.0.0.0.

Variable	Value
	<p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a primary NEAP RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a primary NEAP RADIUS Server is not configured.</p>
SecondaryRadiusServerAddressType	<p>Specifies the IP address type for the secondary NEAP RADIUS Server. Values include unknown, ipv4, and ipv6.</p>
SecondaryRadiusServer	<p>Specifies the IP address for the secondary NEAP RADIUS Server. The default address is 0.0.0.0. The secondary NEAP RADIUS Server is used only if the primary NEAP RADIUS Server is unavailable or unreachable.</p> <p>! Important:</p> <p>An IPv4 address value of 0.0.0.0 indicates that a secondary NEAP RADIUS Server is not configured. An IPv6 value of 00:00:00:00:00:00:00:00 indicates that a secondary NEAP RADIUS Server is not configured.</p>
RadiusServerUdpPort	<p>Specifies the UDP port number for clients to use when trying to contact the NEAP RADIUS Server at the corresponding NEAP RADIUS Server IP address. Values range from 1 to 65535. The default port number is 1812.</p>
RadiusServerTimeout	<p>Specifies the timeout interval between each retry for service requests to the NEAP RADIUS Server. The default is 2 Seconds. Values range from 1 to 60 seconds.</p>
SharedSecret(Key)	<p>Specifies a new value for the NEAP RADIUS Server shared secret key, to a maximum of 16 characters.</p>
ConfirmedSharedSecret(key)	<p>Confirms the value typed in the shared secret key box. If you do not change the NEAP RADIUS Server shared secret key, you do not have to type a value in this box.</p>
AccountingEnabled	<p>Enables or disables RADIUS accounting for a NEAP RADIUS Server instance</p>

Variable	Value
AccountingPort	Specifies the UDP accounting port number for clients to use when trying to contact the NEAP RADIUS server at the corresponding NEAP RADIUS Server IP address. Values range from 0 to 65535.
RetryLimit	Specifies the number of RADIUS retry attempts for a NEAP RADIUS Server instance. Values range from 1 to 5

Configuring Ignition Server as a TACACS+ server using EDM

You can configure Ignition Server to act as the TACACS+S authentication and authentication server, and you can use it as the TACACS+ accounting server. For more information, see Avaya Identity Engines Ignition Server Configuration, NN47280-600.

Prerequisites

- Ignition Server installed and configured in your network
- Configure the following policies for your switch on Ignition Server
 - Access
 - User Authentication
 - User Authorization
- Configure the following optional policies for your switch on Ignition Server:
 - Provisioning Policies that set network session and switch parameters for users
 - Client Posture Policies that require that laptops meet a minimum standard of system health
 - VLAN Assignments that assign each user to an appropriate VLAN
 - Windows machine authentication that checks connecting devices to ensure they are known to the Active Directory before the system permits connection
 - MAC authentication that allows operator-less devices to connect and records which device a user connected with
- Configure an Ignition Server authentication record with a TACACS+ policy **NOTE:** If you use Ignition Server for TACACS+ authorization, you must use Ignition Server for TACACS+ authentication.

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **TACACS+**.
3. In the work area, click the **TACACS+ Server** tab.
4. On the toolbar, click **Insert**.
The Insert TACACS+ Server dialog box appears.
5. Type the address in the **Address** field.
6. Type the port number in the **PortNumber** field.
7. Type the key in the **Key** field.
8. Retype the key in the **Confirm Key** field.
9. Choose the priority in the **Priority** field.
10. Click **Insert**.

Variable definitions

Variable	Value
AddressType	Specifies the type of IP address used on the TACACS+ server.
Address	Indicates the IP address of the TACACS+ server in use.
PortNumber	Indicates the TCP port on which the client establishes a connection to the server.
Key	Indicates the secret key to be shared with this TACACS+ server. Key length zero indicates no encryption is being used.
Confirm Key	Indicates the key in use.
Priority	Determines the order in which the TACACS+ servers are used. Available options are—primary or secondary.

Appendix A: TACACS+ server configuration examples and supported SNMP MIBs

This section contains information about the following topics:

- TACACS+ server configuration examples
- Supported SNMP MIBs and traps

TACACS+ server configuration examples

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

Configuration example: Cisco ACS (version 3.2) server

The following figure shows the main administration window.

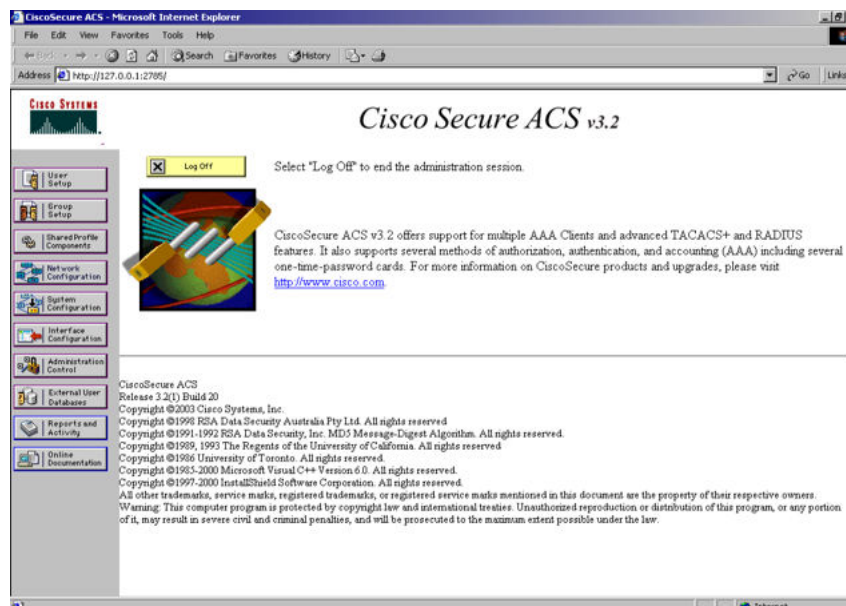


Figure 7: Cisco ACS (version 3.2) main administration window

1. Define the users and the corresponding authorization levels.

If you map users to default group settings, it is easier to remember which user belongs to each group. For example, the rwa user belongs to group 15 to match Privilege level 15. All rwa user settings are picked up from group 15 by default.

The following figure shows a sample Group Setup window.

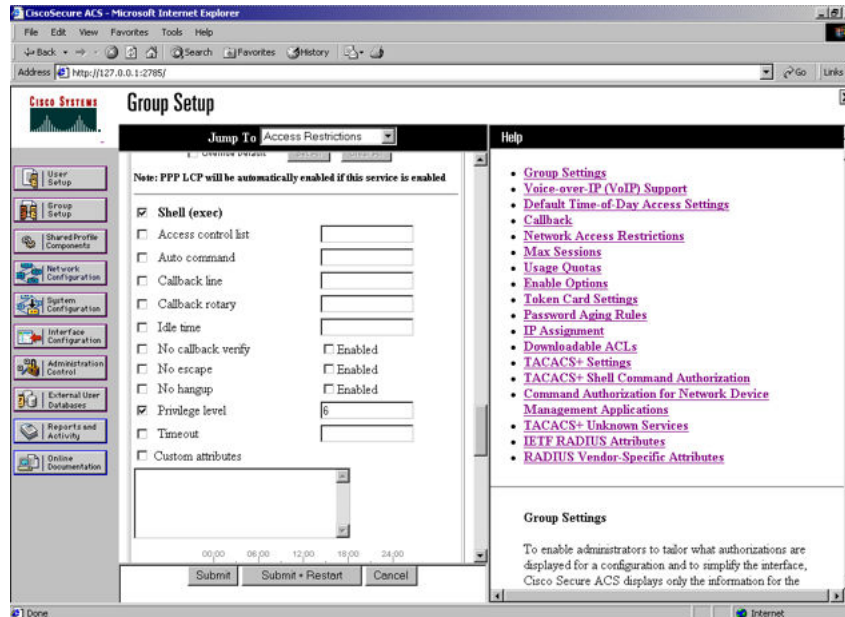


Figure 8: Group Setup window - Cisco ACS server configuration

2. Configure the server settings.

The following figure shows a sample Network Configuration window to configure the authentication, authorization, and accounting (AAA) server for TACACS+.

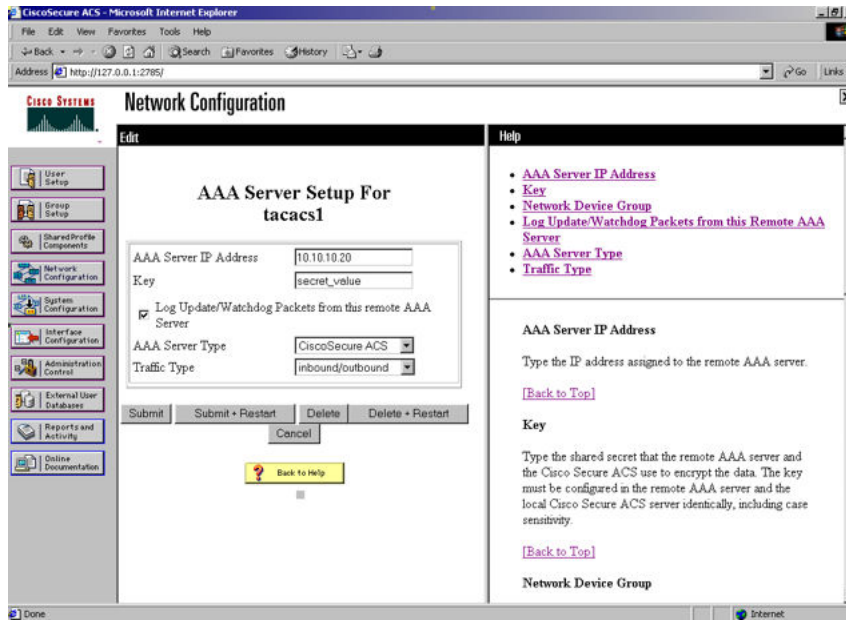


Figure 9: Network Configuration window - server setup

3. Define the client.

The following figure shows a sample Network Configuration window to configure the client. Authenticate using TACACS+. You can use a single-connection, but this must match the configuration on the Avaya Ethernet Routing Switch 5000 Series.

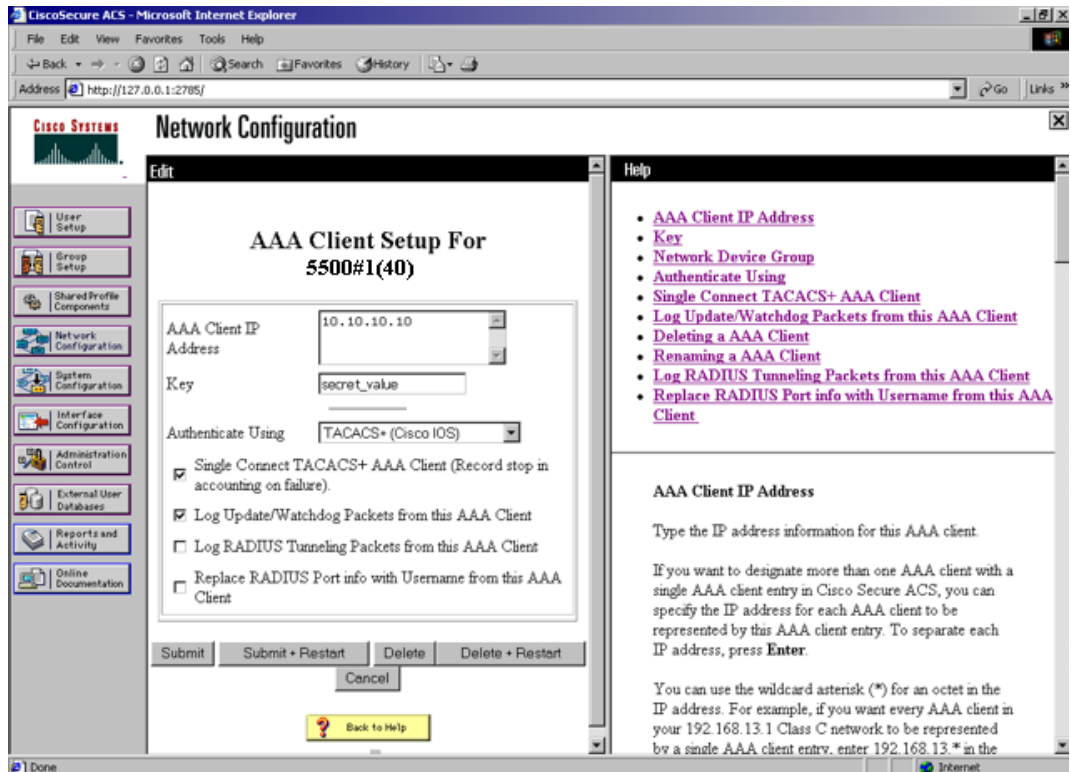


Figure 10: Network Configuration window - client setup

4. Verify the groups you have configured.

In this example, the user is associated with a user group. For more information, see [Figure 11: Group Setup window - viewing the group setup](#) on page 385. The rwa account belongs to group 15, and its privilege level corresponds to the settings for group 15. The ro accounts belong to group 0 and L1 accounts belong to group 2.

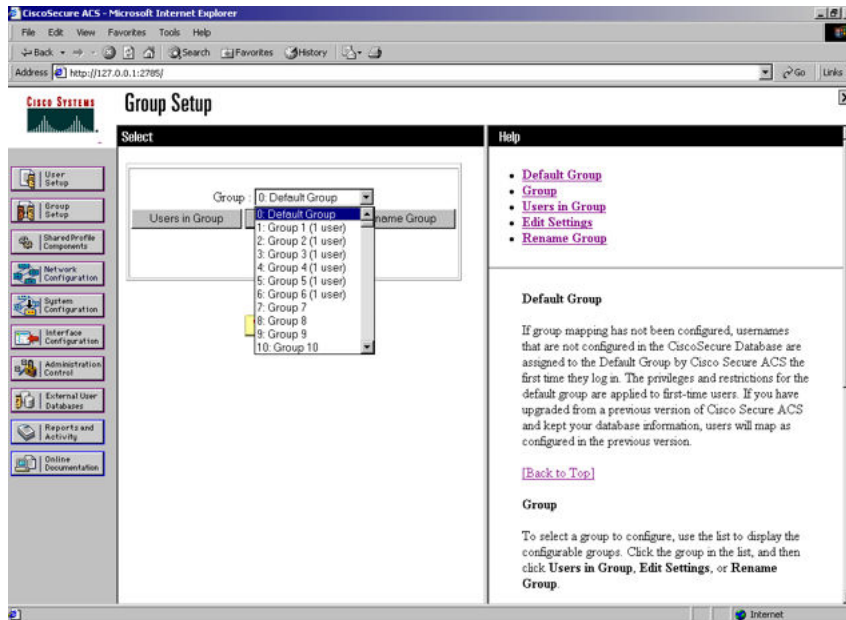


Figure 11: Group Setup window - viewing the group setup

5. Go to **Shared Profile Components**, **Shell Command Authorization Set**.
The Shell Command Authorization Set screen appears.

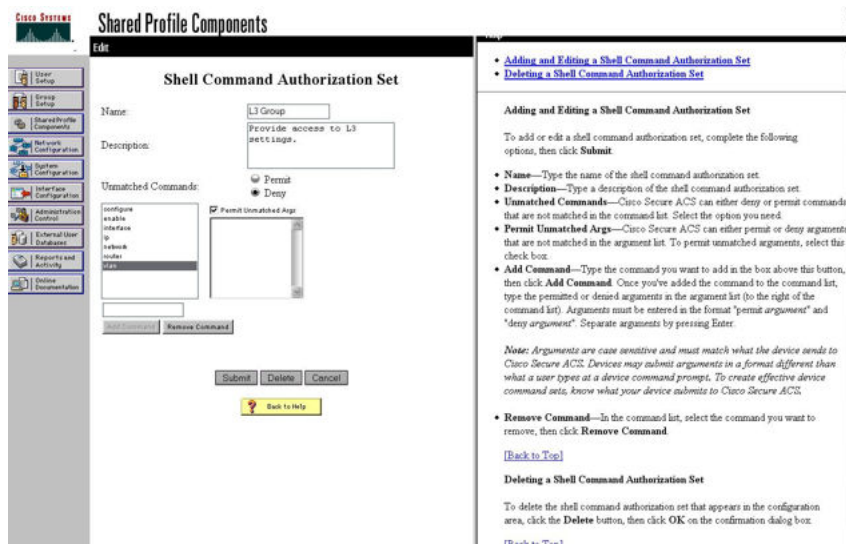


Figure 12: Shared Profile Components window - defining the command set

6. Select the commands to be added to the command set, and specify whether the action is permit or deny.
7. View users, their status, and the corresponding group to which each belongs.

The following figure shows a sample User Setup window. You can use this window to find, add, edit, and view users settings.

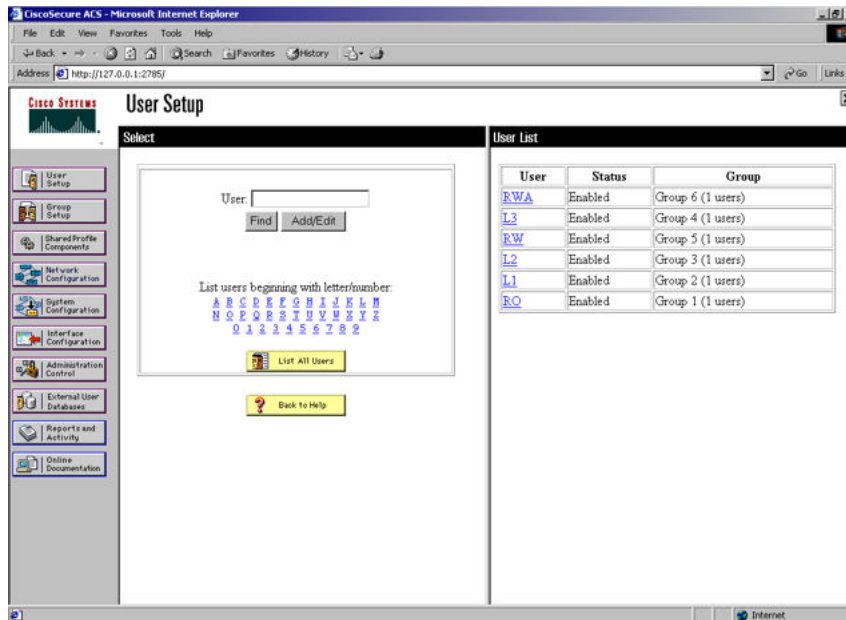


Figure 13: User Setup window - Cisco ACS server configuration

Configuration example: ClearBox server

1. Run the General Extension Configurator and configure the user data source.

In this example, Microsoft Access was used to create a database of user names and authorization levels; the general.mdb file needs to include these users.

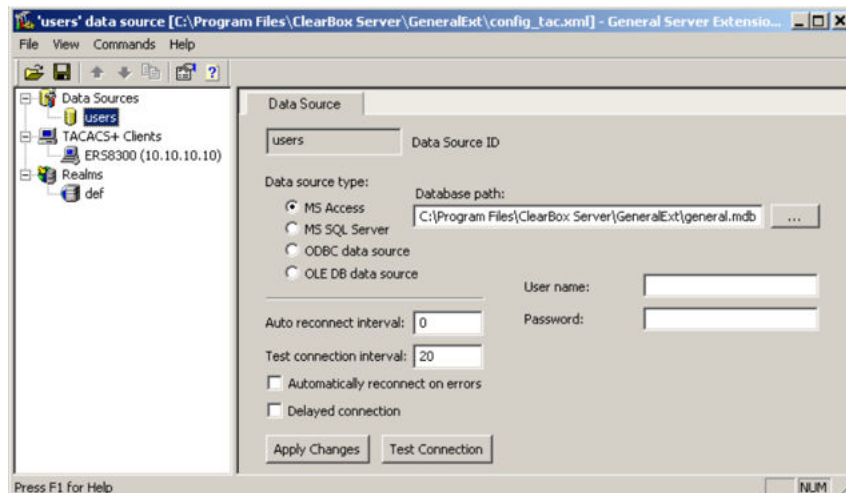


Figure 14: General Extension Configurator

2. Create a Client entry for the switch management IP address by right-clicking the **TACACS+ Clients** item.

In this case, the TACACS+ Client is the Avaya Ethernet Routing Switch 4000. Enter the appropriate information. The shared secret must match the value configured on the Avaya Ethernet Routing Switch 4000.

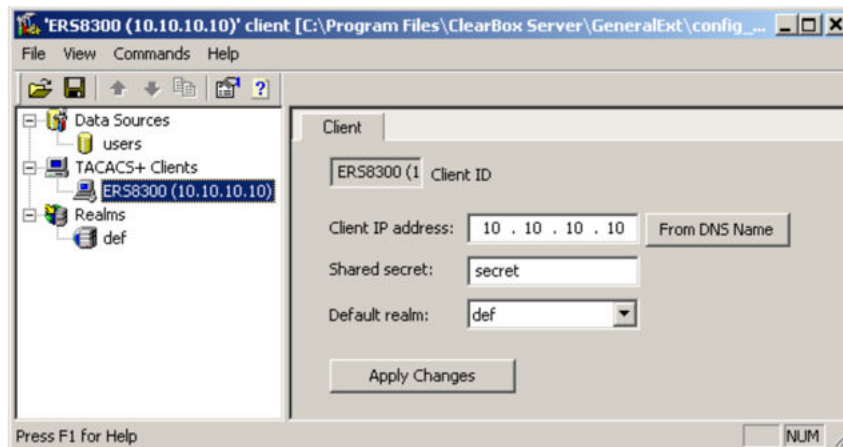


Figure 15: Creating a client entry

The default realm Authentication tab looks like the following figure.

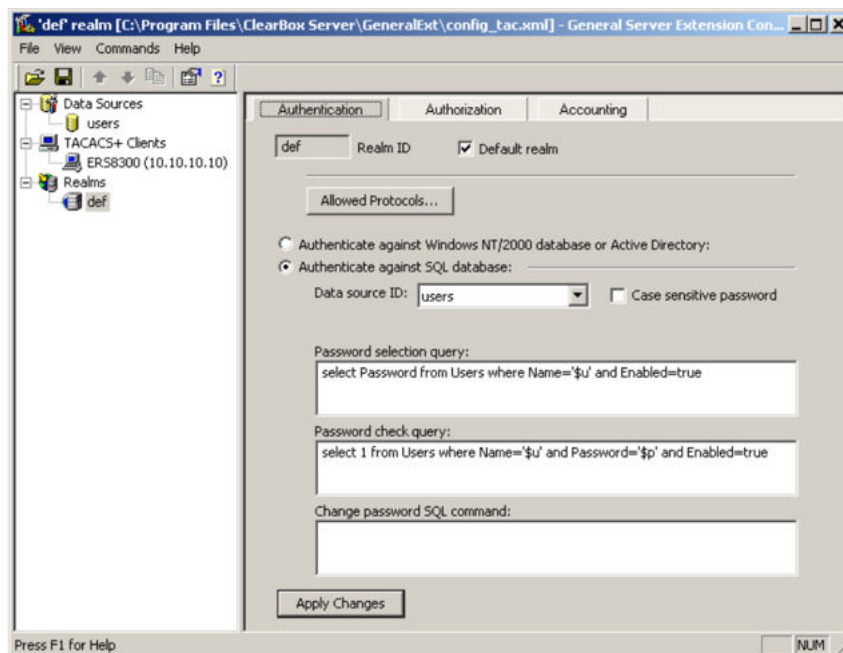


Figure 16: Default realm - Authentication tab

3. Click the **Realms** , **def** , **Authorization** tab.

A new service is required that allows the server to assign certain levels of access.

4. Click the **+** button to add an attribute-value pair for privilege levels.

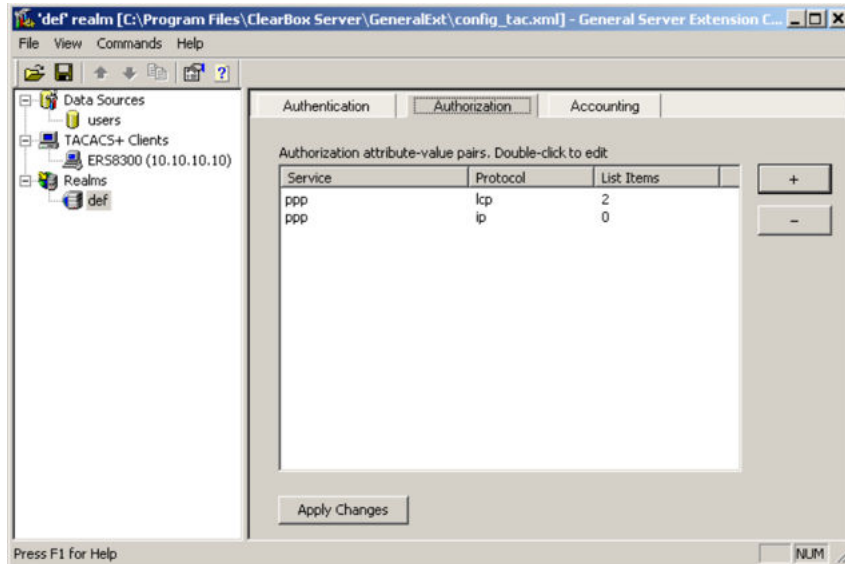


Figure 17: Default realm - Authorization tab

5. Enter information in the window as shown in the following figure to specify the query parameters.

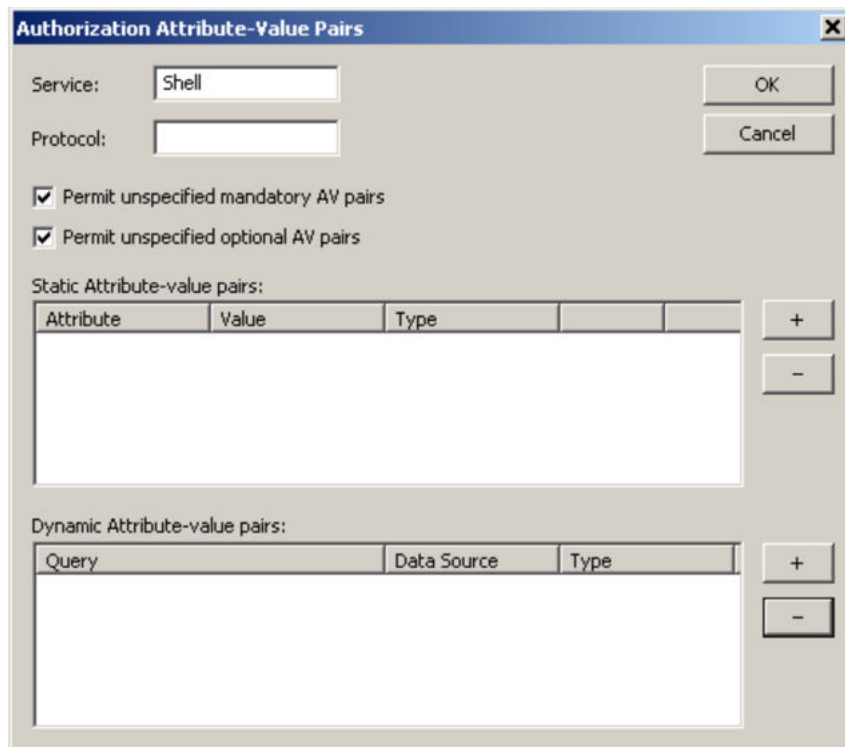


Figure 18: Adding parameters for the query

6. Click + to add the parameters to the query.
7. Use the string shown in the following figure for the authorization query.

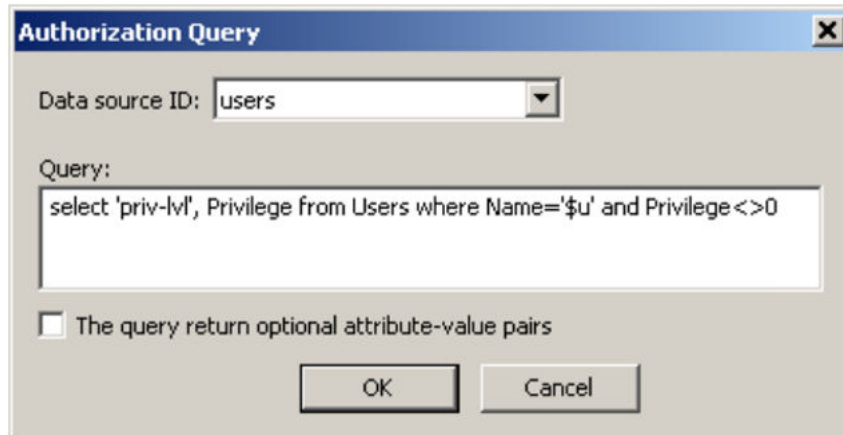


Figure 19: Authorization Query window

The following figure shows the final window.

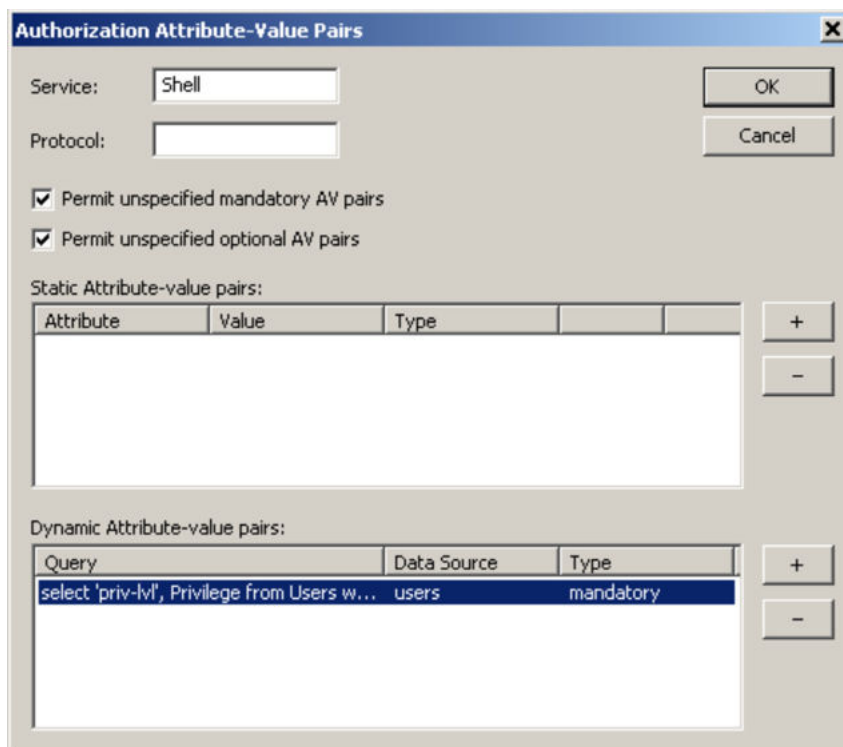


Figure 20: Query parameters added to Authorization Attribute-Value Pairs window

8. Click **OK**.

The information appears on the Authorization tab.

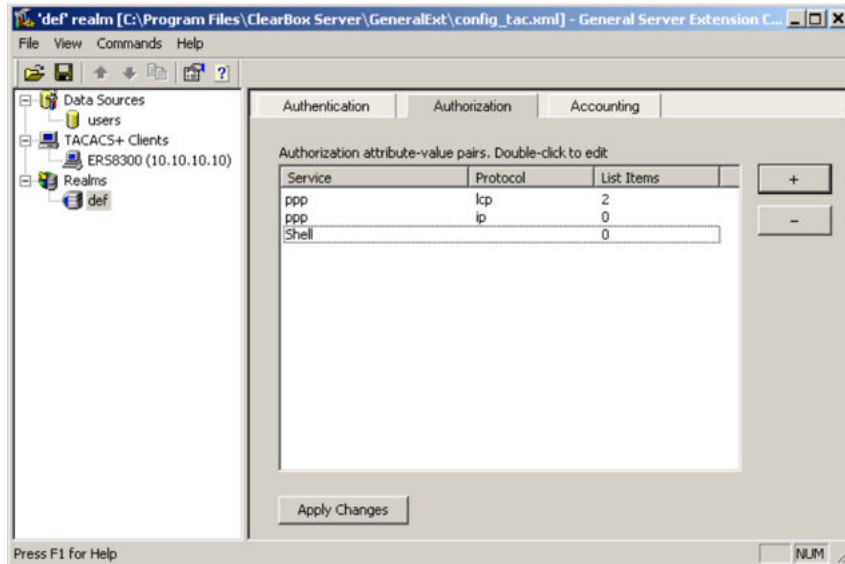


Figure 21: Authorization attribute-value pairs added to Authorization tab

9. Browse the general.mdb file as specified earlier.

The user table can look like the one shown in the following figure. If the Privilege column does not exist, create one and populate it according to the desired access level.

Microsoft Access or third-party software is required to read this file.

If you use the 30-day trial for ClearBox, the user names cannot be more than four characters in length.

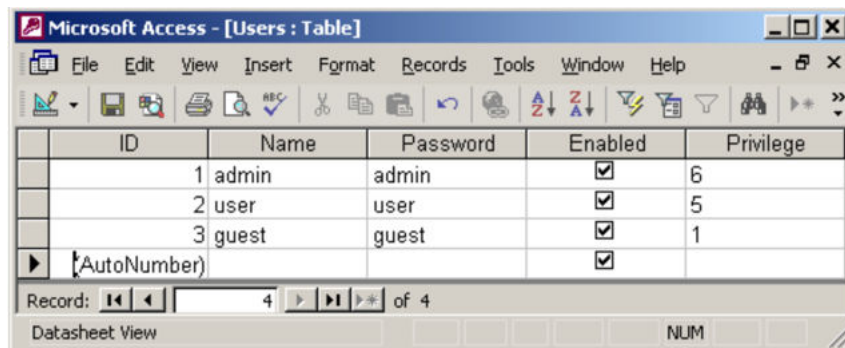


Figure 22: Users table - Microsoft Access

10. Run the Server Manager.

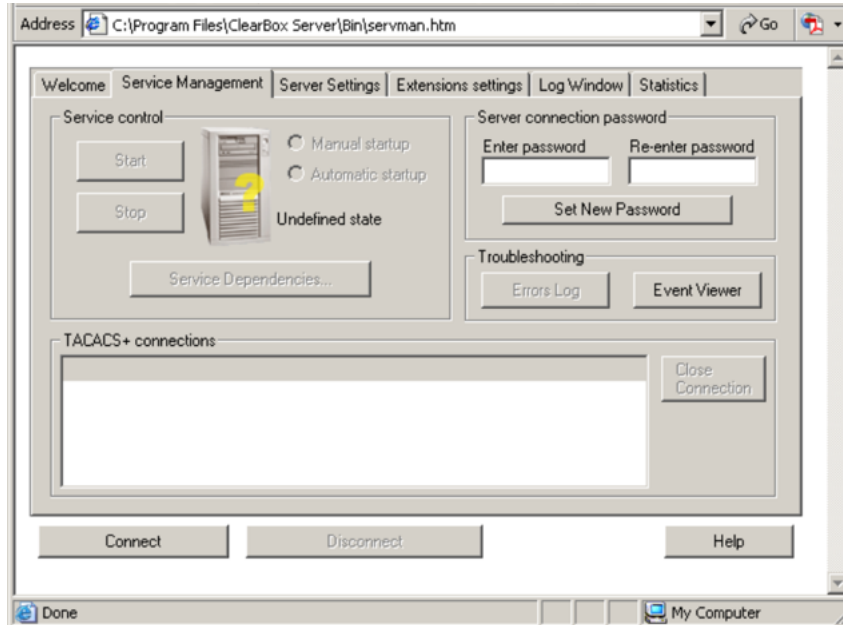


Figure 23: ClearBox Server Manager

11. Click **Connect**.

The Connect to... dialog box appears.

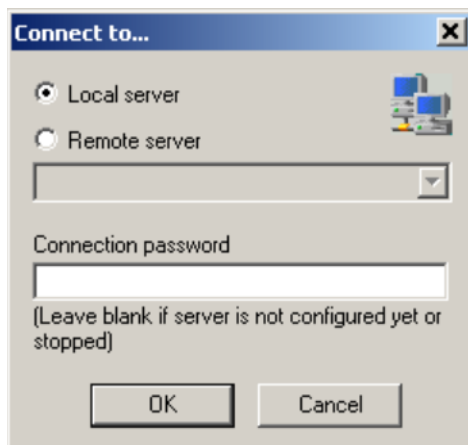


Figure 24: Connect to... dialog box

12. Click **OK** (do not fill in fields).
13. Click **OK** at the warning message.
14. Click **Start**.

The Server Manager can now look like the following figure. Changes to the General Server Extension Configurator require that the server be restarted.

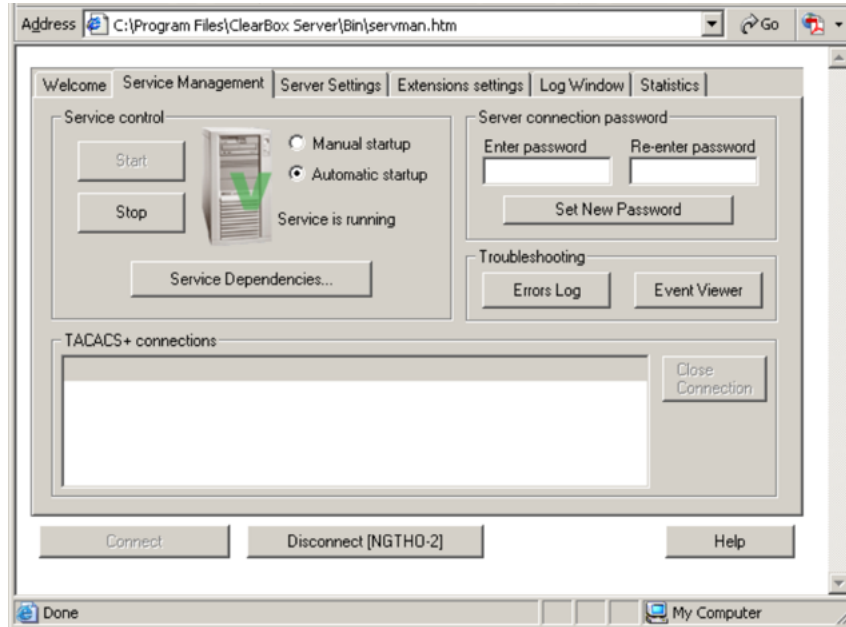


Figure 25: TACACS+ server connected

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.

Supported SNMP MIBs and traps

This section contains information about:

- [Supported MIBs](#) on page 393
- [Supported traps](#) on page 396

Supported MIBs

The following tables list supported SNMP MIBs.

Table 82: SNMP Standard MIB support

MIB name	RFC	File name
RMON-MIB	2819	rfc2819.mib
RFC1213-MIB	1213	rfc1213.mib
IF-MIB	2863	rfc2863.mib
SNMPv2-MIB	3418	rfc3418.mib
EtherLike-MIB	2665	rfc2665.mib
ENTITY-MIB	2737	rfc2737.mib
BRIDGE-MIB	4188	rfc4188.mib
P-BRIDGE-MIB	4363	rfc4363-p.mib
Q-BRIDGE-MIB	4363	rfc4363-q.mib
IEEE8021-PAE-MIB	n/a	eapol-d10.mib
SMIv2-MIB	2578	rfc2578.mib
SMIv2-TC-MIB	2579	rfc2579.mib
SNMPv2-MIB	3418	rfc3418.mib
SNMP-FRAMEWORK-MIB	3411	rfc3411.mib
SNMP-MPD-MIB	3412	rfc3412.mib
SNMP-NOTIFICATION-MIB	3413	rfc3413-notif.mib
SNMP-TARGET-MIB	3413	rfc3413-tgt.mib
SNMP-USER-BASED-MIB	3414	rfc3414.mib
SNMP-VIEW-BASED-ACM-MIB	3415	rfc3415.mib
SNMP-COMMUNITY-MIB	3584	rfc3584.mib

Table 83: SNMP proprietary MIB support

MIB name	File name
S5-AGENT-MIB	s5age.mib
S5-CHASSIS.MIB	s5cha.mib
S5-CHASSIS-TRAP.MIB	s5ctr.trp
S5-ETHERNET-TRAP.MIB	s5etr.trp
RAPID-CITY-MIB	rapidCity.mib
S5-SWITCH-BAYSECURE-MIB	s5sbs.mib
BN-IF-EXTENSIONS-MIB	s5ifx.mib

MIB name	File name
BN-LOG-MESSAGE-MIB	bnlog.mib
S5-ETH-MULTISEG-TOPOLOGY-MIB	s5emt.mib
NTN-QOS-POLICY-EVOL-PIB	pibNtnEvol.mib
BAY-STACK-NOTIFICATIONS-MIB	bsn.mib

Table 84: Application and related MIBs

Application	Related MIBs	File name
Autotopology	S5-ETH-MULTISEG-TOPOLOGY-MIB	s5emt.mib
BaySecure	S5-SWITCH-BAYSECURE-MIB	s5sbs.mib
Extensible Authentication Protocol over LAN (EAPOL)	IEEE8021-PAE-MIB	eapol-d10.mib
IP multicast (IGMP snooping/proxy)	RAPID-CITY-MIB (rcVlanIgmpp group)	rcVlan.mib
Link Aggregation Control Protocol (LACP)	IEEE8023-LAG-MIB; BAY-STACK-LACP-EXT-MIB	ieee8023-lag.mib; bayStackLacpExt.mib
Link Layer Discovery Protocol (LLDP)	LLDP-MIB; LLDP-EXT-DOT1-MIB; LLDP-EXT-DOT3-MIB;	lldp.mib; lldpExtDot1.mib; lldpExtDot3.mib;
MIB-2	RFC1213-MIB	rfc1213.mib
MultiLink Trunking (MLT)	RAPID-CITY-MIB (rcMlt group)	rcMlt.mib
Policy management	NTN-QOS-POLICY-EVOL-PIB	pibNtnEvol.mib
RMON-MIB	RMON-MIB	rfc2819.mib
SNMPv3	SNMP-FRAMEWORK-MIB	rfc3411.mib
	SNMP-MPD-MIB	rfc3412.mib
	SNMP-NOTIFICATION-MIB	rfc3413-notif.mib
	SNMP-TARGET-MIB	rfc3413-tgt.mib
	SNMP-USER-BASED-SM-MIB	rfc3414.mib
	SNMP-VIEW-BASED-ACM-MIB	rfc3415.mib
	SNMP-COMMUNITY-MIB	rfc3584.mib
Spanning Tree	BRIDGE-MIB	rfc4188.mib
for MSTP	NORTEL-NETWORKS-MULTIPLE-SPANNING-TREE-MIB	nnmst.mib

Application	Related MIBs	File name
for RSTP	NORTEL-NETWORKS-RAPID-SPANNING-TREE-MIB	nnrst.mib
System log	BN-LOG-MESSAGE-MIB	bnlog.mib
VLAN	RAPID-CITY-MIB (rcVlan group)	rcVlan.mib

Supported traps

The following table lists supported SNMP traps.

Table 85: Supported SNMP traps

Trap name	Configurable	Sent when
RFC 2863 (industry standard):		
linkUp	Per port	A port link state changes to up.
linkDown	Per port	A port link state changes to down.
RFC 3418 (industry standard):		
authenticationFailure	System wide	There is an SNMP authentication failure.
coldStart	Always on	The system is powered on.
warmStart	Always on	The system restarts due to a management reset.
s5CtrMIB (Avaya proprietary traps):		
s5CtrUnitUp	Always on	A unit is added to an operational stack.
s5CtrUnitDown	Always on	A unit is removed from an operational stack.
s5CtrHotSwap	Always on	A unit is hot-swapped in an operational stack.
s5CtrProblem	Always on	<ul style="list-style-type: none"> • Base unit fails • AC power fails or is restored • RPSU (DC) power fails or is restored • Fan fails or is restored
s5EtrSbsMacAccessViolation	Always on	A MAC address security violation is detected.

Trap name	Configurable	Sent when
entConfigChange	Always on	A hardware change—unit added or removed from stack, GBIC inserted or removed.
risingAlarm fallingAlarm	Always on	An RMON alarm threshold is crossed.
bsnConfigurationSavedToNvram	Always on	Each time the system configuration is saved to NVRAM.
bsnEapAccessViolation	Always on	An EAP access violation occurs.
bsnStackManagerReconfiguration	System-wide	There has been a stack configuration.
LLDP-MIB		
lldpRemTablesChange	System-wide	The value of lldpStatsRemTableLastChangeTime changes.
NORTEL-NETWORKS-RAPID-SPANNING-TREE-MIB:		
nnRstGeneralEvent	Always on	A general event, such as protocol up or protocol down, occurs.
nnRstErrorEvent	System-wide	An error event occurs. Error events include memory failure, buffer failure, protocol migration, new root, and topology change.
nnRstNewRoot	System-wide	A new root bridge is selected in the topology.
nnRstTopologyChange	System-wide	A topology change is detected.
nnRstProtocolMigration	Per port	Port protocol migration occurs.
NORTEL-NETWORKS-MULTIPLE-SPANNING-TREE-MIB:		
nnMstGeneralEvent	Always on	A general event, such as protocol up or protocol down, occurs.
nnMstErrorEvent	System-wide	An error event occurs. Error events include memory failure, buffer failure, protocol migration, new root, and topology change.
nnMstNewRoot	System-wide	A new root bridge is selected in the topology.
nnMstTopologyChange	System-wide	A topology change is detected.
nnMstProtocolMigration	Per port	Port protocol migration occurs.

Trap name	Configurable	Sent when
nnMstRegionConfigChange	System-wide	The MST region configuration identifier changes.

Appendix B: Supported EAP modes and configuration examples

This appendix provides configuration examples that are compatible with various operating modes and scenarios as described in each section.

 **Note:**

From release 5.7 onwards, a new parameter, `mac-max`, is introduced to restrict the maximum number of EAP and NEAP clients allowed per port. Because the limit set by `mac-max` is set by default to 1, and because `mac-max` takes precedence over `eap-mac-max` or `non-eap-mac-max`, some configuration examples in this appendix could function improperly if used with Software Release 5.7.

SHSA authentication mode with or without RADIUS additional attributes with or without Multihost MultiVLAN

The configuration example in this section applies to the following client port 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
- 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 authenticated client is on the port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs but no RADIUS attribute is received, or an invalid RADIUS attribute is received, for the client
- an authenticated client is on the port—the port is included in the RADIUS VLAN ID and it uses the RADIUS VLAN PVID so that valid RADIUS attributes are received for the client

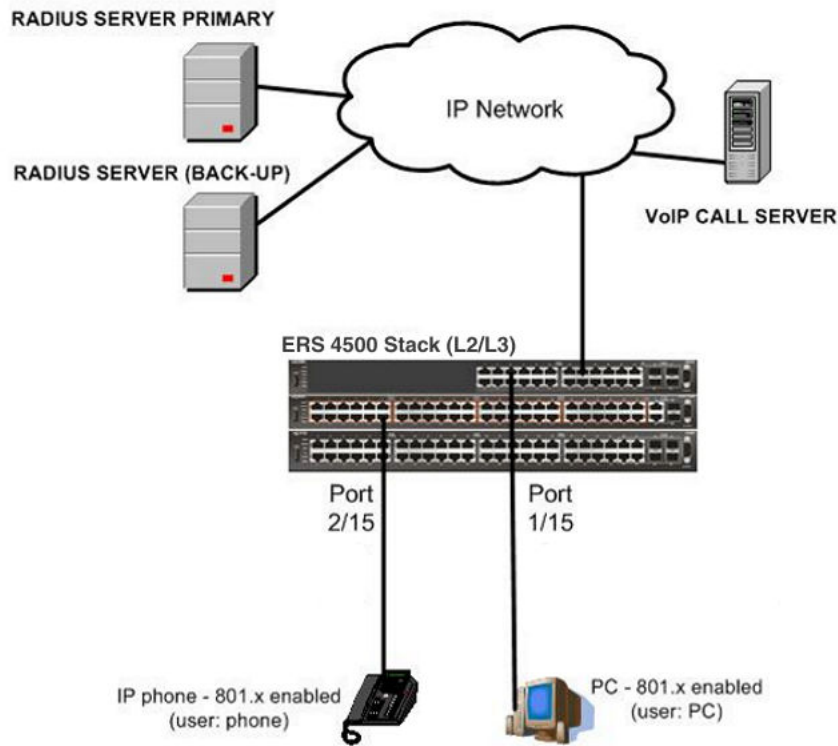


Figure 26: SHSA authentication mode with or without RADIUS additional attributes with or without Multihost MultiVLAN

Scenario

Assume the following settings:

- Primary RADIUS server configured with two users:
 - user: phone with attribute VLAN ID: 200, Port priority: 6
 - user: PC with attribute VLAN ID: 300, Port priority: 2
- Backup RADIUS server configured with the same two users:
 - user: phone with attribute VLAN ID: 200, Port priority: 6
 - user: PC with attribute VLAN ID: 300, Port priority: 2
- Port 2/15—801.x enabled IP phone connected - (user: phone)
 - Initial VLAN ID = 100
 - RADIUS VLAN ID = 200

- Port 1/15—801.x enabled PC connected - (user: PC)
 - Initial VLAN ID = 50
 - RADIUS VLAN ID = 300
- 802.1x phone client VLAN ID/PVID port 2/15 settings:
 - 801.x disabled on port 100/100
 - Unauthenticated client on port 100/100
 - Authenticated (user: phone):
 - 100/100 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - 200/200 (Valid RADIUS attributes received)
- 802.1x PC client VLAN ID/PVID port 1/15 settings:
 - 801.x disabled on port 50/50
 - Unauthenticated client on port 50/50
 - Authenticated client on port (user: PC):
 - 50/50 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - 300/300 (Valid RADIUS attributes received)

Configuration example

1. Configure the RADIUS servers and VLAN settings.

```
ERS4000(config)#ip address 10.100.68.254 netmask 255.255.255.0
default-gateway 10.100.68.1
ERS4000(config)#radius-server host 10.100.68.2
ERS4000(config)#radius-server secondary-host 10.100.68.3
ERS4000(config)#radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)#vlan configcontrol automatic
ERS4000(config)#vlan create 50 type port
ERS4000(config)#vlan create 100 type port
ERS4000(config)#vlan create 200 type port
ERS4000(config)#vlan create 300 type port
ERS4000(config)#vlan members add 50 1/15
ERS4000(config)#vlan members add 100 2/15
```

2. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

3. Confirm the VLAN interface VIDs.

```
ERS4000 (config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

4. 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.

```
ERS4000 (config)#ping 10.100.68.2
(Host is reachable)
ERS4000 (config)#ping 10.100.68.3
(Host is reachable)
```

5. Set the EAPOL status.

```
ERS4000 (config)#interface Ethernet 1/15,2/15
ERS4000 (config-if)#eapol status auto
ERS4000 (config-if)#exit
ERS4000 (config)#eapol enable
```

6. After EAP clients are authenticated, confirm the EAPOL MultiHost status.

```
ERS4000 (config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

7. Confirm the VLAN interface settings.

```
ERS4000 (config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

8. Confirm the VLAN interface VLANs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300				
2/15	200	VLAN #200				

9. Enable EAPOL MultiHost MultiVLAN.

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol multihost multivlan enable
ERS4000(config)#eapol enable
```

10. Confirm EAPOL MultiHost status.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

11. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

12. Confirm the VLAN interface settings.

```
ERS4000 (config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

13. Confirm the VLAN interface VIDs.

```
ERS4000 (config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300	-----	-----	-----	-----
2/15	200	VLAN #200	-----	-----	-----	-----

Alternate configuration

The following operation applies to **SHSA authentication mode (Multihost MultiVLAN option disabled) without valid 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 200 with VLAN ID 123, and VLAN ID 300 with VLAN ID 124, which is not configured on the device.

1. Enable EAPOL MultiHost MultiVLAN.

```
ERS4000 (config)#eapol disable
ERS4000 (config)#no eapol multihost multivlan enable
ERS4000 (config)#eapol enable
```

2. Confirm EAPOL MultiHost status.

```
ERS4000 (config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

3. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

4. Confirm the VLAN interface VLANs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

SHSA authentication mode (with Guest VLAN enabled) with or without RADIUS additional attributes, with or without Multihost MultiVLAN

The configuration example in this section applies to the following client port settings when:

- 801.x disabled on port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs
- an unauthenticated client is on the port—the port is included in the Guest VLAN ID, and the port uses the Guest VLAN PVID
- an authenticated client is on the port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs but no RADIUS attribute is received, or an invalid RADIUS attribute is received, for the client
- an authenticated client is on the port—the port is included in the RADIUS VLAN ID and it uses the RADIUS VLAN PVID so that valid RADIUS attributes are received for the client

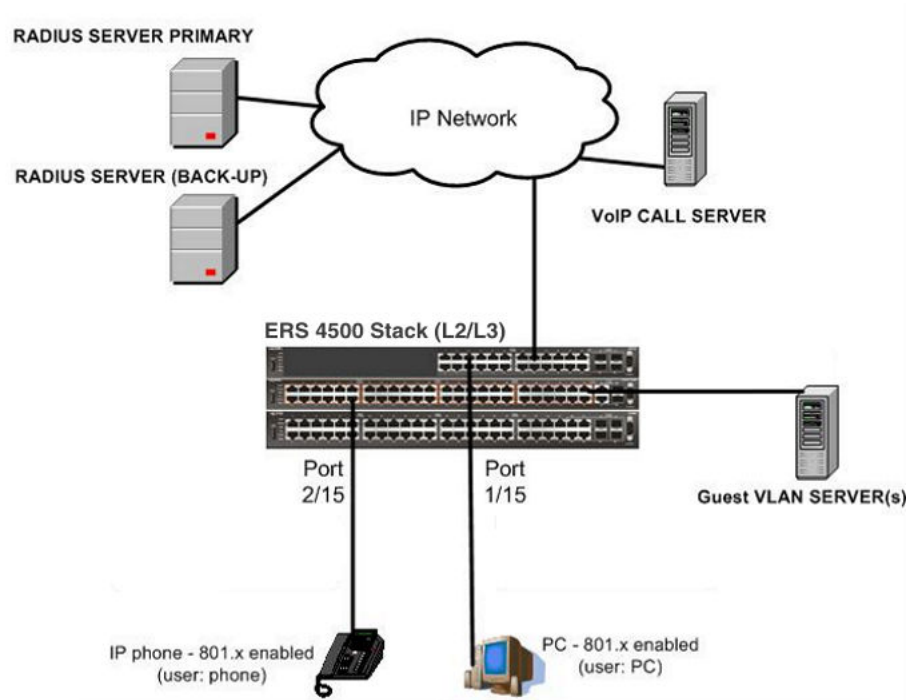


Figure 27: SHSA authentication mode (with Guest VLAN enabled) with or without RADIUS additional attributes, with or without Multihost MultiVLAN

Scenario

Assume the following settings:

1. RADIUS server configurations.
 - A primary server is mandatory. If a back-up server is used, the back-up server configuration must be the same as the primary server configuration.
2. Clients settings:
 - Port 2/15—801.x enabled IP phone connected - (user: phone)
 - Initial VLAN ID = 100
 - Guest VLAN ID = 20
 - RADIUS VLAN ID = 200
 - Port 1/15—801.x enabled PC connected - (user: PC)
 - Initial VLAN ID = 50
 - Guest VLAN ID = 20

- RADIUS VLAN ID = 300

3. Port settings:

- VLAN ID/PVID port settings for 2/15:
 - 801.x disabled - VLAN ID/PVID = port 100/100
 - Unauthenticated client - VLAN ID/PVID = port 20/20
 - Authenticated (user: phone):
 - VLAN ID/PVID = 100/100 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - VLAN ID/PVID = 200/200 (Valid RADIUS attributes received)
- VLAN ID/PVID port settings for 1/15:
 - 801.x disabled - VLAN ID/PVID = port 50/50
 - Unauthenticated client - VLAN ID/PVID = port 20/20
 - Authenticated client on port (user: PC):
 - VLAN ID/PVID = 50/50 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - VLAN ID/PVID = 300/300 (Valid RADIUS attributes received)

Configuration example

1. Configure the RADIUS servers and VLAN settings

```
ERS4000(config)# ip address 10.100.68.254 netmask 255.255.255.0 default-gateway 10.100.68.1
ERS4000(config)# radius-server host 10.100.68.2
ERS4000(config)# radius-server secondary-host 10.100.68.3
ERS4000(config)# radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)# vlan configcontrol automatic
ERS4000(config)# vlan create 20 type port
ERS4000(config)# vlan create 50 type port
ERS4000(config)# vlan create 100 type port
ERS4000(config)# vlan create 200 type port
ERS4000(config)# vlan create 300 type port
ERS4000(config)# vlan members add 50 1/15
ERS4000(config)# vlan members add 100 2/15
```

2. Confirm the VLAN interface settings.

```
ERS4000(config)# sho vlan interface info 1/15,2/15
```

Supported EAP modes and configuration examples

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

3. Confirm the VLAN interface VIDs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

4. 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.

```
ERS4000(config)# ping 10.100.68.2  
(Host is reachable)
```

```
ERS4000(config)# ping 10.100.68.3  
(Host is reachable)
```

5. Set the EAPOL status.

```
ERS4000(config)# eapol guest-vlan vid 20  
ERS4000(config)# eapol guest-vlan enable  
ERS4000(config)# interface Ethernet 1/15,2/15  
ERS4000(config-if)# eapol guest-vlan enable  
ERS4000(config-if)# eapol status auto  
ERS4000(config-if)# exit  
ERS4000(config)# eapol enable  
% Depending on your stack configuration it may take up to 4 minutes for  
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

6. Before EAP clients are authenticated, confirm the EAPOL MultiHost status.

```
ERS4000(config)# show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri

7. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	20	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	20	0	UntagAll	Unit 2, Port 15

8. Confirm the VLAN interface VIDs.

```
show vlan interface vids 1/15,2/15ERS4000(config)#
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	20	VLAN #20				
2/15	20	VLAN #200				

9. After EAP clients are authenticated, confirm the EAPOL MultiHost status.

```
ERS4000(config)# show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

10. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

11. Confirm the VLAN interface VIDs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

Supported EAP modes and configuration examples

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300	-----	-----	-----	-----
2/15	200	VLAN #200	-----	-----	-----	-----

12. Enable EAPOL MultiHost MultiVLAN.

```
ERS4000(config)# eapol disable
ERS4000(config)# eapol multihost multivlan enable
ERS4000(config)# eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

13. Confirm EAPOL MultiHost status.

```
ERS4000(config)# show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

14. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

15. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

16. Confirm the VLAN interface VIDs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300				
2/15	200	VLAN #200				

Alternate configuration

The following operation applies to **SHSA authentication mode with Guest VLAN (Multihost MultiVLAN option disabled) without valid 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 200 with VLAN ID 123, and VLAN ID 300 with VLAN ID 124, which is not configured on the device.

1. Enable EAPOL MultiHost MultiVLAN.

```
ERS4000(config)# eapol disable
ERS4000(config)# no eapol multihost multivlan enable
ERS4000(config)# eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

2. Confirm EAPOL MultiHost status.

```
ERS4000(config)# show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

3. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregister ed Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

4. Confirm the VLAN interface VIDs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

SHSA authentication mode (with Guest VLAN and Fail Open VLAN enabled) with or without RADIUS additional attributes with or without Multihost MultiVLAN

The configuration example in this section applies to the following client port settings when:

- 801.x disabled on port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs
- an unauthenticated client is on the port—the port is included in the Guest VLAN ID, and the port uses the Guest VLAN PVID
- an authenticated client is on the port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs but no RADIUS attribute is received, or an invalid RADIUS attribute is received, for the client
- an authenticated client is on the port—the port is included in the RADIUS VLAN ID and it uses the RADIUS VLAN PVID so that valid RADIUS attributes are received for the client
- RADIUS Server Unreachable (801.x enabled)—the port is included in the Fail Open VLAN, and the port uses the Fail Open VLAN PVID

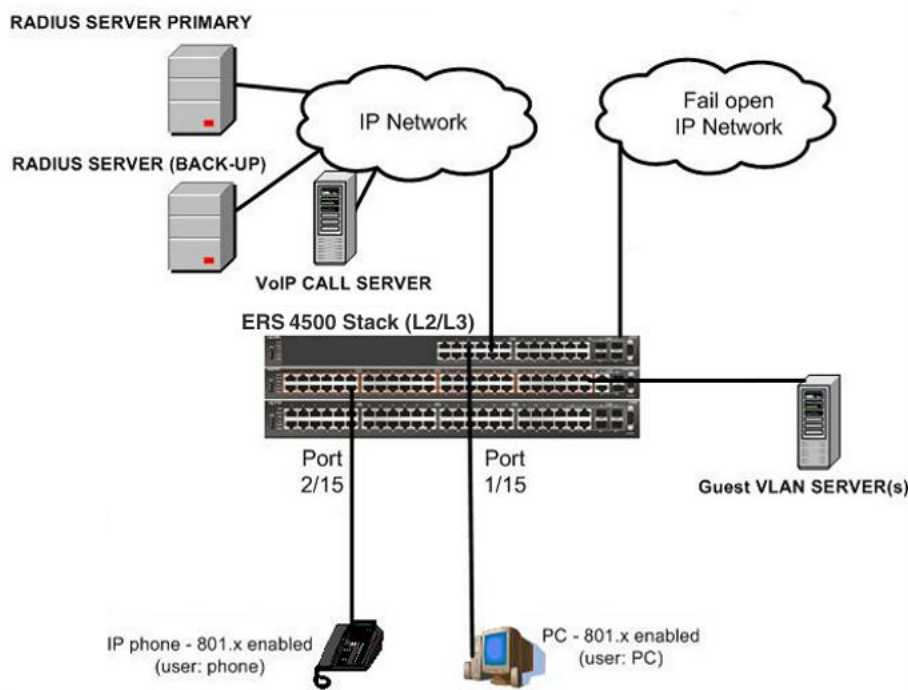


Figure 28: SHSA authentication mode (with Guest VLAN and Fail Open VLAN enabled) with or without RADIUS additional attributes with or without Multihost MultiVLAN

Scenario

Assume the following settings:

1. RADIUS server configurations.
 - Primary server is mandatory. If a back-up server is also used then the back-up server configurations must be the same as for primary server.
2. Clients settings:
 - Port 2/15—801.x enabled IP phone connected - (user: phone)
 - Initial VLAN ID = 100
 - Guest VLAN ID = 20
 - Fail Open VLAN ID = 30
 - RADIUS VLAN ID = 200
 - Port 1/15—801.x enabled PC connected - (user: PC)
 - Initial VLAN ID = 50
 - Guest VLAN ID = 20

- Fail Open VLAN ID = 30
- RADIUS VLAN ID = 300

3. Port settings:

- VLAN ID/PVID port settings for 2/15:
 - 801.x disabled on port - VLAN ID/PVID = 100/100
 - Unauthenticated client on port - VLAN ID/PVID = 20/20
 - Authenticated (user: phone):
 - VLAN ID/PVID = 100/100 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - VLAN ID/PVID = 200/200 (Valid RADIUS attributes received)
 - Radius Server Unreachable (801.x enabled) - VLAN ID/PVID = 30/30
- VLAN ID/PVID port settings for 1/15:
 - 801.x disabled on port - VLAN ID/PVID = 50/50
 - Unauthenticated client on port - VLAN ID/PVID = 20/20
 - Authenticated client on port (user: PC):
 - VLAN ID/PVID = 50/50 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - VLAN ID/PVID = 300/300 (Valid RADIUS attributes received)
 - Radius Server Unreachable (801.x enabled) – VLAN ID/PVID = 30/30

Configuration example

1. Configure the RADIUS servers and VLAN settings.

```
ERS4000(config)# ip address 10.100.68.254 netmask 255.255.255.0 default-gateway
10.100.68.1
ERS4000(config)# radius-server host 10.100.68.2
ERS4000(config)# radius-server secondary-host 10.100.68.3
ERS4000(config)# radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)# vlan configcontrol automatic
ERS4000(config)# vlan create 20 type port
ERS4000(config)# vlan create 30 type port
ERS4000(config)# vlan create 50 type port
ERS4000(config)# vlan create 100 type port
ERS4000(config)# vlan create 200 type port
ERS4000(config)# vlan create 300 type port
ERS4000(config)# vlan members add 50 1/15
ERS4000(config)# vlan members add 100 2/15
```

2. Confirm the VLAN interface settings.

```
ERS4000(config)# sho vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

3. Confirm the VLAN interface VLANs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

4. 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.

```
ERS4000(config)# ping 10.100.68.2
(Host is reachable)
```

```
ERS4000(config)# ping 10.100.68.3
(Host is reachable)
```

5. Set the EAPOL status.

```
ERS4000(config)# eapol guest-vlan vid 20
ERS4000(config)# eapol guest-vlan enable
ERS4000(config)# eapol multihost fail-open-vlan vid 30
ERS4000(config)# eapol multihost fail-open-vlan enable
ERS4000(config)# interface Ethernet 1/15,2/15
ERS4000(config-if)# eapol guest-vlan enable
ERS4000(config-if)# eapol status auto
ERS4000(config-if)# exit
ERS4000(config)# eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

6. Before EAP clients are authenticated, confirm the EAPOL MultiHost status.

```
ERS4000(config)# show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
-----	-----	-----	-----	-----	-----

7. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	20	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	20	0	UntagAll	Unit 2, Port 15

8. Confirm the VLAN interface VLANs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	20	VLAN #20	-----	-----	-----	-----
2/15	20	VLAN #20	-----	-----	-----	-----

9. After EAP clients are authenticated, confirm the EAPOL MultiHost status.

```
ERS4000(config)# show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

10. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

11. Confirm the VLAN interface VLANs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

SHSA authentication mode (with Guest VLAN and Fail Open VLAN enabled) with or without RADIUS additional attributes with or without Multihost MultiVLAN

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300	-----	-----	-----	-----
2/15	200	VLAN #200	-----	-----	-----	-----

12. Disconnect both primary and back-up RADIUS servers from the network (unplug cables from server side).

13. Attempt to reach the primary and back-up RADIUS servers.

```
ERS4000(config)# ping 10.100.68.2
(Host is not reachable)
ERS4000(config)# ping 10.100.68.3
(Host is not reachable)
```

14. After approximately 3 minutes, confirm the EAPOL MultiHost status again.

```
ERS4000(config)# show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

15. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	30	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	30	0	UntagAll	Unit 2, Port 15

16. Confirm the VLAN interface VIDs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	30	VLAN #30	-----	-----	-----	-----
2/15	30	VLAN #30	-----	-----	-----	-----

17. Connect primary or back-up RADIUS server to network (plug in cables from server side). For this example, the primary RADIUS server is connected.

18. After approximately 1 minute, attempt to reach the primary RADIUS server.

```
ERS4000(config)# ping 10.100.68.2
(Host is reachable)
```

19. Confirm the EAPOL MultiHost status again.

```
ERS4000(config)# show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

20. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

21. Confirm the VLAN interface VIDs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300				
2/15	200	VLAN #200				

22. Enable EAPOL MultiHost MultiVLAN.

```
ERS4000(config)# eapol disable
ERS4000(config)# eapol multihost multivlan enable
ERS4000(config)# eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

23. After EAP clients are authenticated, confirm EAPOL MultiHost status.

```
ERS4000(config)# show eapol multihost status
```

SHSA authentication mode (with Guest VLAN and Fail Open VLAN enabled) with or without RADIUS additional attributes with or without Multihost MultiVLAN

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

24. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

25. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit2, Port 15

26. Confirm the VLAN interface VIDs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300	-----	-----	-----	-----
2/15	200	VLAN #200	-----	-----	-----	-----

Alternate configuration

The following operation applies to **SHSA authentication mode with Guest VLAN, Fail Open VLAN (Multihost MultiVLAN option enabled) without valid 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.

```
ERS4000(config)# eapol disable
ERS4000(config)# eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

2. After EAP clients are authenticated, confirm EAPOL MultiHost status.

```
ERS4000(config)# show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

3. Confirm the VLAN interface settings.

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

4. Confirm the VLAN interface VLANs.

```
ERS4000(config)# show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

MHSA authentication mode (with or without RADIUS VLAN and with or without Multihost MultiVLAN enabled)

The configuration example in this section applies to the following client port 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
- 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 authenticated client is on the port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs but no RADIUS attribute is received, or an invalid RADIUS attribute is received, for the client
- an authenticated client is on the port—the port is included in the RADIUS VLAN ID and it uses the RADIUS VLAN PVID so that valid RADIUS attributes are received for the client

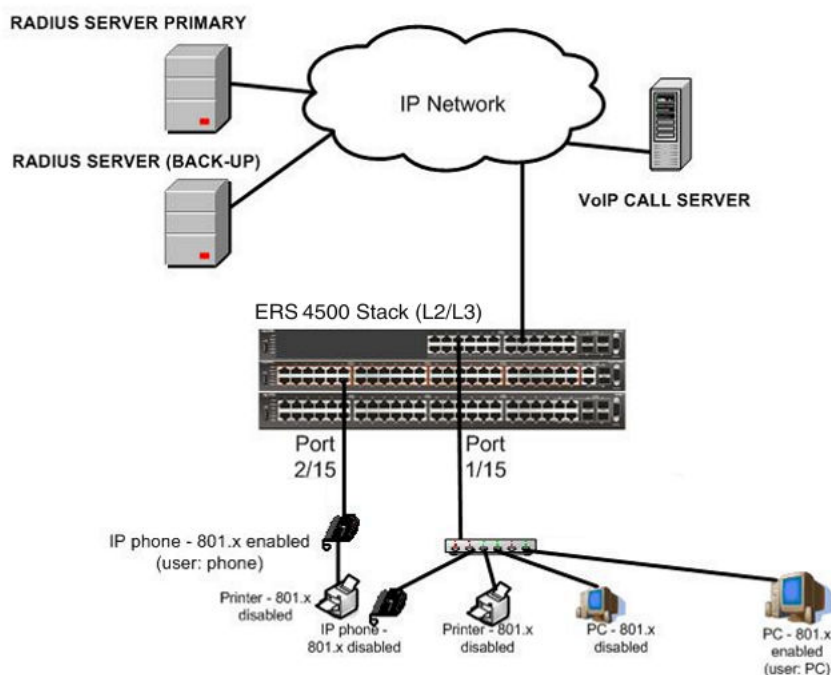


Figure 29: MHSA authentication mode (with or without RADIUS VLAN and with or without Multihost MultiVLAN enabled)

Scenario

Assume the following settings:

- Primary RADIUS server configured with two users:
 - user: phone with attribute VLAN ID: 200, Port priority: 6
 - user: PC with attribute VLAN ID: 300, Port priority: 2
- Backup RADIUS server configured with the same two users:
 - user: phone with attribute VLAN ID: 200, Port priority: 6
 - user: PC with attribute VLAN ID: 300, Port priority: 2
- Port 2/15—801.x enabled IP phone connected - (user: phone)
 - Initial VLAN ID = 100
 - RADIUS VLAN ID = 200
- Port 1/15—801.x enabled PC connected - (user: PC)
 - Initial VLAN ID = 50
 - RADIUS VLAN ID = 300
- 802.1x phone client VLAN ID/PVID port 2/15 settings:
 - 801.x disabled on port 100/100
 - Unauthenticated client on port 100/100
 - Authenticated (user: phone):
 - 100/100 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - 200/200 (Valid RADIUS attributes received)
- 802.1x PC client VLAN ID/PVID port 1/15 settings:
 - 801.x disabled on port 50/50
 - Unauthenticated client on port 50/50
 - Authenticated client on port (user: PC):
 - 50/50 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - 300/300 (Valid RADIUS attributes received)

Configuration example

1. Configure the RADIUS servers and VLAN settings

```
ERS4000(config)# ip address 10.100.68.254 netmask 255.255.255.0 default-gateway
10.100.68.1
ERS4000(config)# radius-server host 10.100.68.2
ERS4000(config)# radius-server secondary-host 10.100.68.3
ERS4000(config)# radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)# vlan configcontrol automatic
ERS4000(config)# vlan create 50 type port
ERS4000(config)# vlan create 100 type port
ERS4000(config)# vlan create 200 type port
ERS4000(config)# vlan create 300 type port
ERS4000(config)# vlan members add 50 1/15
ERS4000(config)# vlan members add 100 2/15
```

2. Confirm the VLAN interface settings

```
ERS4000(config)# sho vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

3. Confirm the VLAN interface VLANs

```
ERS4000(config)#sho vlan interface info 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

4. Confirm that you can reach the RADIUS server

```
ERS4000(config)#ping 10.100.68.2
(Host is reachable)
```

5. Set the EAPOL status

```
ERS4000(config)#interface Ethernet 1/15,2/15
ERS4000(config-if)#eapol multihost auto-non-eap-mhlsa-enable
ERS4000(config-if)#eapol multihost non-eap-mac-max 4
ERS4000(config-if)#eapol multihost enable
ERS4000(config-if)#eapol status auto
ERS4000(config-if)#exit
```

Supported EAP modes and configuration examples

```
ERS4000(config)#eapol multihost auto-non-eap-mhsa-enable  
ERS4000(config)#eapol enable
```

6. Confirm the EAPOL MultiHost status

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

```
ERS450(config)#sho eapol multihost non-eap-mac status
```

Unit/Port	Client MAC Address	State	Vid	Pri
1/15	00:1C:9C:2B:CE:04	Auto-Learned For MHSA	N/A	N/A
2/15	00:1D:3E:4A:BC:01	Auto-Learned For MHSA	N/A	N/A

Total number of authenticated clients: 2

7. Confirm the VLAN interface settings

```
ERS4000(config)# show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

8. Confirm the VLAN interface VLANs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300	-----	-----	-----	-----
2/15	200	VLAN #200	-----	-----	-----	-----

9. Enable EAPOL MultiHost MultiVLAN.

```
ERS4000(config)#eapol disable  
ERS4000(config)#eapol multihost multivlan enable  
ERS4000(config)#eapol enable
```

10. Confirm EAPOL MultiHost status.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

11. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

12. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interfcie info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

13. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 1/14,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300				
2/15	200	VLAN #200				

Alternate configuration

The following operation applies to **MHSA authentication mode (Multihost MultiVLAN enabled) without valid 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 200 with VLAN ID 123, and VLAN ID 300 with VLAN ID 124, which is not configured on the device.

1. Enable EAPOL MultiHost MultiVLAN

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol multihost multivlan enable
ERS4000(config)#eapol enable
```

2. Confirm EAPOL MultiHost status.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

Unit/Port	Client MAC Address	State	Vid	Pri
1/15	00:1C:9C:2B:CE:04	Auto-Learned For MHSA	N/A	N/A
2/15	00:1D:3E:4A:BC:01	Auto-Learned For MHSA	N/A	N/A

3. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregister ed Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit2, Port15

4. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

MHSA authentication mode (Guest VLAN option enabled) with or without RADIUS additional attributes with or without Multihost MultiVLAN

The configuration example in this section applies to the following client port settings when:

- 801.x disabled on port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs
- an unauthenticated client is on the port—the port is included in the Guest VLAN ID, and the port uses the Guest VLAN PVID
- an authenticated client is on the port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs but no RADIUS attribute is received, or an invalid RADIUS attribute is received for the client
- an authenticated client is on the port—the port is included in the RADIUS VLAN ID and it uses the RADIUS VLAN PVID so that valid RADIUS attributes are received for the client

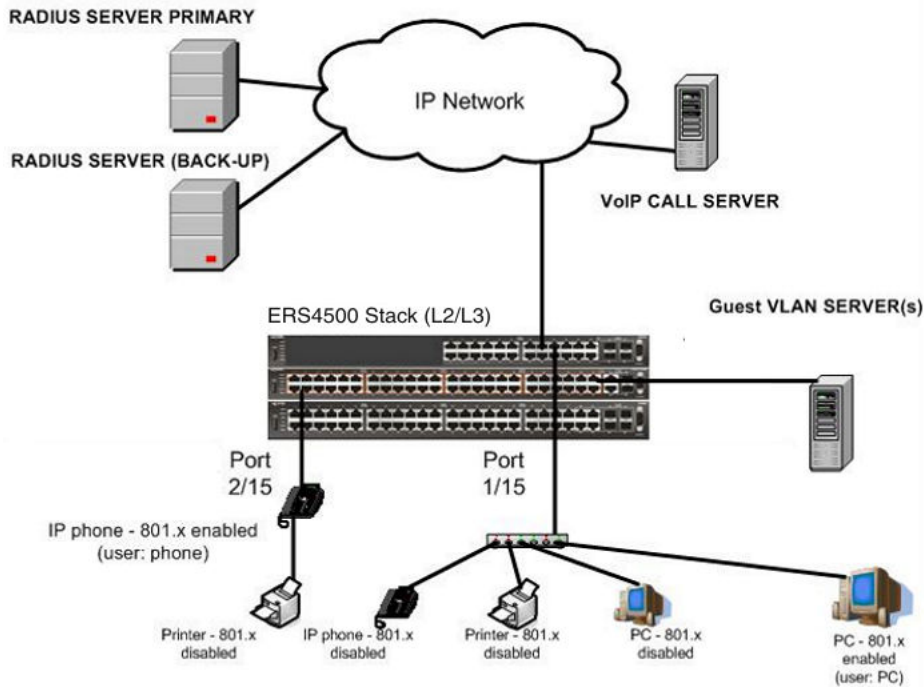


Figure 30: MHTA authentication mode (Guest VLAN option enabled) with or without RADIUS additional attributes with or without Multihost MultiVLAN

Scenario

Assume the following settings:

- Primary RADIUS server configured with two users:
 - user: phone with attribute VLAN ID: 200, Port priority: 6
 - user: PC with attribute VLAN ID: 300, Port priority: 2
- Backup RADIUS server configured with the same two users:
 - user: phone with attribute VLAN ID: 200, Port priority: 6
 - user: PC with attribute VLAN ID: 300, Port priority: 2
- Port 2/15—801.x enabled IP phone connected - (user: phone)
 - Initial VLAN ID = 100
 - Guest VLAN ID = 20
 - RADIUS VLAN ID = 200
- Port 1/15—801.x enabled PC connected - (user: PC)
 - Initial VLAN ID = 50

- Guest VLAN ID = 20
- RADIUS VLAN ID = 300
- 802.1x phone client VLAN ID/PVID port 2/15 settings:
 - 801.x disabled on port 100/100
 - Unauthenticated client on port 20/20
 - Authenticated (user: phone):
 - 100/100 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - 200/200 (Valid RADIUS attributes received)
- 802.1x PC client VLAN ID/PVID port 1/15 settings:
 - 801.x disabled on port 50/50
 - Unauthenticated client on port 20/20
 - Authenticated client on port (user: PC):
 - 50/50 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - 300/300 (Valid RADIUS attributes received)

Configuration example

1. Configure the RADIUS servers and VLAN settings

```
ERS4000(config)#ip address10.100.68.254 netmask 255.255.255.0 default-gateway
10.100.68.1
ERS4000(config)#radius-serverhost 10.100.68.2
ERS4000(config)#radius-server secondary-host 10.100.68.3
ERS4000(config)#radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)#vlan configcontrol automatic
ERS4000(config)#vlan create 20 type port
ERS4000(config)#vlan create 50 type port
ERS4000(config)#vlan create 100 type port
ERS4000(config)#vlan create 200 type port
ERS4000(config)#vlan create 300 type port
ERS4000(config)#vlan members add 50 1/15
ERS4000(config)#vlan members add 100 2/15
```

2. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interfaceinfo 1/15,2/15
```

Supported EAP modes and configuration examples

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

3. Confirm the VLAN interface VLANs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

4. Confirm that you can reach the RADIUS server.

```
ERS4000(config)#ping 10.100.68.2  
(Host is reachable)
```

5. Set the EAPOL status.

```
ERS4000(config)#eapol guest-vlanvid 20  
ERS4000(config)#eapol guest-vlan enable  
ERS4000(config)#interface Ethernet 1/15,2/15  
ERS4000(config-if)#eapol multihost auto-non-eap-mhsa-enable  
ERS4000(config-if)#eapolmultihost non-eap-mac-max 4  
ERS4000(config-if)#eapol multihost enable  
ERS4000(config-if)#eapol status auto  
ERS4000(config-if)#exit  
ERS4000(config)#eapol multihost auto-non-eap-mhsa-enable  
ERS4000(config)#eapol enable  
% Depending on your stack configuration it may take up to 4 minutes for  
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

6. Before EAP clients are authenticated, confirm the EAPOL MultiHost status

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
-----------	-----------------------	-----------	--------------------------	-----	-----

7. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	20	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	20	0	UntagAll	Unit 2, Port 15

8. Confirm the VLAN interface VLANs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	20	VLAN #20				
2/15	20	VLAN #20				

9. After EAP clients are authenticated, confirm the EAPOL MultiHost status.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

Unit/Port	Client MAC Address	State	Vid	Pri
1/15	00:1C:9C:2B:CE:04	Auto-Learned For MHSA	N/A	N/A
2/15	00:1D:3E:4A:BC:01	Auto-Learned For MHSA	N/A	N/A

10. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Supported EAP modes and configuration examples

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

11. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300				
2/15	200	VLAN #200				

12. Enable EAPOL MultiHost MultiVLAN.

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol multihost multivlan enable
ERS4000(config)#eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

13. Confirm EAPOL MultiHost status.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

Unit/Port	Client MAC Address	State	Vid	Pri
1/15	00:1C:9C:2B:CE:04	Auto-Learned For MHTSA	N/A	N/A
2/15	00:1D:3E:4A:BC:01	Auto-Learned For MHTSA	N/A	N/A

14. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

15. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300				
2/15	200	VLAN #200				

Alternate configuration

The following operation applies to **MHSA authentication mode with Guest VLAN (Multihost MultiVLAN enabled) without valid 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 200 with VLAN ID 123, and VLAN ID 300 with VLAN ID 124, which is not configured on the device.

1. Enable EAPOL MultiHost MultiVLAN.

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol multihost multivlan enable
ERS4000(config)#eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

2. Confirm EAPOL MultiHost status.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

Unit/Port	Client MAC Address	State	Vid	Pri
1/15	00:1C:9C:2B:CE:04	Auto-Learned For MHSA	N/A	N/A
2/15	00:1D:3E:4A:BC:01	Auto-Learned For MHSA	N/A	N/A

3. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregister ed Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

4. Confirm the VLAN interface VLANs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

MHSA authentication mode (Guest VLAN and Fail Open VLAN options enabled) with or without RADIUS additional attributes and with or without Multihost MultiVLAN option

The configuration example in this section applies to the following client port settings when:

- 801.x disabled on port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs
- an unauthenticated client is on the port—the port is included in the Guest VLAN ID, and the port uses the Guest VLAN PVID
- an authenticated client is on the port—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs but no RADIUS attribute is received, or an invalid RADIUS attribute is received, for the client

MHSA authentication mode (Guest VLAN and Fail Open VLAN options enabled) with or without RADIUS additional attributes and with or without Multihost MultiVLAN option

- an authenticated client is on the port—the port is included in the RADIUS VLAN ID and it uses the RADIUS VLAN PVID so that valid RADIUS attributes are received for the client
- RADIUS Server Unreachable (801.x enabled)—the port is included in the Fail Open VLAN, and the port uses the Fail Open VLAN PVID

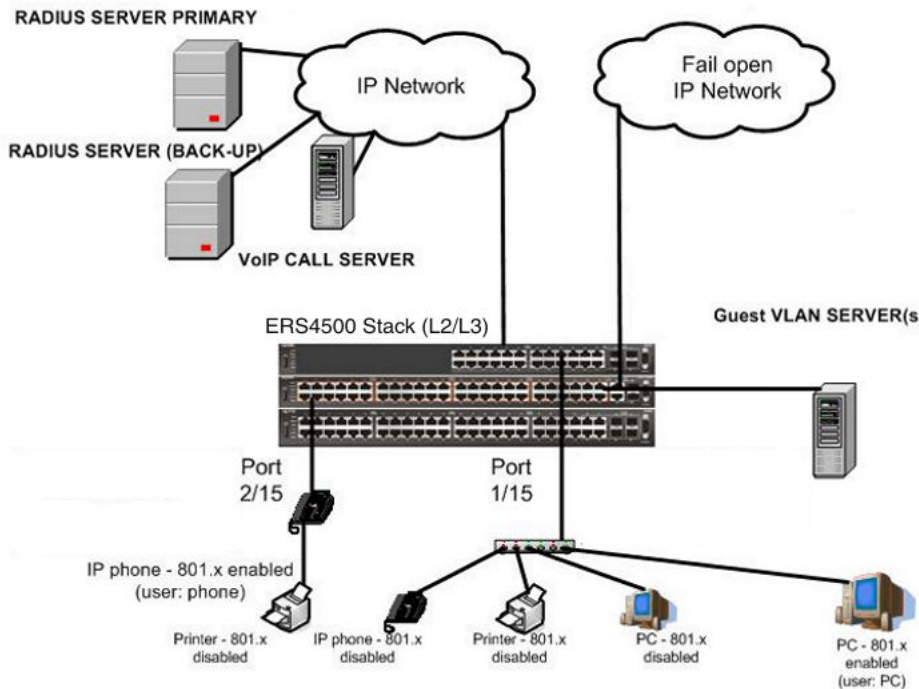


Figure 31: MSHA authentication mode (Guest VLAN and Fail Open VLAN options enabled) with or without RADIUS additional attributes and with or without Multihost MultiVLAN option

Scenario

Assume the following settings:

- Primary RADIUS server configured with two users:
 - user: phone with attribute VLAN ID: 200, Port priority: 6
 - user: PC with attribute VLAN ID: 300, Port priority: 2
- Backup RADIUS server configured with the same two users:
 - user: phone with attribute VLAN ID: 200, Port priority: 6
 - user: PC with attribute VLAN ID: 300, Port priority: 2
- Port 2/15—801.x enabled IP phone connected - (user: phone)
 - Initial VLAN ID = 100
 - Guest VLAN ID = 20

- Fail Open VLAN ID = 30
- RADIUS VLAN ID = 200
- Port 1/15—801.x enabled PC connected - (user: PC)
 - Initial VLAN ID = 50
 - Guest VLAN ID = 20
 - Fail Open VLAN ID = 30
 - RADIUS VLAN ID = 300
- 802.1x phone client VLAN ID/PVID port 2/15 settings:
 - 801.x disabled on port 100/100
 - Unauthenticated client on port 20/20
 - Authenticated (user: phone):
 - 100/100 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - 200/200 (Valid RADIUS attributes received)
 - Radius Server Unreachable (801.x enabled) – 30/30
- 802.1x PC client VLAN ID/PVID port 1/15 settings:
 - 801.x disabled on port 50/50
 - Unauthenticated client on port 20/20
 - Authenticated client on port (user: PC):
 - 50/50 (No RADIUS attribute received or Invalid RADIUS attributes received)
 - 300/300 (Valid RADIUS attributes received)
 - Radius Server Unreachable (801.x enabled) – 30/30

Configuration example

1. Configure the RADIUS servers and VLAN settings

```
ERS4000(config)#ip address 10.100.68.254 netmask 255.255.255.0 default-gateway
10.100.68.1
ERS4000(config)#radius-server host 10.100.68.2
ERS4000(config)#radius-server secondary-host 10.100.68.3
ERS4000(config)#radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)#vlan configcontrol automatic
ERS4000(config)#vlan create 20 type port
ERS4000(config)#vlan create 30 type port
ERS4000(config)#vlan create 50 type port
ERS4000(config)#vlan create 100 type port
ERS4000(config)#vlan create 200 type port
ERS4000(config)#vlan create 300 type port
```


MHSA authentication mode (Guest VLAN and Fail Open VLAN options enabled) with or without RADIUS additional attributes and with or without Multihost MultiVLAN option

```
ERS4000(config)#vlan members add 50 1/15  
ERS4000(config)#vlan members add 100 2/15
```

2. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

3. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

4. Confirm that you can reach the RADIUS server.

```
ERS4000(config)#ping 10.100.68.2  
(Host is reachable)
```

5. Set the EAPOL status.

```
ERS4000(config)#eapol guest-vlan vid 20  
ERS4000(config)#eapol guest-vlan enable  
ERS4000(config)#eapol multihost fail-open-vlan vid 30  
ERS4000(config)#eapol multihost fail-open-vlan enable  
ERS4000(config)#interface Ethernet 1/15,2/15  
ERS4000(config-if)#eapol multihost auto-non-eap-mhlsa-enable  
ERS4000(config-if)#eapol multihost non-eap-mac-max 4  
ERS4000(config-if)#eapol multihost enable  
ERS4000(config-if)#eapol status auto  
ERS4000(config-if)#exit  
ERS4000(config)#eapol multihost auto-non-eap-mhlsa-enable  
ERS4000(config)#eapol enable  
% Depending on your stack configuration it may take up to 4 minutes for  
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

6. Before EAP clients are authenticated, confirm the EAPOL MultiHost status.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri

7. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	20	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	20	0	UntagAll	Unit 2, Port 15

8. Confirm the VLAN interface VLANs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	20	VLAN #20				
2/15	20	VLAN #20				

9. After EAP clients are authenticated, confirm the EAPOL MultiHost status.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

Unit/Port	Client MAC Address	State	Vid	Pri
1/15	00:1C:9C:2B:CE:04	Auto-Learned For MHSA	N/A	N/A
2/15	00:1D:3E:4A:BC:01	Auto-Learned For MHSA	N/A	N/A

10. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

MHSA authentication mode (Guest VLAN and Fail Open VLAN options enabled) with or without RADIUS additional attributes and with or without Multihost MultiVLAN option

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

11. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300				
2/15	200	VLAN #200				

12. Disconnect both primary and back-up RADIUS servers from the network (unplug cables from server side).

13. Attempt to reach the primary and back-up RADIUS servers.

```
ERS4000(config)#ping 10.100.68.2
(Host is not reachable)
ERS4000(config)#ping 10.100.68.3
(Host is not reachable)
```

14. After approximately 3 minutes, confirm the EAPOL MultiHost status again.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri

15. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	30	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	30	0	UntagAll	Unit 2, Port 15

16. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Supported EAP modes and configuration examples

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	30	VLAN #30	-----	-----	-----	-----
2/15	30	VLAN #30	-----	-----	-----	-----

17. Connect primary or back-up RADIUS server to network (plug in cables from server side). For this example, the primary RADIUS server is connected.

18. After approximately 1 minute, attempt to reach the primary RADIUS server.

```
ERS4000(config)#ping 10.100.68.2
(Host is reachable)
```

19. Confirm the EAPOL MultiHost status again.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

20. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

21. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300	-----	-----	-----	-----
2/15	200	VLAN #200	-----	-----	-----	-----

22. Enable EAPOL MultiHost MultiVLAN.

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol multihost multivlan enable
```

MHSA authentication mode (Guest VLAN and Fail Open VLAN options enabled) with or without RADIUS additional attributes and with or without Multihost MultiVLAN option

```
ERS4000(config)#eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

23. After EAP clients are authenticated, confirm EAPOL MultiHost status.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

Unit/Port	Client MAC Address	State	Vid	Pri
1/15	00:1C:9C:2B:CE:04	Auto-Learned For MHSA	N/A	N/A
2/15	00:1D:3E:4A:BC:01	Auto-Learned For MHSA	N/A	N/A

24. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	300	2	UntagAll	Unit 1, Port 15
2/15	No	Yes	200	6	UntagAll	Unit 2, Port 15

25. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	300	VLAN #300				
2/15	200	VLAN #200				

Alternate configuration

The following operation applies to **MHSA authentication mode with Guest VLAN and Fail Open VLAN options enabled (Multihost MultiVLAN option enabled) without valid RADIUS additional 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 200 with VLAN ID 123, and VLAN ID 300 with VLAN ID 124, which is not configured on the device.

1. Enable EAPOL MultiHost MultiVLAN.

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol multihost multivlan enable
ERS4000(config)#eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

2. After EAP clients are authenticated, confirm EAPOL MultiHost status.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
1/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/15	00:1E:CA:FF:C2:94	Authenticated	Idle	N/A	N/A

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

Unit/Port	Client MAC Address	State	Vid	Pri
1/15	00:1C:9C:2B:CE:04	Auto-Learned For MHSA	N/A	N/A
2/15	00:1D:3E:4A:BC:01	Auto-Learned For MHSA	N/A	N/A

3. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 1/15,2/15
```

Unit/Port	Filter Untagged Frames	Filter Unregister ed Frames	PVID	PRI	Tagging	Name
1/15	No	Yes	50	0	UntagAll	Unit 1, Port 15
2/15	No	Yes	100	0	UntagAll	Unit 2, Port 15

4. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 1/15,2/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/15	50	VLAN #50				
2/15	100	VLAN #100				

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

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 – one or multiple initial VLANs are supported, and the port uses one of the initial VLAN PVIDs specified by the user.
- when 802.1X is enabled on the port:
 - an unauthenticated client is on the port with Guest VLAN enabled—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs
 - an 802.1X authenticated client is on the port
 - the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs. In this case no RADIUS attribute is received or an invalid RADIUS attribute is received for the client.
 - the port is included in RADIUS VLAN Id and the port uses a RADIUS VLAN PVID (Valid RADIUS attributes received)
 - an 802.1X authenticated client is on the port
 - the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs. In this case no RADIUS attribute is received, or an invalid RADIUS attribute is received for the client.
 - the port is included in RADIUS VLAN Id and the port uses a RADIUS VLAN PVID (Valid RADIUS attributes received)
 - a non-802.1X authenticated static MAC client—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs
 - a non-802.1X authenticated client is on the port using a DHCP signature—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs

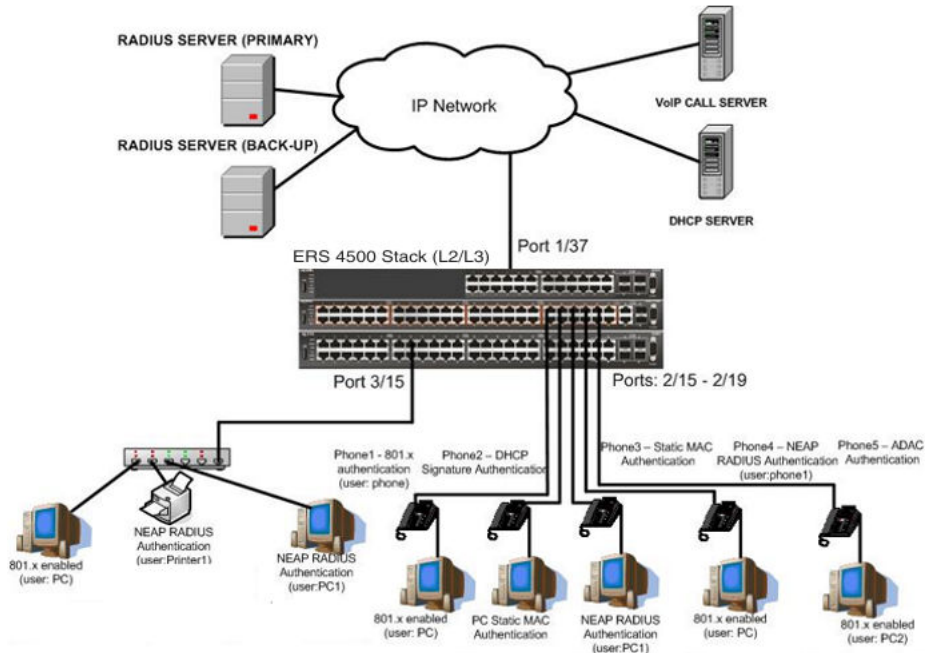


Figure 32: MHMA authentication mode (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes

Scenario

Assume the following settings:

1. RADIUS servers 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 Phone1connected
 - 801.x enabled user PC connected
 - Initial VLAN ID = 50, 200
 - PC RADIUS VLAN ID = 300
 - Port 2/16:
 - DHCP signature authenticated user Phone2 connected
 - Static MAC authenticated user PC connected

- Initial VLAN ID = 50, 200
- 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)

- 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/ 300 (Valid RADIUS attributes received)
- 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
- 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
 - 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)
- 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)

- 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)

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)

- Authenticated (user PC2 authenticated, phone is ADAC authenticated):

- VLAN ID/PVID = 50, 300, 201/ 300 (No RADIUS attribute received/Invalid RADIUS attributes received)

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)

Configuration example

1. Configure the RADIUS servers and VLAN settings

```
ERS4000(config)#ip address 10.100.68.254 netmask 255.255.255.0 default-gateway
10.100.68.1
ERS4000(config)#radius-server host 10.100.68.2
ERS4000(config)#radius-server secondary-host 10.100.68.3
ERS4000(config)#radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)#vlan configcontrol automatic
ERS4000(config)#vlan create 50 type port
ERS4000(config)#vlan create 200 type port
ERS4000(config)#vlan create 300 type port
ERS4000(config)#vlan members add 50 2/15-19,3/15
ERS4000(config)#vlan members add 100 2/15
ERS4500(config)#vlan create 201 voice-vlan
```

2. Confirm the VLAN interface settings.

```
ERS4000(config)#sho 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.

```
ERS4000(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				

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

```
ERS4000(config)#vlan configcontrol flexible
```

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

```
ERS4000(config)#vlan members add 200 2/15,2/17,2/18
ERS4000(config)#vlan members add 300 2/16
ERS4000(config)#vlan members add 300 2/19
ERS4000(config)#vlan port 2/16 pvid 300
ERS4000(config)#vlan port 2/19 pvid 300
```

6. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15,2/16,2/17,2/18
```

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

7. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15,2/16,2/17,2/18
```

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		

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.

```
ERS4000(config)#vlan ports 2/15,2/16,2/17,2/18,2/19 tagging untagpvidOnly
```

9. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15,2/16,2/17,2/18
```

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	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.

```
ERS4000(config)#show vlan interface vids 2/15,2/16,2/17,2/18
```

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).

```
ERS4000(config)#vlan members add 50,200,300 1/37
ERS4000(config)#vlan ports 1/37 tagging tagall
```

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

```
ERS4000(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.

```
ERS4000(config)#show vlan interface vids 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. Use Voice VLAN 201.

```
ERS4000(config)#interface Ethernet 2/19
ERS4000(config-if)#adac detection mac lldp
ERS4000(config-if)#adac enable
ERS4000(config-if)#exit
ERS4000(config)#adac uplink-port 1/37
ERS4000(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).

```
ERS4000(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.

```
ERS4000(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.

```
ERS4000(config)#ping 10.100.68.2
(Host is reachable)
ERS4000(config)#ping 10.100.68.3
(Host is reachable)
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/15 enable
ERS4000(config-if)#eapol port 2/15 status auto
ERS4000(config-if)#eapol multihost port 2/15 eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/15 use-radius-assigned-vlan
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/16 enable
ERS4000(config-if)#eapol port 2/16 status auto
ERS4000(config-if)#eapol multihost port 2/16 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/16 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/16 non-eap-phone-enable
ERS4000(config-if)#eapol multihost non-eap-mac port 2/16 00-19-E1-A2-4D-36
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/17 enable
ERS4000(config-if)#eapol port 2/17 status auto
ERS4000(config-if)#eapol multihost port 2/17 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/17 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/17 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/17 non-eap-use-radius-assigned- vlan
ERS4000(config-if)#eapol multihost non-eap-mac port 2/17 00-19-E1-E5-52-4A
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/18 enable
ERS4000(config-if)#eapol port 2/18 status auto
ERS4000(config-if)#eapol multihost port 2/18 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/18 non-eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/18 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/18 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/18 use-radius-assigned-vlan
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/19 enable
ERS4000(config-if)#eapol port 2/19 status auto
```

Supported EAP modes and configuration examples

```
ERS4000(config-if)#eapol multihost port 2/19 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/19 non-eap-mac-max 1
ERS4000(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.

```
ERS4000(config-if)#no eapol multihost port 2/19 use-radius-assigned-vlan
ERS4000(config-if)#no eapol multihost port 2/19 non-eap-use-radius-assigned-vlan
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 3/15 enable
ERS4000(config-if)#eapol port 3/15 status auto
ERS4000(config-if)#eapol multihost port 3/15 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 3/15 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 3/15 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 3/15 use-radius-assigned-vlan
ERS4000(config-if)#eapol multihost port 3/15 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 3/15 non-eap-use-radius-assigned- vlan
ERS4000(config-if)#exit
```

24. Set the EAPOL MultiHost status.

```
ERS4000(config)#eapol multihost voip-vlan 1 vid 200
ERS4000(config)#eapol multihost voip-vlan 1 enable
ERS4000(config)#eapol multihost allow-non-eap-enable
ERS4000(config)#eapol multihost non-eap-phone-enable
ERS4000(config)#eapol multihost non-eap-use-radius-assigned-vlan
ERS4000(config)#eapol multihost use-radius-assigned-vlan
ERS4000(config)#eapol multihost radius-non-eap-enable
ERS4000(config)#eapol enable
```

25. Enable ADAC.

```
ERS4000(config)#adac enable
```

* Note:

After ADAC is enabled (for tagged-frames and untagged-frames-advanced modes), 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.

```
ERS4000(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.

```
ERS4000(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: Port Members: 1/1,1/35,2/15-19,3/15						
200	VLAN #200	Port	None	0x0000	Yes	IVL	No
	Port Members: Port Members: 1/36,2/15-18						
201	Voice_VLAN	Port	None	0x0000	Yes	IVL	No
	Port Members: 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.

```
ERS4000(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	N/A	N/A
2/17	00:19:E1:E5:52:4A	Authenticated Locally	N/A	N/A
2/17	00:AB:CD:02:00:20	Authenticated By RADIUS	N/A	N/A
2/18	00:19:E1:E2:40:46	Authenticated By RADIUS	N/A	N/A
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	N/A	N/A
3/15	00:AB:CD:01:00:21	Authenticated By RADIUS	N/A	N/A
Total number of authenticated clients: 7				

Supported EAP modes and configuration examples

```
ERS4000(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	N/A	N/A
2/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/18	00:AB:CD:03:00:12		Idle	N/A	N/A
2/19	00:AB:CD:04:00:13	Authenticated	Idle	N/A	N/A
3/15	00:AB:CD:01:00:10	Authenticated	Idle	N/A	N/A
===== Neap Phones =====					
2/16	00:19:E1:E6:09:B1				
Total number of authenticated clients: 6					

29. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 2/16-19,3/15
```

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

30. Confirm the VLAN interface VLANs.

```
ERS4000(config)#show vlan interface vids 2/16-19,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
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 disabled) 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.

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol enable
```

2. Confirm EAPOL MultiHost status.

```
ERS4000(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	N/A	N/A
2/17	00:19:E1:E5:52:4A	Authenticated Locally	N/A	N/A
2/17	00:AB:CD:02:00:20	Authenticated By RADIUS	N/A	N/A
2/18	00:19:E1:E2:40:46	Authenticated By RADIUS	N/A	N/A
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	N/A	N/A
3/15	00:AB:CD:01:00:21	Authenticated By RADIUS	N/A	N/A
Total number of authenticated clients: 7				

```
ERS4000(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	N/A	N/A
2/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/18	00:AB:CD:03:00:12	Authenticated	Idle	N/A	N/A
2/19	00:AB:CD:04:00:13	Authenticated	Idle	N/A	N/A
3/15	00:AB:CD:01:00:10	Authenticated	Idle	N/A	N/A
===== Neap Phones =====					
2/16	00:19:E1:E6:09:B1				
Total number of authenticated clients: 6					

3. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 2/16-19,3/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
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

4. Confirm the VLAN interface settings.

```
ERS4000(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.

```
ERS4000(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	-----	-----	-----	-----

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)

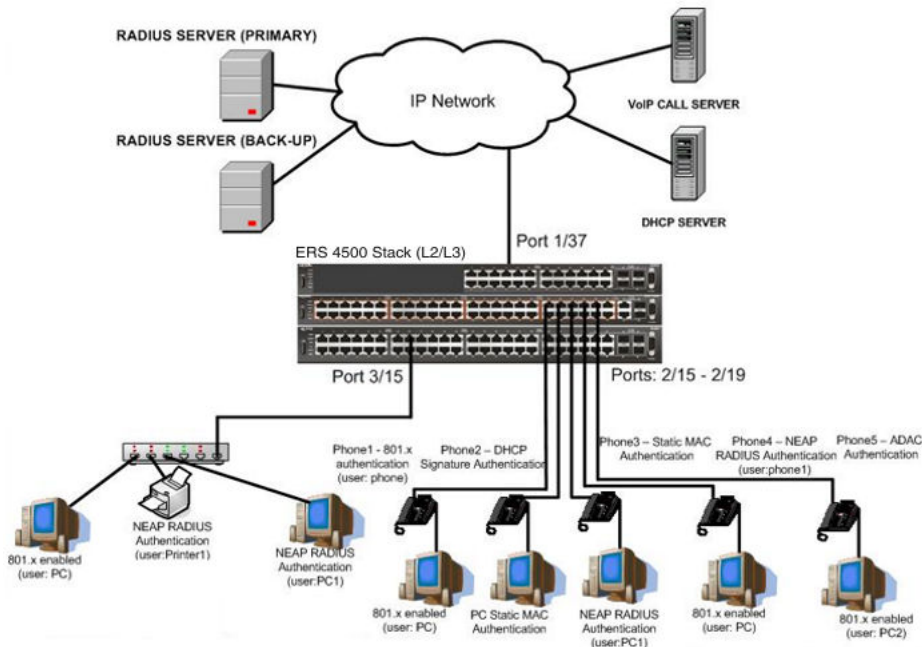


Figure 33: MHMA authentication mode (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes

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 Phone1connected
 - 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

```
ERS4000(config)#ip address 10.100.68.254 netmask 255.255.255.0 default-gateway
10.100.68.1
ERS4000(config)#radius-server host 10.100.68.2
ERS4000(config)#radius-server secondary-host 10.100.68.3
ERS4000(config)#radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)#vlan configcontrol automatic
ERS4000(config)#vlan create 50 type port
ERS4000(config)#vlan create 200 type port
ERS4000(config)#vlan create 300 type port
ERS4000(config)#vlan members add 50 2/15-19,3/15
```

2. Confirm the VLAN interface settings.

```
ERS4000(config)#sho 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 VIDs.

```
ERS4000(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				

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

```
ERS4000(config)#vlan configcontrol flexible
```

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

```
ERS4000(config)#vlan members add 200 2/15,2/17,2/18
ERS4000(config)#vlan members add 300 2/16
ERS4000(config)#vlan members add 300 2/19
ERS4000(config)#vlan port 2/16 pvid 300
ERS4000(config)#vlan port 2/19 pvid 300
```

6. Confirm the VLAN interface settings.

```
ERS4000(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.

```
ERS4000(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.

```
ERS4000(config)#vlan ports 2/15,2/16,2/17,2/18,2/19 tagging untagpvidOnly
```

9. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15,2/16,2/17,2/18,2/19
```

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.

```
ERS4000(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.

```
ERS4000(config)#vlan members add 50,200,300 1/37
ERS4000(config)#vlan ports 1/37 tagging tagall
```

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

```
ERS4000(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.

```
ERS4000(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.

```
ERS4000(config)#interface Ethernet 2/19
ERS4000(config-if)#adac detection mac lldp
ERS4000(config-if)#adac enable
ERS4000(config-if)#exit
ERS4000(config)#adac uplink-port 1/37
ERS4000(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).

```
ERS4000(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.

```
ERS4000(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.

```
ERS4000(config)#ping 10.100.68.2
(Host is reachable)

ERS4000(config)#ping 10.100.68.3
(Host is reachable)
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/15 enable
ERS4000(config-if)#eapol port 2/15 status auto
ERS4000(config-if)#eapol multihost port 2/15 eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/15 use-radius-assigned-vlan
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/16 enable
ERS4000(config-if)#eapol port 2/16 status auto
ERS4000(config-if)#eapol multihost port 2/16 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/16 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/16 non-eap-phone-enable
```

Supported EAP modes and configuration examples

```
ERS4000(config-if)#eapol multihost non-eap-mac port 2/16 00-19-E1-A2-4D-36
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/17 enable
ERS4000(config-if)#eapol port 2/17 status auto
ERS4000(config-if)#eapol multihost port 2/17 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/17 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/17 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/17 non-eap-use-radius-assigned- vlan
ERS4000(config-if)#eapol multihost non-eap-mac port 2/17 00-19-E1-E5-52-4A
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/18 enable
ERS4000(config-if)#eapol port 2/18 status auto
ERS4000(config-if)#eapol multihost port 2/18 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/18 non-eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/18 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/18 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/18 use-radius-assigned-vlan
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/19 enable
ERS4000(config-if)#eapol port 2/19 status auto
ERS4000(config-if)#eapol multihost port 2/19 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/19 non-eap-mac-max 1
ERS4000(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.

```
ERS4000(config-if)#no eapol multihost port 2/19 use-radius-assigned-vlan
ERS4000(config-if)#no eapol multihost port 2/19 non-eap-use-radius-assigned-vlan
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 3/15 enable
ERS4000(config-if)#eapol port 3/15 status auto
ERS4000(config-if)#eapol multihost port 3/15 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 3/15 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 3/15 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 3/15 use-radius-assigned-vlan
ERS4000(config-if)#eapol multihost port 3/15 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 3/15 non-eap-use-radius-assigned- vlan
ERS4000(config-if)#exit
```

24. Set the EAPOL MultiHost status.

```
ERS4000(config)#eapol multihost voip-vlan 1 vid 200
ERS4000(config)#eapol multihost voip-vlan 1 enable
ERS4000(config)#eapol multihost allow-non-eap-enable
ERS4000(config)#eapol multihost non-eap-phone-enable
ERS4000(config)#eapol multihost non-eap-use-radius-assigned-vlan
ERS4000(config)#eapol multihost use-radius-assigned-vlan
ERS4000(config)#eapol multihost radius-non-eap-enable
```

! Important:

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

```
ERS4000(config)#eapol multihost multivlan enable  
ERS4000(config)#eapol enable
```

25. Enable ADAC.

```
ERS4000(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.

```
ERS4000(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.

```
ERS4000(config)#show vlan
```


Supported EAP modes and configuration examples

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.

```
ERS4000(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				


```
ERS4000(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.

```
ERS4000(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	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.

```
ERS4000(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.

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol enable
```

2. Confirm EAPOL MultiHost status.

```
ERS4000(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	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				

```
ERS4000(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.

```
ERS4000(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	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.

```
ERS4000(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.

```
ERS4000(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	-----	-----	-----	-----

MHMA authentication mode with Guest VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes

The configuration example in this section applies to the following client port settings when:

- 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 with Guest VLAN enabled—the port is included in the Guest VLAN ID, and the port uses one of the Guest VLAN PVIDs
 - an authenticated client is on the port with Guest VLAN enabled
 - the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs but no RADIUS attribute is received, or an invalid RADIUS attribute is received, for the client
 - the port is included in RADIUS VLAN Id and the port uses a RADIUS VLAN PVID (Valid RADIUS attributes received)
 - an authenticated client is on the port with Guest VLAN enabled
 - the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs but no RADIUS attribute is received, or an invalid RADIUS attribute is received, and Static MAC is defined for the client
 - the port is included in RADIUS VLAN Id and the port uses a RADIUS VLAN PVID (Valid RADIUS attributes received)
 - an authenticated client is on the port with Guest VLAN enabled and a static defined MAC—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs
 - an authenticated client is on the port with Guest VLAN enabled and using a DHCP signature—the port is included in the initial VLAN ID, and the port uses one of the initial VLAN PVIDs

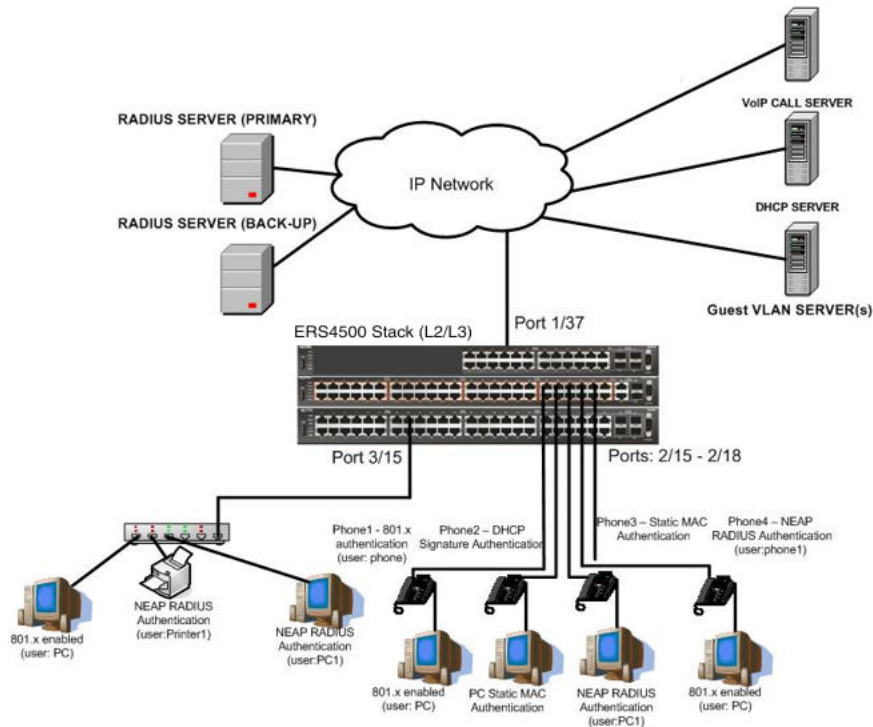


Figure 34: MHMA authentication mode with Guest VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes

Scenario

Assume the following settings:

- Primary RADIUS server configured with six users:
 - EAP user: phone with no VLAN ID radius attribute
 - EAP user: PC with attribute VLAN ID: 300
 - EAP user: PC2 with no VLAN ID radius attribute
 - RADIUS user for phone1 with no VLAN ID radius attribute
 - RADIUS user for PC1 with attribute VLAN ID: 300
 - RADIUS user for Printer1 with attribute VLAN ID: 300
- Backup RADIUS server configured with the same six users:
 - EAP user: phone with no VLAN ID radius attribute
 - EAP user: PC with attribute VLAN ID: 300
 - EAP user: PC2 with no VLAN ID radius attribute
 - RADIUS user for phone1 with no VLAN ID radius attribute

- RADIUS user for PC1 with attribute VLAN ID: 300
- RADIUS user for Printer1 with attribute VLAN ID: 300

All IP Phones are configured to send tag traffic with a VoIP VLAN ID.

- Port 2/15:
 - 801.x authenticated user Phone1connected
 - 801.x enabled user PC connected
 - Guest VLAN ID = 20
 - 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
 - Guest VLAN ID = 20
 - 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
 - Guest VLAN ID = 20
 - Initial VLAN ID = 50, 200
 - PC RADIUS VLAN ID = 300
- Port 2/18:
 - Phone4 – NEAP RADIUS Authentication (user:phone1)
 - 801.x enabled user PC connected
 - Guest VLAN ID = 20
 - Initial VLAN ID = 50, 200
 - PC RADIUS VLAN ID = 300
 - Phone RADIUS VLAN ID = none
- Port 3/15:
 - 801.x enabled user PC connected
 - NEAP RADIUS authenticated user Printer1 connected

- NEAP RADIUS authenticated user PC1 connected
- Guest VLAN ID = 20
- Initial VLAN ID = 50
- RADIUS VLAN ID = 300
- 802.1x phone client VLAN ID/PVID port 2/15 settings:
 - 801.x disabled on 50,200/50
 - Unauthenticated client with 801.x enabled on 20/20
 - Authenticated (user phone authenticated, user PC unauthenticated):
 - 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
 - Authenticated (user phone authenticated, user PC authenticated):
 - 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
 - 50, 200, 300/ 300 (Valid RADIUS attributes received)
- 802.1x PC client VLAN ID/PVID port 2/16 settings:
 - 801.x disabled on 50,300/300
 - Unauthenticated client with 801.x enabled on 20/20
 - Authenticated (Phone DHCP signature OK, EAP VOIP VLAN ID 200 assigned):
 - 50,200,300/300
 - Authenticated (PC MAC defined in static list, PC MAC learned in MAC address table, Phone DHCP signature OK):
 - 50,200,300/300
- 802.1x PC client VLAN ID/PVID port 2/17 settings:
 - 801.x disabled on 50,200/50
 - Unauthenticated client with 801.x enabled on 20/20
 - Authenticated (Phone MAC defined in static list, Phone MAC learned in MAC address table):
 - 50, 200/ 50
 - Authenticated (user PC1 authenticated; Phone MAC defined in static list, Phone MAC learned in MAC address table):
 - 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
 - 50, 200, 300/ 300 (Valid RADIUS attributes received)

802.1x PC client VLAN ID/PVID port 2/18 settings:

- 801.x disabled on 50,200/50
- Unauthenticated client with 801.x enabled on 20/20
- Authenticated (user phone1 authenticated, user PC unauthenticated):
 - 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
- Authenticated (user PC authenticated, user phone1 authenticated):
 - 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
 - 50, 200, 300/ 300 (Valid RADIUS attributes received)

802.1x PC client VLAN ID/PVID port 3/15 settings:

- 801.x disabled on 50/50
- Unauthenticated client with 801.x enabled on 20/20
- Authenticated (at least one user authenticated from : PC, PC1, Printer1):
 - 50/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
 - 300/ 300 (Valid RADIUS attributes received)

Configuration example

1. Configure the RADIUS servers and VLAN settings

```
ERS4000(config)#ip address 10.100.68.254 netmask 255.255.255.0 default-gateway
10.100.68.1
ERS4000(config)#radius-server host 10.100.68.2
ERS4000(config)#radius-server secondary-host 10.100.68.3
ERS4000(config)#radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)#vlan configcontrol automatic
ERS4000(config)#vlan create 20 type port
ERS4000(config)#vlan create 50 type port
ERS4000(config)#vlan create 200 type port
ERS4000(config)#vlan create 300 type port
ERS4000(config)#vlan members add 50 2/15-19,3/15
```

2. Confirm the VLAN interface settings.

```
ERS4000(config)#sho 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 VIDs.

```
ERS4000(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				

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

```
ERS4000(config)#vlan configcontrol flexible
```

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

```
ERS4000(config)#vlan members add 200 2/15,2/17,2/18
ERS4000(config)#vlan members add 300 2/16
ERS4000(config)#vlan port 2/16 pvid 300
```

6. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15,2/16,2/17,2/18
```

Supported EAP modes and configuration examples

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

7. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15,2/16,2/17,2/18
```

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	-----	-----

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.

```
ERS4000(config)#vlan ports 2/15,2/16,2/17,2/18 tagging untagpvidOnly
```

9. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15,2/16,2/17,2/18
```

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

10. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15,2/16,2/17,2/18
```

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	-----	-----

11. Configure the uplink port 1/37 to transport traffic from all VLANs (1,50,200,300).

```
ERS4000(config)#vlan members add 50,200,300 1/37
ERS4000(config)#vlan ports 1/37 tagging tagall
```

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

```
ERS4000(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.

```
ERS4000(config)#show vlan interface vids 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. 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.

```
ERS4000(config)#ping 10.100.68.2
(Host is reachable)
```

```
ERS4000(config)#ping 10.100.68.3
(Host is reachable)
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/15 enable
ERS4000(config-if)#eapol port 2/15 status auto
ERS4000(config-if)#eapol multihost port 2/15 eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/15 use-radius-assigned-vlan
ERS4000(config-if)#eapol guest-vlan port 2/15 enable
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/16 enable
```

Supported EAP modes and configuration examples

```
ERS4000(config-if)#eapol port 2/16 status auto
ERS4000(config-if)#eapol multihost port 2/16 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/16 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/16 non-eap-phone-enable
ERS4000(config-if)#eapol multihost non-eap-mac port 2/16 00-19-E1-A2-4D-36
ERS4000(config-if)#eapol guest-vlan port 2/16 enable
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/17 enable
ERS4000(config-if)#eapol port 2/17 status auto
ERS4000(config-if)#eapol multihost port 2/17 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/17 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/17 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/17 non-eap-use-radius-assigned- vlan
ERS4000(config-if)#eapol multihost non-eap-mac port 2/17 00-19-E1-E5-52-4A
ERS4000(config-if)#eapol guest-vlan port 2/17 enable
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/18 enable
ERS4000(config-if)#eapol port 2/18 status auto
ERS4000(config-if)#eapol multihost port 2/18 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/18 non-eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/18 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/18 use-radius-assigned-vlan
ERS4000(config-if)#eapol guest-vlan port 2/18 enable
ERS4000(config-if)#exit
```

19. Set the EAPOL status for port 3/15.

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 3/15 enable
ERS4000(config-if)#eapol port 3/15 status auto
ERS4000(config-if)#eapol multihost port 3/15 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 3/15 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 3/15 use-radius-assigned-vlan
ERS4000(config-if)#eapol multihost port 3/15 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 3/15 non-eap-use-radius-assigned- vlan
ERS4000(config-if)#eapol guest-vlan port 3/15 enable
ERS4000(config-if)#exit
```

20. Set the Guest VLAN

```
ERS4000(config)#eapol guest-vlan vid 20
ERS4000(config)#eapol guest-vlan enable
```

21. Set the EAPOL MultiHost status.

```
ERS4000(config)#eapol multihost voip-vlan 1 vid 200
ERS4000(config)#eapol multihost voip-vlan 1 enable
ERS4000(config)#eapol multihost allow-non-eap-enable
ERS4000(config)#eapol multihost non-eap-phone-enable
ERS4000(config)#eapol multihost non-eap-use-radius-assigned-vlan
ERS4000(config)#eapol multihost use-radius-assigned-vlan
ERS4000(config)#eapol multihost radius-non-eap-enable
```

22. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 2/15-18,3/15
```

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	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
3/15	No	Yes	50	0	UntagAll	Unit 3, Port 15

23. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	50	VLAN #50	200	VLAN #200	-----	-----
2/16	50	VLAN #50	300	VLAN #300	-----	-----
2/17	50	VLAN #50	200	VLAN #200	-----	-----
2/18	50	VLAN #50	200	VLAN #200	-----	-----
3/15	50	VLAN #50	-----	-----	-----	-----

24. Enable EAPOL globally.

```
ERS4000(config)#eapol enable
```

```
% Depending on your stack configuration it may take up to 4 minutes for  
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

Before any clients authenticate on ports:

25. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15-18,3/15
```

Supported EAP modes and configuration examples

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	20	0	UntagPvid Only	Unit 2, Port 15
2/16	No	Yes	20	0	UntagPvid Only	Unit 2, Port 16
2/17	No	Yes	20	0	UntagPvid Only	Unit 2, Port 17
2/18	No	Yes	20	0	UntagPvid Only	Unit 2, Port 18
3/15	No	Yes	20	0	UntagAll	Unit 3, Port 15

26. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	20	VLAN #20	-----	-----	-----	-----
2/16	20	VLAN #20	-----	-----	-----	-----
2/17	20	VLAN #20	-----	-----	-----	-----
2/18	20	VLAN #20	-----	-----	-----	-----
3/15	20	VLAN #20	-----	-----	-----	-----

After all clients authenticate on ports:

27. Confirm the EAPOL MultiHost status.

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

MHMA authentication mode with Guest VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes

Unit/Port	Client MAC Address	State	Vid	Pri
2/16	00:19:E1:A2:4D:36	Authenticated Locally	N/A	N/A
2/17	00:19:E1:E5:52:4A	Authenticated Locally	N/A	N/A
2/17	00:AB:CD:02:00:20	Authenticated By RADIUS	N/A	N/A
2/18	00:19:E1:E2:40:46	Authenticated By RADIUS	N/A	N/A
3/15	00:AB:CD:01:00:20	Authenticated By RADIUS	N/A	N/A
3/15	00:AB:CD:01:00:21	Authenticated By RADIUS	N/A	N/A

Total number of authenticated clients: 6

ERS4000(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	N/A	N/A
2/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/18	00:AB:CD:03:00:12		Idle	N/A	N/A
3/15	00:AB:CD:01:00:10	Authenticated	Idle	N/A	N/A
===== Neap Phones =====					
2/16	00:19:E1:E6:09:B1				

Total number of authenticated clients: 5

28. Confirm the VLAN interface settings.

ERS4000(config)#sho vlan interface info 2/15-18,3/15

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

29. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

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
3/15	50	VLAN #50	300	VLAN #300	-----	-----

Alternate configuration

The following operation applies to **MHMA authentication mode with Guest VLAN (Multihost MultiVLAN option disabled) 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.

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

2. Confirm EAPOL MultiHost status.

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```


MHMA authentication mode with Guest VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes

Unit/Port	Client MAC Address	State	Vid	Pri
2/16	00:19:E1:A2:4D:36	Authenticated Locally	N/A	N/A
2/17	00:19:E1:E5:52:4A	Authenticated Locally	N/A	N/A
2/17	00:AB:CD:02:00:20	Authenticated By RADIUS	N/A	N/A
2/18	00:19:E1:E2:40:46	Authenticated By RADIUS	N/A	N/A
3/15	00:AB:CD:01:00:20	Authenticated By RADIUS	N/A	N/A
3/15	00:AB:CD:01:00:21	Authenticated By RADIUS	N/A	N/A
Total number of authenticated clients: 6				

ERS4000(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	N/A	N/A
2/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/18	00:AB:CD:03:00:12	Authenticated	Idle	N/A	N/A
3/15	00:AB:CD:01:00:10	Authenticated	Idle	N/A	N/A
===== Neap Phones =====					
2/16	00:19:E1:E6:09:B1				
Total number of authenticated clients: 5					

3. Confirm the VLAN interface settings.

ERS4000(config)#show vlan interface info 2/15-18,3/15

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	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
3/15	No	Yes	50	0	UntagAll	Unit 3, Port 15

4. Confirm the VLAN interface VIDs.

ERS4000(config)#show vlan interface vids 2/15-18,3/15

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		
3/15	50	VLAN #50				

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

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 an initial VLAN – one or multiple initial VLANs are supported, and the port uses one of the initial VLAN PVIDs specified by the user
- when 802.1X is enabled on the port:
 - an unauthenticated client is on the port with Guest VLAN enabled—the port is included only in the Guest VLAN ID, and the port uses the Guest VLAN PVID
 - an authenticated 801.x client is on the port with Guest VLAN enabled
 - the port is added to an initial VLAN and port PVID is the Guest 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 the RADIUS VLAN and the port PVID is the Guest VLAN PVID - the client PVID is set to the RADIUS VLAN PVID (Valid RADIUS attributes received for 801.x client)
 - an authenticated non-801.x client is on the port with Guest VLAN enabled
 - the port is added to an initial VLAN, and the port PVID is the Guest 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 Guest VLAN PVID - the client PVID is set to the 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 with Guest VLAN enabled (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 Guest VLAN PVID - the client uses the initial VLAN PVIDs (client traffic can be sent in multiple initial VLANs)
- an authenticated non-801.x client is on the port with Guest VLAN enabled and using a DHCP signature—the port remains in the Guest VLAN, and the port uses the Guest VLAN PVID - the DHCP client uses the first VOIP VLAN PVIDs (DHCP client traffic cannot be sent in multiple VOIP VLANs, only the first VOIP VLAN defined is used)

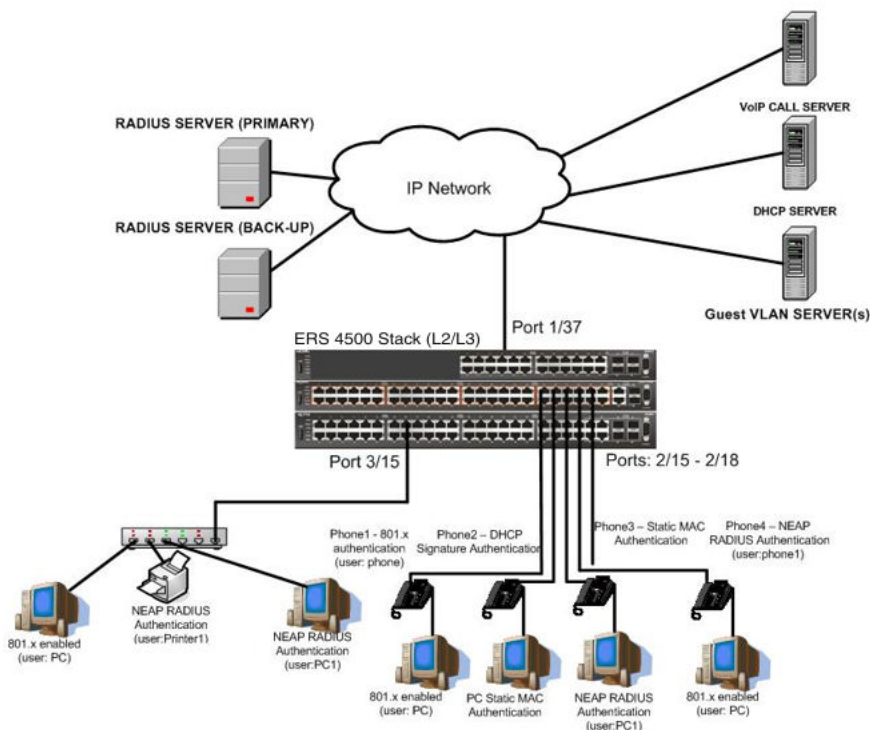


Figure 35: MHMA authentication mode with Guest VLAN (Multihost MultiVLAN option enabled) with or without additional RADIUS attributes

Scenario

Assume the following settings:

1. RADIUS server(s) configurations.
 - 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 Phone1connected
 - 801.x enabled user PC connected
 - Guest VLAN ID = 20
 - 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
 - Guest VLAN ID = 20
 - 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
 - Guest VLAN ID = 20
 - Initial VLAN ID = 50, 200
 - PC RADIUS VLAN ID = 300
- Port 2/18:
 - Phone4 – NEAP RADIUS Authentication (user:phone1)
 - 801.x enabled user PC connected
 - Guest VLAN ID = 20
 - Initial VLAN ID = 50, 200
 - PC RADIUS VLAN ID = 300
 - Phone RADIUS VLAN ID = none
- Port 3/15:
 - 801.x enabled user PC connected
 - NEAP RADIUS authenticated user Printer1 connected
 - NEAP RADIUS authenticated user PC1 connected
 - Guest VLAN ID = 20

- 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 = 20/20
 - Authenticated (user phone authenticated, user PC unauthenticated):
 - VLAN ID/PVID = 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
 - 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/ 300 (Valid RADIUS attributes received)
- 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 = 20/20
 - 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
- 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 = 20/20
 - Authenticated (Phone MAC defined in static list, Phone MAC learned in MAC address table):
 - VLAN ID/PVID = 50, 200/ 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)

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 = 20/20
- Authenticated (user phone1 authenticated, user PC unauthenticated):
 - VLAN ID/PVID = 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
- 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)

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 = 20/20
- 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)

Configuration example

1. Configure the RADIUS servers and VLAN settings

```
ERS4000(config)#ip address 10.100.68.254 netmask 255.255.255.0 default-gateway
10.100.68.1
ERS4000(config)#radius-server host 10.100.68.2
ERS4000(config)#radius-server secondary-host 10.100.68.3
ERS4000(config)#radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)#vlan configcontrol automatic
ERS4000(config)#vlan create 20 type port
ERS4000(config)#vlan create 50 type port
ERS4000(config)#vlan create 200 type port
ERS4000(config)#vlan create 300 type port
ERS4000(config)#vlan members add 50 2/15-19,3/15
```

2. Confirm the VLAN interface settings.

```
ERS4000(config)#sho 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 VIDs.

```
ERS4000(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				

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

```
ERS4000(config)#vlan configcontrol flexible
```

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

```
ERS4000(config)#vlan members add 200 2/15,2/17,2/18
ERS4000(config)#vlan members add 300 2/16
ERS4000(config)#vlan port 2/16 pvid 300
```

6. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15,2/16,2/17,2/18
```


Supported EAP modes and configuration examples

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

7. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15,2/16,2/17,2/18
```

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	-----	-----

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.

```
ERS4000(config)#vlan ports 2/15,2/16,2/17,2/18 tagging untagpvidOnly
```

9. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15,2/16,2/17,2/18
```

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

10. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15,2/16,2/17,2/18
```


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

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	-----	-----

11. Configure the uplink port 1/37 to transport traffic from all VLANs (1,50,200,300).

```
ERS4000(config)#vlan members add 50,200,300 1/37
ERS4000(config)#vlan ports 1/37 tagging tagall
```

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

```
ERS4000(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.

```
ERS4000(config)#show vlan interface vids 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. 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.

```
ERS4000(config)#ping 10.100.68.2
(Host is reachable)
ERS4000(config)#ping 10.100.68.3
(Host is reachable)
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/15 enable
ERS4000(config-if)#eapol port 2/15 status auto
ERS4000(config-if)#eapol multihost port 2/15 eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/15 use-radius-assigned-vlan
ERS4000(config-if)#eapol guest-vlan port 2/15 enable
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/16 enable
ERS4000(config-if)#eapol port 2/16 status auto
ERS4000(config-if)#eapol multihost port 2/16 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/16 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/16 non-eap-phone-enable
ERS4000(config-if)#eapol multihost non-eap-mac port 2/16 00-19-E1-A2-4D-36
ERS4000(config-if)#eapol guest-vlan port 2/16 enable
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/17 enable
ERS4000(config-if)#eapol port 2/17 status auto
ERS4000(config-if)#eapol multihost port 2/17 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/17 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/17 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/17 non-eap-use-radius-assigned- vlan
ERS4000(config-if)#eapol multihost non-eap-mac port 2/17 00-19-E1-E5-52-4A
ERS4000(config-if)#eapol guest-vlan port 2/17 enable
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/18 enable
ERS4000(config-if)#eapol port 2/18 status auto
ERS4000(config-if)#eapol multihost port 2/18 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/18 non-eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/18 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/18 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/18 use-radius-assigned-vlan
ERS4000(config-if)#eapol guest-vlan port 2/18 enable
ERS4000(config-if)#exit
```

19. Set the EAPOL status for port 3/15.

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 3/15 enable
ERS4000(config-if)#eapol port 3/15 status auto
ERS4000(config-if)#eapol multihost port 3/15 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 3/15 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 3/15 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 3/15 use-radius-assigned-vlan
ERS4000(config-if)#eapol multihost port 3/15 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 3/15 non-eap-use-radius-assigned- vlan
ERS4000(config-if)#eapol guest-vlan port 3/15 enable
ERS4000(config-if)#exit
```

20. Set the Guest VLAN.

```
ERS4000(config)#eapol guest-vlan vid 20
ERS4000(config)#eapol guest-vlan enable
```

21. Set the EAPOL MultiHost status.

```
ERS4000(config)#eapol multihost multivlan enable
ERS4000(config)#eapol multihost voip-vlan 1 vid 200
ERS4000(config)#eapol multihost voip-vlan 1 enable
ERS4000(config)#eapol multihost allow-non-eap-enable
ERS4000(config)#eapol multihost non-eap-phone-enable
ERS4000(config)#eapol multihost non-eap-use-radius-assigned-vlan
```

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

```
ERS4000(config)#eapol multihost use-radius-assigned-vlan  
ERS4000(config)#eapol multihost radius-non-eap-enable
```

22. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 2/15-18,3/15
```

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	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
3/15	No	Yes	50	0	UntagAll	Unit 3, Port 15

23. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	50	VLAN #50	200	VLAN #200	-----	-----
2/16	50	VLAN #50	300	VLAN #300	-----	-----
2/17	50	VLAN #50	200	VLAN #200	-----	-----
2/18	50	VLAN #50	200	VLAN #200	-----	-----
3/15	50	VLAN #50	-----	-----	-----	-----

24. Enable EAPOL globally.

```
ERS4000(config)#eapol enable  
% Depending on your stack configuration it may take up to 4 minutes for  
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

Before any clients authenticate on ports:

25. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15-18,3/15
```

Supported EAP modes and configuration examples

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	20	0	UntagPvid Only	Unit 2, Port 15
2/16	No	Yes	20	0	UntagPvid Only	Unit 2, Port 16
2/17	No	Yes	20	0	UntagPvid Only	Unit 2, Port 17
2/18	No	Yes	20	0	UntagPvid Only	Unit 2, Port 18
3/15	No	Yes	20	0	UntagAll	Unit 3, Port 15

26. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	20	VLAN #20	-----	-----	-----	-----
2/16	20	VLAN #20	-----	-----	-----	-----
2/17	20	VLAN #20	-----	-----	-----	-----
2/18	20	VLAN #20	-----	-----	-----	-----
3/15	20	VLAN #20	-----	-----	-----	-----

After all clients authenticate on ports:

27. Confirm the EAPOL MultiHost status.

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

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

Unit/Port	Client MAC Address	State	Vid	Pri
2/16	00:19:E1:A2:4D:36	Authenticated Locally	300	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
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: 6				

ERS4000(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	2
2/18	00:AB:CD:03:00:12		Idle	300	3
3/15	00:AB:CD:01:00:10	Authenticated	Idle	300	2
===== Neap Phones =====					
2/16	00:19:E1:E6:09:B1				
Total number of authenticated clients: 5					

All Guest VLAN enabled ports will service unauthenticated clients (new clients or old clients failing authentication) with Guest VLAN access even if authenticated clients are present on the same port. This behavior is different from MHMA mode with Guest VLAN having Multihost MultiVLAN option disabled, where Guest VLAN was available only until the first client is authenticated on the port.

28. Confirm the VLAN interface settings.

ERS4000(config)#sho vlan interface info 2/15-18,3/15

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	20	0	UntagPvid Only	Unit 2, Port 15
2/16	No	Yes	20	0	UntagPvid Only	Unit 2, Port 16
2/17	No	Yes	20	0	UntagPvid Only	Unit 2, Port 17
2/18	No	Yes	20	0	UntagPvid Only	Unit 2, Port 18
3/15	No	Yes	20	0	UntagAll	Unit 3, Port 15

29. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	20 300	VLAN #20 VLAN #300	50	VLAN #50	200	VLAN #200
2/16	20	VLAN #20	200	VLAN #200	300	VLAN #300
2/17	20 300	VLAN #20 VLAN #300	50	VLAN #50	200	VLAN #200
2/18	20 300	VLAN #20 VLAN #300	50	VLAN #50	200	VLAN #200
3/15	20	VLAN #20	50	VLAN #50	300	VLAN #300

Alternate configuration

The following operation applies to the **MHMA authentication mode with Guest VLAN (Multihost MultiVLAN option enabled) without valid additional RADIUS attributes** configuration example, 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.

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

2. Confirm EAPOL MultiHost status.

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```


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

Unit/Port	Client MAC Address	State	Vid	Pri
2/16	00:19:E1:A2:4D:36	Authenticated Locally	300	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
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: 6				

ERS4000(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
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: 5					

3. Confirm the VLAN interface settings.

ERS4000(config)#show vlan interface info 2/15-18,3/15

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	20	0	UntagPvid Only	Unit 2, Port 15
2/16	No	Yes	20	0	UntagPvid Only	Unit 2, Port 16
2/17	No	Yes	20	0	UntagPvid Only	Unit 2, Port 17
2/18	No	Yes	20	0	UntagPvid Only	Unit 2, Port 18
3/15	No	Yes	20	0	UntagAll	Unit 3, Port 15

4. Confirm the VLAN interface VIDs.

ERS4000(config)#show vlan interface vids 2/15-18,3/15

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	20	VLAN #20	50	VLAN #50	200	VLAN #200
2/16	20	VLAN #20	200	VLAN #200	300	VLAN #300
2/17	20	VLAN #20	50	VLAN 50	200	VLAN #200
2/18	20	VLAN #20	50	VLAN 50	200	VLAN #200
3/15	20	VLAN #20	50	VLAN 50	-----	-----

MHMA authentication mode with Guest VLAN and Fail Open VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes

! Important:

The Ethernet Routing Switch 4000 does not support Multihost MultiVLAN in combination with Fail Open VLAN for software release 5.4.

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 an initial VLAN – one or multiple initial VLANs are supported and the port uses one of the initial VLAN PVIDs specified by the user
- when 802.1X is enabled on the port:
 - an unauthenticated client is on the port with Guest VLAN enabled—the port is included in the Guest VLAN ID and the port uses one of the Guest VLAN PVIDs
 - an authenticated 801.x client is on the port with Guest VLAN enabled
 - the port is added to an initial VLAN and uses one of the initial VLAN PVIDs (port is removed from Guest VLAN). In this case no RADIUS attribute is received, or an invalid RADIUS attribute is received, for the client.

MHMA authentication mode with Guest VLAN and Fail Open VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes

- the port is moved to the RADIUS VLAN (port is removed from Guest VLAN) and the port uses a RADIUS VLAN PVID (Valid RADIUS attributes received).
- a non-801.x authenticated client is on the port with Guest VLAN enabled
 - the port is added to an initial VLAN (port is removed from Guest VLAN), and the port uses one of the initial VLAN PVIDs. In this case no RADIUS attribute is received, or an invalid RADIUS attribute is received for the client.
 - the port is moved to the RADIUS VLAN and the port uses a RADIUS VLAN PVID (Valid RADIUS attributes received).
- an authenticated non-801.x client is on the port with Guest VLAN enabled and a non-801.x static MAC client defined MAC—the port is included in an initial VLAN (port is removed from Guest VLAN), and the port uses one of the initial VLAN PVIDs
- an authenticated non-801.x DHCP client is on the port with Guest VLAN enabled and using a DHCP signature—the port remains in the Guest VLAN and the port uses the Guest VLAN PVID. The port is member of any EAP VOIP VLANs that have been created.
- RADIUS Server Unreachable (801.x enabled)—the port is moved to the Fail Open VLAN (port is removed from Guest VLAN), and the port uses the Fail Open VLAN PVID.

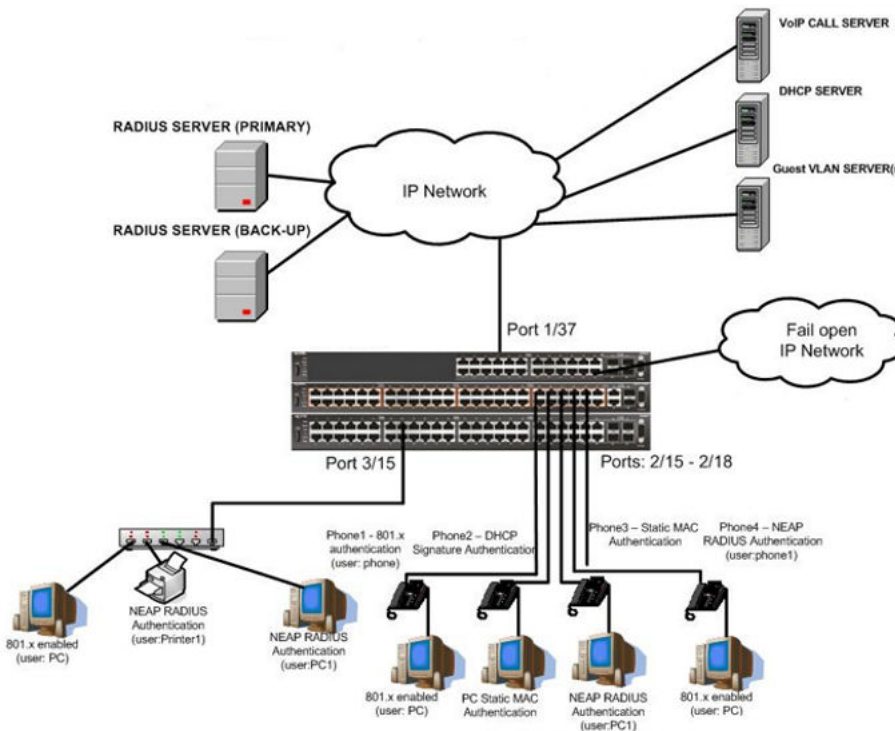


Figure 36: MHMA authentication mode with Guest VLAN and Fail Open VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes

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 Phone1connected
 - 801.x enabled user PC connected
 - Guest VLAN ID = 20
 - Fail Open VLAN ID = 30
 - 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
 - Guest VLAN ID = 20
 - Fail Open VLAN ID = 30
 - 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
 - Guest VLAN ID = 20
 - Fail Open VLAN ID = 30
 - Initial VLAN ID = 50, 200
 - PC RADIUS VLAN ID = 300

- Port 2/18:
 - Phone4 – NEAP RADIUS Authentication (user:phone1)
 - 801.x enabled user PC connected
 - Guest VLAN ID = 20
 - Fail Open VLAN ID = 30
 - Initial VLAN ID = 50, 200
 - PC RADIUS VLAN ID = 300
 - Phone RADIUS VLAN ID = none
- Port 3/15:
 - 801.x enabled user PC connected
 - NEAP RADIUS authenticated user Printer1 connected
 - NEAP RADIUS authenticated user PC1 connected
 - Guest VLAN ID = 20
 - Fail Open VLAN ID = 30
 - 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 = 20/20
 - Authenticated (user phone authenticated, user PC unauthenticated):
 - VLAN ID/PVID = 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
 - 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/ 300 (Valid RADIUS attributes received)
 - RADIUS Server Unreachable (801.x enabled) - VLAN ID/PVID = 30/30
- 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 = 20/20

- 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
- RADIUS Server Unreachable (801.x enabled) - VLAN ID/PVID = 30/30
- 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 = 20/20
 - Authenticated (Phone MAC defined in static list, Phone MAC learned in MAC address table):
 - VLAN ID/PVID = 50, 200/ 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)
 - RADIUS Server Unreachable (801.x enabled) - VLAN ID/PVID = 30/30
- 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 = 20/20
 - Authenticated (user phone1 authenticated, user PC unauthenticated):
 - VLAN ID/PVID = 50, 200/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
 - 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)
 - RADIUS Server Unreachable (801.x enabled) - VLAN ID/PVID = 30/30
- 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 = 20/20
- 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)
- RADIUS Server Unreachable (801.x enabled) - VLAN ID/PVID = 30/30

Configuration example

1. Configure the RADIUS servers and VLAN settings

```
ERS4000(config)#ip address 10.100.68.254 netmask 255.255.255.0 default-gateway 10.100.68.1
ERS4000(config)#radius-server host 10.100.68.2
ERS4000(config)#radius-server secondary-host 10.100.68.3
ERS4000(config)#radius-server key
Enter key: RadiusKey
Enter key: RadiusKey
ERS4000(config)#vlan configcontrol automatic
ERS4000(config)#vlan create 20 type port
ERS4000(config)#vlan create 30 type port
ERS4000(config)#vlan create 50 type port
ERS4000(config)#vlan create 200 type port
ERS4000(config)#vlan create 300 type port
ERS4000(config)#vlan members add 50 2/15-19,3/15
```

2. Confirm the VLAN interface settings.

```
ERS4000(config)#sho 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 VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-19,3/15
```

Supported EAP modes and configuration examples

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	-----	-----	-----	-----

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

```
ERS4000(config)#vlan configcontrol flexible
```

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

```
ERS4000(config)#vlan members add 200 2/15,2/17,2/18
ERS4000(config)#vlan members add 300 2/16
ERS4000(config)#vlan port 2/16 pvid 300
```

6. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15,2/16,2/17,2/18
```

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

7. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15,2/16,2/17,2/18
```

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	-----	-----

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.

```
ERS4000(config)#vlan ports 2/15,2/16,2/17,2/18 tagging untagpvidOnly
```

9. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15,2/16,2/17,2/18
```

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

10. Confirm the VLAN interface VLANs.

```
ERS4000(config)#show vlan interface vids 2/15,2/16,2/17,2/18
```

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	-----	-----

11. Configure the uplink port 1/37 to transport traffic from all VLANs (50,200,300).

```
ERS4000(config)#vlan members add 50,200,300 1/37
ERS4000(config)#vlan ports 1/37 tagging tagall
```

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

```
ERS4000(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 VLANs for uplink port 1/37.

```
ERS4000(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. 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.

```
ERS4000(config)#ping 10.100.68.2
(Host is reachable)
```

```
ERS4000(config)#ping 10.100.68.3
(Host is reachable)
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/15 enable
ERS4000(config-if)#eapol port 2/15 status auto
ERS4000(config-if)#eapol multihost port 2/15 eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/15 use-radius-assigned-vlan
ERS4000(config-if)#eapol guest-vlan port 2/15 enable
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/16 enable
ERS4000(config-if)#eapol port 2/16 status auto
ERS4000(config-if)#eapol multihost port 2/16 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/16 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/16 non-eap-phone-enable
ERS4000(config-if)#eapol multihost non-eap-mac port 2/16 00-19-E1-A2-4D-36
ERS4000(config-if)#eapol guest-vlan port 2/16 enable
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/17 enable
ERS4000(config-if)#eapol port 2/17 status auto
ERS4000(config-if)#eapol multihost port 2/17 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 2/17 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/17 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/17 non-eap-use-radius-assigned- vlan
ERS4000(config-if)#eapol multihost non-eap-mac port 2/17 00-19-E1-E5-52-4A
ERS4000(config-if)#eapol guest-vlan port 2/17 enable
ERS4000(config-if)#exit
```

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

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 2/18 enable
ERS4000(config-if)#eapol port 2/18 status auto
ERS4000(config-if)#eapol multihost port 2/18 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/18 non-eap-mac-max 1
ERS4000(config-if)#eapol multihost port 2/18 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/18 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 2/18 use-radius-assigned-vlan
```



```
ERS4000(config-if)#eapol guest-vlan port 2/18 enable
ERS4000(config-if)#exit
```

19. Set the EAPOL status for port 3/15.

```
ERS4000(config)#interface Ethernet all
ERS4000(config-if)#eapol multihost port 3/15 enable
ERS4000(config-if)#eapol multihost port 3/15 status auto
ERS4000(config-if)#eapol multihost port 3/15 eap-mac-max 1
ERS4000(config-if)#eapol multihost port 3/15 non-eap-mac-max 2
ERS4000(config-if)#eapol multihost port 3/15 allow-non-eap-enable
ERS4000(config-if)#eapol multihost port 3/15 use-radius-assigned-vlan
ERS4000(config-if)#eapol multihost port 3/15 radius-non-eap-enable
ERS4000(config-if)#eapol multihost port 3/15 non-eap-use-radius-assigned- vlan
ERS4000(config-if)#eapol guest-vlan port 3/15 enable
ERS4000(config-if)#exit
```

20. Set the Guest VLAN and Fail Open VLAN.

```
ERS4000(config)#eapol guest-vlan vid 20
ERS4000(config)#eapol guest-vlan enable
ERS4000(config)#eapol multihost fail-open-vlan vid 30
ERS4000(config)#eapol multihost fail-open-vlan enable
```

21. Set the EAPOL MultiHost status.

```
ERS4000(config)#eapol multihost voip-vlan 1 vid 200
ERS4000(config)#eapol multihost voip-vlan 1 enable
ERS4000(config)#eapol multihost allow-non-eap-enable
ERS4000(config)#eapol multihost non-eap-phone-enable
ERS4000(config)#eapol multihost non-eap-use-radius-assigned-vlan
ERS4000(config)#eapol multihost use-radius-assigned-vlan
ERS4000(config)#eapol multihost radius-non-eap-enable
```

22. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 2/15-18,3/15
```

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	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
3/15	No	Yes	50	0	UntagAll	Unit 3, Port 15

23. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

Supported EAP modes and configuration examples

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	-----	-----
3/15	50	VLAN #50	-----	-----	-----	-----

24. Enable EAPOL globally.

```
ERS4000(config)#eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

25. Confirm the VLAN interface settings.

```
ERS4000(config)#sho vlan interface info 2/15-18,3/15
```

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
2/15	No	Yes	20	0	UntagPvid Only	Unit 2, Port 15
2/16	No	Yes	20	0	UntagPvid Only	Unit 2, Port 16
2/17	No	Yes	20	0	UntagPvid Only	Unit 2, Port 17
2/18	No	Yes	20	0	UntagPvid Only	Unit 2, Port 18
3/15	No	Yes	20	0	UntagAll	Unit 3, Port 15

26. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
2/15	20	VLAN #20	-----	-----	-----	-----
2/16	20	VLAN #20	-----	-----	-----	-----
2/17	20	VLAN #20	-----	-----	-----	-----
2/18	20	VLAN #20	-----	-----	-----	-----
3/15	20	VLAN #20	-----	-----	-----	-----

After all clients authenticate on ports:

27. Confirm the EAPOL MultiHost status.

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

MHMA authentication mode with Guest VLAN and Fail Open VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes

Unit/Port	Client MAC Address	State	Vid	Pri
2/16	00:19:E1:A2:4D:36	Authenticated Locally	N/A	N/A
2/17	00:19:E1:E5:52:4A	Authenticated Locally	N/A	N/A
2/17	00:AB:CD:02:00:20	Authenticated By RADIUS	N/A	N/A
2/18	00:19:E1:E2:40:46	Authenticated By RADIUS	N/A	N/A
3/15	00:AB:CD:01:00:20	Authenticated By	N/A	N/A
3/15	00:AB:CD:01:00:21	Authenticated By RADIUS	N/A	N/A

Total number of authenticated clients: 6

ERS4000(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	N/A	N/A
2/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/18	00:AB:CD:03:00:12	Authenticated	Idle	N/A	N/A
3/15	00:AB:CD:01:00:10	Authenticated	Idle	N/A	N/A
=====	Neap Phones	=====			
2/16	00:19:E1:E6:09:B1				

Total number of authenticated clients: 5

28. Confirm the VLAN interface settings.

ERS4000(config)#sho vlan interface info 2/15-18,3/15

Supported EAP modes and configuration examples

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

29. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

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
3/15	50	VLAN #50	300	VLAN #300	-----	-----

30. Disconnect both primary and back-up RADIUS servers from the network (unplug cables from server side).

31. Attempt to reach the primary and back-up RADIUS servers.

```
ERS4000(config)#ping 10.100.68.2
(Host is not reachable)
```

```
ERS4000(config)#ping 10.100.68.3
(Host is not reachable)
```

32. After approximately 3 minutes, confirm the EAPOL MultiHost status again.

```
ERS4000(config)#show eapol multihost status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
-----	-----	-----	-----	-----	-----

```
ERS4000(config)#show eapol multihost non-eap-mac status
```

Unit/Port	Client MAC Address	Pae State	Backend Auth State	Vid	Pri
-----	-----	-----	-----	-----	-----

33. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 2/15-18,3/15
```

Unit/Port	Filter Untagged Frames	Unregistered Frames	PVID	PRI	Tagging	Name
-----	-----	-----	-----	-----	-----	-----
2/15	No	Yes	30	0	UntagPvid Only	Unit 2, Port 15
2/16	No	Yes	30	0	UntagPvid Only	Unit 2, Port 16
2/17	No	Yes	30	0	UntagPvid Only	Unit 2, Port 17
2/18	No	Yes	30	0	UntagPvid Only	Unit 2, Port 18
3/15	No	Yes	30	0	UntagPvid Only	Unit 3, Port 15

34. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
-----	-----	-----	-----	-----	-----	-----
2/15	30	VLAN #30	-----	-----	-----	-----
2/16	30	VLAN #30	-----	-----	-----	-----
2/17	30	VLAN #30	-----	-----	-----	-----
2/18	30	VLAN #30	-----	-----	-----	-----
3/15	30	VLAN #30	-----	-----	-----	-----

35. Connect primary or back-up RADIUS server to network (plug in cables from server side). For this example, the primary RADIUS server is connected.

36. After approximately 1 minute, attempt to reach the primary RADIUS server.

```
ERS4000(config)#ping 10.100.68.2
(Host is reachable)
```

37. Confirm the EAPOL MultiHost status.

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

Supported EAP modes and configuration examples

Unit/Port	Client MAC Address	State	Vid	Pri
2/16	00:19:E1:A2:4D:36	Authenticated Locally	N/A	N/A
2/17	00:19:E1:E5:52:4A	Authenticated Locally	N/A	N/A
2/17	00:AB:CD:02:00:20	Authenticated By RADIUS	N/A	N/A
2/18	00:19:E1:E2:40:46	Authenticated By RADIUS	N/A	N/A
3/15	00:AB:CD:01:00:20	Authenticated By RADIUS	N/A	N/A
3/15	00:AB:CD:01:00:21	Authenticated By RADIUS	N/A	N/A

Total number of authenticated clients: 6

```
ERS4000(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	N/A	N/A
2/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/18	00:AB:CD:03:00:12	Authenticated	Idle	N/A	N/A
3/15	00:AB:CD:01:00:10	Authenticated	Idle	N/A	N/A
=====	Neap Phones	=====			
2/16	00:19:E1:E6:09:B1				

Total number of authenticated clients: 5

38. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 2/15-18,3/15
```


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

39. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```

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
3/15	50	VLAN #50	300	VLAN #300	-----	-----

Alternate configuration

The following operation applies to the **MHMA authentication mode with Guest VLAN and Fail Open VLAN (Multihost MultiVLAN option disabled) without valid additional RADIUS attributes** configuration example, 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.

```
ERS4000(config)#eapol disable
ERS4000(config)#eapol enable
% Depending on your stack configuration it may take up to 4 minutes for
% port vlan membership and vid to take effect on all guest-vlan enabled ports.
```

2. Confirm EAPOL MultiHost status.

```
ERS4000(config)#sho eapol multihost non-eap-mac status
```

Supported EAP modes and configuration examples

Unit/Port	Client MAC Address	State	Vid	Pri
2/16	00:19:E1:A2:4D:36	Authenticated Locally	N/A	N/A
2/17	00:19:E1:E5:52:4A	Authenticated Locally	N/A	N/A
2/17	00:AB:CD:02:00:20	Authenticated By RADIUS	N/A	N/A
2/18	00:19:E1:E2:40:46	Authenticated By RADIUS	N/A	N/A
3/15	00:AB:CD:01:00:20	Authenticated By RADIUS	N/A	N/A
3/15	00:AB:CD:01:00:21	Authenticated By RADIUS	N/A	N/A
Total number of authenticated clients: 6				

```
ERS4000(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	N/A	N/A
2/15	00:50:BF:B8:09:AF	Authenticated	Idle	N/A	N/A
2/18	00:AB:CD:03:00:12	Authenticated	Idle	N/A	N/A
3/15	00:AB:CD:01:00:10	Authenticated	Idle	N/A	N/A
===== Neap Phones =====					
2/16	00:19:E1:E6:09:B1				
Total number of authenticated clients: 5					

3. Confirm the VLAN interface settings.

```
ERS4000(config)#show vlan interface info 2/15-18,3/15
```

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	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
3/15	No	Yes	50	0	UntagAll	Unit 3, Port 15

4. Confirm the VLAN interface VIDs.

```
ERS4000(config)#show vlan interface vids 2/15-18,3/15
```


MHMA authentication mode with Guest VLAN and Fail Open VLAN (Multihost MultiVLAN option disabled) with or without additional RADIUS attributes

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		
3/15	50	VLAN #50				

Appendix C: Sticky MAC address configuration examples

For the sticky MAC address feature to function properly, you must enable MAC security and auto-learning sticky mode globally, and for the specific interfaces on which you are configuring sticky MAC address.

The following configuration examples describe the basic steps required to configure a device to learn sticky MAC addresses on a range of ports, and to manually configure sticky MAC address on and individual port.

Example 1: 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.

```
mac-security auto-learning stickyERS4000(config)#  
Avaya recommends disabling autosave when sticky mac is enabled  
ERS4000(config)#mac-security enable  
ERS4000(config)#no autosave enable  
ERS4000(config)#copy config nvram
```

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

```
ERS4000(config)#interface Ethernet 1/6-14  
ERS4000(config-if)#mac-security auto-learning enable  
ERS4000(config-if)#mac-security auto-learning max-addr <1-25>  
ERS4000(config-if)#mac-security enable  
ERS4000(config-if)#exit
```

3. Verify the MAC security configuration for the interfaces.

```
ERS4000(config)#show mac-security port 1/6-14
```

Unit	Port	Trunk	Security	Auto-Learning	MAC Number
1	6		Enabled	Enabled	2
1	7		Enabled	Enabled	2
1	8		Enabled	Enabled	2
1	9		Enabled	Enabled	2
1	10		Enabled	Enabled	2
1	11		Enabled	Enabled	2
1	12		Enabled	Enabled	2
1	13		Enabled	Enabled	2
1	14		Enabled	Enabled	2

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

```
ERS4000#show mac-security mac-address-table  
Number of addresses: 1
```

Number of addresses: 1			
Unit	Port	Allowed MAC Address	Type
1	8	00-02-A5-E9-00-28	Sticky

Security List	Allowed MAC Address	Type
-----	-----	-----

Example 2: Manually configuring sticky MAC address on and individual port: (Port 1/6 is used for this example.)

1. Enable MAC security and auto-learning globally.

```
ERS4000(config)#mac-security auto-learning sticky  
Avaya recommends disabling autosave when sticky mac is enabled  
ERS4000(config)#copy config nvram  
ERS4000(config)#mac-security enable  
ERS4000(config)#no autosave enable  
ERS4000(config)#mac-security mac-address-table sticky-address 00-02-A5-E9-00-27 port 1/6
```

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

```
ERS4000(config)#interface Ethernet 1/6  
ERS4000(config-if)#mac-security auto-learning enable  
ERS4000(config-if)#mac-security auto-learning max-addr <1-25>  
ERS4000(config-if)#mac-security enable  
ERS4000(config-if)#exit
```

3. Verify the configuration by displaying the MAC security MAC address table.

```
ERS4000#show mac-security mac-address-table  
Number of addresses: 1
```

Number of addresses: 1

Unit	Port	Allowed MAC Address	Type
-----	-----	-----	-----
Trunk	25	00-02-A5-E9-00-27	Sticky

Security List	Allowed MAC Address	Type
-----	-----	-----

Glossary

ACLI	Avaya Command Line Interface (ACLI) is a text-based, common command line interface used for device configuration and management across Avaya products.
ACLI modes	Differing command modes are available within the text-based interface, dependant on the level of user permissions determined by logon password. Each successive mode level provides access to more complex command sets, from the most restrictive—show level only, to the highest configuration levels for routing parameters, interface configuration, and security.
Address Resolution Protocol (ARP)	Maps an IP address to a physical machine address, for example, maps an IP address to an Ethernet media access control (MAC) address.
Advanced Encryption Standard (AES)	A privacy protocol the U.S. government organizations use AES as the current encryption standard (FIPS-197) to protect sensitive information.
American Standard Code for Information Interchange (ASCII)	A code to represent characters in computers. ASCII uses uppercase and lowercase alphabetic letters, numeric digits, and special symbols.
application-specific integrated circuit (ASIC)	An application-specific integrated circuit developed to perform more quickly and efficiently than a generic processor.
AV pairs	AV pairs are strings of text in the form “attribute-value” that are sent between a network access server (NAS) and a TACACS+ daemon as part of the TACACS+ protocol.
Authentication, Authorization, and Accounting (AAA)	Authentication, Authorization, and Accounting (AAA) is a framework used to control access to a network, limit network services to certain users, and track what users do. Authentication determines who a user is before allowing the user to access the network and network services. Authorization allows you to determine what you allow a user to do. Accounting records what a user is doing or has done.
Auto-Detection and Auto-Configuration (ADAC)	Provides automatic switch configuration for IP phone traffic support and prioritization. ADAC can configure the switch whether it is directly connected to the Call Server or uses a network uplink.

Autotopology	An Enterprise Network Management System (ENMS) protocol that automates and simplifies discovery and collection of network topology information, presented in a table.
bandwidth	A measure of transmission capacity for a particular pathway, expressed in megabits per second (Mb/s).
base unit (BU)	When you connect multiple switches into a stack, one unit, and only one unit, must be designated as a base unit to perform stack configuration tasks. The position of the unit select switch, on the back of the switch, determines base unit designation.
bit error rate (BER)	The ratio of the number of bit errors to the total number of bits transmitted in a specific time interval.
Bootstrap Protocol (BootP)	A User Datagram Protocol (UDP)/Internet Protocol (IP)-based protocol that a booting host uses to configure itself dynamically and without user supervision.
brouter port	A single port VLAN that can route IP packets and bridge all non-routable traffic.
daemon	A program that services network requests for authentication and authorization. A daemon verifies, identifies, grants or denies authorizations, and logs accounting records.
Data Encryption Standard (DES)access control entry (ACE)	A cryptographic algorithm that protects unclassified computer data. The National Institute of Standards and Technology publishes the DES in the Federal Information Processing Standard Publication 46-1.
denial-of-service (DoS)	Attacks that prevent a target server or victim device from performing its normal functions through flooding, irregular protocol sizes (for example, ping requests aimed at the victim server), and application buffer overflows.
Distributed MultiLink Trunking (DMLT)	A point-to-point connection that aggregates similar ports from different modules to logically act like a single port, but with the aggregated bandwidth.
Dynamic Address Resolution Protocol Inspection (DAI)	Validates Address Resolution Protocol (ARP) packets in the network to prevent malicious user attacks on hosts, switches, and routers connected to the Layer 2 network by intercepting, logging, and discarding ARP packets with invalid IP-to-MAC address bindings. See also ARP Spoofing.
Dynamic Host Configuration Protocol (DHCP)	A standard Internet protocol that dynamically configures hosts on an Internet Protocol (IP) network for either IPv4 or IPv6. DHCP extends the Bootstrap Protocol (BOOTP).
Dynamic Host Configuration	Allows forwarding of client requests to DHCP servers residing on different IP subnets from the client.

**Protocol relay
(DHCP Relay)****Dynamic Host
Configuration
Protocol Snooping
(DHCP Snooping)**

Prevents DHCP Spoofing attacks by ensuring client ports can only request appropriate DHCP information and are not permitted to source DHCP leases.

**Dynamic Host
Configuration
Protocol Spoofing
(DHCP Spoofing)**

Combats rogue DHCP servers by requiring the identification of the valid DHCP server address and ports where DHCP Spoofing support resides. This action causes the installation of policies on the interfaces that pass or drop traffic, depending on user-defined criteria in the policies.

**Enterprise Device
Manager (EDM)**

A Web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.

**Extensible
Authentication
Protocol over LAN
(EAPoL)**

A port-based network access control protocol. EAPoL provides security in that it prevents users from accessing network resources before they are authenticated.

flash memory

All switch configuration parameters are stored in flash memory. If you store switch software images in flash memory, you can update switch software images without changing switch hardware.

**Gigabit Interface
Converter (GBIC)**

A hotswappable input and output enhancement component, designed for use with Avaya products, that allows Gigabit Ethernet ports to link with other Gigabit Ethernet ports over various media types.

**Hypertext Transfer
Protocol (HTTP)**

Communications protocol for the Web.

**Hypertext Transfer
Protocol, Secure
(HTTPS)**

Communications protocol used to access a secure Web server.

**Internet Control
Message Protocol
(ICMP)**

A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.

**Internet
Engineering Task
Force (IETF)**

A standards organization for IP data networks.

**Internet Group
Management
Protocol (IGMP)**

IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.

Internet Protocol Manager (IP Manager)	Used to limit access to switch management features by defining IP addresses allowed access to the switch.
Internet Protocol version 4 (IPv4)	The protocol used to format packets for the Internet and many enterprise networks. IPv4 provides packet routing and reassembly.
Internet Protocol version 6 (IPv6)	An improved version of the IP protocol, IPv6 improves the IPv4 limitations of security and user address numbers.
Layer 2	Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are: Ethernet and Frame Relay.
Layer 3	Layer 3 is the Network Layer of the OSI model. An example of a Layer 3 protocol is Internet Protocol (IP).
Link Aggregation	Provides the mechanism to create and manage trunk groups automatically using Link Aggregation Control Protocol (LACP).
Link Aggregation Control Protocol (LACP)	A network handshaking protocol that provides a means to aggregate multiple links between appropriately configured devices.
link aggregation group (LAG)	A group that increases the link speed beyond the limits of one single cable or port, and increases the redundancy for higher availability.
Link Layer Discovery Protocol (LLDP)	Link Layer Discovery Protocol is used by network devices to advertise their identities. Devices send LLDP information at fixed intervals in the form of Ethernet frames, with each frame having one Link Layer Discovery Protocol Data Unit.
Local Area Network (LAN)	A data communications system that lies within a limited spatial area, uses a specific user group and topology, and can connect to a public switched telecommunications network (but is not one).
management information base (MIB)	The MIB defines system operations and parameters used for the Simple Network Management Protocol (SNMP).
mask	A bit string that the device uses along with an IP address to indicate the number of leading bits in the address that correspond with the network part.
Media Access Control (MAC)	Arbitrates access to and from a shared medium.
Message Digest 5 (MD5)	A one-way hash function that creates a message digest for digital signatures.

MultiLink Trunking (MLT)	A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.
Multiple Spanning Tree Protocol (MSTP)	Configures multiple instances of the Rapid Spanning Tree Protocol (RSTP) on the switch.
multiplexing	Carriage of multiple channels over a single transmission medium; a process where a dedicated circuit is shared by multiple users. Typically, data streams intersperse on a bit or byte basis (time division), or separate by different carrier frequencies (frequency division).
network access server (NAS)	A network access server (NAS) is a single point of access to a remote device. The NAS acts as a gateway to guard the remote device. A client connects to the NAS and then the NAS connects to another device to verify the credentials of the client. Once verified the NAS allows or disallows access to the device. Network access servers are almost exclusively used with Authentication, Authorization, and Accounting (AAA) servers.
Network Time Protocol (NTP)	A protocol that works with TCP that assures accurate local time keeping with reference to radio and atomic clocks located on the Internet. NTP synchronizes distributed clocks within milliseconds over long time periods.
NonVolatile Random Access Memory (NVRAM)	Random Access Memory that retains its contents after electrical power turns off.
Open Shortest Path First (OSPF)	A link-state routing protocol used as an Interior Gateway Protocol (IGP).
out of band (OOB)	Network dedicated for management access to chassis.
policing	Ensures that a traffic stream follows the domain service provisioning policy or service level agreement (SLA).
port	A physical interface that transmits and receives data.
Port Access Entity (PAE)	Software that controls each port on the switch. The PAE, which resides on the device, supports authenticator functionality. The PAE works with the Extensible Authentication Protocol over LAN (EAPoL).
port mirroring	A feature that sends received or transmitted traffic to a second destination.
port VLAN ID	Used to coordinate VLANs across multiple switches. When you create a port-based VLAN on a switch, assign a VLAN identification number (VLAN ID) and specify the ports that belong to the VLAN.

prefix

prefix	A group of contiguous bits, from 0 to 32 bits in length, that defines a set of addresses.
Protocol Data Units (PDUs)	A unit of data that is specified in a protocol of a specific layer and that consists of protocol-control information of the specific layer and possibly user data of that layer.
quality of service (QoS)	QoS features reserve resources in a congested network, allowing you to configure a higher priority to certain devices. For example, you can configure a higher priority to IP deskphones, which need a fixed bit rate, and, split the remaining bandwidth between data connections if calls in the network are more important than the file transfers.
Random Access Memory (RAM)	Memory into which you can write and read data. A solid state memory device used for transient memory stores. You can enter and retrieve information from storage position.
Rapid Spanning Tree Protocol (RSTP)	Reduces the recovery time after a network breakdown. RSTP enhances switch-generated Topology Change Notification (TCN) packets to reduce network flooding.
rate limiting	Rate limiting sets the percentage of traffic that is multicast, broadcast, or both, on specified ports.
Read Write All (RWA)	An access class that lets users access all menu items and editable fields.
redundant power supply unit (RPSU)	Provides alternate backup power over a DC cable connection into an Avaya Ethernet Routing Switch.
Remote Authentication Dial-in User Service (RADIUS)	A protocol that authenticates, authorizes, and accounts for remote access connections that use dial-up networking and Virtual Private Network (VPN) functionality.
Remote Network Monitoring (RMON)	Creates and displays alarms for user-defined events, gathers cumulative statistics for Ethernet interfaces, and tracks statistical history for Ethernet interfaces.
request for comments (RFC)	A document series published by the Internet Engineering Task Force (IETF) that describe Internet standards.
Routing Information Protocol (RIP)	A distance vector protocol in the IP suite, used by IP network-layer protocol, that enables routers in the same AS to exchange routing information by means of periodic updates. You often use RIP as a very simple interior gateway protocol (IGP) within small networks.
routing switch	Virtualizes the physical router interfaces to switches. A virtual router port, or interface, acts as a router port to consolidate switching and routing functions in the

broadcast domain, or between broadcast domains, and enable IP routing for higher traffic volumes.

Secure Shell (SSH)	SSH uses encryption to provide security for remote logons and data transfer over the Internet.
Secure Sockets Layer (SSL)	An Internet security encryption and authentication protocol for secure point-to-point connections over the Internet and intranets, especially between clients and servers.
Simple Network Time Protocol (SNTP)	Provides a simple mechanism for time synchronization of the switch to any RFC 2030-compliant Network Time Protocol (NTP) or SNTP server.
spanning tree	A simple, fully-connected active topology formed from the arbitrary physical topology of connected bridged Local Area Network components by relaying frames through selected bridge ports. The protocol parameters and states that are used and exchanged to facilitate the calculation of the active topology and to control the bridge relay function.
Spanning Tree Protocol (STP)	MAC bridges use the STP to exchange information across Local Area Networks to compute the active topology of a bridged Local Area Network in accordance with the Spanning Tree Protocol algorithm.
Split MultiLink Trunking (SMLT)	An Avaya extension to IEEE 802.1AX (link aggregation), provides nodal and link failure protection and flexible bandwidth scaling to improve on the level of Layer 2 resiliency.
stack	Stackable Avaya Ethernet Routing Switches can be connected in a stack configuration of two or more units, up to eight units maximum. A switch stack operates and is managed as a single virtual switch.
stack IP address	An IP address must be assigned to a stack so that all units can operate as a single entity.
stand-alone	Refers to a single Avaya Ethernet Routing Switch operating outside a stack.
Terminal Access Controller Access Control System plus	Terminal Access Controller Access Control System plus (TACACS+) is a security protocol that provides centralized validation of users who attempt to gain access to a router or network access server. TACACS+ uses Transmission Control Protocol (TCP) for its transport to ensure reliable delivery and encrypts the entire body of the packet. TACACS+ provides separate authentication, authorization, and accounting services. TACACS+ is not compatible with previous versions of TACACS.
Transmission Control Protocol (TCP)	Provides flow control and sequencing for transmitted data over an end-to-end connection.
Transmission Control Protocol/	Provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems—TCP/IP signifies

Internet Protocol (TCP/IP)	the family of common Internet Protocols that define the Internet. Transmission Control Protocol is connection oriented and provides reliable communication and multiplexing, and IP is a connectionless protocol providing packet routing.
Trivial File Transfer Protocol (TFTP)	A protocol that governs transferring files between nodes without protection against packet loss.
trunk	A logical group of ports that behaves like a single large port.
User Datagram Protocol (UDP)	In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.
Virtual Link Aggregation Control Protocol (VLACP)	Virtual Link Aggregation Control Protocol (VLACP) is a Layer 2 handshaking protocol that can detect end-to-end failure between two physical Ethernet interfaces.
Virtual Local Area Network (VLAN)	A Virtual Local Area Network is a group of hosts that communicate as if they are attached to the same broadcast domain regardless of their physical location. VLANs are layer 2 constructs.
Virtual Private Network (VPN)	A Virtual Private Network (VPN) requires remote users to be authenticated and ensures private information is not accessible to unauthorized parties. A VPN can allow users to access network resources or to share data.
Voice over IP (VOIP)	The technology that delivers voice information in digital form in discrete packets using the Internet Protocol (IP) rather than the traditional circuit-committed protocols of the public switched telephone network (PSTN).
XFP	A pluggable 10 gigabit transceiver capable of providing different optical media for a switch. The XFP is similar to an SFP transceiver but is larger in size.