ExtremeSwitching

Configuring Security on Ethernet Routing Switch 4900 and 5900 Series

Release 7.7
9035790 Rev.AA
July 2019

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

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

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

This document provides procedures and conceptual information to configure security features on the following platforms:

- Ethernet Routing Switch 4900 Series
- Ethernet Routing Switch 5900 Series

The security function includes tasks related to product security such as the management and protection of resources from unauthorized or detrimental access and use. This document includes information that supports the configuration and ongoing management of the following:

- communications
- data security
- user security
- access

Examples and network illustrations in this document may illustrate only one of the supported platforms. Unless otherwise noted, the concept illustrated applies to all supported platforms.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons

Icon	Alerts you to...
Important:	A situation that can cause serious inconvenience.
Note:	Important features or instructions.
Tip:	Helpful tips and notices for using the product.
Danger:	Situations that will result in severe bodily injury; up to and including death.
Warning:	Risk of severe personal injury or critical loss of data.
Caution:	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.

Table continues…

Convention	Description
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...`, you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (|)	A vertical line (|) separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. For example, if the command syntax is `access-policy by-mac action { allow | deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

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

Current Product Documentation	www.extremenetworks.com/documentation/

Table continues…

Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

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

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

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

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

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

   Note:
   You can modify your product selections or unsubscribe at any time.
4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

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

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this Document

The following section details what is new in this document.

Viewing EAPOL Unauthenticated Clients

EDM support to view EAP and Non-EAP unauthenticated clients. For more information, see Viewing EAPOL Unauthenticated Clients on page 210.

3DES for SNMP

In this release, 3DES is no longer supported as an SNMP privacy protocol option.

Chapter 3: Security fundamentals

This chapter provides conceptual content to help you configure and customize the security services on the switch.

Security fundamentals

This section describes the hardware-based and software-based security features supported by the switch.

Hardware-based security

Network administrators enable or disable the USB or serial console ports on the switch 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 HTTP as the default mode. You can select the Web server mode with the CLI 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.

Campus security example

The following figure shows a typical campus configuration using the RADIUS-based and MAC-address-based security features for the switch.

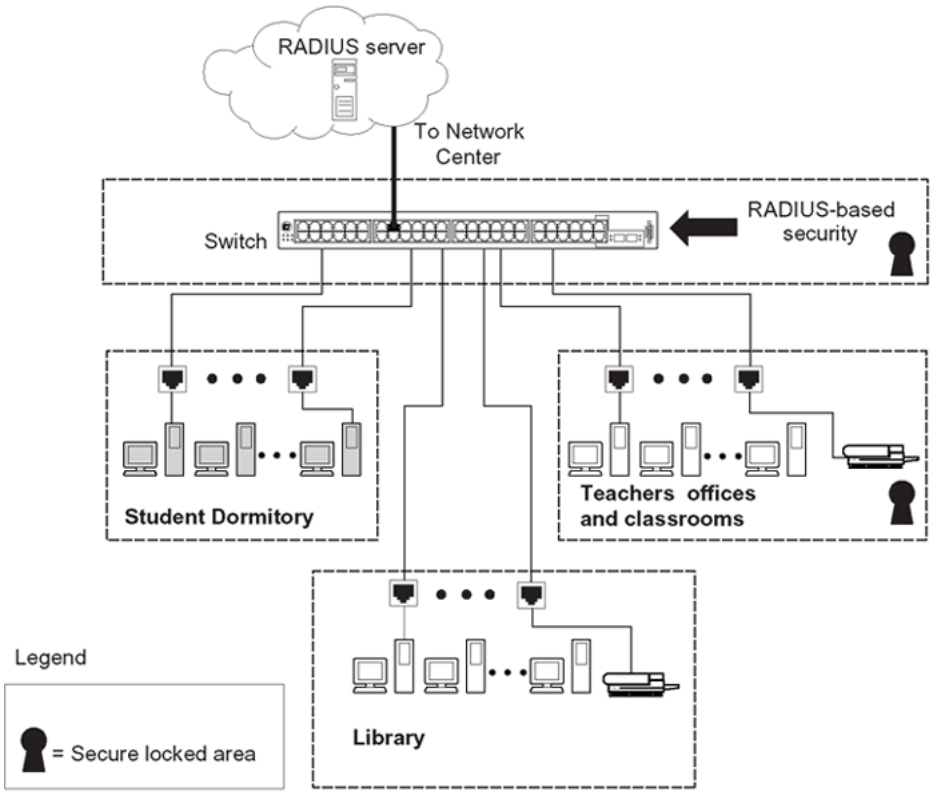


Figure 1: Security features of the switch

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 424.

  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 326.

  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.

Password protection

For each switch model, there is only a secure software image available.

On a switch, there is no access security enabled by default. This allows a user to access the switch either via the local serial port, HTTP (WEB), or through Telnet without any user name or password protection.

Password protection for serial console, Telnet, WEB, or SSH (user name and password) can be added using local user names and passwords or authentication against an external RADIUS or TACACS+ server. In regards to SSH, password authentication can be enabled or disabled in addition to using SSH with public key authentication.

There are two default users on a switch: the RW user, with read-write permissions and the RO user, with read-only permissions. The RO user can access only User EXEC and Privileged EXEC modes. The RW user can access all CLI command modes. Eight more users with read-only or read-write rights can be added.

For more information about multiple user accounts, see Multiple local RW and RO user accounts on page 30

The default password for RO is `user` and `secure` for RW.

Note:

User names and passwords are only applicable after you enable local password security.

Note:

The RO and RW passwords cannot be the same.

Enabling telnet password protection, either local user/password or against a RADIUS server, also applies to WEB access.

Password security

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

When you enable password security, the following happens:

- Current passwords remain unchanged if they meet the required specifications. If they do not meet the required specifications, 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 one used passwords.
- Password verification is required.

When you disable password security, the following happens:

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

For more information about enabling password security, see Configuring password security on page 47.

With Password Security enabled, the following features and requirements are active:

Password length and valid characters

Valid passwords are from 8 to 255 characters long. The password is not required to contain a minimum of lowercase, capital, numbers or special symbols characters. 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 CLI. The default is three retries.

Password history

You can configure the switch to keep a maximum history of the last 12 passwords. Default password history is 1. If you set the password for the fourth time and the history size is set to 3, you can reuse the password that you used the first time. You cannot reuse a password stored in history.

Password aging time

Passwords expire after a specified aging period. The aging period is configurable, with a range of 1 day to approximately 365 days. The default aging period is 0 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.

Note:

When a password expires, the password must be changed through CLI.

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.

Password display masking

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

Password sequential and repeated characters

The switch does not allow the use of passwords that contains sequential characters, such as *ab, ba, qw, wq, 12, 21, !@, @!*, or repeated characters, such as *11, aa,* @@. Sequential strings include the following ones, in forward and reverse order, uppercase letters included:

- `abcdefghijklmnopqrstuvwxyz`
- `01234567890`
- `qwertyuiop`
- `asdfghjkl`
- `zxcvbnm`
- `!@#$%^&*()`

Password complexity

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

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

Table 3: Password complexity rules

Type	Description	Value range	Minimum length	Default value when the feature is enabled	Default value when switch is upgraded from an unsupported to a supported release for first time
Length	Specifies number of characters in password.	8 to 255	8 characters	8	10
Character	Specifies the number of			0–0–0–0	2-2-2-2

Table continues…

Type	Description	Value range	Minimum length	Default value when the feature is enabled	Default value when switch is upgraded from an unsupported to a supported release for first time
	character from each character type that need to be included in password.			Where, x-y-z-t specify the number of characters from each character type. Following are the details: • x — lowercase • y — uppercase • z — numeric • t — special characters	
	Character type				
	lowercase	a to z	0 to 9	0	2
	uppercase	A to Z	0 to 9	0	2
	numeric	0 to 9	0 to 9	0	2
	special characters	(!, @, #, $, %, ^, &, *, (,), -, +, =, _	0 to 9	0	2
History	Number of passwords retained in history	0 to 12		1	3
Sequential	Checks for sequential characters within passwords when enabled. For example, abcdefgh.	Enable or Disable		Enable	Enable
Check-repeated	Checks for repeated characters within passwords when enabled. For example, aa.	Enable or Disable		Enable	Enable

Password aging

Passwords expire after a specified aging period. The values for aging must be configured.

Note:

When a password expires, the password must be changed through CLI.

The default values are different when the switch is upgraded from an unsupported to a supported release for the first time.

The following table lists the password aging rules and their default values:

Table 4: Password aging rules

Rule	Description	Value range	Default value when the feature is enabled	Default value when switch is upgraded from an unsupported to a supported release for first time
Password expiration	Number of days before password expiration	1-2730	180	90 days
Warning	Number of warning days before password expiration	30 days	10 days	30 days
Failed login attempts	Number of consecutive failed login attempts before lockout Failures are counted only for consecutive login failures. The lockout count is reset after a successful login. This is configurable using username lockout-retries.		0 for no lockout	3 times
Unlock timer value	Automatic unlock timer value for disabled accounts	1 to 365 days	7 days. This timer re-enables the username after the specified number of days if the username is disabled due to inactivity timeout.	inactive period is 90 days or 360 days

Extreme Networks recommends that you use an active clock configured correctly through NTP or SNTP before configuring password aging-time, password delay-time, password notifications, password password-change-rate-limiter, and password unlock-timer.

After downgrading from a supported to unsupported release, the default passwords are applied for RW and RO users. The default passwords for RO and RW are:

- RW — securepasswd or secure
- RO — userpasswd or user

Lockout for failed logon attempts

The lockout for failed logon attempts feature prevents brute force hacking. Following a consecutive number of log on failures, the user account used for connecting is locked out for a configurable amount of time. After upgrade the feature is enabled and applies to all user accounts, with the exception of the last unlocked account with RW rights. The default lockout interval is set to one minute.

After upgrade from 7.0 or 7.1, the value for the number of telnet access retries after upgrade is 3 and user is locked after 3 failed (incorrect) password attempts. The last RW unlocked account cannot be locked.

Multiple local RW and RO user accounts

With multiple users support, you can create eight more users on a switch in addition to the default two users, therefore avoiding the use of shared accounts. User actions are visible through the analysis of audit records.

New users can have read-write or read-only permissions. Each user can access the switch through the local serial port, telnet, SSH, or HTTP (web). A user name and a password are required when users connect to the switch if authentication is enabled (not a default setting). The authentication against an external RADIUS or TACACS+ server is supported. Radius fallback extends the search for local users if the radius server is unavailable.

Log files display when and how read-only (RO) and read-write (RW) users logged in, including the source IP address from where the login occurred.

Any RW user has administrator rights to create, remove, or modify other users. Exceptions are the default RO and RW users, which cannot be deleted.

The audit log displays information containing the user name for the authenticated user. SYSLOG displays information when a user logs in or logs out.

Each user name must be unique.

For security reasons, if a login attempt fails, the error feedback does not indicate if the failed login is due to an invalid user name or an invalid password. As well, response times for invalid user name and invalid user name/password pair are identical, to prevent identification of which of the two failed. The passwords are encrypted and do not appear in any log.

Limitations

The following limitations apply:

- EDM allows the authentication of any of the 10 supported users, but not more than the number of maximum HTTP/HTTPS sessions.
- Users can log into switch using SSH, Telnet, serial, or EDM connections.

  A new user can be logged into a maximum of 20 sessions at a time. The maximum number of sessions is 18 at a time.
- When a unit is joining a stack, all users created on the base unit are also created on non-base units.

- When disabling telnet all users connected through telnet are disconnected. When disabling SSH, all users connected through SSH are disconnected.
- Boot default can be initialized only by RW users.

Feature operation during upgrade

Passwords are retained when the software is upgraded from a release that does not support Password complexity and Password aging and lockout features.

For more information about configuring multiple local user accounts, see:

- Configuring multiple local RW and RO users accounts on page 58
- Displaying local user information on page 59

RO user access to Telnet and SSH

With this feature you can log in read-only (RO) mode and connect from the switch to other device using Telnet or SSH connections.

Disable SSH Client and Telnet Out

Only the users with Read-Write access can enable or disable the remote access for themselves and for everyone else.

The remote access can be configured to allow users to enable or disable SSH Client and Telnet Out access on a device. The configuration is supported only through CLI and can be used only on base unit.

If the remote connection is disabled, all open SSH Client or Telnet Out sessions are disabled for all users including the users with Read-Write access. Also, remote access changes done by Read-Write users, propagates to all open sessions on device (console, telnet or SSH).

CLI audit

CLI audit provides a means for tracking CLI commands.

A special area of flash memory reserved for CLI 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 CLI 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)
- CLI command itself

By default CLI 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.

Trace

Trace 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.

MIB Enhancements

This release adds the following MIB enhancements so that Extreme Management Center can be supported:

- Entity MIB
- Dot1Q MIB
- P-Bridge MIB

For more information about Entity MIB, Dot1Q MIB, and P-Bridge MIB, see Configuring Security on Ethernet Routing Switch 4900 and 5900 Series.

Dot1Q MIB

This release adds support for the following MIB tables so that Extreme Management Center can provision VLANs:

- dot1VlanCurrentTable – Contains current configuration information for each VLAN configured on the switch.
- dot1qVlanStaticTable – Contains static configuration information for each VLAN configured on the switch.
- dot1qPortVlanTable – Contains per-port control and status information for VLAN configuration.

Entity MIB

Entity MIB support is enhanced to provide full basic support for Extreme Management Center.

The Entity MIB assists in the discovery of functional components on the switch. In this release, Entity MIB support has been implemented and enhanced for the following:

- Physical Table — Describes the physical entities managed by a single agent.
- Alias Mapping Table — This table contains mappings between Logical Index, Physical Index pairs, and alias object identifier values. It allows resources managed with other MIB modules (repeater ports, bridge ports, physical and logical interfaces) to be identified in the physical entity hierarchy.
- Physical Contains Table — This table contains simple mappings between Physical Contained In values for each container or containee relationship in the managed system. The indexing of this table allows a network management station (NMS) to quickly discover the Physical Index values for all children of a given physical entity.
- Last Change Time Table — Represents the value of sysUpTime when the Entity MIB configuration was last changed.

P-Bridge MIB

This release adds support for the P-Bridge MIB Table.

- dot1dExtBase Group
  - dot1dDeviceCapabilities
  - dot1dTrafficClassesEnabled
  - dot1dGmrpStatus
  - dot1dPortCapabilitiesTable

Summary of security features

Information about some of the security features available on the switch, see Table 5: MAC security on page 33 through Table 9: SNMPv3 security on page 35.

Table 5: 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.

Table continues…

MAC security	Description
Configuring using interfaces	CLI, ASCII configuration file, SNMP, and EDM.
Restrictions and limitations	—
Reference	s5sbs MIB (S5-SWITCH-BAYSECURE-MIB)
Comments	—

Table 6: 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. • 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.
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. • 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, CLI, ASCII configuration file.
Restrictions and limitations	Not applicable.

Table 7: 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 reenable 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 Command Line Interface (CLI).

Table continues…

EAPOL	Description
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 8: IP Manager security

IP Manager	Description
Description	IP Manager is an extension of Telnet. It provides an option to enable or disable access for SSH, 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 SSH, 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 CLI.
Restrictions and limitations	Not applicable.

Table 9: 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) and Advanced Encryption Standard (AES)—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.)

Table continues…

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), Command Line Interface (CLI), ASCII configuration file, and SNMP Set requests.

Table 10: 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	Command Line Interface (CLI) and Enterprise Device Manager (EDM).

Table 11: 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	Command Line Interface (CLI) and Enterprise Device Manager (EDM).

Security configuration and management using CLI

This section describes the methods and procedures necessary to configure security on the switch using the Command Line Interface (CLI).

Depending on the scope and usage of the commands listed in this section, 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 CLI, see the Configuring Systems on Ethernet Routing Switch 4900 and 5900 Series.

USB port and serial console port control using CLI

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

Disabling serial console ports

About this task

Disable serial console ports to deny users console access to the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable serial console ports on all switches in a stack:

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

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

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

Variable definitions

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

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

Enabling serial console ports

About this task

Enable serial console ports to grant users console access to the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable serial console ports on all switches in a stack:

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

   OR

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

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

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

   OR

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

Variable definitions

Use the data in the following table to use the **`serial-console`** command.

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

Viewing serial console port status

About this task

View serial console port status to display the operational status of serial console ports on all switches in a stack or on a stand-alone switch.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show serial-console
   ```

3. View the status of a specific serial console port on the switch

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

Example

```
Switch>enable
Switch#show serial-console
Serial Console: Enabled
```

Variable definitions

Use the data in the following table to use 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

About this task

Disable USB ports to deny users console access to USB ports on the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable USB ports on all switches in a stack:

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

3. Disable the USB port on a stand-alone switch:

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

Variable definitions

Use the data in the following table to use the **usb-host-port** command.

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

Enabling USB ports

About this task

Enable USB ports to grant users console access to the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable USB ports on all switches in a stack:

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

OR

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

3. Enable the USB port on a stand-alone switch:

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

OR

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

Variable definitions

Use the data in the following table to use the **usb-host-port** command.

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

Viewing USB port status

About this task

View USB port status to display the operational status of USB ports on all switches in a stack or on a stand-alone switch.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. View the status of USB ports on all switches in a stack:

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

3. View the status of the USB port on a stand-alone switch:

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

Variable definitions

Use the data in the following table to use the **show serial-console** command.

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

HTTP/HTTPS port configuration using CLI

This section describes HTTP/HTTPS port configuration.

Setting the switch HTTP port

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

Before you begin

Disable SSL.

About this task

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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
{1024–65535}	Specifies a value for the switch HTTP port, ranging from 1024 to 65535. DEFAULT: 80

Restoring the switch HTTP port to default

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.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   default http-port
   ```

Displaying the switch HTTP port value

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

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show http-port
```

Example

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

Restoring the switch HTTPS port to default

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

Before you begin

Disable SSL.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable Definitions

Use the data in the following table to use the **`https-port`** command.

Variable	Value
{1024–65535}	Specifies a value for the switch HTTPS port, ranging from 1024 to 65535. DEFAULT: 443

Restoring the switch HTTPS port to default using CLI

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:

```
enable
configure terminal
```

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

```
default https-port
```

Displaying the switch HTTPS port value using CLI

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show https-port
   ```

Example

```
Switch>enable
Switch#show https-port
HTTPS Port: 443
```

Setting the user name and password

The username authentication feature enhances the security level of the switch 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.

Setting user name and password

About this task

Configures the system user name and password for serial console port, Telnet, and EDM access to a switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the system user name and password.

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

3. Set the read-only and read-write user name to default values.

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

Variable definitions

Use the data in the following table to use the **username** command.

Variable	Value
<username> <password>	Enter your user name for the first variable, and your password for the second variable. The default user name values are RO for read-only access and RW for read/write access.
ro | rw	Sets the read-only (ro) user name or the read-write (rw) user name. If you omit this optional variable, the command applies to both read-only and read-write users.

Setting CLI password

About this task

Assigns passwords for selected types of access using CLI, Telnet, or RADIUS security.

This procedure changes the password only and does not affect the configured user name.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Change the read-only and read-write passwords for serial console port and Telnet access to a switch.

   ```
   username {RO | RW} password
   ```

3. Change the password authentication type for serial console port or Telnet access to a switch.

   ```
   cli password [serial | telnet ] [local | none | radius | tacacs]
   ```

Variable definitions

Use the data in the following table to use the **`cli password`** command.

Variable	Value
read-only|read-write	Modify the read only password or the read/write password.
<password>	Specify the 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.

Table continues…

Variable	Value
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 | tacacs	Indicates the password type you are modifying: • none: disable the password • local: uses the locally defined password for serial console or Telnet access. • radius: uses RADIUS authenticatin 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

About this task

Displays the current user name and password authentication configuration for the switch.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display current user name and password authentication configuration.

   ```
   show cli password type
   ```

Example

```
Switch#show cli password type
Console Password Type: Local Password
Telnet Password Type: None
```

Variable definitions

Variable	Value
type	Displays the current password type configured for serial console and Telnet access. Values include: • local: the system local password is used • none: no password is used • radius: RADIUS password authentication is used • tacacs: TACACS+ AAA services are used

Configuring remote connection

About this task

Users with Read-Write access can configure remote access and allow users to enable or disable SSH Client and Telnet Out access on device.

When the remote access is disabled, all users are not allowed to open sessions. Only the users with Read-Write role can enable or disable the remote access for themselves and for everyone else. By default, the remote access is disabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable SSH Client and Telnet Out access on a device:

   ```
   remote connection enable
   ```

3. Display the remote connection status:

   ```
   show remote connection
   ```

4. **(Optional)** Disable SSH Client and Telnet Out access on a device:

   ```
   remote connection disable
   ```

Example

Following is an example to enable remote connection:

```
Switch(config)#remote connection enable
% Remote access has been enabled on this device !
```

Following is an example to disable remote connection:

```
Switch(config)#remote connection disable
% Remote access has been disabled on this device !
```

Following is an example to display remote connection status:

```
Switch(config)#show remote connection
% Remote access for this device is: Disabled
Switch(config)#ssh 192.0.2.1
% Remote access is disabled on this device !
Switch(config)#telnet 192.0.2.1
% Remote access is disabled on this device !
% Remote access is disabled on this device !
```

Configuring password security

CLI 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.

Enabling or disabling password security

About this task

Enables or disables the password security feature.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable password security.

   ```
   password security
   ```

3. Disable password security.

   ```
   no password security
   ```

Configuring password retry attempts

About this task

Configures the number of times a user can retry a password. The default retry attempts is 3 for SSH and 3 for telnet.

Note:

After upgrading from software releases 7.2.0.0 or 7.2.0.200, the **`telnet-access retry 3`** command replaces the **`telnet-access retry 0`** command. The default value is set from 0 to 3 after upgrade.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the number of retry attempts for telnet.

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

3. Configure the number of retry attempts for SSH.

   ```
   ssh retries <1-100>
   ```

Configuring password aging-time

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password aging time:

   ```
   password aging-time [username <name>]<0–365>
   ```

3. Return password aging-time to default value:

   ```
   default password aging-time
   ```

4. Verify the settings:

   ```
   show password aging-time
   ```

Example

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

Variable definitions

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

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

Configuring password check-repeated

About this task

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

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password check-repeated:

   ```
   password check—repeated [enable | disable]
   ```

3. Return check-repeated to default value (enabled):

   ```
   default password check—repeated
   ```

4. Verify the settings:

   ```
   show password check-repeated
   ```

Example

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

Variable definitions

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

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

Configuring password check-sequential

About this task

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

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password check-sequential:

   ```
   password check—sequential [enable | disable]
   ```

3. Return check-sequential to default value (enabled):

   ```
   default password check—sequential
   ```

4. Verify the settings:

   ```
   show password check-sequential
   ```

Example

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

Variable definitions

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

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

Configuring password complexity

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password complexity:

   ```
   password complexity [lower—case <0-9> | numeric <0-9> | special <0-9> | upper-case <0-9>]
   ```

3. Return password complexity to default value:

   ```
   default password complexity
   ```

4. Verify the settings:

   ```
   show password complexity
   ```

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#password complexity lower-case 0
Switch(config)#password complexity numeric 3
```

```
Switch(config)#password complexity special 1
Switch(config)#password complexity upper-case 2
Switch(config)#show password complexity
Complexity:2-0-3-1
Upper-case: 2
Lower-case: 0
Numeric: 3
Special: 1
```

Variable definitions

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

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

Configuring password delay-time

About this task

Configure the amount of delay time after three failed login attempts within a second. The default value is 60 seconds.

If the delay-time is configured as 0 second, then there is no delay.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password delay-time:

   ```
   password delay—time <0–3600>
   ```

3. Restore password delay-time to default:

   ```
   default password delay—time
   ```

4. Verify the settings:

   ```
   show password delay-time
   ```

Example

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Switch(config)#default password delay-time
Switch(config)#show password delay-time
Delay-time is: 60 seconds


Switch(config)#password delay-time 20
Switch(config)#show password delay-time
Delay-time is: 20 seconds
```

Variable definitions

The following table describes variables that you use with the **password delay-time** command.

Variable	Definition
<0–3600>	Specifies the amount of delay time after 3 login attempts in seconds. Default is 60 seconds.

Configuring password login failure notification message

About this task

Configure the notification message to users encountering a login failure. By default, there is no notification message.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password login-failure-notification.

   ```
   password login—failure—notification <message>
   ```

3. Verify the notification message.

   ```
   show password login—failure—notification
   ```

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#password login-failure-notification
ifuhaveforgottonyourpassword,contactadministrator
Switch(config)#show password login-failure-notification
Failure-login-notification is: ifyouhaveforgottonyourpassword,contactadministrator
```

Variable definitions

The following table describes variables that you use with the **password login-failure-notification** command.

Variable	Definition
<Word>	Specifies the notification message that the user sees for incorrect login. Maximum 99 characters.

Configuring minimum password length

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the minimum length for a password:

   ```
   password min-length <8–255>
   ```

3. Restore the minimum length of a password to default value:

   ```
   default password min-length
   ```

4. Verify the settings:

   ```
   show password min-length
   ```

Example

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

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

Variable definitions

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

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

Configuring password notifications

About this task

Configure the password expiration notifications. The password expiration notification appears when logged on using console, telnet or SSH. By default, the expiry notification appears before 10 days.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password expiry notifications:

   ```
   password notifications <1–90>
   ```

3. Restore password expiry notification to default value:

   ```
   default password notifications
   ```

4. Verify the settings:

   ```
   show password notifications
   ```

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#password notifications 14
Switch(config)#show password notifications
Pre-expiration notification interval 14 days


Switch(config)#default password notifications
Switch(config)#show password notifications
Pre-expiration notification interval 10 days
```

Variable definitions

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

Variable	Definition
<1–90>	Specifies the notification interval in days before password expires. Default is 10 days.

Configuring force password change on first login

About this task

Configure force password change on first login. By default, the force password change is disabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password change on first login:

   ```
   password password-change-on-first-login [disable | enable]
   ```

3. Restore to default value:

   ```
   default password password-change-on-first-login
   ```

4. Verify the settings:

```
show password password-change-on-first-login
```

Example

```
Switch# show password password-change-on-first-login
Password-change-on-first-login option is disabled
```

Variable definitions

The following table describes variables that you use with the **password password-change-on-first-login** command.

Variable	Definition
disable	Disables password change on first login. Default is disabled.
enable	Enables password change on first login

Configuring maximum number of password changes

About this task

Configure the maximum number of password changes per day.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password change rate limiter:

   ```
   password password-change-rate-limiter <1–10>
   ```

3. Restore to default value:

   ```
   default password password-change-rate-limiter
   ```

4. Verify the settings:

   ```
   show password password-change-rate-limiter
   ```

Example

```
Switch# show password password-change-rate-limiter
Maximum number of password changes per day is: 1
```

Variable definitions

The following table describes variables that you use with the **password password-change-rate-limiter** command.

Variable	Definition
<1–10>	Specifies the maximum number of password changes allowed per day. Default is 1.

Password history configuration using CLI

You can configure the switch to keep a maximum history of twelve passwords. The default password history configuration is 1.

Configuring password history

About this task

Configure the maximum number of passwords retained in history. You can configure the switch to keep a maximum history of the last 12 passwords. Default password history is 1.

For example, if the password history size is 3 and you set the password for the fourth time, you can reuse the password that you used the first time. You cannot reuse a password stored in history.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password history:

   ```
   password password-history <0–12>
   ```

3. Return password history to default value:

   ```
   default password password-history
   ```

4. Verify the settings:

   ```
   show password password-history
   ```

Example

```
Switch# show password password-history
Maximum number of passwords in history: 1
```

Variable definitions

The following table describes variables that you use with the **`password password-history`** command.

Variable	Definition
<0-12>	Specifies the number of passwords retained in history. Default is 1.

Viewing password history

About this task

Displays the number of passwords currently stored in the password history table.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display password history configuration.

   ```
   show password password-history
   ```

Example

```
Switch#show password password-history
Number of passwords in history is 3.
```

Configuring username inactive period

Use the following procedure to configure the number of days after witch a user account becomes disabled if he doesn't use the account.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure username inactive period:

   ```
   username <username> inactive-period <0-360>
   ```

3. Disable or return username inactive period to default value:

   ```
   default username <username>
   ```

4. Verify the settings:

   ```
   show username <username>
   ```

Example

The following example displays sample output for the `username inactive-period` command.

```
Switch# show username RW
Inactive period:    20 days
```

Variable definitions

Use the data in the following table to use the `username inactive period` command.

Variable	Definition
<0-360>	Specifies the number of days after which a user is disabled if he does not use the account. Default is 0 days.

Configuring password unlock timer

About this task

Configure the number of days after which a disabled user account due to inactive period is re-enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure password unlock timer:

   ```
   password unlock-timer <1–365>
   ```

3. Disable or return password unlock timer to default value:

   ```
   default password unlock-timer
   ```

4. Verify the settings:

   ```
   show password unlock-timer
   ```

Example

```
Switch# show password unlock-timer
Unlock-timer value is 1 days
```

Variable definitions

The following table describes variables that you use with the **`password unlock-timer`** command.

Variable	Definition
<1-365>	Specifies the number of days after which a disabled user account due to inactivity period is re-enabled. Default is 7 days.

Configuring multiple local read-write (RW) and read-only (RO) users accounts

Use the following procedure to create, modify and delete local users.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. To create a user, enter the following command:

```
username add <username> role-name {RO|RW} [password]
```

3. To delete a user, enter the following command:

```
no username <username>
```

4. To enable a user, enter the following command:

```
username <username> enable
```

5. To disable a user, enter the following command:

```
no username <username> enable
```

6. To change the password for a specific user, enter the following command:

```
username <username> password
```

7. To change the password for the current user, enter the following command:

```
username password
```

8. To reset the settings for a user to default, enter the following command:

```
default username <username>
```

9. To enable or disable ssh access for a user enter the following command:

```
username <username> ssh-access [enable | disable]
```

10. To enable or disable telnet access for a user enter the following command:

```
username <username> telnet-access [enable | disable]
```

Variable Definitions

Variable	Value
<username>	Specifies the user name.

Displaying local user information

Use the following procedure to display local user information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display all users currently logged on to the system:

```
show who
```

3. Display all usernames and roles:

```
show username
```

4. Display information related to a specific user:

```
show username <username>
```

5. Display role-related information:

```
show role
```

Variable Definitions

Variable	Value
<username>	Specifies the user name.

Configuring lockout for failed logon attempts

Use the information in this section to configure the lockout for failed logon attempts feature.

Configuring the number of retries for failed logon attempts

Use the following procedure to configure the number of retries for failed logon attempts.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the number of times the user can enter an incorrect password for telnet before the connection closes:

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

3. Configure the number of times the user can enter an incorrect password for SSH before the connection closes:

```
ssh retries <1-100>
```

Variable Definitions

Use the data in the following table to use the **`telnet-access retry`** and **`ssh retries`** commands.

Variable	Value
<1-100>	Specifies the number of times the user can enter an incorrect password before the connection closes for Telnet. Enter an integer from 1–100. After upgrade the number of retries is 3. At default the number of retries is 3 for Telnet

Table continues…

Variable	Value
<1-100>	Specifies the number of times the user can enter an incorrect password before the connection closes for SSH. Enter an integer from 1–100. After upgrade the number of retries is 3. At default the number of retries is 3 for SSH.

Configuring the number of retries for user lockout

Use the following procedure to configure how many incorrect logins are allowed until the user is locked out.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the number of lockout retries:

   ```
   username lockout-retries <0-100>
   ```

3. Reset the number of lockout retries to default:

   ```
   default username lockout-retries
   ```

Variable definitions

The following table describes variables that you use with the **`username lockout-retries command`** command.

Variable	Definition
<0-100>	Specifies the number of incorrect password logins until the user is locked-out. Default value is 0 (no lockout).

Configuring the lockout interval for failed logon attempts

Use the following procedure to configure the lockout interval for failed logon attempts.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the lockout interval:

   ```
   username lockout-time <0-60>
   ```

3. To reset the lockout interval to default, enter the following command:

   ```
   default username lockout-time
   ```

Variable Definitions

Use the data in the following table to use the **username lockout-time** command.

Variable	Value
<0-60>	Specifies the duration (in minutes) of session lockout which occurs when the threshold on the number of incorrect loggins is exceeded. Default value is 1 minute.

Unlocking a locked-out user

Use the following procedure to unlock a locked-out user.

Before you begin

Log on with RW rights.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Unlock a locked-out user:

   ```
   username <username>  unlock
   ```

Variable Definitions

Use the data in the following table to use the **username unlock** command.

Variable	Value
<username>	Specifies the user account to unlock.

Configuring the inactivity timeout for administrative access

Use the following procedure to configure the inactivity timeout for administrative access.

Following an inactivity period, all administrative connections to the switch (telnet, web or SSH) are closed when a timeout value is reached. The default timeout value is 15 minutes.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Set the inactivity timeout value:

   ```
   telnet-access inactive-timeout <0-60>
   ```

Variable Definitions

Use the data in the following table to use the **telnet-access inactive-timeout** command.

Variable	Value
<0-60>	Specifies in minutes the duration before an inactivity session terminates

CLI Audit log configuration

CLI Audit provides a means for tracking CLI commands.

Displaying the CLI audit log

About this task

Displays the command history audit log stored in NVRAM.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display the CLI audit log.

   ```
   show audit log [asccfg | config | serial | telnet]
   ```

Example

```
Switch#show audit log config
Audit Log Save To NVRAM: Enabled
```

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.

Configuring the CLI audit log

About this task

Enables or disables the CLI audit log. You can also set the audit log to default (enabled).

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable CLI audit log.

   ```
   audit log save
   ```

   OR

   ```
   default audit log
   ```

3. Disable CLI audit log.

   ```
   no audit log
   ```

Example

```
Switch(config)#default audit log
Switch(config)#show audit log config
Audit Log Save To NVRAM: Enabled
```

Configuring the web server for client browser requests

Before you begin

- Enable SSL.

About this task

Configures the web server to respond to HTTPS only, or both HTTPS and HTTP client browser requests when SSL is enabled.

The default is https-only.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the web server to respond to HTTPS client browser requests only.

   ```
   https-only
   ```

3. Configure the web server to respond to both HTTPS and HTTP client browser requests.

   ```
   no https-only
   ```

Viewing the web server client browser request configuration

About this task

Displays whether the web server is configured to respond to HTTPS only, or both HTTPS and HTTP client browser requests when SSL is enabled.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display web server client browser request configuration.

   ```
   show https-only
   ```

Example

```
Switch#show https-only
HTTPS only: enabled
```

Disabling IP Source Guard using CLI

Follow this procedure to disable IP Source Guard to allow all IP traffic to go through without being filtered.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable

   configure terminal

   interface ethernet <port number>
   ```

2. Disable IP Source Guard.

   ```
   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`** 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 CLI

This section describes procedures to display, configure, and disable the trace level feature. This troubleshooting feature provides dynamic detailed error and event information.

Displaying trace information using CLI

Follow this procedure to show trace level information for the modules and the supported module list.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Show trace level information for the modules.

   ```
   show trace level
   ```

   OR

   Show the supported module list.

   ```
   show trace list
   ```

Configuring trace using CLI

Use this procedure to configure trace level and trace output to the console.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. **(Optional)** Display the available module or submodule options:

   ```
   trace module hint
   ```

   OR

   ```
   trace module {ospf | igmp | pim | rip |eap | ntp | ipmc} submodule
   hint
   ```

3. Display the trace status:

   ```
   show trace status
   ```

4. Configure the trace level:

   ```
   trace module {ospf | igmp | pim | rip |eap | ntp | ipmc} [submodule
   <submodule_ID>] level {critical | error | warning | info | debug |
   no-display} [unit <1-8>]
   ```

   OR

   Set trace screen on or off:

   ```
   trace screen <enable|disable>
   ```

Note:

The default is disable (off).

Variable Definitions

The following table describes the parameters for configuring the **`trace`** command.

Variable	Value
module	Sets the trace module: • OSPF • IGMP • PIM • RIP • EAP • NTP • IPMC
level	Sets the trace level: • critical—displays only critical level errors • error—displays critical and error levels • warning—displays errors from critical to warning • info—displays informational errors • debug— displays all errors • no-display—disables error displaying **Note:** For **`trace`** to display any information, the trace level must be different from *no-display* for at least one module, and trace output must be enabled.
<enable | disable>	Enable indicates the trace feature is on. Disable is the default and indicates the trace screen is off. **Note:** For troubleshooting purposes, the trace screen should be on (enable).

Disabling trace using CLI

Use this procedure to disable the trace for all modules.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Disable the trace for all modules.

```
trace shutdown
```

Security configuration and management using Enterprise Device Manager

This section describes the methods and procedures necessary to configure security on the switch using Enterprise Device Manager (EDM).

Enabling VoIP VLAN using EDM

Use the following procedure to activate the VoIP VLAN.

Procedure

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.

   Repeat Step 4 and Step 5 until all required parameters have been amended.
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

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 the 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 respond to both HTTPS and HTTP client browser requests. **Important:** 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

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: • 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: • 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.
SecurityAction	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. A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include: • 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.

Table continues…

Variable	Value
	Important: da means destination addresses.
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
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.

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

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 displays.
5. Type a number for the security list in the **SecurityListIndx** 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
SecurityListIndx	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

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. Clear 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
SecurityListIndx	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

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
SecurityListIndx	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.

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

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 displays.
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 **AccessCtrlType** to allow a MAC address on multiple ports.

   OR

Clear **AccessCtrlType** to disallow a MAC address on multiple ports.

10. Type a value in the **SecureList** 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
BrdIndx	Indicates the index of the board. This corresponds to the unit. **Important:** If a BrdIndx is specified, the SecureList field is 0.
PortIndx	Indicates the index of the port. **Note:** If a PortIndx is specified, the SecureList field is 0.
MACIndx	Indicates the index of MAC addresses that are designated as `allowed` (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 `node allowed` . A MAC address can be allowed on multiple ports.
SecureList	Indicates the index of the security list. This value is meaningful only if BrdIndx and PortIndx values are set to zero. For other board and port index values, 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: • **Static** • **Sticky** • **AutoLearn**
Lifetime	Indicates the time period before the system automatically deletes an AuthConfig entry.

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

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**.

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

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 `node allowed` or `node blocked type`.
CurrentActionMode	Indicates the value representing the type of information contained, including: • noAction—Port does not have security assigned to it, or the security feature is turned off. • partitionPort—Port is partitioned.

Table continues…

Variable	Value
	• partitionPortAndsendTrap— Port is partitioned and traps are sent to the trap receive station. • Filtering—Port filters out the frames, where the destination address field is the MAC address of unauthorized station. • FilteringAndsendTrap—Port filters out the frames, where the destination address field is the MAC address of unauthorized station. Trap are sent to trap receive station. • sendTrap—A trap is sent to trap receive stations. • 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: • 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

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
BrdIndx	Indicates the index of the board. This corresponds to the slot containing the board. The index is 1 where it is not applicable.
PortIndx	Indicates the index of the port on the board. This corresponds to the port on that a security violation was seen.

Table continues…

Variable	Value
MACAddress	Indicates the MAC address of the device attempting unauthorized network access (MAC address-based security).

Configuring Mac DA filters using EDM

Use the following procedure to configure Mac DA filters using EDM.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **MAC Security**.
3. Click the **Mac DA Filters** tab.
4. On the toolbar, click **Insert**.
5. Type a value in the **Index** box.
6. Type a value in the **MacAddress** box.
7. Click **Insert**.

Variable definitions

Use the data in the following table to use the **Mac DA Filters** tab

Variable	Value
Index	Indicates the MAC address index (10 addresses can be configured).
MacAddress	Indicates the MAC address index (10 addresses can be configured).

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

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	Specifies the type of the password to use. Values include: • 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	Specifies the read-only password for stack or switch access. The following are the requirements for the password: • The maximum length is 255 characters. • Password must contain 10 characters. A minimum of two uppercase characters, two lowercase characters, two numbers, and two special characters.
Read-Write Switch Password	Specifies the read-write password for stack or switch access. The following are the requirements for the password: • The maximum length is 255 characters. • Password must contain 10 characters. A minimum of two uppercase characters, two lowercase characters, two numbers, and two special characters.

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

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: • 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. The following are the requirements for the password: • The maximum length is 255 characters. • Password must contain 10 characters. A minimum of two uppercase characters, two lowercase characters, two numbers, and two special characters.
Read-Write Stack Password	Specifies the read-write password for stack or switch access. The following are the requirements for the password: • The maximum length is 255 characters. • Password must contain 10 characters. A minimum of two uppercase characters, two lowercase characters, two numbers, and two special characters.

Chapter 4: Dynamic Host Configuration Protocol Snooping

This chapter provides conceptual information and procedure to configure Dynamic Host Configuration Protocol (DHCP) Snooping using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

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 per unit.

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 81for 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 Command Line Interface (CLI), Enterprise Device Manager (EDM), and SNMP.

For more information about configuring DHCP snooping through CLI see DHCP snooping configuration using CLI on page 83. For more information about configuring DHCP snooping through EDM, see DHCP snooping configuration using EDM on page 95.

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 Ethernet Routing Switch 4900 and 5900 Series.

DHCP snooping configuration using CLI

This section describes how you can configure DHCP snooping to provide security to your network by preventing DHCP spoofing, using CLI.

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 CLI

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 the following procedure to enable or disable DHCP snooping for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enable DHCP globally.

   ```
   [default] [no] ip dhcp-snooping <enable> <option82>
   ```

Variable definitions

Use the data in the following table to use the **`ip dhcp-snooping`** command.

Variable	Value
<enable>	Enables DHCP snooping globally on the switch.
[default]	Configures DHCP snooping on the switch to default values.
[no]	Disables DHCP snooping globally on the switch.
<option82>	When selected, enables DHCP snooping with Option 82 globally on the switch.

Viewing the global DHCP snooping configuration

Use the following procedure to view the global DHCP snooping configuration to review and confirm the DHCP snooping configuration for the switch.

Procedure

1. Enter User EXEC mode.
2. View the global DHCP snooping configuration.

   ```
   show ip dhcp-snooping
   ```

Configuring VLAN-based DHCP snooping using CLI

You must enable DHCP snooping separately for each VLAN. If DHCP snooping is disabled on a VLAN, the switch forwards DHCP reply packets to all applicable ports, regardless of whether the port is trusted or untrusted.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable DHCP snooping on a VLAN.

   ```
   [default] [no] ip dhcp-snooping vlan <vidlist> [option82]
   ```

Variable definitions

Use the data in the following table to use the **`ip dhcp-snooping vlan`** 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.
<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.
[option82]	When selected, enables DHCP snooping with Option 82 on a VLAN.

Viewing the VLAN-based DHCP snooping configuration using CLI

View the VLAN-based DHCP snooping configuration to review and confirm the DHCP snooping configuration for a VLAN.

Procedure

View the VLAN-based DHCP snooping configuration.

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

The output displays only the VLANs enabled for DHCP snooping.

Configuring port-based DHCP snooping using CLI

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

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. Configure port-based DHCP snooping.

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

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

   ```
   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.
option82-subscriber-id <WORD>	Specifies the DHCP Option 82 subscriber Id for the port. Value is a character string between 0 and 64 characters.
<portlist>	Specifies a port or group of ports.
<trusted>	When selected, the port or ports automatically forward DHCP replies.

Table continues…

Variable	Value
<untrusted>	When selected, the port or ports filter DHCP replies through DHCP snooping.

Viewing the port-based DHCP snooping configuration using CLI

View the port-based DHCP snooping configuration to review and confirm the DHCP snooping configuration for a port or group of ports.

Procedure

View the VLAN-based DHCP snooping configuration

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

The output displays only the VLANs enabled for DHCP snooping.

Variable definitions

The following table defines optional parameters that you can enter with the **`show ip dchp-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 CLI

Use this procedure to add entries for devices with static IP addresses to the DHCP binding table.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Add entries to the DHCP binding table.

   ```
   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`** 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.
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 CLI

Use this procedure to delete entries for devices with static IP addresses from the DHCP binding table.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Delete entries from the DHCP binding table.

   ```
   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

Use this procedure to display DHCP binding table entries.

Note:

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.

Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display the DHCP binding table:

```
show ip dhcp-snooping  binding  [address <A.B.C.D> | <H.H.H >] [port
<portlist>][summary]
```

Variable definitions

Use the data in the following table to use the `show ip dhcp-snooping  binding` command.

Variable	Definition
address <A.B.C.D>	Identifies the access port for a specific MAC or IP address.
[port <portlist>]	Identifies MAC and IP addresses binding from a specific port or list of ports.
summary	Displays the DHCP snooping binding table summary.

Configuring DHCP Snooping external save using CLI

Use this procedure to save the DHCP Snooping database to an external USB drive or TFTP

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. Synchronize the switch with an NTP server.
3. Configure DHCP Snooping external save.

```
ip dhcp-snooping external-save [enable] {[tftp <ipv4address> |
<ipv6address> | [usb <unit 1-8> ]} filename <filename>
```

Variable definitions

The following table defines parameters that you enter with the **`ip dhcp-snooping external-save`** command.

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.

Table continues…

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.

Before you begin

- 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 the server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. 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

Use the data in the following table to use the **`ip dhcp-snooping external-save sftp`** command.

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 CLI

Use this procedure to disable DHCP Snooping external save for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable DHCP Snooping external save.

   ```
   no ip dhcp-snooping external-save enable
   ```

   OR

   ```
   default ip dhcp-snooping external-save
   ```

Restoring the externally-saved DHCP Snooping database using CLI

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.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Restore the externally-saved DHCP Snooping database.

   ```
   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. 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.

OR

3. 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 CLI

Use this procedure to display DHCP Snooping external save configuration information for the switch.

Procedure

Display DHCP Snooping external save configuration information

```
show ip dhcp-Snooping external-save
```

Example

```
Switch>enable
Switch#show ip dhcp-snooping external-save
DHCP Snooping external save: Disabled
DHCP Snooping external device:
DHCP Snooping external filename:
DHCP Snooping external last sync:
DHCP Snooping external sync flag: True (changes will be synchronized at next wr
ite)
```

DHCP Snooping Layer 2 configuration using CLI example

Figure 2: Layer 2 configuration example on page 92 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 Layer 2 VLAN (VLAN #1 by default). You can configure the DHCP client lease time on the DHCP server.

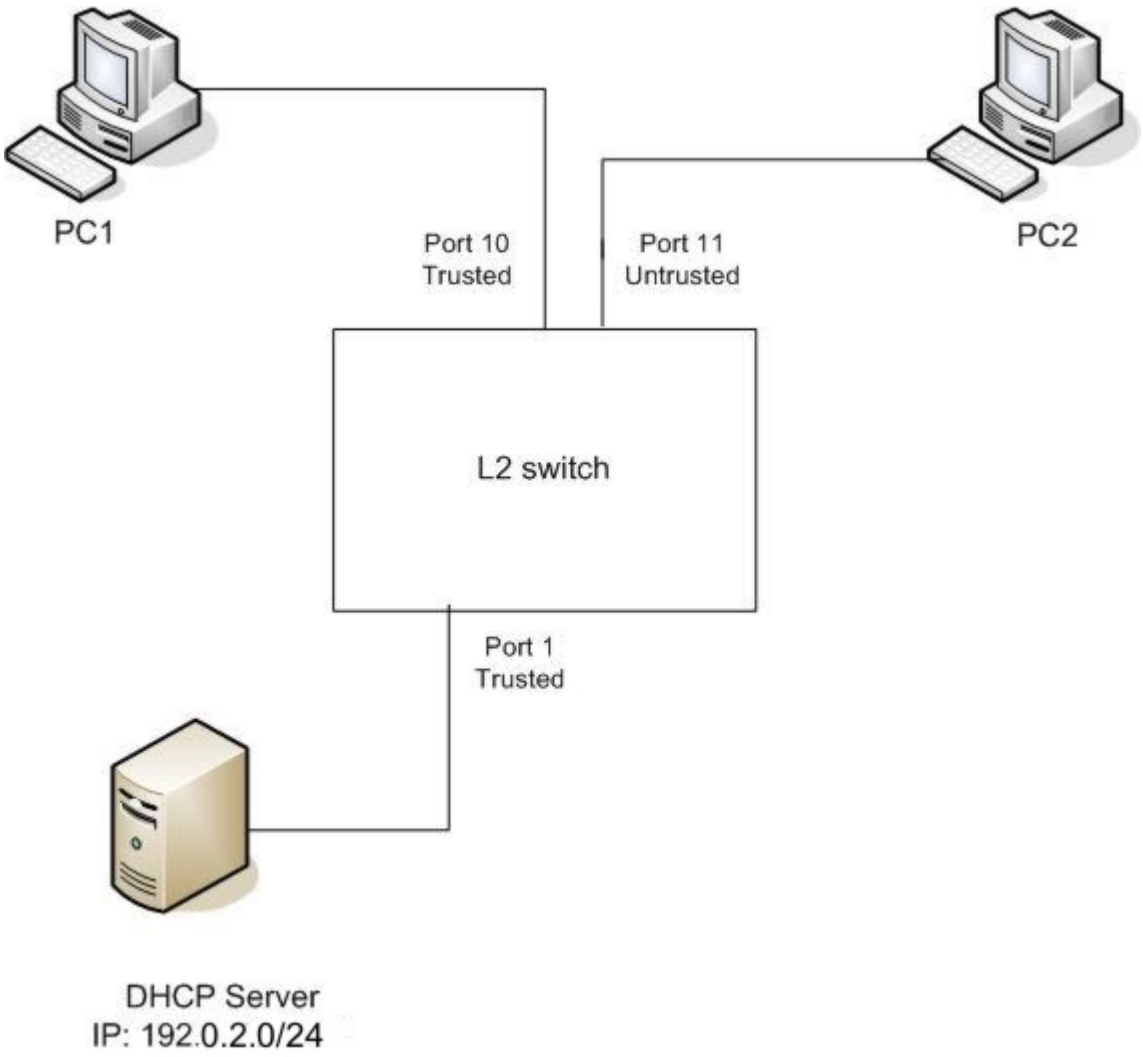


Figure 2: Layer 2 configuration example

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 in this configuration example.

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 CLI 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.

```
Switch(config)# show ip dhcp-snooping


Global DHCP snooping state: Enabled
DHCP
VLAN Snooping
---- --------
1 Enabled
```

```
Switch(config)# show ip dhcp-snooping interface 1,10,11


DHCP
Port Snooping
---- --------
1 Trusted
10 Trusted
11 Untrusted
```

```
Switch(config)# show ip dhcp-snooping binding


MAC IP Lease (sec) VID Port ----------------------------------------
--------------------
Total Entries: 0
```

```
Switch# sho running-config


! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch <Switch#>
! Software version = vx.x.x.x
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.

```
Switch(config)# show ip dhcp-snooping binding


MAC IP Lease (sec) VID Port ------------------------------------
--------------------------
00-02-44-ab-2d-f4 192.0.2.10 86460 1 11
Total Entries: 1
```

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.

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.

Procedure

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**.

Configuring DHCP Snooping external save using EDM

Use the following procedures to store the DHCP Snooping database to:

- an external TFTP server. See Configuring_DHCP_Snooping_external_save_to_an_external_TFTP_server on page 96.
- an external SFTP server. See Configuring_DHCP_Snooping_external_save_to_an_external_SFTP_server on page 97.
- a USB drive. See Configuring_DHCP_Snooping_external_save_to_a_USB_drive on page 98.

Configuring DHCP Snooping external save to an external TFTP server

Use this procedure to store the DHCP Snooping database to an external TFTP server.

Procedure

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** check box to enable DHCP Snooping external save.

   OR

   In the DHCP Snooping External Save section, clear the **Enabled** check box 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**.

Variable definitions

Variable	Value
DHCP Snooping External Save	
Enabled	Enables or disables DHCP Snooping External Save.
SyncFlag	Indicates if changes in the DHCP Snooping binding table are synchronized on the external device. Values include: • 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.

Table continues…

Variable	Value
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 external save to an external SFTP server

Use this procedure to store the DHCP Snooping database to an external SFTP server.

Procedure

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** check box to enable DHCP Snooping external save.

   OR

   In the DHCP Snooping External Save section, clear the **Enabled** check box to
5. Click an **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**.

Next steps

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.
- Configure the sshc user name.
- Configure the sshc password if it is needed for restore.

Variable definitions

Variable	Value
DHCP Snooping External Save	
Enabled	Enables or disables DHCP Snooping External Save.
SyncFlag	Indicates if changes in the DHCP Snooping binding table are synchronized on the external device. Values include: • 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 external save to a USB drive

Use this procedure to store the DHCP Snooping database to a USB drive.

Procedure

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** check box to enable DHCP Snooping external save.

   OR

In the DHCP Snooping External Save section, clear the **Enabled** check box 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.
SyncFlag	Indicates if changes in the DHCP Snooping binding table are synchronized on the external device. Values include: • 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

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: select **true** to enable DHCP snooping for the VLAN, or select **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: select **true** to enable DHCP snooping with Option 82 for the VLAN, or select **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

1. Proceed with one of the following paths:
   - From the navigation tree, double-click **Security**, click **DHCP Snooping**, then select the **DHCP Snooping-port** tab.
   - From the **Device Physical View**, use Ctrl-click to select more than one port, right-click **Edit** then click the **DHCP Snooping** tab.

- From the **Device Physical View**, use Ctrl-click to select more than one port, then follow the navigation tree to **Edit > Chassis > Ports > DHCP Snooping** tab.

2. In the port row, double-click the cell in the **DhcpSnoopingIfTrusted** column.
3. Select a value from the list: select **trusted** or **untrusted**.
4. Double-click the **DhcpSnoopingIfOption82SubscriberId** for a port.
5. Type a subscriber ID value for the port.
6. 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 perform the following procedures:

- View DHCP client lease static entries. See Viewing_DHCP_binding_information_using_EDM on page 101.
- Create DHCP client lease static entries. See Creating_static_DHCP_binding_table_entries_using_EDM on page 102.
- Delete DHCP client lease static entries. See Deleting_DHCP_binding_table_entries_using_EDM on page 103.

Viewing DHCP binding information using EDM

Use the following procedure to view DHCP binding information.

Procedure

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

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 displays.
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

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.

Chapter 5: Dynamic Address Resolution Protocol Inspection

This chapter provides conceptual information and procedures to configure Dynamic Address Resolution Protocol (Dynamic ARP) Inspection using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

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 81.

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 CLI or Enterprise Device Manager (EDM). For more information about configuring this feature with CLI, see Configuring dynamic ARP inspection on page 105. For more information about configuring this feature with EDM, see Configuring_dynamic_ARP_inspection_on_VLANs_using_EDM on page 111 and Configuring_dynamic_ARP_inspection_on_ports_using_EDM on page 111.

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 104.

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 VLANs on page 105.
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 106.

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 CLI on page 83or Configuring global DHCP snooping using EDM on page 95.

Enabling dynamic ARP inspection on the VLANs

You must enable dynamic ARP inspection separately for each VLAN.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable dynamic ARP inspection on a VLAN.

   ```
   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.

Disabling dynamic ARP inspection on the VLANs

Use the following procedure to disable dynamic ARP inspection on the VLANs.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable dynamic ARP inspection on a VLAN.

   ```
   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

Use this procedure 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.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. 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.

   ```
   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.

Returning a port or range of ports to default values

Use this procedure to return a port or range of ports to default values.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. Return a port or range of ports to default values.

   ```
   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.

Returning all ports in the interface to default values

Use this procedure to return all ports to default values.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. Return all ports in the interface to default values.

   ```
   default ip arp-inspection port ALL
   ```

Viewing dynamic ARP inspection settings

Use this procedure to view the VLANs on which dynamic ARP inspection has been enabled.

Note:

Either Global Configuration mode or Interface Configuration mode can be used.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. OR

   Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

3. View the VLANs on which dynamic ARP inspection has been enabled.

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

   The output lists only the VLANs enabled for dynamic ARP inspection.

Viewing ports and their associated dynamic ARP inspection status (trusted or untrusted)

Follow this procedure to view ports and their associated dynamic ARP inspection status (trusted or untrusted).

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.

Note:

Either Global Configuration mode or Interface Configuration mode can be used.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. OR

   Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

3. View port settings.

   ```
   show ip arp-inspection interface [<interface type>] [<port>]
   ```

Dynamic ARP inspection Layer 2 configuration example

This configuration example uses the same network setup and configuration created in the DHCP snooping configuration using CLI on page 83 section and illustrated by DHCP snooping layer 2 configuration using CLI example on page 91. 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 DHCP snooping configuration using CLI on page 83.

```
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
```

```
Switch# sho running-config



! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch <Switch#>
! Software version = vx.x.x.x
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
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.

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

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 Step 3 through Step 5 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

1. Proceed with one of the following paths:
   - From the navigation tree, double-click **Security**, click **Dynamic ARP Inspection (DAI)**, then select the **ARP Inspection-port** tab.
   - From the **Device Physical View**, use Ctrl-click to select more than one port, right-click **Edit** then click the **ARP Inspection** tab.
   - From the **Device Physical View**, use Ctrl-click to select more than one port, then follow the navigation tree to **Edit > Chassis > Ports > ARP Inspection** tab.
2. Double-click the **ARPInspectionIfTrusted** cell for a port.
3. From the list, select **trusted** or **untrusted**.
4. Repeat the above steps for additional ports as required.
5. Click **Apply**.

Chapter 6: Enhanced Secure Mode

This chapter provides conceptual information on Enhanced Secure Mode and procedures to configure Enhanced Secure Mode using Command Line Interface (CLI).

Enhanced Secure Mode

The switch defaults to higher level of security when Enhanced Secure Mode is enabled.

The following security enhancements are available in this operating mode:

- The switch supports multiple role-based access levels.
- Every attempt to access the product requires a username and password to be presented for authentication.
- The switch enforces stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.
- The audit logging is enabled by default and cannot be disabled or modified. The audit records all valid activities performed on the system, including the identity of each user through its username, IP and session ID and the date and time stamp of access attempt. If you configure a remote Syslog server, the switch sends each issued command and security log to this remote server. The log file is not affected by a restart, default boot or upgrade. Log encryption is supported.
- The command for configuring the switch banner provides an option to display the DoD approved banner.
- TFTP protocol is disabled by default.
- The switch uses NTP as default clock source. NTP authentication keys are hidden in CLI and ASCII config.

By default, enhanced secure mode is disabled. You must restart the switch after enabling or disabling the feature in order to apply the new setting.

Note:

Starting with 7.4.1, configuration is transferable between operating modes with enhanced secure mode enabled and secure mode disabled. When switching modes of operation, the switch or stack does not reset to default configuration.

Feature operation when Enhanced Secure Mode is enabled

The following table contains information about feature functionality when Enhanced Secure Mode is enabled.

	Enhanced Secure Mode enabled	Enhanced Secure Mode disabled
Syslog:		
Secure Syslog	Supported through the Mocana SSH Port forwarding tunnel support	No SSH Port forwarding tunnel support
Remote Syslog connection type	UDP, TCP or SSH secured TCP connection	UDP connection
Clock, Network Time Protocol Clients:		
Default clock source	The switch uses NTP as default clock source	The switch uses SNTP as default clock source
NTP authentication key support	SHA1	MD5 (Enhanced Secure Mode enabled)
NTP authentication keys visibility	The switch hides NTP authentication keys in CLI and ASCII config	NTP authentication keys are not hidden
Authentication/Access-level and Banner Requirements:		
Password protection	The switch requires password to gain administrative access to the switch	The switch allows login without authentication
Maximum wait time for TCP connections to be established with the switch	10 seconds or less	75 seconds or less
TFTP Protocol	TFTP protocol is turned off by default	TFTP protocol is turned on by default
Authentication	Every attempt to access requires a username and password	Only when authentication is set, username and password is required
Telnet-Access	Telnet access is enabled by default, permitting any existing user ID in the system (including any default user ID)	Telnet access is enabled by default.
Local user accounts database	Role based. The switch supports multiple configurable roles.	Access rights based. The switch only supports read-write (RW) and read-only (RO) users.
Initial userID/Password	The default username and password are *admin/password*	When authentication is enabled, default users are *RW* and *RO* with *secure* and *user* passwords.
Banner	The default banner is the static banner.	The default banner is the static banner.

Upgrade considerations

Upgrading from a previous version not supporting Enhanced Secure Mode maintains the existing non Enhanced Secure configuration. If you switch to Enhanced Secure Mode after upgrade, the configuration is defaulted.

Upgrading to a newer release supporting Enhanced Secure Mode maintains the existing configuration parameters including the following:

- Users and passwords
- Network configuration
- Settings for TFTP, TELNET, SSH protocols.

Multiple user roles

When Enhanced Secure Mode is enabled, the switch supports multiple management accounts and role-based authentication.

Each username is associated with a certain role. Each role provides authorization rights for viewing or executing groups of commands. The Security Administrator can create groups of CLI commands (or use the default groups of commands) and associate some groups to a role, specifying which rights the role has for each group of commands

There are four default roles on the switch. Each of these roles grants user access to configuring or viewing specific command groups. The Security Administrator can also define other roles.

The switch provides the following default roles:

- System security administrator
- System administrator
- Application administrator
- Emergency user

Note:

When Enhanced Secure Mode is enabled, the EDM interface is disabled by default. After enabling the web server, only a user associated with the Security Administrator role can access the EDM interface.

The administrator initially logs on to the switch using the default login of *admin* and the default password of *password*. After the first login, the switch prompts the administrator to create a new username and password. The new user has Security Administrator privileges and the initial administrator user is deleted.

Note:

By default, the switch does not allow repeated characters or sequential characters in the new passwords. Sequential strings include the following ones, in forward and reverse order, uppercase letters included:

- `abcdefghijklmnopqrstuvwxyz`
- `01234567890`
- `qwertyuiop`
- `asdfghjkl`
- `zxcvbnm`
- `!@#$%^&*()`

The Security Administrator then creates other users and configures default passwords for them. After the first authentication, the switch prompts each user to create a new password, in order to ensure that the user is the only person knowing the password associated with his account. After the new username and password are entered, the default username and password are deleted and no subsequent attempts to login to the switch using the default username and password are permitted.

User access can be restricted based on time of day interval. The number of concurrent sessions for a user is configurable, with a default of 12 sessions.

When a login attempt fails, it can be due to an invalid username or an invalid password. In either case, there is no error feedback indicating which of two failed. There are no differences between the response time for entering an invalid username or an invalid password for that username, as a time difference can be used to determine that a username failed and not the password.

Note:

Reset the switch to factory default if the switch manager loses or forgets access credentials and the switch gets locked,

Remote access

The switch supports RADIUS or TACACS-based remote user authentication and authorization. When a remote server is not available, local authentication is available.

The RADIUS server allows three types of users: Security, System and Application administrators. The users can login through SSH, Telnet and serial every time the server is accessible and the proper key is configured. The Security Administrator can also login through Web. All successful connections are audited.

The TACACS+ server allows Security administrator user and accepts SSH, Telnet and serial connection if the TACACS+ server is accessible and has configured the proper key. All successful logins are audited.

Default roles

The following table details the access level for the default roles.

Access level	Description
Security administrator	The Security administrator access level permits read-write access to create, delete other logins, create, delete, modify or assign roles, install ASG keys, install licenses, install PKI certificates and keys and read-write access to system parameters such as IP addresses or upgrade software, and the ability to start and stop services.
Emergency Administrator	This privilege access level has the same rights as security administrators but can log on by serial even if another authentication method is set on switch. An account timeout can be set for the account assigned with this role. The user with emergency administrator role can log on device only by serial or telnet port, not by SSH or Web. This user is also the only account allowed for RADIUS or TACACS+ authentication fallback, in case the connectivity to remote access servers is temporarily lost.
Application Administrator	The Application Administrator has read-only access to most switch configurations and status information.
System Administrator	The System Administrator has read-write access to system parameters such as IP addresses or upgrade software, and has the ability to start and stop services.

Default command groups

The following table contains details about the default command groups.

CLI command group	CLI commands general description
cli-basic-group	Contains all the commands available for all the users: `configure terminal, default, enable, end, exit, interface *, logout, no, show, username password *`
security-cmds-group	Contains the commands related to logins, access to the debug menu, create, delete, modify user accounts, assign or define roles and command groups: `banner *, cli *, cli-command-group *, cmd-interface *, dbg *, menu *, password *, role *, tech *, ssh *, ssl *, system last-exception *, username *, web-server *`

Table continues…

CLI command group	CLI commands general description
system-cmds-group	System command group which contains all system commands: `accept *, adac *, application *, area *, arp *, arp-table *, as-boundary-router *, asset-id *, auto-negotiation-advertisements *, auto-negotiation-capabilities *, auto-pvid *, auto-vlink *, autosave *, autotopology *, blink-leds * , boot * , brouter *, cfm *, clear *, clear-stats *, clock *, config-network *, config-usb-loadonboot *, configure *, copy *, count *, cpu-utilization *, csnp-interval *, ddi-logging *, default-cost *, default-metric *, device-role*, disable *, download *, duplex *, eap-all *, eapol *, ecmp *, edm *, enable *, end *, energy-saver *, enhanced-secure-mode *, environmental *, except *, exit *, fa *, find *, flash *, flowcontrol *, head *, help *, hop-limit *, host-route *, http-port *, https-only *, https-port *, i-sid *, install *, interfaces *, ip *, ip-blocking *, ip-source-address *, ipmgr *, ipv6 *, is-type *, isis *, ist * , jumbo-frames *, l2 *, lacp *, license *, link-state *, lldp *, logging *, logout *, mac-address-table *, mac-security *, managed-config-flag *, manual-area *, manualtrigger *, match *, max-lsp-gen-interval *, maximum-path *, memory-utilization *, mem-show *, metric *, mgmt.-port *, min-lsp-gen-interval *, mlt *, mvr *, name *, network *, no-more *, nsna *, ntp *, nvram *, ospf *, overload *, overload-on-startup *, ping *, ping-virtual-address *, poe *, poe-main-status *, poe-port-status *, poe-power-measurement *, poe-shutdown *, port-mirroring *, port-statistics *, preference *, psnp-interval *, qos *, quickconfig * , radius *, radius-server *, range *, rate-limit *, redistribute *, reload *, renew *, renumber *, restore *, retransmit-lsp-interval *, rfc1583-compatibility *, rip *, rmon *,`

Table continues…

CLI command group	CLI commands general description
	route-map *, router *, router-id *, router-preference *, run *, running-config *, save *, script *, serial-console *, serial-security *, shared-port *, sftp-server *, shutdown *, slamon *, slpp *, slpp-guard *, smlt *, snmp *, snmp-server *, sntp *, spanning-tree *, spbm *, speed *, spf-delay *, sshc *, stack *, stack-info *, stack-monitor *, storm-control *, sys-info *, sys-name *, system, system verbose *, system-id *, tacacs *, tail *, tdr *, telnet *, telnet-access *, terminal *, tftp-access *, tftp-server *, timers *, toggle-next-boot-image *, trace *, traceroute *, trap *, ui-button *, usb-files *, usb-host-port *, vlacp * , vlan *, wan-mode *, write *, who *
audit-cmds-group	audit *

Limitations

The following feature limitations apply:

- The switch supports up to 32 CLI command groups.
- The switch supports up to 32 roles.
- The switch supports up to 10 user accounts.
- The switch supports one account for emergency user.
- The Emergency user can login only via serial or Telnet.
- The lockout is disabled after reset.
- Time settings function only when the clock source is synchronized.
- The switch supports user login via SSH, using username and password, DSA key or RSA key. If the Security administrator loads a public key on switch, the user that has the corresponding private key can log on switch as any user, including the security_admin.

Note:

Only a public key can be stored on switch.

Audit logging in enhanced secure mode

Audit logging allows the recording of CLI commands issued on the switch or stack in an unalterable audit file. The feature is enabled by default in Enhanced Secure Mode and cannot be disabled or altered by any individual.

Only the Security, Emergency or System administrators have access to the audit log . The Security or Emergency administrators can also configure the encryption of the log file.

The audit log survives a restart and initialization of the switch. Every command issued on the switch is stored in the local log. If a remote syslog server is configured, each command is also sent to it. The audit log cannot be deleted, except through disabling the Enhanced Secure Mode, which resets the switch to default settings. For this reason, the commands *audit log save* and *no audit log* do not exist in enhanced secure mode.

Note:

The maximum number of records in the local audit log is 159, with newer entries replacing the oldest. On the remote syslog server there is no such limit, meaning that the remote server can record a complete history of the commands issued on the switch.

The following table details the audit logging behavior when Enhanced Secure Mode is enabled or disabled.

	Enhanced Secure ON mode	**Enhanced Secure OFF mode**
Log File encryption	The log is encrypted with Mocana AES encryption.	No encryption
Access	• The audit log is unalterable by any individual. • The contents are available only to Security, Emergency and System administrators. • The default encryption key can be modified only by the Security and Emergency Administrators. • The log cannot be deleted except through switching the security mode.	• All users can view the audit log. • The log cannot be deleted except through switching the security mode.
Tracking	The identity of each user is tracked by the audit record through its username, IP and session id.	The identity of users is tracked by the audit record through its username and role only if user authentication is enabled.
Recording	Records the date and time stamp of access attempt.	Records the date and time stamp of access attempt.
	Records all valid activities performed on the system.	Records only the commands.
	The audit file captures the following events: • All successful log-in attempts • Invalid user authentication attempt • Unauthorized attempts to access system resources	The audit log does not record the security relevant actions.

Table continues…

	Enhanced Secure ON mode	Enhanced Secure OFF mode
	• Each logout or session termination • All software downloads	
Login, logout and session initiation	The audit system is configured to audit login, logout and session initiation.	No support.
Audit trail	Protected against modification or deletion.	No support.
Log storage on a non-volatile medium	The device supports log storage on a non-volatile medium. The log is not affected by a restart or a default boot.	The device supports log storage on a non-volatile medium. The log is not affected by a restart or a default boot.

Configuring Enhanced Secure Mode

Use the procedures in this section to configure Enhanced Secure Mode.

Enabling Enhanced Secure Mode

Use the following procedure to enable Enhanced Secure Mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable Enhanced Secure Mode:

   ```
   enhanced-secure-mode enable
   ```

3. Restart the switch.

Disabling Enhanced Secure Mode

Use the following procedure to disable Enhanced Secure Mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable Enhanced Secure Mode:

   ```
   enhanced-secure-mode disable
   ```

3. Restart the switch.

Creating a group of commands

Use the following procedure to create a group of commands.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create a group of commands:

   ```
   cli-command-group <group_name>
   ```

Variable Definitions

The following table describes the parameters for the `cli-command-group` command.

Variable	Value
<group_name>	Specifies the command group name.

Configuring the TFTP protocol

Use the following procedure to enable or disable the TFTP protocol on switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable TFTP protocol:

   ```
   tftp-access enable
   ```

3. Disable TFTP protocol:

   ```
   tftp-access disable
   ```

   OR

   ```
   default tftp-access
   ```

Assigning commands to a group of commands

Use the following procedure to assign commands and subcommands to a command group.

Before you begin

Create the command group for which to assign commands.

About this task

Note:

Assigning to a group a command already present in another group removes that command from the latter group.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Assign a command to a group of commands:

   ```
   cli-command-group <group_name> [<CLI_command_name>  [ALL | hint |
   <CLI_subcommand_name> ALL | hint]]
   ```

Example

The following example displays sample output for the `cli-command-group` command.

```
Switch(config)#cli-command-group MyCmdGroup hint

-----------------------------------------------
User Executive subcommands
-----------------------------------------------
Exec commands:
  blink-leds              Blink the LEDs on the display panel to identify the
                          unit
  boot                    Reset the switch/stack
  clear                   Clear system parameters
  clock                   Execute clock time setting
  configure               Enter configuration mode
  copy                    Copy files
  disable                 Turn off privileged commands
  download                Download and run new image
  enable                  Turn on privileged commands
  energy-saver            Manually activate or deactivate energy saver
  exit                    Exit from the EXEC
  help                    Description of the interactive help system
  install                 Quick Install & Setup Script
  ip                      IP operations
  l2                      Trigger a CFM message
  logout                  Exit from the EXEC and end the current session

Switch(config)#cli-command-group MyCmdGroup banner ALL
% Command moved from security-cmds-group to MyCmdGroup

Switch(config)#
```

Variable Definitions

The following table describes the parameters for the `cli-command-group` command.

Variable	Value
<group_name>	Specifies the command group name.
<CLI_command_name>	Specifies the command to assign to a group of commands. Use the `hint` parameter to check the available commands.
<CLI_subcommand_name>	Specifies the subcommand to assign to a group of commands. Use the `hint` parameter to check the available commands.
hint	Lists available commands or subcommands.
ALL	Adds all subcommands.

Removing commands from a command group

Use the following procedure to remove commands or subcommands from a command group.

About this task

Note:

You cannot delete or modify commands that belong to the `cli-basic-group` command group.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Remove a command or subcommand from a group of commands:

   ```
   no cli-command-group <group_name>  [<command_name>  [ALL |
   <subcommand_name> ALL]]
   ```

Variable Definitions

The following table describes the parameters for the `no cli-command-group` command.

Variable	Value
<group_name>	Specifies the group from which to remove a command or subcommand.
<command_name>	Specifies the name of a command to remove from the group of commands.
<subcommand_name>	Specifies the name of a subcommand to remove from the group of commands.

Table continues…

Variable	Value
ALL	Removes all commands or subcommands from the group of commands.

Removing a command group

Use the following procedure to remove a command group.

About this task

Note:

You cannot remove the default command groups.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Remove the group of commands:

   ```
   no cli-command-group <group_name>
   ```

3. Confirm group deletion.

Variable Definitions

The following table describes the parameters for the `no cli-command-group` command.

Variable	Value
<group_name>	Specifies the command group to be removed.

Displaying command group information

Use the following procedure to display all command groups or all commands from a command group.

About this task

Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display all existing command groups:

   ```
   show cli-command-group
   ```

3. Display all commands from a command group:

   ```
   show cli-command-group <group_name>
   ```

Example

The following example displays sample output for the `show cli-command-group` command.

```
Switch(config)#show cli-command-group
    CLI command groups:
    cli-basic-group
    security-cmds-group
    system-cmds-group
    audit-cmds-group
    MyCmdGroup
Switch(config)#show cli-command-group MyCmdGroup
    CLI commands:
    fa proxy
    vlan *

Switch(config)#
```

Variable Definitions

The following table describes the parameters for the `show cli-command-group` command.

Variable	Value
<group_name>	Specifies the command group for which to display information.

Restoring command groups to default

Use the following procedure to restore a command group or all command groups to the default set of commands.

About this task

Note:

Restoring all command groups to default removes all custom command groups. Restoring a custom command group to default removes all commands from that group.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Restore a command group to default commands:

   ```
   default cli-command-group <group_name>
   ```

3. Restore all command groups to default:

   ```
   default cli-command-group
   ```

Variable Definitions

The following table describes the parameters for the `default cli-command-group` command.

Variable	Value
<group_name>	Specifies the command group for which to restore default commands.

Creating a role

Use the following procedure to create a custom role.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create a custom role:

   ```
   role <role_name>
   ```

Variable Definitions

The following table describes the parameters for the `role` command.

Variable	Value
<role_name>	Specifies the name of the custom role.

Assigning a group of commands to a role

Use the following procedure to assign a group of commands to a role.

Before you begin

Create the role for which to assign commands if it does not exist.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Assign a group of commands to a role:

   ```
   role <role_name> [show-only <command_group_A> | show-config
   <command_group_B>]
   ```

Variable Definitions

The following table describes the parameters for the `role` command.

Variable	Value
<role_name>	Specifies the role for which to assign commands.
show-only <command_group_A>	Specifies the group of commands for which the specified role will have show-only privileges.
show-config <command_group_B>	Specifies the group of commands for which the specified role will have full privileges (show, configure, no and default).

Displaying role information

Use the following procedure to display the command groups assigned with a role and the role rights for each group.

Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display command groups assigned to a role:

   ```
   show role
   ```

Example

The following example displays sample output for the `show role` command.

```
Switch(config)#show role
Roles                            Groups                           Rights
-------------------------------- -------------------------------- ------------
app_administrator                cli-basic-group                  show-config
                                 system-cmds-group                show-only
security_administrator           cli-basic-group                  show-config
                                 security-cmds-group              show-config
                                 system-cmds-group                show-config
                                 audit-cmds-group                 show-config
system_administrator             cli-basic-group                  show-config
                                 system-cmds-group                show-config
                                 audit-cmds-group                 show-only
emergency_administrator          cli-basic-group                  show-config
                                 security-cmds-group              show-config
                                 system-cmds-group                show-config
                                 audit-cmds-group                 show-config
MyRoleA                          cli-basic-group                  show-config
                                 security-cmds-group              show-config
                                 audit-cmds-group                 show-only
Switch(config)#
```

Creating a user

Use the following procedure to create a new user.

About this task

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Create a new user:

```
username add <user_name> password <user_password>
```

3. Create a new user and specify access parameters at creation time:

```
username add <user_name> {daily-access-interval access-start-hour
<0-24> access-stop-hour <0-24> | inactive-period <1-360> | max-
number-of-sessions <1-12> | role-name <role_name>} password
<user_password>
```

4. Confirm the password.

Variable Definitions

The following table describes the parameters for the `username add` command.

Variable	Value
<user_name>	Specifies the user name.
<user_password>	Specifies the user password.
daily-access-interval	Specifies the day interval during which the user can access the switch. The default interval is 0-24.
inactive-period	Specifies the period during which the user must access the switch in order to not be locked out. The default value is 360 days.
max-number-of-sessions	Specifies the number of concurrent sessions allowed for a user. The default value is 12.
role-name <role_name>	Specifies the role for the new user.

Displaying user information

Use the following procedure to display user information.

Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display information related to a specific user:

```
show username <user_name>
```

3. Display all existing users and their roles.

```
show username
```

4. Display all users currently logged into the system:

```
show who
```

Example

The following example displays sample output for the `show username` command.

```
Switch:(config)#show username

Lockout timeout: 60 min
Lockout retries: 5
Emergency account timeout: not set

Username:           systemadmn
-------------------------------------------
ntp authentication-key 100 type md5/sha1
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Verify the NTP key:
FED1(config)#sh ntp key
Key Id      Key                     Key Type
-------------------------------------------
100         ********                MD5
200         ********                SHA1
SSH access: Enabled
TELNET access: Enabled

Username:           security_adm
-------------------------------------------
Role name:          security_administrator
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled
```

Variable definitions

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

Variable	Value
<user_name>	Specifies the user name.

Removing a user

Use the following procedure to remove a user.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Remove a user:

```
no username <user_name>
```

Variable definitions

The following table describes the parameters for the `no username` command.

Variable	Value
<user_name>	Specifies the user name.

Assigning a role to a user

Use this procedure to assign a role to a user.

Following are the default roles:

- `app_administrator`
- `security_administrator`
- `system_administrator`
- `emergency_administrator`

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Assign a role to a user:

   ```
   username <user_name>  role-name  <role_name>
   ```

Variable definitions

The following table describes the parameters for the `username <user_name>  role-name <role_name>` command.

Variable	Value
<user_name>	Specifies the user name.
<role_name>	Specifies the role name.

Enabling a user

Use the following procedure to enable a user.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Enable a user:

```
username <user_name> enable
```

OR

```
default username <user_name> enable
```

Variable definitions

The following table describes the parameters for the `username <user_name> enable` command.

Variable	Value
<user_name>	Specifies the user name.

Disabling a user

Use the following procedure to disable a user.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Disable a user:

```
no username <user_name> enable
```

Variable definitions

The following table describes the parameters for the `no username <user_name> enable` command.

Variable	Value
<user_name>	Specifies the user name.

Configuring user access parameters

Use the following procedure to configure access parameters for a user.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Configure daily access intervals:

```
username <user_name>  daily-access-interval access-start-hour
<0-24>access-end-hour <0-24>
```

3. Remove daily restrictions:

```
no username <user_name> daily-access-interval
```

4. Reset the daily access interval to default:

```
default username <user_name> daily-access-interval
```

5. Configure the maximum inactive period before the user is locked-out:

```
username  <user_name>   inactive-period <1-360>
```

6. Reset the inactive period for a user to default:

```
default username <user_name>  inactive-period
```

7. Configure the maximum number of concurrent sessions:

```
username <user_name> max-number-of-sessions <1-12>
```

8. Reset the number of concurrent sessions to default:

```
default username <user_name> max-number-of-sessions
```

Variable definitions

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

Variable	Value
<user_name>	Specifies the user name.
daily-access-interval	Specifies the day interval during which the user can access the switch. The default interval is 0-24.
inactive-period	Specifies the period during which the user must access the switch in order to not be locked out. The default value is 360 days.
max-number-of-sessions	Specifies the number of concurrent sessions allowed for a user. The default value is 12.

Configuring SSH access for a user

Use the following procedure to configure SSH access for a user.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Enable SSH access for a user:

```
username <user_name> ssh-access enable
```

3. Disable SSH access for a user:

```
username <user_name> ssh-access disable
```

OR

```
no username <user_name> ssh-access
```

Variable definitions

The following table describes the parameters for the `username <user_name> ssh-access` command.

Variable	Value
<user_name>	Specifies the user name.

Configuring telnet access for a user

Use the following procedure to configure telnet access for a user.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable SSH access for a user:

```
username <user_name> telnet-access enable
```

3. Disable telnet access for a user:

```
username <user_name> telnet-access disable
```

OR

```
no username <user_name> telnet-access
```

Variable definitions

The following table describes the parameters for the `username <user_name> telnet-access` command.

Variable	Value
<user_name>	Specifies the user name.

Changing the password for the current user

Use the following procedure to change the password for the current user:

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Change the password for the current user:

   ```
   username password
   ```

Configuring the lockout interval

Use the following procedure to configure the lockout interval for all users.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the lockout interval:

   ```
   username lockout-time <0-60>
   ```

3. Reset the lockout interval to default value:

   ```
   default username lockout-time
   ```

Variable definitions

The following table describes the parameters for the `username lockout-time` command.

Variable	Value
<0-60>	Specifies the duration of session lockout, in minutes. Session lockout occurs when the threshold on the number of incorrect logins is exceeded.

Configuring emergency account timeout

Use the following procedure to configure the timeout for the emergency account.

About this task

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the timeout for the emergency account:

   ```
   username  emergency_account_timeout   <1-360>
   ```

Variable definitions

The following table describes the parameters for the `username emergency_account_timeout` command.

Variable	Value
<1-360>	Specifies the period during which the emergency user must access the switch in order to not be locked out.

Configure the audit log encryption key

Use the following procedure to change the audit encryption key.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Change the audit encryption key:

   ```
   audit encryption-key aes-cbc
   ```

Configuring password security restrictions

Use the following procedure to configure password security restrictions in enhanced secure mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the password validity period:

   ```
   password aging-time [username <name>]<0-365>
   ```

3. Configure the password change interval:

```
password change-interval <1-999>
```

4. Configure whether the switch accepts repeated consecutive characters in the password:

   ```
   password check—repeated [enable | disable]
   ```

5. Configure whether the switch accepts sequential characters in a password

   ```
   password check—sequential [enable | disable]
   ```

6. Configure password complexity

   ```
   password complexity [lower—case <0-9> | numeric <0-9> | special <0-9> | upper-case <0-9>]
   ```

7. Configure the password delay-time:

   ```
   password delay—time <0-3600>
   ```

8. Configure the password encryption key:

   ```
   password encryption-key aes-cbc
   ```

9. Configure the interval for post-expiration log in:

   ```
   password grace-period <1-365>
   ```

10. Configure the failure notification message:

    ```
    password login-failure-notification "<message>"
    ```

11. Configure the minimum length for a password:

    ```
    password min-length <8-255>
    ```

12. Configure password expiry notifications:

    ```
    password notifications <1-90>
    ```

13. Configure whether the switch enforces a password change on first login

    ```
    password password-change-on-first-login [disable | enable]
    ```

14. Configure the maximum number of password changes per day:

    ```
    password password-change-rate-limiter <1-10>
    ```

15. Configure the maximum number of passwords retained in history:

    ```
    password password-history <0-12>
    ```

16. Configure the number of post-expiration logins:

    ```
    password post-expiration-login <0-10>
    ```

17. Configure the number of days after which a disabled user account due to inactive period is re-enabled.

    ```
    password unlock-timer <1-365>
    ```

18. Verify password security restrictions:

```
show password {aging-time | change-interval | check-repeated |
check-sequential | complexity | delay-time | grace-period | login-
failure-notification | min-length | notifications | password-change-
on-first-login | password-change-rate-limiter | password-history |
post-expiration-login | unlock-timer}
```

19. Reset password security restrictions to default values:

```
default password {aging-time | change-interval | check-repeated |
check-sequential | complexity | delay-time | grace-period | min-
length | notifications | password-change-on-first-login | password-
change-rate-limiter | password-history | post-expiration-login |
unlock-timer}
```

Variable definitions

The following table describes the parameters for the `password` command.

Variable	Value
aging-time <0-365>	Specifies the number of days the password remains valid. The default value is 0.
aging-time [username]	Specifies the user for which you configure the aging time.
change-interval <1-999>	Specifies the password change interval, in hours.
check-repeated [enable | disable]	Specifies whether the switch accepts repeated characters in a password: • disable—Accepts repeated consecutive characters. • enable—Forbids repeated consecutive characters. The default value is disabled.
check-sequential [enable | disable]	Specifies whether the switch accepts sequential characters in a password: • disable—Accepts repeated sequential characters. • enable—Forbids repeated sequential characters. The default value is disabled.
lower-case <0–9>	Specifies the minimum number of lower-case characters that can be included in the password.
numeric <0–9>	Specifies the minimum number of numeric characters that can be included in the password.
special <0–9>	Specifies the minimum number of special characters (!, @, #, $, %, ^, &, *, (,), -, +, =, _) that can be included in the password.
upper-case <0–9>	Specifies the minimum number of upper-case characters that can be included in the password.
delay-time <0–3600>	Specifies the amount of delay time after 3 login attempts, in seconds. Default is 60 seconds.

Table continues…

Variable	Value
encryption-key aes-cbc	Enables internal password encryption.
grace-period <1-365>	Specifies the interval in which the user can login after his password expires.
login-failure-notification "<message>"	Specifies the notification message that the user sees after an incorrect login. The maximum length is 99 characters.
min-length <8–255>	Specifies the minimum length for a password
notifications <1–90>	Specifies the notification interval in days before the password expires. Default is 10 days.
password-change-on-first-login [disable | enable]	Specifies whether the switch enforces a password change on first login: • disable—Disables password change on first login. • enable—Enables password change on first login. The default value is disabled.
password-change-rate-limiter <1-10>	Specifies the maximum number of password changes allowed per day. Default is 1.
password-history <0-12>	<0-12> Specifies the number of passwords retained in history. Default is 1.
post-expiration-login <0-10>	Specifies the number of allowed post-expiration logins.
unlock-timer <1–365>	<1-365> Specifies the number of days after which a disabled user account due to inactivity period is re-enabled. Default is 7 days.

Chapter 7: EAPOL-based security fundamentals

This chapter provides conceptual information and procedures to configure EAPOL-based security using Command Line Interface (CLI) and Enterprised Device Manager (EDM).

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.

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 switch, 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 MHMA-MV 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.
- You cannot manually configure VLAN membership, PVID, priority, tagging, filter-untagged frame and filter-unregistered frames on EAP enabled ports

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
  - 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, such as Microsoft Windows 8 Client, Linux client or other client with EAPOL support

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

EAPOL-based security configuration rules

The following configuration rules apply when you use EAPOL-based security:

- Before configuring EAPOL-based security, 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 (the mirroring port)
- IP Source Guard

- All VLANs on the EAP port must be on same Spanning Tree Groups (STG) and this is applicable for all EAP VLANs (Guest, Fail Open, initial and RADIUS Assigned VLAN). This is because EAP for untagged traffic cannot be supported on port members belonging to VLANs from different STGs.If an administrator wants to configure EAP port in a RADIUS Assigned VLAN from the other STG, then the initial VLAN or Guest-VLAN (if used) must be moved to the new STG. This is a manual configuration.
- All VLANs of the EAP ports must belong to same Multiple Spanning Tree Protocol (MSTP). But it is complicated because there can be an inexistent VLAN mapped to another Multiple Spanning Tree Instances (MSTI), but not a member of that MSTI.

  Example: Consider an initial VLAN to Common Internal Spanning Tree (CIST) and VLAN 10 (inexistent) mapped to MSTI3. An EAP client connects with VLAN10 using auto create option; VLAN10 is created and unmapped from MSTI3 and added to CIST where the initial VLAN is part of. This damages all MSTP configurations because the VLAN-MSTI mappings are different. Use the EAP auto create VLAN option for scenarios where it is really required, like Fabric Attach (FA). Otherwise, this can damage MSTP area if RAVs are not created but already mapped to different MSTIs other than initial, Guest, or Fail Open VLANs.
- It is recommended to set MSTP Edge Port to True (or Spanning Tree Fast Learning if in STPG mode) on EAP-enabled ports. This will prevent topology change notifications from being sent on that port and MAC addresses will not be cleared on outside topology changes, preventing EAP clients from re-authenticating because of these

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

Advanced EAPOL features

The switch supports the following main EAPOL modes:

- Multiple Host with Single Authentication (MHSA)
- Multiple Host with Multiple Authentication MultiVLAN (MHMA-MV)

Note:

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

Client reauthentication

If you configure the switch to reauthenticate clients in one of the main modes (MHSA or MHMA-MV), every time a reauthentication occurs, the port is moved to the new RADIUS Assigned VLAN, if it differs from the last reauthentication of the client.

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.
- 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.
- 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 from authenticated client will be transmitted properly in the RADIUS assigned VLAN or in the original VLAN.

Note:

A VLAN configured as Guest VLAN cannot be erased, even if EAPOL is disabled.

When the switch is running in SPBM mode, you must associate the configured Guest VLAN with an I-SID.

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.

When the switch declares the RADIUS servers unreachable, the port is copied to the Fail Open VLAN. All clients already authenticated will still be able to access their RADIUS-assigned VLAN, while all the new clients will access the FOV. 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, only the unauthenticated clients are aged in order to re-authenticate. Authenticated clients do not need to re-authenticate. If appropriate, the clients are 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.

The Fail Open VLAN feature is disabled by default for an EAP or non-EAP enabled port.

When the RADIUS servers become unreachable, if the Fail Open VLAN is defined then all EAP-enabled ports are copied to Fail Open VLANs across 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 and does not process EAP packets received on the EAP enabled ports.

When the switch is running in SPBM mode, you must associate the configured Fail Open VLAN with an I-SID.

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.

Fail Open VLAN Continuity Mode

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

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

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

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

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

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

Note:

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

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

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

Note:

When an EAP or NEAP client tries to re-authenticate and the RADIUS server is not reachable, the switch keeps the client in the VLAN currently assigned by RADIUS and maintains any applicable policies. If necessary, the switch provides appropriate communication back to the EAP supplicant to indicate that re-authentication was successful.

Fail Open VLAN improvements

With this enhancement, after a port is removed from Fail Open VLAN, only the unauthenticated clients are aged in order to re-authenticate. Authenticated clients do not need to re-authenticate.

Multiple Host with Multiple Authentication MultiVLAN

Multiple Host with Multiple Authentication MultiVLAN (MHMA-MV) is the default EAP mode. In this mode, the switch allows finite number of EAP and Non-EAP users or devices with unique MAC addresses on a port.

Each user must perform authentication before the port allows traffic from the corresponding MAC address to the VLAN. The treatment of unauthenticated users on a port depends on the state of the Guest VLAN.

If Guest VLAN is enabled, then traffic from all authenticated users are sent into their RAV or initial VLAN and traffic from unauthenticated users are sent into the configured Guest VLAN. In this case, the port is not set to Unauthorized state if the number of unauthenticated users is greater than 32 + eap_mac_max. If Guest VLAN is disabled, then the traffic from all authenticated users are sent into their RAV or initial VLAN and traffic from unauthenticated users are dropped. In this case, the port is set to Unauthorized state if the number of unauthenticated users is greater than 32 + eap_mac_max.

Each authenticated user can be assigned to different VLANs on the same port, while unauthenticated clients can still have access to the Guest VLAN, if defined.

The advantages of MultiVLAN capabilities are seen only when **`use-radius-assigned-vlan`** or **`non-eap-user-radius-assigned-vlan`** commands are used for EAP or Non-EAP clients. If attribute is not received from the RADIUS server or the previous options are not enabled, the traffic from unauthenticated clients are forwarded to the initial VLAN given by PVID value.

Automatic configuration

MHMV automatic configuration command applies predefined configuration over a set of ports depending on the command mode used — Global or Interface. The result of the command can be seen in the running configuration module on the indicated ports. The settings applied can be modified manually on each port.

RADIUS-assigned VLAN

RADIUS-assigned VLAN provides greater flexibility and a more centralized assignment. This feature can be useful in an IP Phone setup where the phone traffic is directed to the Voice over IP (VoIP) VLAN and the PC Data traffic is directed to the assigned VLAN. Each client authenticated will be assigned into its own VLAN, without any port PVID changes.

Important:

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

Consider the following setup:

- 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)

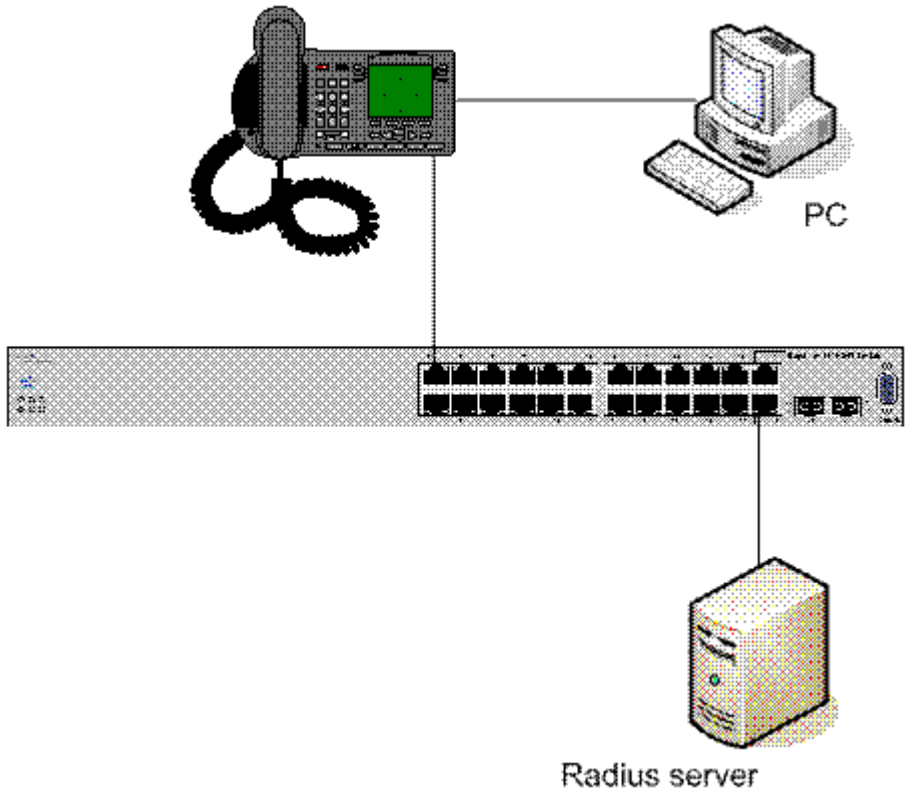


Figure 3: RADIUS-assigned VLAN in MHMA-MV mode

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

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

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

   ```
   Switch(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, 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-MV

When you enable this option the switch will no longer transmit periodically Request Identities packets on EAP enabled ports. 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:

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

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

   ```
   Switch(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-MV

With this enhancement you can move a port to a specific VLAN even if that switch port operates in EAP MHMA-MV mode.

This enhancement has one restriction. If you have multiple EAP clients authenticating on a switch port (as you normally can in MHMA-MV 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:

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

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

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

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

802.1X or non-EAP with VLAN names

The 802.1X or non-EAP with VLAN names functionality enhances the switch to match RADIUS assigned VLANs based on either the VLAN number or a VLAN name. 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.

Accounting Session ID format enhancement

EAP 802.1x session identifiers are used to track all clients across the network when the RADIUS accounting is enabled. These sessions are not always unique. The Accounting Session ID format enhancement extends the session ID with the IP address of the switch in order to prevent duplicate sessions.

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.

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.

- 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 150.
  - 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 or sent into Guest VLAN if this feature is enabled.

  EAPOL authentication is not affected.
- 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 or sent into Guest VLAN. 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.

  Note:

  This behavior is only valid for when Guest VLAN is not enabled. If Guest VLAN is enabled, this rule does not apply.
- 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 187.

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.

  The default password format for a non-eap client is his mac-address.

Note:

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 EAP and Non-EAP clients are allowed to negotiate access on that port but only one host will be allowed to perform authentication.
- After the first EAP or Non-EAP client successfully authenticates on a port, no other clients may negotiate authentication on that port. 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.
- The first authenticated user can also be a NEAP user.

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

MHSA No-Limit

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

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

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 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 globally enable RADIUS for non-EAP clients.

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
- 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 12: EAPOL Multihost access

Scenario	Action
• No authenticated hosts on the port.	Allow

Table continues…

Scenario	Action
• Guest VLAN is enabled.	
• New host MAC address is authenticated.	Allow
• 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
• Host is an IP Phone. • Port is configured for ADAC (allowed PhoneMac, not callSvr, not Uplink).	Allow
• 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
• 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 switch utilizes the same RADIUS server used for RADIUS authentication.

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

Non-EAP accounting

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

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

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

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

Fail Open UBP

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

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

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

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

Limitations:

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

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

User Based Policies filter-on-MAC

When using user based policies, you can add filter-on-MAC options in EAP configuration:

```
eapol user-based-policies filter-on-mac enable
```

```
eapol multihost non-eap-user-based-policies filter-on-mac enable
```

Enabling filter-on-MAC forces the UBP policy to use the MAC address of the supplicant when matching the traffic.

In MHSA mode, only one user can authenticate on the switch and other mac addresses are allowed to pass when ingress unit via authenticated port. In such cases the UBP policy with filter-on-MAC enable will match only the supplicant traffic. Traffic from other users (mac addresses) on that port will not match the UBP policy. When you need to match traffic from all the users on a port in MHSA mode, the UBP filter-on-MAC must be disabled.

EAP and Fabric Attach

With EAP and Fabric Attach (FA), the switch can forward traffic from EAP/NEAP clients over the SPB cloud. The traffic for authenticated clients is mapped to I-SIDs received from the RADIUS server.

For more information about EAP and FA, see Configuring Fabric Connect on Ethernet Routing Switch 4900 and 5900 Series.

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 13: 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: • 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: • 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*

Table continues…

Event	Accounting information logged at server
	• Output octet count for the session* • Input packet count for the session* • Output packet count for the session* **Note:** Octet and packet counts are by port and therefore provide useful information only when ports operate in the SHSA mode.

The following table summarizes the accounting termination causes supported.

Table 14: 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

Configuring EAPOL security

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

Important:

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

Enabling or disabling EAPOL-based security

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Enable EAPOL-based security:

```
eapol enable
```

3. Disable EAPOL-based security:

```
eapol disable
```

Modifying EAPOL-based security parameters for a specific port

About this task

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

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface ethernet <port number>
```

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

```
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>]
```

Variable definitions

Use the data in the following table to use the **`eapol`** command.

Parameter	Description
port <portllist>	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: • authorized — port is always authorized • unauthorized — port is always unauthorized

Table continues…

Parameter	Description
	• auto — port authorization status depends on the result of the EAP authentication
traffic-control {in-out I in}	Sets the level of traffic control: • 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 0 to 65535. **Note:** EAP client passes quickly through the Held state when the value is 0.
transmit-interval <num>	Specifies a waiting period for response from supplicant for EAP Request or 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/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.

Displaying the current EAPOL-based security status

About this task

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

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the current EAPOL-based security status:

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

Example

```
Switch>enable
Switch#show eapol
EAPOL Administrative State:  Disabled
Port-mirroring on EAP ports:  Disabled
EAPOL User Based Policies:  Disabled
EAPOL User Based Policies Filter On MAC Addresses:  Disabled
Port:  1
    Admin Status:  F Auth
    Auth:  Yes
    Admin Dir:  Both
    Oper Dir:  Both
    ReAuth Enable:  No
    ReAuth Period:  3600
    Quiet Period:  60
    Supplic Timeout:  30
    Server Timeout:  30
    Max Req:  2
    RDS DSE:  No
Port:  2
    Admin Status:  F Auth
    Auth:  Yes
    Admin Dir:  Both
    Oper Dir:  Both
    ReAuth Enable:  No
    ReAuth Period:  3600
    Quiet Period:  60
    Supplic Timeout:  30
    Server Timeout:  30
    Max Req:  2
    RDS DSE:  No
Port:  3
    Admin Status:  F Auth
----More (q=Quit, space/return=Continue)----
```

Variable definitions

Use the data in the following table to use the **`show eapol`** command.

Parameter	Description
port <portllist>	Specifies the ports to display. If no port is entered, all ports are displayed.
multihost {interface |status }	Displays EAPOL multihost configuration. Select interface to display multihost port configuration and status to display multihost port status. **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

Table continues…

Parameter	Description
	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.
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.

Resetting EAP settings globally

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

This command resets the following EAP settings:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Reset all EAP settings globally:

   ```
   default eap-all
   ```

Resetting EAP settings at the port level

About this task

Reset all EAP settings at the port level. This command resets:

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

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. Reset all EAP settings at the port level:

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

Variable definitions

Use the data in the following table to use the **`default eap-all`** command.

Variable	Value
<port-list>	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..\

Configuring predefined settings

If you use MHMV automatic configuration, all other EAP settings from the port and from the global configuration will be defaulted.

Depending on the command mode, the predefined settings are applied over a set of ports. The following predefined settings are applied on the set of ports if the MHMV automatic configuration command is used while in Global or Interface command modes:

Global command mode	Interface command mode
enable RADIUS authentication for Non-EAP clients	enable RADIUS authentication for Non-EAP clients
use Radius Assigned VLAN	use Radius Assigned VLAN
non-EAP use RADIUS Assigned VLAN	Non-EAP use RADIUS Assigned VLAN
enable MultiVLAN	enable Multi Host
disable the IP address and port number password format	eapol status auto
	eap-mac-max, neap-mac-max and mac-max

Note:

If Port Mirroring or MLT is active on a port, an error is displayed and no settings are applied on that port.

About this task

Use the following procedure to apply MHMV automatic configuration with predefined settings over a set of ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Apply MHMV automatic configuration for the set of ports:

   ```
   eapol multivlan auto-config port <portrange> | all
   ```

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#eapol multivlan auto-config port 1/2-10,2/all
```

Displaying the status of the session ID format

About this task

Use the following procedure to display the status of the session ID format.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show eapol acct-session-id
   ```

Displaying the session ID of an EAP client

About this task

Use the following procedure to display the session ID of an EAP client.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To display the session ID of an EAP client, enter the following command:

   ```
   show eapol multihost status verbose
   ```

Configuring accounting session ID format

About this task

Use the following procedure to configure the accounting session ID format.

The accounting session ID format is enabled by default.

Note:

Session ID contains only the inband configured IP address.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable the accounting session ID format, enter the following command:

   ```
   [default] eapol acct-session-id  extend-with-addr
   ```

3. To disable the accounting session ID format, enter the following command:

   ```
   no eapol acct-session-id extend-with-addr
   ```

4. Press Enter.

Enabling and disabling Non-EAP client re-authentication

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable Non-EAP re-authentication:

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

3. Disable Non-EAP re-authentication:

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

   OR

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

Viewing the non-EAP client re-authentication

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Display the configuration status of NEAP re-authentication:

   ```
   show eapol multihost
   ```

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#show eapol multihost
Allow Local Non-EAP Clients                          :  Disabled
Non-EAP RADIUS Authentication                        :  Disabled
Non-EAP AutoLearned After Single Authent (MHSA)      :  Disabled
Non-EAP DHCP Phone Authentication                    :  Disabled
EAPoL Request Packet Generation Mode                 :  Multicast
EAP RADIUS Assigned VLANs                            :  Enabled
Non-EAP RADIUS Assigned VLANs                        :  Enabled
Non-EAP RADIUS Password Attribute Format             :  MACAddr
Non-EAP User Based Policies                          :  Disabled
Non-EAP User Based Policies Filter On MAC Addresses  :  Disabled
EAP Protocol                                         :  Enabled
Non-EAP ReAuthentication                             :  Disabled
ADAC Non-EAP Phone Authentication                    :  Disabled
Fail Open VLAN                                       :  Disabled
Fail Open VLAN ID                                    :  1
Fail Open VLAN Continuity Mode                       :  Disabled
Switch(config)#
```

Clearing non-EAP authenticated clients from ports

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Clear authenticated NEAP clients from a specified port:

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

Variable definitions

Use the data in the following table to use the **clear eapol non-eap** command.

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

EAPOL User Based Policy Configuration using CLI

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

Before you begin

A 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.

About this task

Perform the following procedure to enable 802.1x (RADIUS server accounting) User Based Policy settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable 802.1x (RADIUS server accounting) User Based Policy settings:

   ```
   eapol user-based-policies { [enable] [filter-on-mac enable] }
   ```

Variable definitions

Use the data in the following table to use the **eapol user-based-policies** command.

Parameter	Description
enable	Configures 802.1x User Based Policies settings.
filter-on-mac enable	Enables filtering on MAC addresses.

Disabling EAPOL User Based Policies

About this task

Disable 802.1x (RADIUS server accounting) User Based Policy settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable 802.1x (RADIUS server accounting) User Based Policy settings:

   ```
   no eapol user-based-policies { [enable] [filter-on-mac enable] }
   ```

Variable definitions

Use the data in the following table to use the **`eapol user-based-policies`** command.

Parameter	Description
enable	Disables 802.1x (RADIUS server accounting) User Based Policy settings.
filter-on-mac enable	Disables filtering on MAC addresses.

Setting EAPOL User Based Policy as Default

About this task

Perform the following procedure to set EAPOL User Based Policy as the default.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Set the EAPOL User Based Policy as the default:

   ```
   default eapol user-based-policies { [enable] [filter-on-mac
   enable] }
   ```

Variable definitions

Use the data in the following table to use the **`default eapol user-based-policies`** command.

Parameter	Description
enable	Disables 802.1x (RADIUS server accounting) User Based Policy settings.
filter-on-mac enable	Disables filtering on MAC addresses.

Copying port EAP settings

Use the following command to copy EAP settings from one port to another.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Copy port EAP settings:

   ```
   eap copy-eap-settings src-port <source_port> dst-port
   <destination_port>
   ```

Variable definitions

The following table describes the parameters for the `eap copy-eap-settings` command.

Variable	Value
src-port <source_port	Specifies the source port for copying EAP settings.
dst-port <destination_port	Specifies the destination port for copying EAP settings.

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.

Setting the guest VLAN for EAPOL

About this task

Use the following procedure to set the guest VLAN globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Set the guest VLAN:

```
eapol guest-vlan enable vid <1-4094>
```

Variable definitions

Use the data in the following table to use the **eapol guest-vlanS** command.

Parameter	Description
enable	Enable Guest VLAN.
<vid>	Guest VLAN ID.

Disabling guest VLAN for EAPOL

About this task

Use the following procedure to disable the guest VLAN.

Note:

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.

If the switch is running in SPBM mode, guest VLAN must be a C-VLAN with an I-SID configured on it.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Disable guest VLAN:

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

OR

```
default eapol guest-vlan
```

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

Use the commands in this section to allow a non-EAP phone to function with the Guest VLAN enabled.

Enabling EAPOL VoIP VLAN

About this task

Perform this procedure to enable the EAPOL multihost VoIP VLAN.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable the EAPOL multihost VoIP VLAN:

   ```
   eapol multihost voip-vlan <1-5> {[enable] [vid <1-4094>]}
   ```

Variable definitions

Use the data in the following table to use the **`eapol multihost`** 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

About this task

Perform this procedure to disable the EAPOL multihost VoIP VLAN.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable the EAPOL multihost VoIP VLAN:

   ```
   no eapol multihost voip-vlan <1-5> [enable]
   ```

Variable Definitions

Use the data in the following table to use the **`no eapol multihost`** 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

About this task

Perform this procedure to configure the EAPOL multihost VoIP VLAN as the default setting.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the EAPOL multihost VoIP VLAN:

   ```
   default eapol multihost voip-vlan <1-5> [enable] [vid]
   ```

Variable Definitions

Use the data in the following table to use the **`default eapol multihost`** 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

About this task

Perform this procedure to display information related to the EAPOL multihost VoIP VLAN.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Display information related to the EAPOL multihost VoIP VLAN:

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

3.

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#show eapol multihost voip-vlan
Voip Vlan State    Vid
--------- -------- ----
1         Disabled N/A
2         Disabled N/A
3         Disabled N/A
4         Disabled N/A
5         Disabled N/A
```

Multihost Non-EAP User Based Policy Configuration using CLI

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

Before you begin

RADIUS server must be configured

Note:

If the RADIUS server is not configured, an error appears while loading the ASCII file.

About this task

Perform the following procedure to enable 802.1x (RADIUS server accounting) Multihost Non- EAP User Based Policy settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enable 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy settings:

   ```
   eapol multihost non-eap-user-based-policies { [enable][filter-on-mac
   enable] }
   ```

Variable definitions

Use the data in the following table to use the **`apol multihost non-eap-user-based-policies`** command.

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

About this task

Perform the following procedure to disable 802.1x (RADIUS server accounting) Multihost Non- EAP User Based Policy settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy settings:

   ```
   no eapol multihost non-eap-user-based-policies { [enable][filter-onmac enable] }
   ```

Variable definitions

Use the data in the following table to use the **`no eapol multihost non-eap-user-based-policies`** command.

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

About this task

Perform the following procedure to set 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy as the default configuration.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Set 802.1x (RADIUS server accounting) Multihost Non-EAP User Based Policy settings as default configuration:

   ```
   default eapol multihost non-eap-user-based-policies { [enable] [filter-on-mac enable] }
   ```

Variable definitions

Use the data in the following table to use the **`default eapol multihost non-eap-user-based-policies`** command.

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 CLI

Use the procedures in this section to configure the 802.1X non-EAP with Fail Open VLAN using CLI.

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 conenct to the RADIUS server has occurred.

If the switch is running in SPBM mode, Fail Open VLAN must be a C-VLAN with an I-SID configured on it.

Enabling EAPOL Fail Open VLAN

About this task

Use this procedure to enable the EAPOL Fail Open VLAN. To configure Fail Open VLAN support you must globally enable Fail Open VLAN, set the guest VLAN ID and enable Fail Open VLAN on specific ports on an interface.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable the EAPOL Fail Open VLAN:

   ```
   eapol multihost fail-open-vlan {[enable] [vid <1-4094>]}
   ```

Variable definitions

Use the data in the following table to use the **`eapol multihost fail-open-vlan`** 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

About this task

Perform this procedure to disable the EAPOL Fail Open VLAN.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Disable the EAPOL Fail Open VLAN:

```
no eapol multihost fail-open-vlan
```

Setting EAPOL Fail Open VLAN as the default

About this task

Perform this procedure to set the EAPOL Fail Open VLAN as the default.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Set the EAPOL Fail Open VLAN as the default:

```
default eapol multihost fail-open-vlan [enable] [vid]
```

Variable Definitions

Use the data in the following table to use 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

About this task

Perform this procedure to display information related to the EAPOL Fail Open VLAN.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Display the status of the fail-open VLAN

```
show eapol multihost fail-open-vlan
```

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#show eapol multihost fail-open-vlan
Fail Open VLAN Enabled        : No
Fail Open VLAN ID             : 1
Fail Open VLAN Continuity Mode: Disabled
```

Fail Open VLAN Continuity mode configuration using CLI

Use the procedures in this section to configure Fail Open VLAN Continuity mode using CLI.

Enabling EAPOL Fail Open VLAN

About this task

Use this procedure to enable the EAPOL Fail Open VLAN. To configure Fail Open VLAN support you must globally enable Fail Open VLAN, set the guest VLAN ID and enable Fail Open VLAN on specific ports on an interface.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable the EAPOL Fail Open VLAN:

   ```
   eapol multihost fail-open-vlan {[enable] [vid <1-4094>]}
   ```

Disabling EAPOL Fail Open VLAN Continuity mode

About this task

Perform this procedure to disable EAPOL Fail Open VLAN continuity mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

About this task

Perform this procedure to display information related to EAPOL Fail Open VLAN Continuity mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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 Fail Open UBPs on ports

About this task

Use this procedure to configure Fail Open UBPs on ports.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

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

   ```
   eapol multihost fail-open-vlan ubp <ubp_name>
   ```

Variable definitions

Use the data in the following table to use the `eapol multihost fail-open-vlan` command.

Variable	Definition
ubp	User Base Policy when FOV is active.
<ubp_name>	UBP name

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 158.
   b. the desired ports are enabled for multihost mode. For more information, see Configuring multihost support on page 180.
   c. guest VLAN is disabled locally (for the desired interface ports). For more information, see Configuring guest VLANs on page 169.
2. Enable MHSA globally on the switch. For more information, see Enabling support for MHSA globally on page 179.

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 179.
   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.

Enabling and disabling support for MHSA globally

About this task

Enable support for MHSA globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable support for MHSA globally:

   ```
   eapol multihost auto-non-eap-mhsa-enable
   ```

3. Disable support for MHSA globally:

   ```
   no eapol multihost auto-non-eap-mhsa-enable
   ```

   OR

   ```
   default eapol multihost auto-non-eap-mhsa-enable
   ```

Configuring interface and port settings for MHSA

About this task

Configure MHSA settings for a specific port or for all ports on an interface.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. Configure MHSA settings for a specific port or for all ports on an interface:

   ```
   eapol multihost [port <portlist>] auto-non-eap-mhsa-enable non-eap-mac-max <value>
   ```

Variable definitions

Use the data in the following table to use the **`eapol multihost`** command.

Parameters and variables	Description
<portlist>	Specify the list of ports to which you want the settings to apply.
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. • <value> is an integer in the range 1 to 32. The default is 1. **Important:** The configurable maximum number of non EAPOL clients for each port is 32, but the usual maximum allowed for each port should be lower. The combined maximum should be approximately 200 for each box and 800 for a stack.

Viewing MHSA settings and activity

For more information about the commands to view MHSA settings and non EAPOL host activity, see Viewing non EAPOL host settings and activity on page 193.

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.

Disabling EAPOL multihost support

About this task

Disable the EAPOL multihost.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface ethernet <port number>
```

2. Disable the EAPOL multihost.

```
no eapol multihost [<portlist>] [allow-non-eap-enable] [radius-non-eap-enable] [auto-non-eap-mhsa-enable] [non-eap-phone-enable] [use-radius-assigned-vlan]
```

Variable definitions

Use the data in the following table to use the **`no eapol multihost`** command.

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
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 IP Phone clients.
use-radius-assigned-vlan	Disables use of RADIUS-assigned VLAN.

Configuring interface EAPOL multihost settings

About this task

Use the following procedure to control the interface multihost settings.

Procedure

1. Enter Interface Configuration mode:

```
enable

configure terminal

interface ethernet <port number>
```

2. Configure interface EAPOL multihost settings:

```
eapol multihost { [adac-non-eap-enable] [allow-non-eap-enable] [auto-non-eap-mhsa-enable] [eap-mac-max <1-32>] [eap-packet-mode {multicast | unicast}] [eap-protocol-enable] [mac-max <1-64>] [mhsa-no-limit] [non-eap-mac-max <1-32>] [non-eap-phone-enable] [non-eap-use-radius-assigned-vlan] [port] [radius-non-eap-enable] [use-radius-assigned-vlan] [radius-non-eap-delay <0-20>]}
```

Variable definitions

Use the data in the following table to use the **`eapol multihost`** command.

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.
mhsa-no-limit	Allows an unlimited number of auto-authenticated non-EAPOL clients on the port.
non-eap-mac-max	Specifies the maximum number of non-EAP MAC addresses allowed per port.
non-eap-phone-enable	Enables 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.
non-eap-mac [port <portlist>] <H.H.H>	Allows the specified non-EAP MAC address.
radius-non-eap-delay <0-20>	Specifies the global delay time for non-EAP authentication, in seconds, in order to give priority to EAP authentication. A delay of 0 means an instantaneous attempt to authenticate Non-EAP clients through the Radius server. **Note:** Network latency and internal synchronization between tasks running on the switch might give slightly different results than the time configured.

Disabling interface EAPOL multihost settings

About this task

Use the following procedure to disable interface multihost settings.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable

   configure terminal

   interface ethernet <port number>
   ```

2. Disable interface EAPOL multihost settings:

   ```
   no eapol multihost [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][mhsa-no-limit] [adac-non-eap-enable] [eap-protocol-enable]
   ```

Variable definitions

Use the data in the following table to use the **`eapol multihost`** command.

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.
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 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-radius-assigned-vlan	disables use of RADIUS-assigned VLAN values in the MHMA-MV mode.
mhsa-no-limit	disables allowing an unlimited numbers of auto-learned NEAP clients on port.
adac-non-eap-enable	disable authentication of non-EAP phones using ADAC.
eap-protocol-enable	disable EAP protocol on port.

Configuring EAPOL multihost settings to default

About this task

Set the EAPOL multihost feature to the defaults.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   ```

```
configure terminal

interface ethernet <port number>
```

2. Configure EAPOL multihost settings to default:

```
default eapol multihost [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] [non-eap-use-radius-assigned-vlan][mhsa-no-limit]
```

Variable definitions

Use the data in the following table to use the **`default eapol multihost`** command.

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).
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 IP Phone clients as non-EAP type.
non-eap-use-radius-assigned-vlan	enables 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-radius-assigned-vlan	enables use of RADIUS-assigned VLAN values in the MHMA-MV mode.
mhsa-no-limit	disables allowing an unlimited numbers of auto-learned NEAP clients on port.

Configuring the maximum number of EAP clients

About this task

Configure the maximum number of EAP clients.

Procedure

1. Enter Interface Configuration mode:

```
enable

configure terminal
```

```
interface ethernet <port number>
```

2. Configure the maximum number of EAP clients:

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

Variable definitions

Use the data in the following table to use the **`eapol multihost`** command.

Variable	Value
<portlist>	Specify the ports for which you are setting the maximum number of EAP clients.
<num>	Specify the maximum number of EAP clients allowed. RANGE: 1–32

Setting the maximum number of clients allowed per port

About this task

Restrict the maximum number of clients allowed per port.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Restrict the maximum number of clients allowed per port:

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

Example

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

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

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

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

Variable definitions

Use the data in the following table to use the **eapol multihost** command.

Variable	Value
<portlist>	Specify the ports for which you are setting the maximum number of clients.
<num>	Specify the maximum number of EAP and NEAP clients allowed per port. RANGE: 1–64 DEFAULT: 1

Disabling RADIUS-assigned VLAN use in MHMA-MV mode

About this task

Globally disable RADIUS-assigned VLAN use in MHMA-MV mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable RADIUS-assigned VLAN use in MHMA-MV mode:

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

   OR

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

Variable definitions

Use the data in the following table to use the **no eapol multihost** and **default eapol multihost** commands.

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

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 158.
   b. the desired ports are enabled for multihost mode. For more information, see Configuring multihost support on page 180.
   c. guest VLAN is disabled locally (for the desired interface ports). For more information, see Configuring guest VLANs on page 169.
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 187.
   b. RADIUS authentication. For more information, see Enabling RADIUS authentication of non-EAPOL hosts on EAPOL-enabledports on page 188.
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 192.
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 193.

By default, support for non EAPOL hosts on EAPOL-enabled ports is disabled.

Enabling local authentication of non EAPOL hosts on EAPOL-enabled ports

About this task

For local authentication of non-EAPOL hosts on EAPOL-enabled ports, you must enable the feature globally on the switch and locally for ports on the interface.

Procedure

1. Enable local authentication of non-EAPOL hosts globally on the switch:
   a. Enter Global Configuration mode:

      ```
      enable
      configure terminal
      ```

   b. Enable local authentication of non-EAPOL hosts globally :

      ```
      eapol multihost allow-non-eap-enable
      ```

2. Enable local authentication of non-EAPOL hosts or a specific port or for all ports on an interface:
   a. Enter Interface Configuration mode:

      ```
      enable
      configure terminal
      interface ethernet <port number>
      ```

   b. Enable local authentication of non-EAPOL hosts for a specific port or for all ports:

      ```
      eapol multihost [port <portlist>] allow-non-eap-enable
      ```

Variable definitions

Use the data in the following table to use the **`eapol multihost`** command.

Variable	Value
<portlist>	Specifies the port or list of ports on which you want to enable non-EAPOL hosts using local authentication. If you do not specify a port parameter, the command applies to all ports on the interface.

Enabling RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports

About this task

For RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports, you must enable the feature globally on the switch and locally for ports on the interface.

Procedure

1. Enable RADIUS authentication of non-EAPOL hosts globally:
   a. Enter Global Configuration mode:

      ```
      enable
      configure terminal
      ```

   b. Enable RADIUS authentication of non-EAPOL hosts globally :

      ```
      eapol multihost radius-non-eap-enable
      ```

2. Enable RADIUS authentication of non-EAPOL hosts for a specific port or for all ports on an interface:
   a. Enter Interface Configuration mode:

      ```
      enable
      configure terminal
      interface ethernet <port number>
      ```

b. Enable RADIUS authentication of non-EAPOL hosts for a specific port or for all ports on an interface:

```
eapol multihost [port <portlist>] radius-non-eap-enable
```

Variable definitions

Use the data in the following table to use the **eapol multihost** command.

Variable	Value
<portlist>	Specifies the port or list of ports on which you want to enable non-EAPOL hosts using local authentication. If you do not specify a port parameter, the command applies to all ports on the interface.

Configuring the format of the RADIUS password attribute when authenticating non-EAP MAC addresses using RADIUS

About this task

Use the following procedure to configure the format of the RADIUS password when authenticating non-EAP MAC addresses using RADIUS.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. Configure the format of the RADIUS password:

```
eapol multihost non-eap-pwd-fmt {[ip-addr] [mac-addr] [port-number]
[key] [key-string <key-string>] [padding] [no-padding]}
```

Variable definitions

Use the data in the following table to use the **eapol multihost non-eap-pwd-fmt** command.

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.

Setting the configurable key for RADIUS NEAP password

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:

   ```
   enable
   configure terminal
   ```

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>
   ```

   Note:

   If you are using an 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.

Variable definitions

Use the data in the following table to use the **`eapol multihost non-eap-pwd-fmt`** command.

Parameter	Description
key-string *<key-string>*	Define a string up to 32 ASCII characters.

Displaying RADIUS NEAP password settings

About this task

Display the password fields and padding.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Display the password fields and padding:

   ```
   show eapol multihost non-eap-pwd-fmt
   ```

3. Display the key used:

   ```
   show eapol multihost non-eap-pwd-fmt key
   ```

Note:

The password is displayed in cleartext only when password security is not enabled. Otherwise, the password is displayed as a string of asterisks.

Example

```
Switch>enable
Switch#show eapol multihost non-eap-pwd-fmt
Non-EAPOL RADIUS Password Attribute Format:  IpAddr.MACAddr.PortNumber
Padding: Disabled
```

```
Switch>enable
Switch#show eapol multihost non-eap-pwd-fmt key
EAPoL NEAP Password Format Key:**********
```

Enabling RADIUS-assigned VLAN for non-EAP MACs

About this task

Enable RADIUS-assigned VLAN use for non-EAP MACs in the MHMA-MV mode.

Procedure

1. Enable RADIUS-assigned VLAN use for non-EAP MACs in the MHMA-MV mode:
   a. Enter Global Configuration mode:

      ```
      enable
      configure terminal
      ```

   b. Enable RADIUS-assigned VLAN use for non-EAP MACs in the MHMA-MV mode:

      ```
      eapol multihost [non-eap-use-radius-assigned-vlan]
      ```

2. Enable RADIUS-assigned VLAN use for non-EAP MACs in the MHMA-MV mode for a specific interface:
   a. Enter Interface Configuration mode:

      ```
      enable
      configure terminal
      interface ethernet <port number>
      ```

   b. RADIUS-assigned VLAN use for non-EAP MACs in the MHMA-MV mode for a specific interface:

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

Variable definitions

Use the data in the following table to use the **`eapol multihost non-eap-use-radius-assigned-vlan`** command.

Variable	Value
<portlist>	Defines the port on which to enable RADIUS-assigned VLAN use for non-EAP configured in the MHMA-MV mode. You can enter a single port, several ports or a range of ports.

Disabling RADIUS-assigned VLAN for non-EAP MACs

About this task

Disable RADIUS-assigned VLAN use for non-EAP macs in the MHMA-MV mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable RADIUS-assigned VLAN use for non-EAP macs in the MHMA-MV mode:

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

   OR

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

Specifying the maximum number of non EAPOL hosts allowed

About this task

Configure the maximum number of non EAPOL hosts allowed for a specific port or for all ports on an interface.

Note:

The configurable maximum number of non- EAPOL clients for each port is 32, the maximum allowed for each port should be lower. The combined maximum should be approximately 200 for each box and 800 for a stack.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. Configure the maximum number of non EAPOL hosts allowed for a specific port or for all ports on an interface:

   ```
   eapol multihost [port <portlist>] non-eap-mac-max <value>
   ```

Variable definitions

Use the data in the following table to use the **eapol multihost** command.

Variable	Value
<portlist>	Specify the list of ports to which you want the setting to apply. 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>	Specify the maximum number of non EAPOL clients allowed on the port at one time. RANGE: 1–32 DEFAULT: 2

Creating the allowed non EAPOL MAC address list

About this task

Specify the MAC addresses of non EAPOL hosts allowed on a specific port or on all ports on an interface, for local authentication.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. Specify the MAC addresses of non EAPOL hosts allowed:

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

Variable definitions

Use the data in the following table to use the **eapol multihost non-eap-map** command.

Variable	Value
<portlist>	Specify the port on which you want to allow the specified non EAPOL hosts.
<H.H.H>	Specify 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 Displaying global settings for non EAPOL hosts on page 194.

- port settings. For more information, see Displaying port settings for non EAPOL hosts on page 195.
- allowed MAC addresses, for local authentication. For more information, see Displaying allowed MAC addresses on page 195.
- current non EAPOL hosts active on the switch. For more information, see Displaying current non EAPOL host activity on page 196.
- status in the Privilege Exec mode. For more information, see Displaying the current EAPOL-based security status on page 160.

Displaying global settings for non EAPOL hosts

About this task

Display global settings for non EAPOL hosts on EAPOL-enabled ports.

Note:

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.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Display global settings for non EAPOL hosts on EAPOL-enabled ports.

   ```
   show eapol multihost
   ```

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#show eapol multihost
Allow Local Non-EAP Clients                          :  Disabled
Non-EAP RADIUS Authentication                        :  Disabled
Non-EAP AutoLearned After Single Authent (MHSA)      :  Disabled
Non-EAP DHCP Phone Authentication                    :  Disabled
EAPoL Request Packet Generation Mode                 :  Multicast
EAP RADIUS Assigned VLANs                            :  Enabled
Non-EAP RADIUS Assigned VLANs                        :  Enabled
Non-EAP RADIUS Password Attribute Format             :  MACAddr
Non-EAP User Based Policies                          :  Disabled
Non-EAP User Based Policies Filter On MAC Addresses  :  Disabled
EAP Protocol                                         :  Enabled
Non-EAP ReAuthentication                             :  Disabled
ADAC Non-EAP Phone Authentication                    :  Disabled
Fail Open VLAN                                       :  Disabled
Fail Open VLAN ID                                    :  1
Fail Open VLAN Continuity Mode                       :  Disabled
```

Displaying port settings for non EAPOL hosts

About this task

Display non EAPOL support settings for each port.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Display non EAPOL support settings for each port:

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

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch#show eapol multihost interface
Unit/Port:  1/1
    Total Maximum Number of Clients                    :  1
    Maximum Number of  EAP Clients                     :  1
    Maximum Number of Non-EAP Clients                  :  1
    Allow Local Non-EAP Clients                        :  Disabled
    Non-EAP RADIUS Authentication                      :  Disabled
    Non-EAP AutoLearned After Single Auth (MHSA)       :  Disabled
    Non-EAP DHCP Phone Authentication                  :  Disabled
    EAPoL Request Packet Generation Mode               :  Multicast
    EAP RADIUS Assigned VLANs                          :  Enabled
    Non-EAP RADIUS Assigned VLANs                      :  Enabled
    EAP Protocol                                       :  Enabled
    ADAC Non-EAP Phone Authentication                  :  Disabled
    MHSA No limit Non-EAP Authentication               :  Disabled
```

Variable definitions

Use the data in the following table to use the **`show eapol multihost interface`** command.

Variable	Value
<portlist>	Specify the list of ports you want to view. 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.

Displaying allowed MAC addresses

About this task

Display the MAC addresses of non EAPOL hosts allowed to access ports on an interface.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Display the MAC addresses of non EAPOL hosts allowed to access ports on an interface:

```
show eapol multihost non-eap-mac interface [<portlist>]
```

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch#show eapol multihost non-eap-mac interface
Port Allowed MAC Address    Port Allowed MAC Address
---- -------------------    ---- -------------------
Total number of locally configured MAC addresses:  0
```

Displaying current non EAPOL host activity

About this task

Display current non EAPOL host activity.

Note:

If you apply the **`show eapol multihost non-eap-mac 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.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. Display current non EAPOL host activity:

```
show eapol multihost non-eap-mac status [<portlist>]
```

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#show eapol multihost non-eap-mac status
Port Client MAC Address State                          Vid  Pri
---- ------------------ ------------------------------ ---- ---
Total number of authenticated clients: 0
```

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 15: EAP per port features

Feature	Behavior
Non-EAP	The functionality is present when multihost and non-EAP are enabled per port.
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).

Variables

Use the data in the following table to use the **`no eapol multihost eap-protocol-enable`** command.

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.

Enabling IP phone clients on an EAP-enabled port

Enable this feature to allow an IP phone client and an EAP PC to exist together on a port. To enable 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 158).
   - Multihost is enabled on the desired ports. (See Configuring multihost support on page 180).
   - NonEAP is enabled globally and locally (on the desired interface ports). (See Configuring support for non-EAPOL hosts on EAPOL-enabled ports on page 187).
   - Filtering is enabled (to capture DHCP packets and to look for the IP phone Signature).

     Important:

     You should not enable the following two features 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 IP phone clients globally on the switch. See Enabling and disabling IP phone clients as a non-EAP type globall on page 198.
3. Enable IP phone clients locally or for specific ports on the interface. See Enabling IP phone clients in the interface mode on page 199.
4. Specify the maximum number of non EAPOL MAC addresses allowed: the maximum number allowed is 32.

Enabling and disabling IP Phone clients as a non-EAP type globally

About this task

Globally enable IP Phone clients as a non-EAP type.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Globally enable IP Phone clients as a non-EAP type:

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

3. Disable IP Phone clients as a non-EAP type:

```
no eapol multihost {[non-eap-phone-enable]}
```

OR

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

Variable definitions

Use the data in the following table to use the **`eapol multihost {[non-eap-phone-enable]}`** command.

Parameter	Description
non-eap-phone-enable	globally enables IP Phone clients as a non-EAP type.

Enabling IP phone clients in the interface mode

About this task

Enable IP phone clients in the interface mode.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface ethernet <port number>
```

2. Enable IP phone clients in the interface mode:

```
eapol multihost [port <portlist>][non-eap-phone-enable]
```

3. Disable IP phone clients in the interface mode:

```
no eapol multihost [port <portlist>] [non-eap-phone-enable]
```

OR

```
default eapol multihost [port <portlist>] [non-eap-phone-enable]
```

Variable definitions

Use the data in the following table to use the **`eapol multihost [port <portlist>][non-eap-phone-enable]`** command.

Parameter	Description
<portlist>	Specify the port or ports on which you want 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 IP phone clients as a non-EAP type, on the desired port or ports.

Configuring Wake on LAN with simultaneous 802.1X Authentication

Before you begin

- Configure the primary RADIUS server
- Configure the shared secret
- Enable EAPOL

About this task

Authenticate 802.1X and Wake on LAN simultaneously by changing the 802.1X port configuration control.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. Enable the EAPOL administrative state:

   ```
   eapol port <port_list> traffic-control in
   ```

Variable Definitions

Use the data in the following table to use the **`eapol port <port_list> traffic-control in`** command.

Variable	Value
<port_list>	Specify 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

`Switch(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`
	`Switch(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`

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

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.
UserBasedPoliciesEnabled	Enables the User Based Policies.
UserBasedPoliciesFilterOnMac	Enables the User Based Policies filtering on MAC addresses.
AllowPortMirroringOnEap	Enables or disables port mirroring on EAPOL-enabled ports.
GuestVlanEnabled	Enables or disables the Guest VLAN.
GuestVlanId	Sets the VLAN ID of the Guest VLAN.
MultiHostAllowNonEapClient	Enables or disables support for non EAPOL hosts on EAPOL-enabled ports.
MultiHostSingleAuthEnabled	Enables or disables Multiple Host Single Authentication (MHSA).
MultiHostRadiusAuthNonEapClient	Enables or disables RADIUS authentication of non EAPOL hosts on EAPOL-enabled ports.
MultiHostRadiusNonEapDelay	Specifies the global delay time for non-EAP authentication, in seconds, in order to give priority to EAP authentication. A delay of 0 means an instantaneous attempt to authenticate non-EAP clients through the Radius server. **Note:** Network latency and internal synchronization between tasks running on the switch might give slightly different results than the configured time.
MultiHostAllowNonEapPhones	Enables or disables 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.
MultiHostEapPacketMode	Enables or disables the choice of packet mode (unicast or multicast) in the Multihost mode.
MultiHostUseMostRecentRadiusAssigne dVlan	Enables or disables the use of the most recent RADIUS VLAN. **Note:** You must also enable MultiHostUseMostRecentRadiusAssignedVlan on each port to enable the feature.
MultiHostMultiVlan	Enables or disables the multiple VLAN capability for EAP and non-EAP hosts. DEFAULT: disabled
MultiHostEapProtocolEnabled	Enables or disables the processing of EAP protocol packets.
MultiHostFailOpenVlanEnabled	Enables or disables the EAPOL multihost Fail Open VLAN.

Table continues…

Variable	Value
	Important: 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.
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. • ipAddr — include switch IP address string • macAddr — include MAC address string • portNumber — include port string • key — include configurable key string • padding — With the **padding** option unchecked, the RADIUS password uses dots only to separate fields. This is the default setting. With the option checked, the RADIUS password uses dots for every missing parameter.
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.

Enabling or disabling non-EAP client re-authentication using EDM

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

Procedure

1. 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 **MultiHostNeapReauthenticationEnabled** to enable NEAP reauthentication.

   OR

   Clear **MultiHostNeapReauthenticationEnabled** to disable NEAP reauthentication.
5. On the toolbar, click **Apply**.

Port-based EAPOL configuration using EDM

Use the following procedures to configure EAPOL security parameters for single or multiple port.

Configuring port-based EAPOL for an individual port

About this task

Configure EAPOL security parameters for an individual port.

Procedure

1. On the **Device Physical View** select a port.
2. Right-click the port.
3. From the drop-down menu, click **Edit** or from the navigation tree, select **Edit** > **Chassis** > **Port**.
4. In the work area, click the **EAPOL** tab.
5. Configure the parameters as required.
6. In the toolbar, click **Apply**.

Variable definitions

Use the data in the following table to configure EAPOLsecurity parameters for an individual port.

Variable	Value
PortProtocolVersion	Specifies the EAP Protocol version running on this port.
PortCapabilities	Specifies the Port Access Entity (PAE) functionality implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Initializes the port EAPOL state. **Important:** Set this attribute to True to initialize the port EAPOL state.
PortReauthenticateNow	Reauthenticates the client.

Table continues…

Variable	Value
	Important: Set this attribute to True to reauthenticate the client.
PaeState	Specifies the current authenticator PAE state machine state value.
BackendAuthState	Specifies the current state of the Backend Authentication state machine.
AdminControlledDirections	Specifies the current value of the administrative controlled directions parameter for the port. Available options are: • both • in Default is in.
OperControlledDirections	Specifies the current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	Specifies the current value of the controlled port status parameter for the port.
AuthControlledPortControl	Specifies the current value of the controlled port control parameter for the port. Available options are: • forcedUnauthorized • auto • forcedAuthorized Default is forcedAuthorized.
QuietPeriod	Specifies the current value of the time interval between authentication failure and new authentication start. Value ranges between 0 and 65535 seconds. Default value is 60 seconds.
SupplicantTimeout	Specifies the time period to wait for a response from the supplicant for all EAP packets except EAP Request/Identity. The default is 30 seconds. The time interval can be between 1 and 65535.
ServerTimeout	Specifies the time period to wait for a response from the RADIUS server. The default is 30 seconds. The time interval can be between 1 and 65535 seconds.
MaximumRequests	Specifies the number of allowed retries while sending packets to the supplicant. The default is 2 seconds. The number of retries can be between 1.

Table continues…

Variable	Value
ReAuthenticationPeriod	Specifies the time interval between successive reauthentications. The default is 3600 seconds. The time interval can be between 1 and 604800.
ReAuthenticationEnabled	Specifies if reauthentication is required. **Important:** Set this attribute to True to reauthenticate an existing supplicant at the time interval specified in the ReauthenticationPeriod field.
KeyTxEnabled	Specifies the value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns a value of False because key transmission is irrelevant.
LastEapolFrameVersion	Specifies the protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	Specifies the source MAC address carried in the most recently received EAPOL frame.

Configuring port-based EAPOL for multiple ports

About this task

You can configure the EAPOL security parameters on multiple ports using the Security or Edit folder from the navigation tree.

Procedure

1. Do any one of the following:
   a. On the **Device Physical View** use CTRL+ click to select more than one port.
   b. Right-click the port or group of ports.
   c. From the drop-down menu, select **Edit** or from the navigation tree, select **Edit** > **Chassis** > **Port**.
   d. On the work area, click the **EAPOL** tab.

   Or

   a. From the navigation tree, double-click **Security**.
   b. In the Security tree, double-click **802.1X/EAP**.
   c. In the work area, click the **EAPOL Ports** tab.
2. Optionally, to configure parameters for multiple ports, you can use the Multiple Port Configuration section as below.
3. In the work area, in the Make Selection section of the Multiple Port Configuration pane, click the Switch/Stack/Ports ellipsis (...) to open the Port Editor dialog. If there is no Switch/Stack/

Ports selection and you have already selected ports from the **Device Physical View**, proceed to the next step.

a. In the Port Editor window, click the ports you want to configure. If you want to configure all ports, click **All**.

b. Click **OK** to return to the Make Selection pane.

The ports you selected appear in the Switch/Stack/Ports box.

4. To change the configuration of the selected ports, in the Multiple Port Configuration pane, double-click the cell beneath the column heading that represents the parameter you want to change and do one of the following:
   - If applicable, select a value from a drop-down list.
   - Otherwise, type a value in the cell.
5. In the Make Selection pane, click **Apply Selection**.

   The changes appear in the table.
6. **(Optional)** Click **Clear Selection** to clear Multiple Port Configurations or click **Hide Non-Editable** to display only those parameters that are editable in the Multiple Port Configuration pane for the selected ports.

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.
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
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.

Configuring advanced port-based EAPOL using EDM

About this task

Configure advanced EAPOL security parameters for an individual port or multiple ports.

Procedure

1. Follow one of the following paths:
   - From the **Device Physical View**, select a port, or use Ctrl-click to select more than one port, right-click **Edit** then click the **EAPOL Advance** tab.
   - From the **Device Physical View**, select a port, or use Ctrl-click to select more than one port, then follow the navigation tree to **Edit > Chassis > Ports > EAPOL Advance** tab.
   - From the navigation tree, select **Security > 802.1X/EAP**, and click the **EAPOL Advance Ports** tab.
2. Configure the parameters as required.
3. Optionally, to configure parameters for multiple ports, you can use the Multiple Port Configuration section as below.
4. In the work area, in the Make Selection section of the Multiple Port Configuration pane, click the Switch/Stack/Ports ellipsis (...) to open the Port Editor dialog. If there is no Switch/Stack/Ports selection and you have already selected ports from the **Device Physical View**, proceed to the next step.
   a. In the Port Editor window, click the ports you want to configure. If you want to configure all ports, click **All**.
   b. Click **OK** to return to the Make Selection pane.

   The ports you selected appear in the Switch/Stack/Ports box.
5. To change the configuration of the selected ports, in the Multiple Port Configuration pane, double-click the cell beneath the column heading that represents the parameter you want to change and do one of the following:
   - If applicable, select a value from a drop-down list.
   - Otherwise, type a value in the cell.
6. In the Make Selection pane, click **Apply Selection**.

   The changes appear in the table.
7. **(Optional)** Click **Clear Selection** to clear Multiple Port Configurations or click **Hide Non-Editable** to display only those parameters that are editable in the Multiple Port Configuration pane for the selected ports.
8. In the toolbar, click **Apply**.

Variable definitions

Variable	Value
PortNumber	Indicates the port number. Appears only if multiple ports were selected.
DefaultEapAll	Enables or disables the default EAP settings.
GuestVlanEnabled	Enables or disables Guest VLAN functionality.
GuestVlanId	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. **Important:** Use 0 to indicate a global Guest VLAN ID.
MultiHostMaxMacs	Specifies the maximum number of clients allowed on this port. The default is 2. The maximum number can be between 1 and 64.
MultiHostEapMaxNumMacs	Specifies the maximum number of EAPOL-authenticated clients allowed on this port. The default is 2. 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 2. The maximum number can be between 1 and 32.
MultiHostSingleAuthEnabled	Enables or disables Multiple Host with Single Authentication (MHSA) support for non EAPOL clients.
MultihostSingleAuthNoLimit	Specifies whether there is a limit on the number of auto-authenticated non-EAPOL clients. A value of true indicates no limit, false indicates there is a limit. DEFAULT: false
MultiHostRadiusAuthNonEapClient	Enables or disables support for non EAPOL clients using RADIUS authentication.
MultiHostAllowNonEapPhones	Enables or disables support for 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).
EapProtocolEnabled	Enables or disables EAP protocol.

Table continues…

Variable	Value
FailOpenVlanId	Specifies the fail open VLAN ID. The value range is from -1 to 4094. Enter -1 to use port PVID or 0 to use global Fail Open VLAN ID. By default, the value is 0.
FailOpenVlanEnabled	Enables or disables the Fail Open VLAN. By default, it is disabled.
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.

Viewing EAPOL Unauthenticated Clients

Use this procedure to view the unauthenticated clients for a port.

Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **802.1X/EAP**.
3. In the work area, click the **EAPOL Unauthenticated Status** tab.

EAPOL Unauthenticated Status tab field descriptions

The following table describes the fields on the **EAPOL Unauthenticated Status** tab.

Name	Description
PortNumber	Specifies the port number associated with the client.
ClientMACAddr	Specifies the MAC address of the client.
Type	Specifies the reason for unauthentication.
RadiusStatus	Specifies the status for clients authenticated by the RADIUS server.

Graphing port EAPOL statistics using EDM

Use this procedure to display and graph port EAPOL statistics.

Procedure

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.
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

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.
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.

Table continues…

Variable	Value
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 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

1. From the **Device Physical View**, select a port.
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. In the work area, click the **EAPOL Advance** tab.
6. On the toolbar, click **Multi Hosts**, then the **Multi Host Status** tab.

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

1. From the **Device Physical View**, select a port.
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. In the work area, click the **EAPOL Advance** tab.
6. On the toolbar, click **Multi Hosts**, then the **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.

Viewing Multihost DHCP authenticated information using EDM

Use this procedure to view multiple host DHCP authenticated information for a port.

Note:

The Multi Hosts and Non-EAP MAC buttons are not available when configuring multiple ports on the EAPOL Advance tab. To make use of these two options, you can select only one port.

Procedure

1. From the **Device Physical View**, select a port.
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. In the work area, click the **EAPOL Advance** tab.
6. On the toolbar, click **Multi Hosts**, then the **Multi Host DHCP Authenticated** tab.

Variable definitions

Use the data in the following table to view Multihost DHCP Authenticated session information.

Field	Description
PortNumber	Specifies the port number in use.
ClientMACAddr	Specifies the MAC address of the client.
Username	Specifies the client user name.

Allowed non-EAP MAC address list configuration using EDM

This section describes the procedures 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

- AddingAMACAddressToTheAllowedNonEAPMACAddressListUsingEDM on page 216
- DeletingAMACAddressFromTheAllowedNonEAPMACAddressListUsingEDM_5_8 on page 217

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.

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.

Procedure

1. From the **Device Physical View**, select a port.
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. In the work area, click the **EAPOL Advance** tab.
6. In the tool bar, click the **Non-EAP MAC** button.

7. In the work area, click the **Allowed non-EAP MAC**tab.
8. On the tool bar, click **Insert**.
9. Enter a MAC address to add to the list of allowed non-EAPOL clients.
10. Click **Insert**.
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

Procedure

1. From the **Device Physical View**, select a port.
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. In the work area, click the **EAPOL Advance** tab.
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. In the work area, click the **Allowed non-EAP MAC**tab.
8. In the **ClientMACAddr** column, click a client MAC Address to delete.
9. On the tool bar, click **Delete**.
10. Click **Yes** to confirm the deletion.
11. 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

1. From the **Device Physical View**, select a port.
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. In the work area, click the **EAPOL Advance** tab.
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. Click the **Non-EAP Status** tab.

Variable definitions

The following table describes the fields of the **Non-EAP Status** tab.

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: • rejected: the MAC address cannot be authenticated on this port • locallyAuthenticated: the MAC address was authenticated using the local table of allowed clients • radiusPending: the MAC address is awaiting authentication by a RADIUS server • radiusAuthenticated: the MAC address was authenticated by a RADIUS server • adacAuthenticated: the MAC address was authenticated using ADAC configuration tables • mhsaAuthenticated: the MAC address was 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.

Chapter 8: FIPS 201-2 Standard

This chapter provides conceptual information and procedures to configure FIPS 201-2 standard (Personal Identity Verification of Federal Employees and Contractors) using Command Line Interface (CLI) .

FIPS 201-2 Standard Fundamentals

The FIPS 201-2 standard (Personal Identity Verification of Federal Employees and Contractors) specifies the usage of integrated circuit cards to store the identity credentials of the cardholder. The ERS 4900 and ERS 5900 Series support the authentication using smart card technology for remote device management. The switches use SSH and X.509v3 certificates, which are stored on the smart card.

The Personal Identity Verification (PIV) card supports the following authentication mechanisms:

- X.509v3 Certificate for PIV Authentication
- X.509v3 Certificate for Card Authentication

PIV and Card Authentication

The process for PIV and Card authentication is as follows:

1. The PIV Authentication or the Card Authentication certificate is read from the PIV Card Application.
2. The relying system validates the PIV Authentication certificate from the PIV Card Application using standards-compliant PKI path validation to ensure that it is neither expired nor revoked and that it is from a trusted source.
3. The cardholder is prompted to submit a PIN, which is used to activate the card.
4. The relying system issues a challenge string to the card and requests an asymmetric operation in response.
5. The card responds to the previously issued challenge by signing it using the PIV Authentication private key.
6. The relying system verifies that the card’s response is the expected response to the issued challenge.
7. A unique identifier from the PIV Authentication certificate is extracted and passed as input to the access control decision.

For information about configuring SSH x509v3 Authentication and configuring SSH Server, see SSH x509v3 Authentication and SSH Server configuration on page 484.

SSH x509v3 Authentication and SSH Server Configuration using CLI

This section provides procedures to configure SSH x509v3 Authentication and SSH Server using CLI.

Configuring the SSH Server

Use the following procedure to configure the SSH server and setup the trust point to be used. The key and CSR can be generated locally but this document describes the method of importing those files generated elsewhere. Online procedure can also be applied for obtaining digital certificates.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enter the following command to confirm Enhanced Secure Mode is enabled:

   ```
   show enhanced-secure-mode

   Switch(config)# show enhanced-secure-mode 2018-04-03 09:38:06 GMT
   +00:00 Enhanced Secure Mode: Enabled
   ```

3. Enter the following command to confirm the clock is synchronized:

   ```
   show clock

   Switch(config)# show clock System Clock time : 2018-04-03 10:14:43
   GMT+02:00 SNTP time : 2018-04-03 10:14:43 GMT+02:00Daylight saving
   recurring time is disabledDaylight saving time is disabledTime zone
   is set to 'Buc', offset from UTC is 02:00
   ```

4. Import the key contained in the switch subject certificate from USB / SFTP

   ```
   Switch(config)#certificate key CAC-server.key.pem import usb filename CAC-
   server.key.pemSwitch(config)#certificate key CAC-server.key.pem import sftp
   filename CAC-server.key.pem username sftp Enter SFTP server password:

   Switch(config)#show certificate key Name Type Size
   ---------------------------------------------- ----- ---- CAC-
   server.key.pem RSA 2048
   ```

5. Configure the certificate subject parameters:

```
Switch(config)#certificate subject common-name CAC-server
Switch(config)#certificate subject e-mail jsmith@extremenetworks.com
Switch(config)#certificate subject unit BayPv
Switch(config)#certificate subject organization Extreme Networks
Switch(config)#certificate subject locality Buc
Switch(config)#certificate subject province Buc
Switch(config)#certificate subject country RO
Switch(config)#sh certificate subject
Common-name           : CAC-server
E-mail                : jsmith@extremenetworks.com
Organizational unit   : BayPv
Organization          : Extreme Networks
Locality              : Buc
State/Province        : Buc
Country               : RO
Include IP address    : false
FQDN                  :
```

6. Configure the trustpoint on the switch.

```
Switch(config)#certificate ca CAC common-name IPSEC key-name CAC-server.key.pem
Switch(config)#sh certificate ca CAC
Name                          : CAC
Common-name                   : IPSEC
KeyName                       : CAC-server.key.pem
CaUrl                         :
UsePost                       : false
SubjectCertValidityDays       : 365
Regenerate key on re-enroll   : false
Auto-renew                    : disabled
Use for                       :
CA contains a complete chain  : false
LastAction                    : no-op
LastActionStatus              : none
LastActionFailureReason       : OK
```

7. Import ROOT CA and subject certificates from USB/SFTP.

```
Switch(config)#certificate ca CAC import usb filename ca.cert.pem
Switch(config)#certificate ca CAC import usb filename CAC-server.pem
Switch(config)#certificate ca CAC import sftp filename ca.cert.pem username sftp
Enter SFTP server password:
Switch(config)#certificate ca CAC import sftp filename CAC-server.pem username sftp
Enter SFTP server password:

Switch#show certificate ca CAC
Name                          : CAC
Common-name                   : IPSEC
KeyName                       : CAC-server.key.pem
CaUrl                         :
UsePost                       : false
SubjectCertValidityDays       : 365
Regenerate key on re-enroll   : false
Auto-renew                    : disabled
Use for                       :
CA contains a complete chain  : true
LastAction                    : no-op
LastActionStatus              : none
LastActionFailureReason       : OK

Type          File name                   Not valid before   Not valid after
------------- --------------------------- ------------------ ------------------
```

```
rootCa        ca.cert.pem                 05/17/17 12:11:06  05/12/37 12:11:06
subjectCert   CAC-server.pem              03/29/18 15:32:39  04/08/19 15:32:39

Switch(config)#show certificate ca CAC file CAC-server.pem
2018-04-03 09:42:50 GMT+00:00
FileName                : CAC-server.pem
Associated context name : CAC
Associated context type : CA
File type               : subjectCert
Version number          : X.509 v3
Serial number           : 10:1E
Issuer name             : CO=RO, P=Buc, L=Buc, O=Extreme Networks, OU=BayPv,
CN=IPSEC, EM=jsmith@extremenetworks.com
Not valid before        : 03/29/18 15:32:39
Not valid after         : 04/08/19 15:32:39
Signature algorithm     : sha256withRSAEncryption
Signature               : 2B:34:8B:62:62:6F:2A:
73:52:A4:EC:E9:F0:B6:74:14:A5:B3:35:97:7F:9F:87:BB:A5:05:20:7A:23:31:71:BB:2A:3D:
14:6
5:3B:E3:E5:6B:96:90:B7:DA:68:0E:8E:19:CD:5B:D3:53:06:88:1A:81:97:65:B1:5C:2D:B1:DB:
60:9C:CE:8D:74:3D:28:58:51:EB:C5:EB:74:E2:5E:35:2
9:DB:BE:7C:FA:EC:93:08:A6:B5:2A:08:84:22:9F:77:CA:31:C9:6B:99:24:57:A2:EF:
13:C0:ED:E8:EB:2D:B8:BE:78:CD:28:6C:0A:91:5B:9D:97:75:79:A
A:CE:CB:EA:D2:42:24:2A:EB:83:35:69:AC:D0:32:16:66:DD:73:7E:CC:BF:AF:
61:60:07:D2:6A:E4:C7:98:18:26:E8:Switch:F3:99:1E:BB:5A:F1:57:31:19:7
E:0B:E8:8D:7A:A7:4F:C0:A6:F6:68:70:14:6F:98:1E:B1:EC:10:A1:86:14:BD:30:BE:A1:9D:
59:40:C1:A8:40:FE:03:36:FD:46:A0:26:74:CA:BA:24:B0:8
0:D0:1A:4E:74:EA:1B:0E:9E:E3:CC:12:D7:18:EC:42:66:33:FA:6B:1C:
53:15:28:17:89:1D:C5:05:3D:00:96:29:AB:9A:3E:B1:82:02:9F:80:44:8B:90:1
B:D6:3B:A4:55:CA:C7:C5:0E:EF:E1:B0:DC:AD:83:4C:0E:A4:5E:62:23:A6:D4:BA:
10:84:2C:FF:E2:A7:5F:A5:9C:60:CC:7F:19:36:AE:CD:FC:E6:4C:25:D
3:CE:16:23:81:AE:DD:14:90:E3:F7:C9:C6:3F:DC:27:70:DF:21:27:2B:78:F1:9B:F8:D7:6A:9F:
7D:4C:E2:73:BE:E9:11:A1:8D:21:55:75:B8:8F:D6:48:4
1:24:91:5D:0E:5C:6E:B5:64:01:96:D2:E6:DC:0C:4F:F4:E3:14:3B:AA:2E:31:47:11:C5:6E:1D:
04:04:F4:0E:7A:C7:3B:05:F6:B6:A2:FA:CB:F2:56:3B:2
B:D2:1F:0D:FA:37:08:45:47:E5:24:3D:3D:
51:F1:B7:AE:CF:F6:FE:A1:55:D3:65:5E:FF:C3:A2:42:9A:72:0B:2D:30:D0:AF:
2D:E5:21:F2:A5:5C:40:12:A
A:0C:9D:43:D4:5A:E5:F1:14:FA:44:D3:19:80:D4:C0:ED:61:0F:4F:91:B4:F6:A9:99:4F:3C:FB:
37:0A:AE:03:46:87:38:CA:B6:D8:49:B4:0A:94:BD:9D:6
9:AA:30:00:47:7E:0B:59:DE:FC:BC:D3:8C:01:77:FD:0B:DF:22:B5:52:6A:B7:2E:B3:BE:4F:
57:9B:7A:06:4C:5C:35:33:D1:91
Subject                 : CO=RO, P=Buc, L=Buc, O=Extreme Networks, OU=BayPv,
CN=IPSEC, EM=jsmith@extremenetworks.com
Public key algorithm    : rsaEncryption
Public key              : 30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:
01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:9D:F
8:C6:86:3A:12:95:D7:9C:58:9D:2E:6E:98:AC:CB:EC:2E:04:FA:60:FD:
6C:E8:07:E4:20:74:1D:C6:47:E4:2F:12:13:C6:18:A9:A0:05:80:29:96:78:F9:A
A:16:01:6B:82:D8:35:FF:D5:58:6B:B1:ED:C9:BE:75:20:91:8E:BA:26:45:67:6E:D6:15:BA:CC:
26:A5:F5:0A:E2:7A:13:34:0C:00:82:A7:9E:9E:45:BF:C
2:93:9D:5C:43:B5:E7:27:C6:9A:06:EB:35:2F:A7:16:D5:1F:A3:DA:D7:AF:E6:EC:3C:
07:56:C7:21:49:08:D4:D0:E0:78:45:63:C7:93:01:0C:CA:0B:B4:4
D:2A:4D:24:B1:A4:2F:CB:32:17:73:AE:D4:ED:9A:D6:5E:15:62:33:81:F3:19:E5:51:FF:52:DF:
7F:E1:D2:4D:2A:4E:91:A5:9D:D9:8A:CF:EF:D5:48:32:0
C:B1:BC:E5:EE:3B:49:94:73:1E:F9:40:CA:B2:FB:EA:11:74:19:89:89:82:98:E4:4C:BC:
35:76:08:2B:55:D9:67:C4:99:84:0E:1A:0C:CF:E2:A5:E0:F3:F
6:23:26:98:16:6E:99:AF:CC:68:6B:46:97:35:61:C1:96:91:3A:08:46:4D:72:91:B3:1E:
35:94:C3:31:D4:75:01:6D:02:03:01:00:01
Has basic constraint    : true
Has key usage           : true
Is CA                   : false
Key usage               :
Status                  : active
CDP url                 : http://192.0..2.1
```

```
OCSP url                : http://192.0.2.1:2561
Extended key usage      : TLS Web Server Authentication
```

8. Configure the trustpoint to be used for SSH-server.

```
Switch(config)#certificate ca CAC use-for ssh-server
Switch#show certificate ca CAC
Name                           : CAC
Common-name                    : IPSEC
KeyName                        : CAC-server.key.pem
CaUrl                          :
UsePost                        : false
SubjectCertValidityDays        : 365
Regenerate key on re-enroll    : false
Auto-renew                     : disabled
Use for                        : SSH-Server
CA contains a complete chain   : true
LastAction                     : no-op
LastActionStatus               : none
LastActionFailureReason        : OK
```

9. Import in the trust store root CA and Intermediate CA that signed the certificate from the card

```
certificate trust-store import sftp filename Self-signedTrustAnchorCertificate.cer
username sftp
certificate trust-store import sftp filename RSA2048IssuingCACertificate.cer
username sftp
show certificate trust-store
2018-04-05 11:53:35 GMT+00:00
Type           File name                    Not valid before   Not valid after
-------------- ---------------------------- ------------------ ------------------
interCa        RSA2048IssuingCACertificate.cer 10/01/10 08:30:00  10/01/30
08:30:00
rootCa         Self-signedTrustAnchorCertificate.cer 10/01/10 08:30:00  10/01/30
08:30:00
```

Using an Idenity for SSH Server

Use the following procedure to use an identity for the SSH server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the following command:

   ```
   certificate ca <ca-name> use-for ssh-server
   ```

Example

```
Switch(config)#certificate ca IPSEC use-for ?
  ssh-server  Use as identity for SSH Server

Switch(config)#show certificate ca IPSEC
Name                           : IPSEC
Common-name                    : IPSEC-ICA
KeyName                        : TEST.key.der
CaUrl                          : http://10.100.94.41:8080/ejbca/publicweb/apply/scep/test/
```

```
pkiclient.exe
UsePost                          : true
SubjectCertValidityDays          : 365
Regenerate key on re-enroll      : false
Auto-renew                       : disabled
Use for                          : SSH-Server
CA contains a complete chain     : true
LastAction                       : enroll
LastActionStatus                 : success
LastActionFailureReason          : OK
```

Clearing Idenity Usage for SSH Server

Use the following procedure to remove identity usage for the SSH server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   no certificate ca <ca-name> use-for
   ```

Configuring SSH X.509v3 Authentication

Use the following procedure to configure SSH X.509v3 authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command to enable SSH X.509v3 Authentication:

   ```
   ssh x509v3-auth
   ```

   Note:

   You cannot enable x509v3 authentication if there is no trustpoint configured for SSH.

3. Enter the following command to disable SSH X.509v3 Authentication:

   ```
   no ssh x509v3-auth
   ```

   Note:

   You cannot disable a trustpoint if SSH x509v3 authentication is configured.

Example

The following sample output displays when you try to enable x590v3 authentication without a trustpoint configured for SSH:

```
Switch(config)#ssh x509v3-auth
%Cannot modify settings
% No CA is configured for SSH Server.
```

The following sample output displays when you try to disable a trustpoint when SSH x509v3 authentication is configured:

```
Switch(config)#no certificate ca CAC use-for
% Cannot modify settings
% CA is currently used for SSH x509v3Auth
```

Displaying SSH X.509v3 Authentication

Use the following procedure to display SSH X.509v3 authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enter the following command:

   ```
   show ssh global
   ```

Example

```
Switch(config)#show ssh global
Active SSH Sessions     :  0
Version                 :  Version 2 only
Port                    :  22
Authentication Timeout  :  60
DSA Authentication      :  True
RSA Authentication      :  True
Password Authentication :  True
X.509v3 Authentication  :  True
X.509v3 Username Overwrite  : False
X.509v3 Strip Domain    :  False
X.509v3 Use-Domain      :
Auth Retries            :  3
SSH Rekey               :  False
SSH Rekey-Interval      :  3600000
SSH Rekey-DataLimit     :  1
Auth Key TFTP Server    :  192.0.2.1
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys           :  Exist
RSA Host Keys           :  Exist
Enabled                 :  False
```

Chapter 9: Identity Engines Ignition Server

This chapter provides conceptual information on Identity Engines Ignition Server and procedures to configure Identity Engines Ignition Server communication using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

Extreme Networks Identity Engines Ignition Server

Extreme Networks 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
- acccount 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 Identity Engines Ignition Server, see Support Portal.

Ignition Server configuration using CLI

This section describes how to configure the switch as a network access device in the Identity Engine Ignition Server solution using CLI.

Configuring Ignition Server as a RADIUS server using CLI

Use this procedure to configure Ignition Server to act as the RADIUS server for your switches and access points.

For more information about Identity Engines Ignition Server, see Support Portal.

Before you begin

Ensure the following conditions are met.

- 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 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 with which device a user connected.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure the reachability of the RADIUS server.

   ```
   radius reachability mode use-radius [username <username> password
   <password>]
   ```

3. Configure RADIUS server account information on the switch.

   ```
   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.

Table continues…

Variable	Value
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 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 10 seconds.
used-by <eapol | non-eapol>	Specifies the RADIUS server as an EAP RADIUS Server or a Non-EAP (NEAP) RADIUS Server. • 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 CLI

Use this procedure to configure Ignition Server to act as the EAP RADIUS server for your switches and access points.

For more information about Identity Engines Ignition Server, see Support Portal.

Before you begin

Ensure the following:

- 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 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 with which device a user connected.
- EAP configured on your switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure the reachability of the EAP RADIUS server.

   ```
   radius reachability mode use-radius [username <username> password
   <password>]
   ```

3. Configure EAP RADIUS server account information on the switch.

   ```
   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 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 CLI

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 Identity Engines Ignition Server, see Support Portal.

Before you begin

Ensure the following:

- 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 with which device a user connected.
- Non-EAP configured on your switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure the reachability of the non-EAP RADIUS server.

   ```
   radius reachability mode use-radius [username <username> password
   <password>]
   ```

3. Configure non-EAP RADIUS server account information on the switch.

   ```
   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>	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 <1–66535>	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 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

Table continues…

Variable	Value
	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 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 CLI

You can configure Ignition Server to act as the TACACS+ authentication and authorization server, and you can use it as the TACACS+ accounting server.

For more information about Identity Engines Ignition Server, see Support Portal.

Before you begin

Ensure the following:

- Ignition Server is 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 with which device a user connected.
- 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.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure switch TACACS+ server settings.

   ```
   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>	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. **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 <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.

Ignition Server configuration using Enterprise Device Manager

This section describes how to configure the switch 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 Ingition Server to act as the RADIUS server for your switches and access points. For more information about Identity Engines Ignition Server, see Support Portal.

Before you begin

Ensure the following prerequisites have been met:

- 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.

Procedure

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.
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.
Reachability	Specifies the RADIUS server reachability mode. Values include: • 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. • configuredValue — uses the value in the RadiusAccoutingInterimUpdatesInterval dialog box • radiusServer — uses the value applied by the RADIUS server
EncapsulationProtocol	Specifies the type of encapsulation for the RADIUS packets. Values include: • 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. **Important:** 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.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary Global RADIUS Server. Values include unknown, ipv4, and ipv6.
SecondaryRadiusServer	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. **Important:** 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.
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

Table continues…

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 Ignition Server as an EAP RADIUS Server using EDM

You can configure Ingition Server to act as the EAP RADIUS server for your switches and access points. For more information about Identity Engines Ignition Server, see Support Portal.

Before you begin

Ensure the following prerequisites have been met:

- 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.

Procedure

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: • 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.

Table continues…

Variable	Value
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. • configuredValue — uses the value in the RadiusAccoutingInterimUpdatesInterval dialog box • radiusServer — uses the value applied by the RADIUS server
EncapsulationProtocol	Specifies the type of encapsulation for the RADIUS packets. Values include: • 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. **Important:** 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.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary EAP RADIUS Server. Values include unknown, ipv4, and ipv6.
SecondaryRadiusServer	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.

Table continues…

Variable	Value
	Important: 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.
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 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 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 Ingition Server to act as the non-EAP RADIUS server for your switches and access points. For more information about Identity Engines Ignition Server, see Support Portal.

Before you begin

Ensure the following prerequisites have been met:

- 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

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 RADIUS Reachability box select **useRadius**.
5. **(Optional)** In the RADIUS Accounting section, select values to configure RADIUS
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: • 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. • configuredValue — uses the value in the RadiusAccoutingInterimUpdatesInterval dialog box • radiusServer — uses the value applied by the RADIUS server
EncapsulationProtocol	Specifies the type of encapsulation for the RADIUS packets. Values include: • 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.

Table continues…

Variable	Value
PrimaryRadiusServer	Specifies the IPv4 or IPv6 address for the primary NEAP RADIUS Server. The default address is 0.0.0.0. **Important:** 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.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary NEAP RADIUS Server. Values include unknown, ipv4, and ipv6.
SecondaryRadiusServer	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. **Important:** 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.
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.
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

Table continues…

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 Ingition Server to act as theTACACS+S authentication and authentication server, and you can use it as the TACACS+ accounting server.

For more information about Identity Engines Ignition Server, see Support Portal.

Before you begin

Ensure the following Prerequisites have been met:

- 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.

Procedure

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 displays.

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.

Chapter 10: IP Manager

You can limit access to the switch management features 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, configure ranges of IP addresses that are allowed to access the switch.

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

Configuring IP Manager

To configure the IP Manager to control management access to the switch:

- Enable IP Manager.
- Configure the IP Manager list.

Enabling or disabling IP Manager

About this task

Enables IP Manager to control Telnet, SNMP, or HTTP access.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable IP Manager control.

   ```
   ipmgr {telnet | snmp | web | ssh }
   ```

3. Disable IP Manager control.

   ```
   no ipmgr {telnet | snmp | web | ssh }
   ```

Variable definitions

The following table defines parameters that you can enter with the **ipmgr** command.

Variable	Value
telnet	Enables the IP Manager list check for Telnet access.
snmp	Enables the IP Manager list check for SNMP, including EDM.
web	Enables the IP Manager list check for web connections.
ssh	Enables IP Manager control over SSH sessions.
no	Disables IP Manager for a management system.

Configuring the IP Manager list

About this task

Specify the source IP addresses or address ranges that have access to the switch or stack when IP Manager is enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Specify the source IP addresses or address ranges that have access to the switch or stack when IP Manager is enabled.

   `ipmgr source-ip <list_ID> <ipv4_addr> [mask <mask>]` for IPv4 entries with list ID between 1 and 50

   OR

   `ipmgr source-ip <list_ID> <ipv6_addr/prefix>` for IPv6 entries with list ID between 51 and 100

3. Deny access to the switch or stack for specified source IP addresses or address ranges.

   ```
   no ipmgr source-ip <list_ID>
   ```

Variable definitions

The following table defines parameters that you can enter with the **ipmgr** command.

Variable	Value
<list_ID>	Specifies an integer value. A value In the range of 1 to 50 uniquely identifies an IPv4 entry in the IP Manager list. A value in the range of 51 to 100 uniquely identifies an IPv6 entry in the IP Manager list.
<ipv4_addr>	Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation.
<ipv6addr/prefix>	Specifies the source IPv6 address and prefix form which access is allowed.
mask *<mask>*	Specifies the subnet mask from which access is allowed. Enter the IP mask in dotted-decimal notation.
no	Denies access to the switch or stack for specified source IP addresses or address ranges. Both the IP address and mask for the specified entry are set to 255.255.255.255 for IPv4, and to ffff.ffff.ffff.ffff.ffff.ffff.ffff.ffff/128 for IPv6 entries. If you do not specify a <list_ID> value, the command resets the entire list to factory defaults.

Viewing IP Manager settings

About this task

Displays IP Manager settings.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display IP Manager settings.

   ```
   show ipmgr [ IPv4 ] [ IPv6 ]
   ```

Example

```
Switch#show ipmgr IPv4
TELNET Access: Enabled
SNMP Access:   Enabled
WEB Access:    Enabled
SSH Access:    Disabled
TELNET IP List Access Control: Enabled
SNMP IP List Access Control:   Enabled
WEB IP List Access Control:    Enabled
```

```
SSH IP List Access Control:    Enabled
Allowed Source IP Address  Allowed Source Mask
-------------------------  ------------------
1  0.0.0.0                    0.0.0.0
2  255.255.255.255            255.255.255.255
3  255.255.255.255            255.255.255.255
4  255.255.255.255            255.255.255.255
5  255.255.255.255            255.255.255.255
6  255.255.255.255            255.255.255.255
...
Switch#
Switch#show ipmgr ipv6
TELNET Access: Enabled
SNMP Access:   Enabled
WEB Access:    Enabled
SSH Access:    Disabled
TELNET IP List Access Control: Enabled
SNMP IP List Access Control:   Enabled
WEB IP List Access Control:    Enabled
SSH IP List Access Control:    Enabled
Allowed Source IPv6 Address
-------------------------------------------
51 ::/0
52 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
53 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
54 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
55 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
...
```

Chapter 11: IP Source Guard

This chapter provides conceptual information and procedures to configure IP Source Guard using Command Line Interface (CLI) and Enterprise Device Manger (EDM).

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 80. 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 switch 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.

You should not enable IPSG on MLT, DMLT and LAG ports.

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

Table 16: 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

Table continues…

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

You can configure IP Source Guard using the Command Line Interface (CLI), Enterprise Device Manager, and SNMP.

IP Source Guard configuration using CLI

This section describes how you configure IP Source Guard using the Command Line Interface (CLI).

Important:

You should not enable IP Source Guard on trunk ports.

Important:

You should carefully manage the number of applications running on the switch 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 CLI on page 83.
- 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

Note:

You can configure EAP and IP source guard simultaneously on the same port.

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. IP Source Guard should not be enabled on trunk ports.

Enabling IP Source Guard using CLI

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.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable

   configure terminal

   interface ethernet <port number>
   ```
2. Enable IP Source Guard.

   ```
   ip verify source [interface {[<interface type>] [<interface id>]}]
   ```

Variable definitions

The following table defines parameters that you enter with the **ip verify source** 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 CLI

To view IP Source Guard port configuration information, open the TACACs configuration screen by selecting Applications > configuration settings for interfaces.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View IP Source Guard port configuration.

   ```
   show ip verify source [interface {<interface type>] [<interface id>]
   ```

Variable definitions

The following table defines parameters that you enter with the **show ip verify source** 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 CLI

View IP Source Guard-allowed addresses to display a single IP address or a group of IP addresses that IP Source Guard allows.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View IP Source Guard-allowed addresses.

```
show ip source binding [<A.B.C.D.>] [interface {[<interface type>]
[<interface id>]}]
```

Variable definitions

The following table defines parameters that you enter with the **show ip source binding** 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.

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:

You should not enable IP Source Guard on trunk ports.

Important:

You should carefully manage the number of applications running on the switch 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 D52HCP snooping configuration using EDM on page 95.
- 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. Extreme Networks recommends that you do not enable IP Source Guard on trunk ports.

Configuring IP Source Guard on a port

Use this procedure to configure IP Source Guard to enable or disable a higher level of security on a port.

Procedure

1. Follow one of the following paths:
   - From the **Device Physical View**, select a port, or use Ctrl-click to select more than one port, right-click **Edit** then click the **IP Source Guard** tab.
   - From the **Device Physical View**, select a port, or use Ctrl-click to select more than one port, then follow the navigation tree to **Edit > Chassis > Ports > IP Source Guard** tab.
   - In the navigation tree, go to **Security > IP Source Guard (IPSG) > IP Source Guard-port** tab.
2. Double-click the **Mode** box for a port.
3. Select **ip** from the list to enable IP Source Guard.

   OR

   Select **disabled** from the list to disable IP Source Guard.
4. Repeat the above steps to configure IP Source Guard for additional ports.
5. On the toolbar, click **Apply**.
6. 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

Use this procedure to configure IP Source Guard to enable or disable a higher level of security on multiple ports.

Procedure

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

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, select **Filter**
6. From the Filter window, select the Condition option.
7. Select the Column filter options.
8. Select the columns to be filtered.
9. Specify the string criteria for the selected columns.
10. **(Optional)** Clear **Ignore Case** to make the string criteria for the selected columns case sensitive.
11. Click **Filter**.

    The filtered options display in the table.
12. On the toolbar, click **Filter**.
13. In the **IP Source Guard-addresses - Filter** dialog box, select the required parameters for displaying port IP Source Guard information.
14. Click **Filter**.

    IP Source Guard information for the specified IP addresses is displayed 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: • 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 • 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

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.

Chapter 12: IPv6 First Hop Security

This chapter provides conceptual information on IPv6 First Hop Security and procedures to configure IPv6 First Hop Security using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

IPv6 First Hop Security

This section provides conceptual information on IPv6 First Hop Security (FHS).

What is IPv6?

Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol (IP).

IPv6 is expected to coexist with and eventually replace IPv4. IPv6 provides a larger address space to support future Internet growth. IPv6 is increasingly deployed in enterprise, university, and government networks. The success of the IPv6 deployment depends on the network security and quality of service (QoS) that it offers when compared to Internet Protocol version 4 (IPv4).

IPv6 security concerns

The enhancements in IPv6 provide better security in certain areas, but some of these areas are still open to exploitation by attackers. This section identifies the IPv6 FHS concerns associated with Router Discovery, Neighbor Discovery, and Dynamic Host Configuration Protocol version 6 (DHCPv6).

Router Discovery

IPv6 nodes use the Neighbor Discovery Protocol (NDP) to discover other nodes on the link. NDP is also used to determine the node link-layer addresses to find routers, and to maintain reachability information about the paths to active neighbors (RFC 4861), but it has some First Hop Security concerns.

RFC 4861 resolves link-local specific problems including Router Discovery, Prefix Discovery, stateless address autoconfiguration (SLAAC), IPv6 address resolution (replaces IPv4 ARP),

Neighbor Unreachability Detection (NUD), Duplicate Address Detection (DAD), and redirection, but it does not resolve Denial of Service (DoS) attack.

For example, consider the following figure where the host attempts to discover the router on its local segment. The host uses Internet Control Message Protocol version 6 (ICMPv6) messages, which rely heavily on multicast. In this scenario, Host A attempts to discover routers on its link through router discovery. Host A sends a router solicitation message requesting information about routers on its local segment. The router in turn replies with a router advertisement for a lifetime x. Host A then installs a default route in its routing table with a time x before another router discovery cycle is initiated.

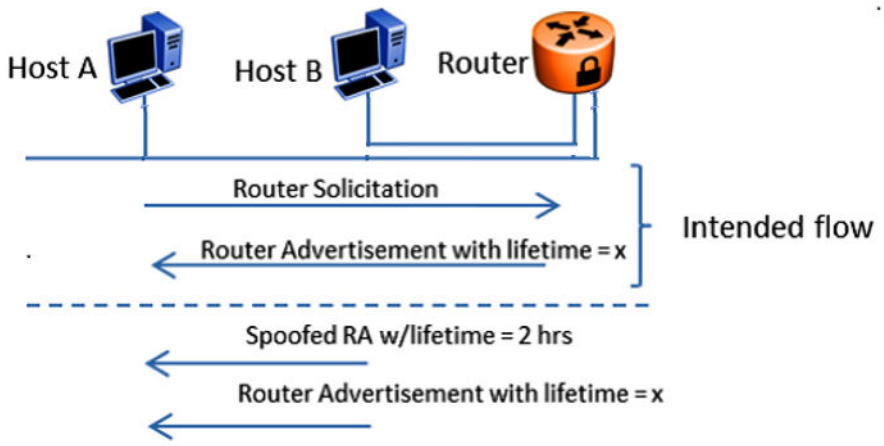


Figure 4: Message Flow IPv6 Router Discovery

If there is an intruder, Host B, on the segment, the intruder can attempt to insert itself as the router by spoofing the legitimate router advertisement and set the lifetime to two hours. According to RFC 4862, “If Remaining Lifetime is less than or equal to two hours, ignore the Prefix Information option with regard to the valid lifetime, unless the Router Advertisement from which this option was obtained has been authenticated.” Host A removes the installed default route that points to the legitimate router after two hours. Host B is then free to send another router advertisement inserting itself as the default route for Host A. Host B now receives all packets intended for the default gateway from Host A. This constitutes a DoS attack, as Host A potentially loses access to the network beyond the legitimate router. Host B can then utilize this to initiate further attacks.

Even though IPv6 can use SEcure Neighbor Discovery (SEND) as an option, the implementation of the SEND is not common. Implementation of SEND can open the door for the first hop attack with respect to the previously-defined threats which is solved by RFC 4861. The FHS predominantly addresses these kinds of threats. FHS takes care of the threats caused by the immediate node to another immediate node attached to the same FHS device.

Stateless Address Autoconfiguration

As defined in RFC 4862, SLAAC enables an IPv6 endpoint to obtain an IPv6 address from the link it is coming up on without requiring DHCPv6 address allocation.

IPv6 address autoconfiguration is stateless, therefore it does not require a mechanism to track the address allocations before it assigns a new address. The address allocation is based on the IPv6 prefix information provided by ICMPv6 router advertisements.

The following figure illustrates the steps involved in deploying the IPv6 address autoconfiguration attack.

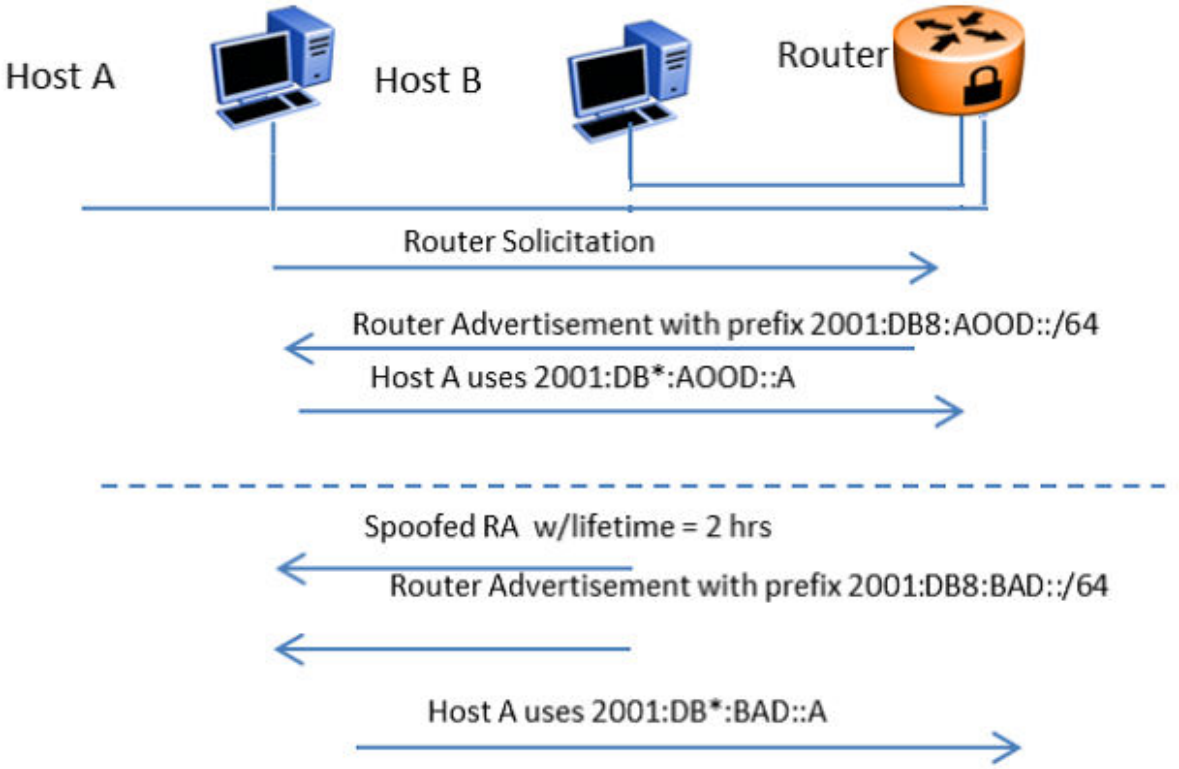


Figure 5: Stateless Address Autoconfiguration

When Host A wants to receive an IPv6 address, it sends an ICMPv6 router solicitation requesting the link information. The router responds with an ICMPv6 router advertisement providing the IPv6 address prefix (shown as 2001:DB8:A00D::/64) on the link with a lifetime x. Then, Host A can pick an address (shown as 2001:DB8:A00D::A) on the link and start using it after checking the duplicate address availability (DAD). If malicious Host B manages to insert itself in the link, it can spoof an ICMPv6 router advertisement from a router that sets the lifetime for the link to two hours. According to RFC 4862, “If Remaining Lifetime is less than or equal to two hours, ignore the Prefix Information option with regards to the valid lifetime, unless the Router Advertisement from which this option was obtained has been authenticated”. This can cause the Host A address to expire in two hours, and Host B can then send a new router advertisement with a new prefix (shown as 2001:DB8:FAFE::/64). On seeing the new prefix, Host A picks a new address (shown as 2001:DB8:FAFE::A). Depending on the network configuration, the router Access Control Lists (ACL) can deny the new address from traversing the network, and therefore Host A can be blocked from accessing beyond the next hop router, or even its link-local peers. If IPv6 address autoconfiguration is used and FHS protection is not employed, Host B can potentially black-hole hosts in its local link by spoofing two IPv6 router advertisements.

Neighbor Discovery

Neighbor Discovery (ND) is similar to Router Discovery but ND is used for hosts.

ND performs operations such as address resolution, DAD, Neighbor Unreachability Detection (NUD), and redirection. Along with Router Discovery, in IPv6 there are also ND ICMPv6 messages that are responsible for network discovery - ICMPv6 Neighbor Solicitation (NS) and Neighbor Advertisement (NA). This section describes concerns related to Neighbor Discovery.

The following figure illustrates the steps involved in deploying an address resolution attack.

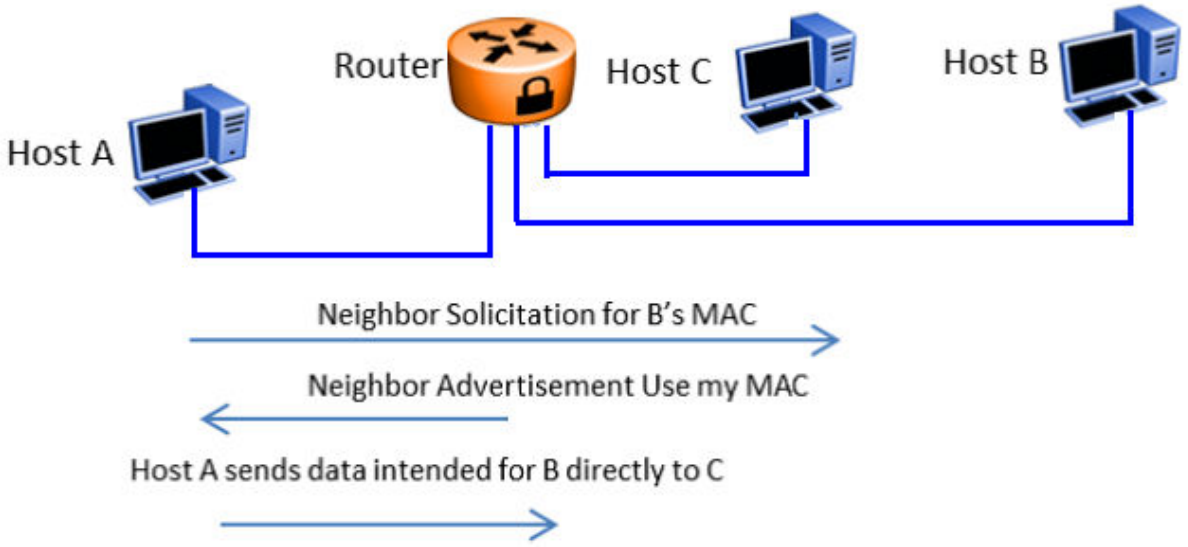


Figure 6: IPv6 Neighbor Discovery

Address resolution is the process that an endpoint (shown as Host A) follows when it wants to forward a packet to another endpoint (shown as Host B) in the local link when it does not know its Layer 2 address. Host A resolves the IP address of Host B into a MAC address and then forwards the packet by setting the Host B MAC address as the Layer 2 frame's destination MAC address.

In IPv4, ARP is responsible for address resolution and in IPv6, ICMPv6 is responsible for that service. Host A sends an ICMPv6 NS requesting the link-layer address for Host B. When Host B sends an ICMPv6 NA response, Host A knows the MAC address for sending the frame. At the same time, Host A creates a neighbor cache entry for Host B that binds the MAC for Host B to its IPv6 address (similar to the ARP table in IPv4).

If malicious Host C manages to insert itself in the link, it can impersonate Host B and intercept all packets that were originally destined for Host B. Therefore, if proper FHS protections are not employed, Host B can perform a man-in-the-middle attack or intercept traffic.

Duplicate Address Detection

Duplicate Address Detection (DAD) is an IPv6 protocol that enables an endpoint to verify the IP address uniqueness. In essence, a host sends a probe message to verify if the address is claimed

by other hosts. The following figure illustrates the steps involved in deploying a duplicate address attack.

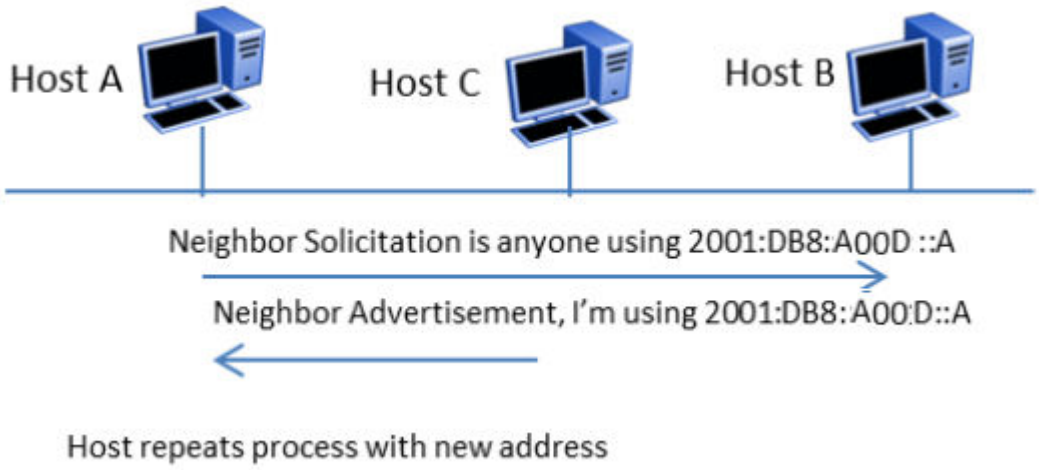


Figure 7: IPv6 Duplicate Address Detection

In IPv6, when Host A wants to perform DAD, it sends an ICMPv6 Neighbor Solicitation (NS) for the address it wants to claim (for example, 2001:DB8:A00D::A). Host A can use the address if other hosts do not respond with an ICMP Neighbor Advertisement (NA) stating the address is taken.

In this scenario, DAD can be susceptible to attacks by malicious Host C, which wants to prevent host A from receiving an IPv6 address. When Host A sends an NS for 2001:DB8:A00D::A, Host C can send an NA stating the address is taken. If Host A tries to claim another address (for example, 2001:DB8:A00D::AA), Host C can send an NS and claim it. Essentially, Host C can claim every address with which Host A performs DAD, and prevent Host A from obtaining an IPv6 address to communicate with the network.

DHCPv6

DHCPv6 (RFC 3315) describes how a host can acquire an IPv6 address and other configuration options from a server that is available on its local link. DHCPv6 is described as a stateful protocol that is compatible with the SLAAC design requirement. In other words, DHCPv6 can operate in a stateless fashion where it provides configuration information to nodes and does not perform address assignments (RFC 3736). In addition, it can operate in a stateful manner, where it assigns IPv6 addresses and configuration information to hosts that request it.

As in IPv4 DHCP, DHCPv6 is susceptible to rogue server attacks. In other words, if DHCPv6 is used to provide IPv6 addresses to the hosts, an attacker that managed to insert a rogue DHCPv6 server in the link can potentially assign addresses and configuration options to the link hosts. In turn, the attacker can deploy man-in-the-middle, traffic interception, or blackhole traffic, similar to those in the stateless address autoconfiguration scenario. Therefore, it is important to use DHCP protections for both IPv4 and IPv6.

First Hop Security

First Hop Security improves local network security by employing a number of mitigation techniques. This section describes the base set functionality which provides protection from a wide host of rogue or mis-configured users, and this can be extended with additional features for different deployment scenarios. For example, see the following topology.

Sample topology

In the following topology, Layer 2 switch SW-1 is connected to another Layer 2 switch SW-2. SW-2 is connected to three hosts and SW-1 is connected to two hosts.

In this network, if FHS is enabled only on SW-1, then it can only save the nodes which are directly connected to it. To protect the good node connected to SW-2, the FHS must be enabled on SW-2.

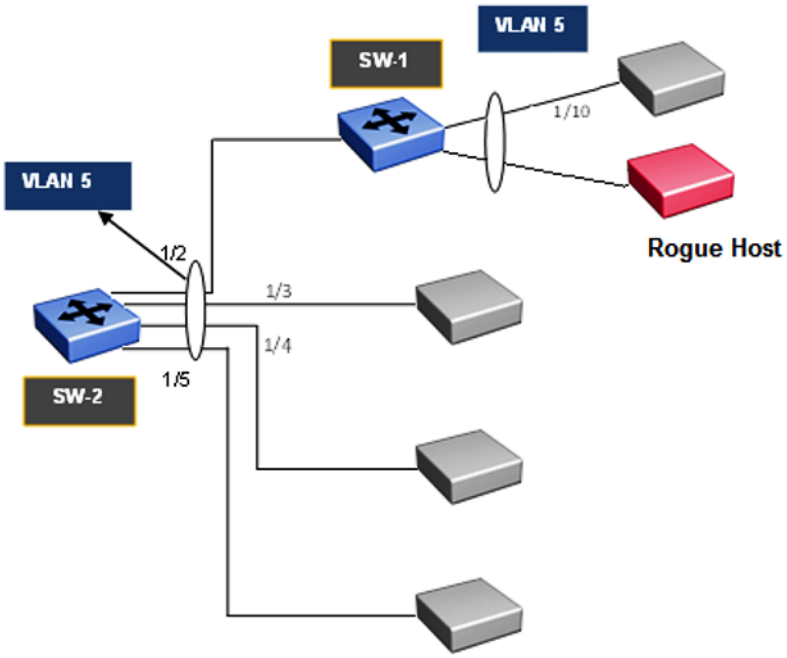


Figure 8: First Hop Security topology

First Hop Security contains the majority of the RIPE 554 mandatory requirements for Layer 2 switches. This includes the following:

- DHCPv6–guard or DHCPv6 filtering
- RA-guard or Router Advertisement filtering
- Dynamic IPv6 Neighbor solicitation or advertisement inspection
- Neighbor reachability detection inspection
- Duplicate Address Detection inspection

DHCPv6–guard

DHCPv6–guard provides Layer 2 security to DHCPv6 clients by protecting them against rogue DHCPv6 servers. DHCPv6–guard ensures that Layer 2 device filters DHCPv6 messages meant for DHCPv6 clients. The basic filtering criterion is that the Layer 2 device discards the DHCPv6 messages if they are not received on a specified Layer 2 device port.

The following are DHCPv6 topology samples:

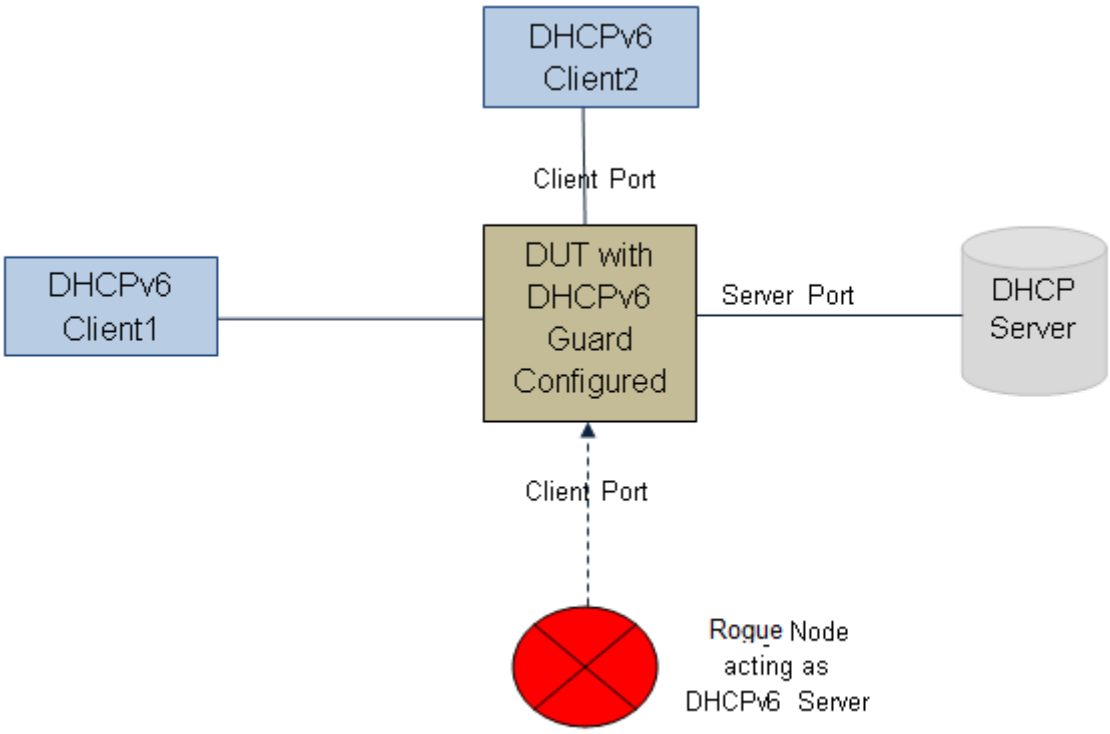


Figure 9: DHCPv6 Topology 1

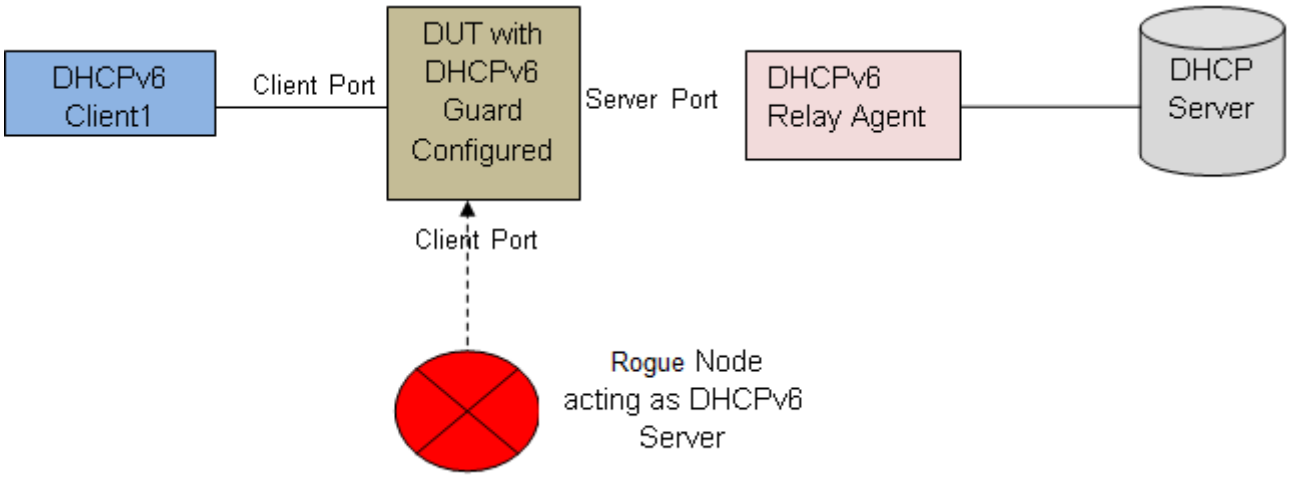


Figure 10: DHCPv6 Topology 2

DHCPv6–guard policies configuration

DHCPv6-guard policies can be configured using CLI, SNMP and EDM. The following policies are supported for DHCPv6–guard.

Port-based filtering using device-role

Port-based filtering using device-role is an interface-based configuration. Only a DHCPv6 server or relay agent can send a DHCPv6 advertisement or reply. By configuring the device-role attached to the port (whether it is a client or server), the rogue server generating DHCPv6 advertisement or reply packets can be blocked if these packets are received on a port configured as a client. The role of a device can be configured on a single port or Multi-link Trunking (MLT).

In DHCPv6 Guard Topology 1, only DHCPv6 server packets (that is, advertisement, reply) received on a port configured as a Server Port accept the packets and process them for security validation and forwarding. The Client port drops the packets if it receives packets generated from a DHCPv6 rogue server.

Server or relay agent IP address based filtering

Server or relay agent IP address-based filtering enables the verification of the advertised DHCP server and relay address in messages with the configured authorized server access list. In DHCPv6-guard Topology 1 and Topology 2, you can configure the access list to accept DHCPv6 server packets from a specific Source IPv6 address such as a DHCPv6 server or DHCPv6 relay IPv6 address. If so, in case DHCPv6 relay is used, you must configure the access-list to accept server packets from the relay agent link-local address.

Advertising IP prefix-based filtering

Advertising IP prefix-based filtering enables verification of the advertised prefixes in DHCP reply messages with the configured authorized prefix list.

Server preference-based filtering

Server preference-based filtering enables verification by checking if the advertised preference (in preference option) is greater than or less than the specified limit.

RA-guard

IPv6 hosts can configure themselves automatically when connected to a routed IPv6 network using the ND Protocol through ICMPv6 router discovery messages. When the host is connected to the network for the first time, it sends a link-local router solicitation multicast request for its configuration parameters. It the host is configured correctly, routers respond to the request with a Router Advertisement (RA) packet. The RA packet contains network-layer configuration parameters.

There is a risk of rogue RAs in a shared Layer 2 network segment when SEND support is not complete or if the infrastructure to support SEND is not available. The RA is generated maliciously by the unauthorized or improperly-configured routers connecting to the segment. RA-guard provides complementary solutions in those environments where SEND is not suitable or fully supported by all devices involved. RA-guard implementation validates RAs on behalf of hosts and potentially simplifies some of these challenges.

RA-guard can be seen as a superset of SEND with regard to router authorization. RA-guard filters RAs based on few criteria. The criteria can range from a simplistic “RA disallowed on a given interface” to “RA allowed from pre-defined sources” and up to a full-fledged SEND “RA allowed from authorized sources only”.

In addition to filtering RAs, RA-guard introduces the concept of router authorization proxy. Instead of each node on the link analyzing RAs and making an individual decision, a legitimate “node-in-the-middle” performs the analysis on behalf of all other nodes on the link.

Stateless and statefull RA-guards are available. This document discusses only the stateless RA-guard function.

Stateless RA-guard examines incoming RAs and decides whether to forward or block them based on the information found in the message or in the Layer 2 device configuration. The following is the typical information available in the received frames that are used for RA validation:

- Port on which the frame is received
- Source IP Address
- Prefix list which RA carries
- Link-Layer Address of the sender

After the Layer 2 device validates the RA frame content against the configuration, the RA is forwarded to its destination, whether unicast or multicast. If not validated, the RA is dropped at the Layer 2 device.

RA-guard policies description

This section describes the RA-guard policies. The following policies are supported for RA-guard:

- Port-based filtering using device role (host or router)
- Source IP-based filtering – IPv6 Access list
- Advertised IP prefix-based filtering – IPv6 Access list
- Source MAC address-based filtering – MAC Access list
- RA packet for managed address configuration flag validation

- RA packet for hop count limit validation
- RA packet for Router Preference validation

Port-based filtering using device-role

This is an interface based configuration. According to ND RFC 4861, only the IPv6 router can generate the RA packets. By configuring the role of the device attached to the port whether it is a host or router, the rogue host which is generating RA packets can be blocked. This can be configured on a single port or Multi-Link Trunking (MLT).

Note:

The preceding configuration is supported only on single port interfaces.

In the following topology, the Device Under Test (DUT) switch is connected to a Layer 3 router and three hosts. Because the “Router” is directly connected to the port 1/2, the device-role of the port 1/2 is configured in “Router” mode. Similarly, other three hosts are connected to port number 1/3, 1/4 and 1/5 corresponding to the device-role of ports 1/3, 1/4, and 1/5, and they are configured in “Host” Mode.

The host connected to the port 1/4 is a Rogue Host and if it is trying to send RA packets, then the DUT switch drops those RA packets received on the interface 1/4 as the device-role of this port is “Host” Mode.

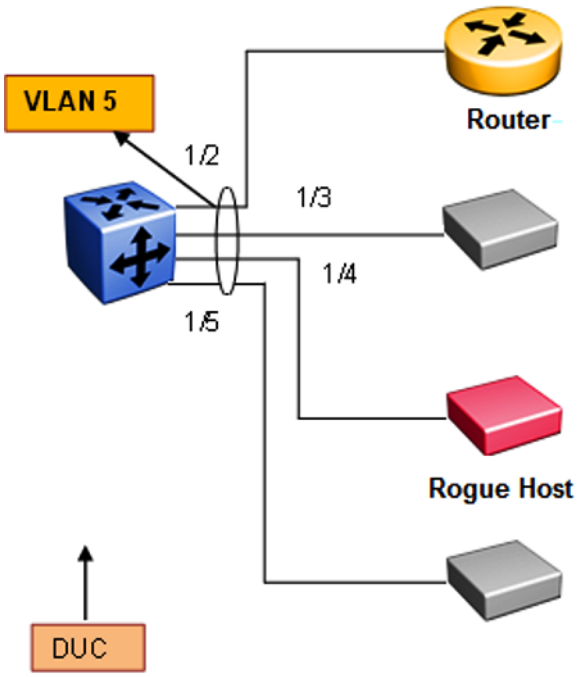


Figure 11: RA-guard Topology1

Source IP-based filtering

A Source IP-based filtering policy enables the source IP address verification of the RA packets against the configured authorized source IP or subnet list.

The following figure illustrates the IPv6 ICMP RA data packet outline. This RA-guard policy verifies the IPv6 source IP (SrcIP) in the IPv6 Header against the configured authorized Source IP or subnet list.

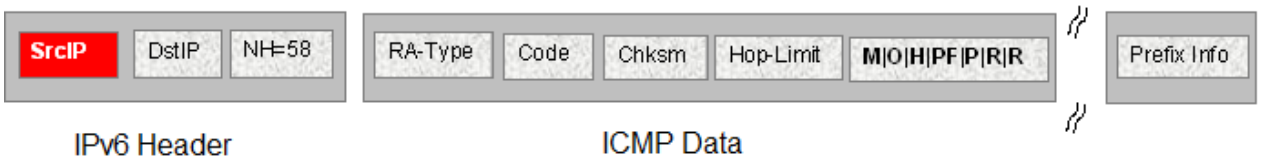


Figure 12: IPv6 ICMP RA data packet online

Advertised IP prefix-based filtering

Advertised IP prefix-based filtering enables the verification of the advertised prefixes in inspected messages against the configured authorized prefix list. This filtering policy can be applied on an interface or globally.

The following figure illustrates the IPv6 ICMP RA data packet outline. This RA-guard policy verifies the RA (Prefix Information) in ICMPv6 data against the configured authorized source IP or subnet list.

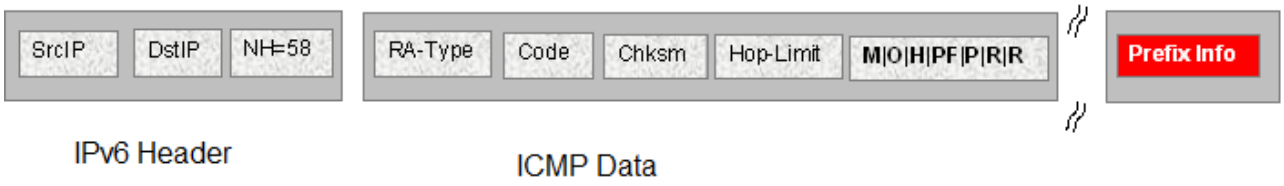


Figure 13: IPv6 ICMP RA data packet outline

Source MAC address-based filtering

Source MAC address-based filtering enables the source MAC address of the RA packets verification against the configured authorized MAC list.

The following figure illustrates the IPv6 Ethernet packet. This RA-guard policy verifies the received RA packets source MAC address against the configured authorized MAC access list.

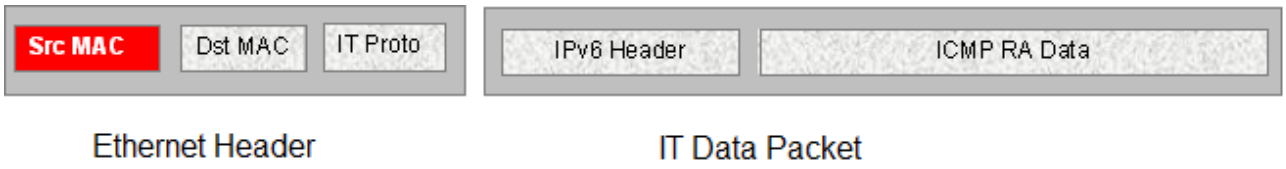


Figure 14: IPv6 Ethernet packet

RA packet for managed address configuration flag validation

In the RA packets, there is an “M” flag (managed address configuration flag) that can be configured to indicate that the address assignments are available through DHCPv6. This means that DHCPv6 takes care of the interface address assignment in that LAN segment. If a filtering policy is enabled, then all the RA packets without an “M” flag are dropped. By default, this validation is not performed.

The following figure illustrates IPv6 ICMP RA data packet outline for managed address configuration.

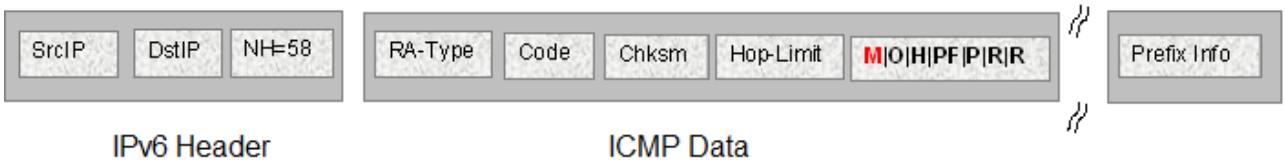


Figure 15: IPv6 ICMP RA data packet outline

RA packet for hop count limit validation

RA packet for hop count limit validation policy verifies the advertised RA message if the hop count limit is within the configured hop count limit. If the received hop count limit is not within the configured limit, then those RA packets are dropped.

The following figure illustrates IPv6 ICMP RA data packet outline for hop count limit validation.

Figure 16: IPv6 ICMP RA data packet outline

RA packet for router preference validation

The RA packet contains the Router Preference as part of the flags field. This can be high, medium, or low. This filtering policy option verifies if the advertised default router preference parameter value is lower than or equal to a specified limit.

The following figure illustrates IPv6 ICMP RA data packet outline for router preference validation.

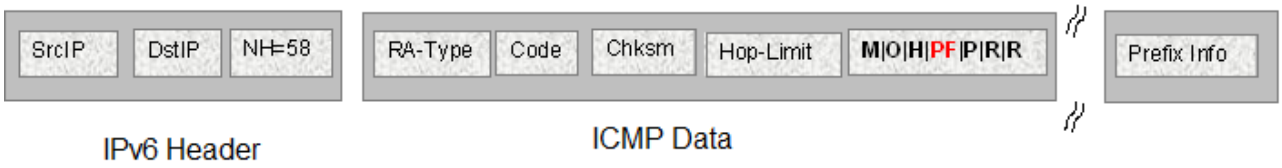


Figure 17: IPv6 ICMP RA data packet outline for router preference validation

ND-inspection

IPv6 ND inspection learns and secures bindings for stateless auto configuration addresses and DHCPv6 (stateful configuration) binding in Layer 2 neighbor tables.

FHS analyzes NDP and DHCPv6 packets to build a trusted Source Binding Table (SBT). SBT allows the FHS to know the source IPv6 address binding information like location (source IP belongs to which interface) and MAC address attached to the source IP.

This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on Duplicate Address Detection (DAD), Neighbor Unreachability Detection (NUD) and address resolution using Neighbor Solicitation (NS) or Neighbor Advertisement (NA).

Source Binding Table

Neighbor source IP address are learned on the ports where ND-inspection is enabled.

In the case of conflicting ND packets from different ports or VLANs, the SBT entry is chosen based on the priority given to the ND packets. The priorities are derived from the ND packet and how their source address is learned. The high priority values are the most preferred ND entries. The following is the priority list based on their hex values:

1. NA from trusted port (non ND-inspection enabled port) – (hex – 00000020)
2. SBT entry learns this entry as a DHCP leant interface IP – (hex – 00000010)
3. SBT entry learns this entry by tracking from DAD – (hex – 00000008)
4. ICMPv6 optional Source-link-layer is same as source Ethernet MAC address – (hex – 00000002)
5. Packet from access port – (hex – 00000001)

Note:

Static SBT entries are preferred over any dynamically-learned SBT.

SBT Entry Values:

The following are the different SBT entry states:

INCOMPLETE–This is the state where the neighbor IP address is in the process of validation. In this state, except for the RA packet, other ND packets are dropped. The validation is done by sending DAD message to all the ports in the VLAN and the best ND packet is selected depending on the priority (hex value). If ND is found in the DHCP tracking table, entry is transitioned immediately to REACHABLE without further validation.

REACHABLE–This is the state where the neighbor IP address is already validated. In this state, all ND packets matching the SBT entry are forwarded and rest of the packets undergo validation. A reachable timer runs for each entry. This timer is refreshed when the FHS-enabled switch receives any ND packets matching SBT entry. If the reachable timer expires, it moves to a STALE state. But static SBT entry is always in a REACHABLE state.

STALE–This is the state transition from REACHABLE after the reachable timer expires. In this state, any ND packet matching the SBT entry change its state to REACHABLE and the rest of the packets are validated. A stale timer runs for each entry. After the timer expires, the corresponding SBT entry is deleted from the SBT.

DOWN–This is the state of the SBT entry when the corresponding interface goes down. In this state, any ND packet matching the IP address in the SBT entry updates the SBT entry and moves the state to REACHABLE, and forwards the packet.

Note:

If the system receives a packet without LL option, the packet is dropped and moves to an INCOMPLETE state, then sends a DAD message towards the source port to get the LL option information. If the response is not received within seven seconds, this entry is deleted.

There is a down timer for each down entry. After this timer expires, the corresponding SBT entry is deleted from the SBT.

In all the previous states, if the switch receives an ND packet without source-link-layer option and if the existing SBT entry priority is 0, then the switch sends a DAD packet towards the source to learn the source-link-layer address. If the node does not respond to the DAD message, then those ND messages are ignored.

Duplicate Address Detection

Duplicate Address Detection (DAD) is a mechanism used to detect duplicate IP address in the same VLAN domain. This is achieved by sending a simple NS message with source IP address of “0::0” (Unspecified IP address) and the NS target IP address as its own new IP address. If any other network device is assigned the same source IP address, then that device sends a NA message in response to the DAD-NS message. If the node does not receive any response from other devices before the DAD timeout, the IP address is assigned.

What is the security threat

There can be a rogue network device attached to the same VLAN domain which can fabricate the fake NA response for the DAD-NS request and prevent other nodes from assigning its IP address.

How to guard the DAD mechanism

If the Layer 2 device connected to the Host or Router in a star topology builds a Source Binding Table (SBT) by learning the source IP address attached to the particular port or VLAN, then it can validate the received NA packets. If NA packet is valid, then DAD mechanism can be protected.

Neighbor Unreachability Detection

Neighbor Unreachability Detection (NUD) is a mechanism used to detect neighbor reachability in the same VLAN domain. This mechanism is used to detect the reachability of the default gateway and is triggered by the upper layer to determine the node reachability. The NUD node sends a targeted NS message to the specific node (using unicast destination IP address). If the node does not receive an NA message in response to NUD-NS message within the NUD timeout, the node declares the other node is not reachable.

What is the security threat

There can be a rogue network device attached to the same VLAN domain that can fabricate a fake NA response for the NUD-NS request and pretend that the node is reachable even though the actual node is not reachable.

In this case, if the default gateway is not reachable, then the rogue network device can fake that default gateway is still reachable; therefore, the host does not choose the other default gateway and all the traffic goes to a black hole.

How to guard the NUD mechanism

If the Layer 2 device connected to the Host or Router in a star topology builds a source binding table by learning the source IP address attached to the particular port or VLAN, then it can validate the received NA packets. If NA packet is valid, then NUD mechanism can be protected.

Neighbor Address Discovery

Neighbor Address Discovery is a mechanism to learn the neighbor's link layer address for the given IPv6 address. This is equivalent to the Address Resolution Protocol (ARP) mechanism in IPv4. NS is equivalent to ARP-Request in IPv4, and similarly NA is equivalent to ARP-Reply in IPv4.

What is an NS/NA security threat

There can be a rogue network device attached to the same VLAN domain which can fabricate the fake NA response for the NS request and provide the wrong link layer address. If the fake NA is the latest NA for the received NS message, the most recent NA is used in the Neighbor cache (IPv6 address against MAC entries). This can block the traffic from flowing through the right path causing traffic disruption.

How to guard NS/NA mechanism

If the Layer 2 device connected to the host or router in a star topology builds a source binding table by learning the source IP address attached to the particular port or VLAN, then it can validate the received NA packets. If the NA packet is valid, the NS/NA mechanism of learning the IPv6 address against the link layer address can be protected.

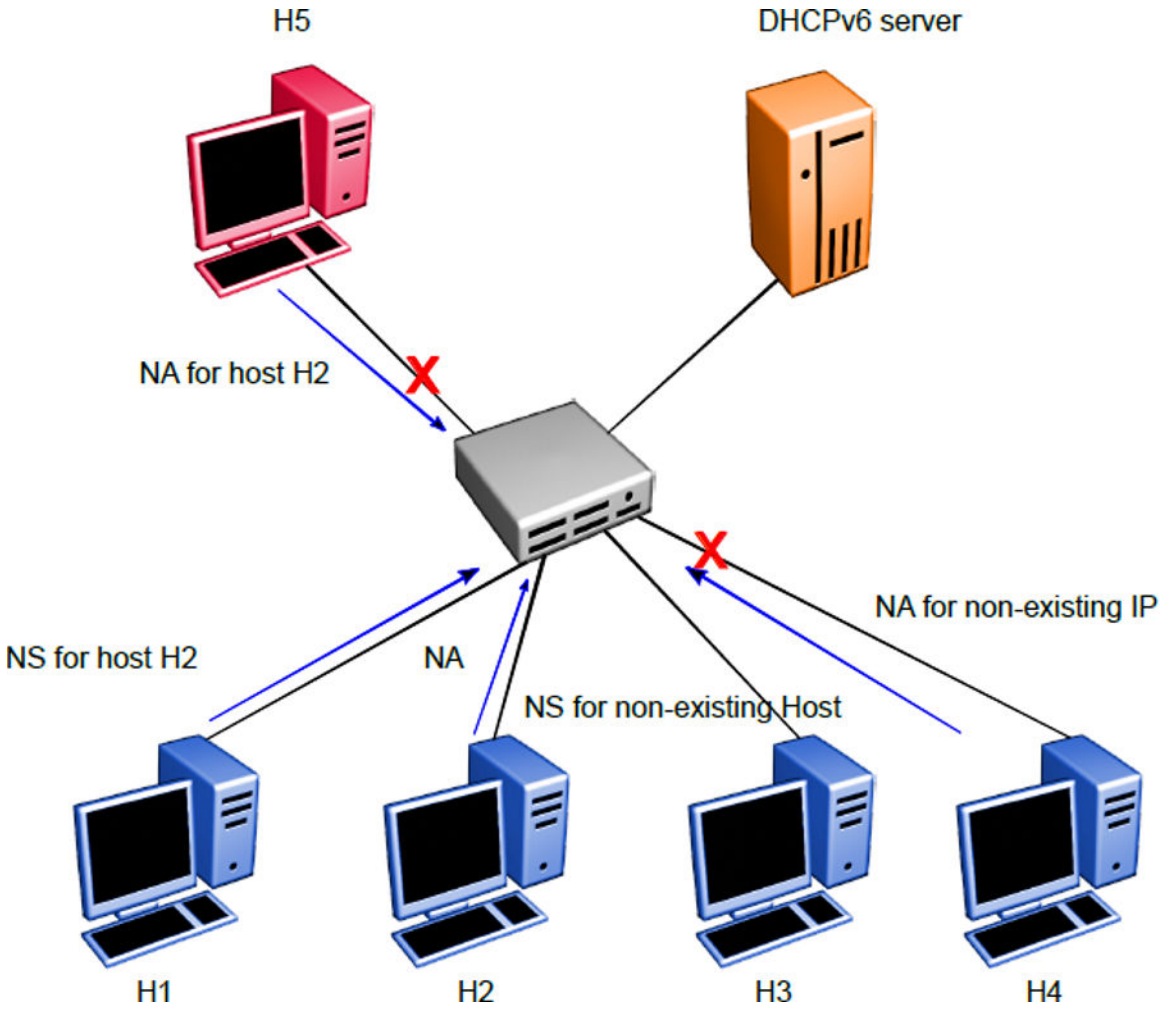


Figure 18: DAD/NUD/NS/NA attack prevention using ND-inspection

Table 17: Security Binding Table

IP-H1	MAC-H1	INTF-H1
IP-H2	MAC-H2	INTF-H2
IP-H3	MAC-H3	INTF-H3
IP-H4	MAC-H4	INTF-H4
IP-H5	MAC-H5	INTF-H5

On enabling ND-inspection on the ports, the First Hop Security module begins learning the neighbor source IP address on the configured port using the DAD mechanism and builds a Security Binding Table (SBT).

If the First Hop Security switch receives any ND message and if source IP address entry is not present in the SBT, then the FHS module begins the process of learning the source or target IP address using the DAD mechanism and drops the ND messages until the verification is successful.

Counters for monitoring the violation and send SNMP TRAP for the violation are maintained.

In the preceding example, in the H5 case, the H2 IP address is already learned in the SBT and the source IP address port points to the port which is connected to the host H2. The NA incoming port is an incorrect port and therefore, NA packet with the forged address is dropped (NS/NA or NUD attack)

In the H4 case, the NA target IP address is not present in the SBT. Therefore, the NA packet is dropped and the FHS module begins the process of learning the IP address. After the learning process, the IP address is not detected and this entry is not added to the SBT table (DAD or NUD attack)

First Hop Security feature consists the following functional blocks:

- Configuring First Hop Security specific policies
- Capturing and verifying First Hop Security specific packets against the configured policies

Capturing and verifying FHS specific packets against the configured policies

First Hop Security filters can be installed only if the global FHS is enabled. The DHCPv6-guard or RA-guard filters are created as a part of First Hop Security filter with port bit mask “0”.

The following is a high-level procedure to capture DHCPv6 or ND packets received on a physical port:

1. Enable FHS globally.
2. Enable DHCPv6-guard or RA-guard or ND-inspection globally.
3. Create DHCPv6-guard or RA-guard policy.
4. Attach DHCPv6-guard and/or RA-guard policy and/or ND-inspection to a physical port.

By attaching the DHCPv6-guard or RA-guard policy on a port, the DHCPv6-guard or RA-guard port bit mask filter for that particular physical port is set. Similarly, detaching the DHCPv6-guard or RA-

guard policy from a physical port resets the DHCPv6-guard or RA-guard port bit mask filter for that particular physical port.

After DHCPv6-guard or RA-guard policies are configured on the physical port, the DHCPv6 or ND packets are captured on the local CPU. The DHCPv6-guard or RA-guard policy denied packets are dropped and rest of the DHCPv6 or RA packets are forwarded to the corresponding outgoing ports. In the case of ND-inspection, denied packets are dropped and SNMP trap is sent.

Limitations

The following limitations exist in the First Hop Security:

- If this feature is enabled, the IP packet destined for the IPv6 link-local (fe80::0/10) or all-node multicast (ff02::0/16) address with the following extension header options are dropped:
  - Routing
  - Destination
  - Hop-by-Hop (except for MLD packets)
  - Mobility
  - Fragmentation extension option with other preceding extension options
- A Fragmented DHCPv6 or RA packet is dropped.
- All ND packets are software forwarded on the FHS enabled interfaces.
- DHCPv6-guard, RA-guard, or ND-inspection does not work on devices connected on the shared media or on the tunneled interfaces.
- DHCPv6-guard or RA-guard policies are not VLAN based.
- In the case of trunk ports, the statistics are incremental on the lowest active port in the trunk.
- Rate limiting cannot be applied.
- Dynamic learning is not supported for ND packets with IPv6 any-cast address. A static SBT configuration is required
- In the case of ND-inspection, DAD or DHCP track learning is based on the interface readiness and the time interval in which the host sends the DAD message to the new interface.
- FHS statistics is not updated during Temporary Base Unit (TBU) takeover,

IPv6 Source Guard

IPv6 Source Guard is an extension to the IPv6 FHS feature which works in conjunction with ND Inspection and DHCPv6 Guard to ensure the forwarded traffic is from valid hosts on the network. IPv6 Source Guard is a Layer 2 port-to-port basis feature that works similar to IPv4 Source Guard.

IPv6 Source Guard can only be enabled on ports if FHS and ND Inspection are enabled. The ports with ND inspection enabled are referred to as **untrusted** ports and the ports with ND inspection not

enabled are called **trusted** ports. All traffic sourced on a trusted port is forwarded by the switch and these ports are considered secure. Traffic sourced on the untrusted ports is subject to action by IPv6 Source Guard. When IPv6 Source Guard is enabled on a port, the switch links packets from devices with the addresses learned in the SBT. The binding table includes the MAC address to IPv6 address of nodes on the local LAN/VLAN that are validated through ND and DHCPv6 Guard. IPv6 Source Guard does not validate the hosts, but utilizes the binding table to block or drop traffic coming from mismatched source IPv6 addresses. If the source IPv6 address is not in the source binding table, then it is invalidated. IPv6 addresses arriving on the untrusted port are dropped, but are allowed to transmit NS/NA, RS/RA and DHCP packets in order to validate themselves. Data from a validated IP address is forwarded across the switch as normal.

The IPv6 Source Guard has a per-port filter which allows data from the validated IPv6 host. By default, the traffic is denied from all hosts when IPv6 source guard is enabled on an untrusted port. A fixed number of filters are installed to allow a fixed number of validated hosts and an additional filter is installed to drop all the unmatched traffic. When the IPv6 addresses are removed from the SBT, Source Guard removes the corresponding configuration from the filter to block the address again.

Note:

Operation fails and an error is displayed when you try to enable Source Guard on a port when sufficient filters are not available.

Limitations

The following limitations exists in IPv6 Source Guard:

1. The data filtering in IPv6 Source Guard is based only on IPv6 address match and not on VLAN ID and Source-MAC-Address match.
2. When the per-port limit of the maximum allowed IPv6 source addresses (default-value 5) is reached, the data from all other addresses (even if they are in the SBT) are dropped. A per-port overflow counter is incremented each time an address added to the SBT cannot be configured by IPv6 Source Guard.
3. IPv6 Source Guard is enabled on a port only if resources are available to allow **<max-allowed-addr>** IPv6 source addresses.
4. In case of trunk ports, IPv6 Source Guard needs to be separately enabled on each port, so resources are allocated to allow **<max-allowed-addr>** IPv6 source addresses on each port of the trunk.
5. The maximum number of allowed IPv6 addresses are limited by the maximum SBT entries which is configurable between the valid range of 1 to 1024.

Upgrade Requirements

When you upgrade from 7.0, IPv6 Source Guard is not automatically enabled if ND Inspection was enabled in the 7.0 configuration.

IPv6 FHS configuration using CLI

This section describes how to configure IPv6 First Hop Security (FHS) and how to protect the network by mitigating the various types of attacks, such as address spoofing, remote address resolution cache exhaustion (denial of service attacks) using CLI.

Note:

FHS does not solve all cases of denial of services like blocking flooding of the IPv6 messages.

FHS configuration

Configure IPv6 FHS features to enable IPv6 link security and management over the Layer 2 links.

Enabling or disabling FHS globally

About this task

You must enable First Hop Security for FHS RA-guard or DHCPv6–guard to be operational.

Enabling FHS globally installs the required filters for FHS. Disabling FHS, uninstalls FHS. By default, FHS is disabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable IPv6.

   ```
   ipv6 enable
   ```

3. Enable First Hop Security globally.

   ```
   ipv6 fhs enable
   ```

4. Disable First Hop Security globally.

   ```
   no ipv6 fhs enable
   ```

   OR

   ```
   default ipv6 fhs enable
   ```

Managing the FHS IP access list

About this task

You can create an FHS IP access list or add IP prefixes to an existing IP access list.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. Create an FHS IP access list or add IP prefixes to an existing IP access list.

   ```
   ipv6 fhs ipv6-access-list <ip-access-list-name> <ip-prefix>/<ip-mask-length> [ge <ip-mask-length>] [le <ip-mask-length>] [mode <allow | deny>]
   ```

3. Delete an FHS IP access list or delete a particular ip-prefix from the IP access list.

   ```
   no ipv6 fhs ipv6-access-list <ip-access-list-name> [<ip-prefix>/<ip-mask-length>]
   ```

   OR

   ```
   default ipv6 fhs ipv6-access-list <ip-access-list-name> [<ip-prefix>/<ip-mask-length>]
   ```

Example

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ipv6 fhs ipv6-access-list ACCName fe80::221:2fff:fe31:5376/24
Switch(config)#
```

Variable definitions

Use the data in the following table to use the **`ipv6 fhs ipv6-access-list`** command.

Variable	Description
<ip-access-list-name>	Specifies the IP access list name.
<ip-prefix>/<ip-mask-length>>	Specifies the IP prefix and IP mask length to be added to the IP access list.
ge *<ip-prefix>/<ip-mask-length>>*	Specifies the IP range start mask length. By default, the value is 0.
le *<ip-prefix>/<ip-mask-length>>*	Specifies the IP range end mask length. By default, the value is 0.
mode <*allow* | *deny*>	Specifies the access mode. By default, the value is allow.

Displaying FHS IPv6 access list information

About this task

Displays the current FHS IPv6 access list information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display the current FHS IPv6 access list information.

```
show ipv6 fhs ipv6-access-list [<access-list-name>]
```

Example

```
Switch#show ipv6 fhs ipv6-access-list


     Access list name : AccName
ip_prefix         : fe80::221:2fff:fe31:5376
mask_len          : 24
mask_range_from   : 0
mask_range_to     : 0
mode              : Allow
Switch#
```

Job aid

The following table shows the field descriptions for the **`show ipv6 fhs ipv6-access-list`** command.

Field	Description
Access list name	Indicates the IP access list name.
ip_prefix	Indicates the IP prefix added to the IP access list.
mask_len	Indicates prefix mask length added to the IP access list.
mask_range_from	Indicates the IP range start mask length.
mask_range_to	Indicates the IP range end mask length.
mode	Indicates the access mode.

Managing the FHS MAC access list

About this task

You can create an FHS MAC access list or add MAC addresses to an existing MAC access list.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create an FHS MAC access list or add MAC addresses to an existing MAC access list.

   ```
   ipv6 fhs mac-access-list <mac-access-list-name> <MAC-address> [mode
   <allow | deny>]
   ```

3. Delete an FHS MAC access list or delete a particular MAC address from the MAC access list.

   ```
   no ipv6 fhs mac-access-list <mac-access-list-name> [<MAC-address>]
   ```

   OR

   ```
   default ipv6 fhs mac-access-list <mac-access-list-name> [<MAC-
   address>]
   ```

Variable definitions

Use the data in the following table to use the **ipv6 fhs mac-access-list** command.

Variable	Description
<mac-access-list-name>	Specifies the MAC access list name.
<MAC-Address>	Specifies the MAC address to be added or deleted.
mode *<allow | deny>*	Specifies the access mode. By default, the value is Allow

Displaying FHS MAC access list information

About this task

Displays the current FHS MAC access list information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display the current FHS MAC access list information.

   ```
   show ipv6 fhs mac-access-list [<mac-list-name>]
   ```

Example

```
Switch#show ipv6 fhs mac-access-list


     Access list name : MACList
S.No   MAC-Address         ACL-Mode
1      10:20:30:40:50:60   Allow
Switch#
```

Job aid

The following table shows the field descriptions for the **show ipv6 fhs mac-access-list** command.

Field	Description
Access list name	Indicates the FHS access list name.
MAC-Address	Indicates the MAC address.
ACL-Mode	Indicates the ACL mode.

Displaying current FHS configuration

About this task

Displays the current FHS configuration.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the current FHS configuration.

```
show ipv6 fhs capture-policy [interface <port_list>]
```

Example

```
Switch#show ipv6 fhs capture-policy
-------------------------------------------------------------------------
port  Protocol     Policy Name              PktsRcv PktsDrop DynLearn
-------------------------------------------------------------------------
 1      DHCP         dhcpg                    0        0        -
        NDI          None                     9        1       TRUE
 2      NDI          None                     0        0       TRUE
```

Job aid

The following table shows the field descriptions for the **`show ipv6 fhs capture-policy`** command.

Field	Description
port	Indicates the port number.
Protocol	Indicates the protocol.
Policy Name	Indicates the policy name.
PktsRcv PktsDrop	Indicates the received and dropped packets.
DynLearn	Indicates the dynamically learnt neighbor source IP address. If there is a rogue, you can add a static entry to the SBT for legitimate reachability and disable dynamic learning. The rogue ND packets arriving at this port are dropped allowing only the ND packets matching the statically configured SBT entry.

Displaying FHS status

About this task

Displays the current FHS status.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the current FHS configuration.

```
show ipv6 fhs status
```

Example

```
Switch>show ipv6 fhs status
IPv6 FHS                          : Disabled
IPv6 Dhcpv6-guard                 : Disabled
IPv6 RA-guard                     : Disabled
IPv6 ND inspection                : Disabled
```

```
IPv6 ND reach lifetime            : 300 sec
IPv6 ND stale lifetime            : 86400 sec
IPv6 ND down lifetime             : 86400 sec
SBT table maximum dynamic entries : 512
SBT table overflow counter        : 0
```

DHCPv6–guard policy configuration

DHCP-DHCPv6–guard policy blocks DHCP reply and advertisement messages that originate from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients.

Enabling or disabling DHCPv6–guard globally

About this task

Enabling DHCPv6–guard globally installs filters on the configured interfaces. By default, the filters are disabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable IPv6.

   ```
   ipv6 enable
   ```

3. Enable FHS globally.

   ```
   ipv6 fhs enable
   ```

4. Enable DHCPv6–guard globally.

   ```
   ipv6 dhcp guard enable
   ```

5. Disable DHCPv6–guard globally.

   ```
   no ipv6 dhcp guard enable
   ```

Managing the DHCP Guard policy

About this task

Configure or modify the DHCP-guard policy.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create a DHCP guard policy.

```
ipv6 dhcp guard policy <policy_name>
```

3. Delete a DHCP guard policy.

```
no ipv6 dhcp guard policy <policy_name>
```

OR

```
default ipv6 dhcp guard policy <policy_name>
```

Note:

You cannot delete a policy that is already attached to an interface.

Variable definitions

Use the data in the following table to use the **ipv6 dhcp guard policy** command.

Variable	Description
<policy_name>	Specifies the created or deleted DHCP guard policy name.

Clearing the DHCP Guard statistics

About this task

Clears the DHCP guard statistics.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Clear the DHCP guard statistics.

```
ipv6 dhcp guard clear stats [<port_list>]
```

Variable definitions

Use the data in the following table to use the **ipv6 dhcp guard clear stats** command.

Variable	Description
<port_list>	Specifies the list of ports. If the ports are not specified, the DHCP guard statistics are cleared for all ports.

Managing a DHCP Guard policy on an interface

About this task

Applies a DHCP-guard policy to a specific interface.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. Apply a DHCP guard policy.

```
ipv6 dhcp guard attach-policy <policy_name>
```

3. Detach a DHCP guard policy from an interface.

```
no ipv6 dhcp guard attach-policy <policy_name>
```

OR

```
default ipv6 dhcp guard attach-policy <policy_name>
```

Variable definitions

Use the data in the following table to use the **ipv6 dhcp guard attach-policy** command.

Variable	Description
<policy_name>	Specify the name of the DHCP guard policy to be attached or detached.

Configuring DHCP Guard in dhcp-guard mode

About this task

Configures DHCP guard under dhcp-guard mode.

Procedure

1. Enter DHCP Guard Configuration mode.

```
enable
configure terminal
ipv6 dhcp guard policy <policy-name>
```

2. Enable verification of the role of the device attached to the port.

```
device-role { client | server }
```

3. Specify IPv6 access list to verify IPv6 addresses.

```
match server access-list <ipv6-access-list-name>
```

4. Remove DHCP guard filtering for the sender's IPv6 addresses.

```
no match server access-list <ipv6-access-list-name>
```

OR

```
default match server access-list <ipv6-access-list-name>
```

5. Specify IPv6 prefix list to verify advertised prefixes.

```
match reply prefix-list <ipv6-prefix-list-name>
```

6. Remove DHCP guard filtering for advertised prefixes.

   `no match reply prefix-list <ipv6-prefix-list-name>`

   OR

   `default match reply prefix-list <ipv6-prefix-list-name>`

7. Specify the minimum limit for verification of the advertised preference.

   `preference min limit <0-255>`

8. Set the minimum limit for verification of the advertised preference to its default value.

   `default preference min limit`

9. Specify the maximum limit for verification of the advertised preference.

   `preference max limit <0-255>`

10. Set the maximum limit for verification of the advertised preference to its default value.

    `default preference max limit`

Variable definitions

Use the data in the following table to use the **`dhcp-guard`** configuration mode commands.

Variable	Description
match server access-list *<ipv6–access-list-name>*	Enables verification of the sender's IPv6 address in inspected messages from the configured authorized device source access list specified. **Note:** If the access-list is not attached, the inspection does not occur. If the list is attached and it does not match any IP prefixes in the list, the switch drops the DHCPv6 packet. If you wish to change this behavior, add a dummy ip-prefix "0.0.0.0/0" with the Allow option, which changes the default drop to default Allow.
{ no | default } match server access-list *<ipv6–access-list-name>*	Removes the sender's IPv6 address based DHCPv6–guard filtering.
match reply prefix-list *<ipv6–prefix-list-name>*	Enables verification of the advertised prefixes in DHCP reply messages from the configured authorized prefix list. If prefix-list is not configured, this check is bypassed. An empty prefix list is treated as a permit. **Note:** If the access-list is not attached, the inspection does not occur. If the list is attached and it does not match any IP prefixes in the list, the switch drops the DHCPv6 packet. If you wish to change this behavior, add a dummy ip-prefix "0.0.0.0/0" with the Allow option, which changes the default drop to default Allow.

Table continues…

Variable	Description
{ no | default } match reply prefix-list *<ipv6–prefix-list-name>*	Removes the advertised prefix-based DHCP-guard filtering.
preference min limit*<0–255>*	Enables verification if the advertised preference (in preference option) is greater than the specified limit. If preference is not specified, this check is bypassed. While changing the preference limit, ensure the maximum limit is greater than the minimum limit.
default preference min limit	Sets the specified limit to its default value. By default, the value is 0.
preference max limit*<0–255>*	Enables verification if the advertised preference (in preference option) is less than the specified limit. If preference is not specified, this check is bypassed. **Note:** The preference check is ignored if the minimum and maximum values are zero.
default preference max limit	Sets the specified limit to its default value. By default, the value is 0.

Displaying DHCPv6–guard policy

About this task

Displays DHCP-guard policy information for all the configured DHCP-guard policies or a particular policy name.

Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display DHCP-guard policy information.

   ```
   show ipv6 dhcp guard policy <policy-name>
   ```

Example

```
Switch#show ipv6 dhcp guard policy dhcpg
DHCP guard policy name :dhcpg
Device role : Client
Server ip ACL Policy : None
Reply ip prefix ACL Policy : None
Router preference minimum limit : 0
Router preference maximum limit : 0
```

Variable definitions

Use the data in the following table to use the `show ipv6 dhcp guard policy` command.

Variable	Description
<policy-name>	Displays DHCP-guard policy information for all the configured DHCP-guard policies. Policy name is an optional parameter. If policy name is provided, only the DHCP-guard policy of the specified policy-name is displayed.

Job aid

The following table shows the field descriptions for the **`show ipv6 dhcp guard policy`** command.

Field	Description
DHCP guard policy name	Indicates the DHCPv6-guard policy name.
Device role	Indicates if the device role is client or server.
Server ip ACL Policy	Indicates if the received DHCP-server packet source IP matches the configured IP ACL.
Reply ip prefix ACL Policy	Indicates if the received DHCP-server prefix in the packet matches the configured IP ACL.
Router preference minimum limit	Indicates the advertised router preference minimum limit.
Router preference maximum limit	Indicates the advertised router preference maximum limit.

RA-guard configuration

IPv6 RA-guard provides support to the administrator to block or reject unwanted RA-guard messages that arrive at the network switch platform. The routers use Router Advertisements (RAs) to announce themselves on the link. The RA-guard feature analyzes these RAs and filters out bogus RAs sent by unauthorized routers. The RA-guard feature compares configuration information on the Layer 2 device with the information found in the received RA frame. After the Layer 2 device validates the content of the RA frame and router redirect frame against the configuration, it forwards the RA to its destination. If the RA frame content is not validated, the RA is dropped.

Enabling or disabling RA–guard globally

About this task

Enables the RA-guard globally. By default, RA-guard is disabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable IPv6.

   ```
   ipv6 enable
   ```

3. Enable FHS globally.

   ```
   ipv6 fhs enable
   ```

4. Enable RA-guard globally.

   ```
   ipv6 nd raguard enable
   ```

5. Disable RA–guard globally.

   ```
   no ipv6 nd raguard enable
   ```

Managing the RA-guard policy

About this task

Configure or modify RA-guard policy. This command also enables the RA-guard configuration mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create the RA-guard policy.

   ```
   ipv6 nd raguard policy <policy-name>
   ```

3. Delete the RA-guard policy.

   ```
   no ipv6 nd raguard policy <policy-name>
   ```

   OR

   ```
   default ipv6 nd raguard policy <policy-name>
   ```

   Note:

   You cannot delete a policy that is attached to an interface.

Variable definitions

Use the data in the following table to use the **`ipv6 nd raguard policy`** command.

Variable	Description
<policy_name>	Specifies the name of the RA-guard policy to be created or deleted. This is a mandatory parameter in this command.

Clearing RA-guard statistics

About this task

Clears the RA-guard statistics.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Clear the DHCP guard statistics.

   ```
   ipv6 nd raguard clear stats [<port-number>]
   ```

Variable definitions

Use the data in the following table to use the **`ipv6 nd raguard clear stats`** command.

Variable	Description
<port_list>	Specifies the list of ports. If you do not specify any port, the DHCP guard statistics are cleared for all ports.

Managing RA-guard on an interface

About this task

Applies or detaches a RA-guard policy on the specific interface.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. Apply a RA-guard policy.

   ```
   ipv6 nd raguard attach-policy <policy-name>
   ```

3. Detach a RA-guard policy from an interface.

   ```
   no ipv6 nd raguard attach-policy <policy-name>
   ```

   OR

   ```
   default ipv6 nd raguard attach-policy <policy-name>
   ```

Variable definitions

Use the data in the following table to use the **`ipv6 nd raguard attach-policy`** command.

Variable	Description
<*policy_name*>	Specifies the name of the RA-guard policy to be attached or detached.

Configuring RA-guard in raguard mode

About this task

Configures RA-guard under the raguard mode.

Procedure

1. Enter RA-guard Configuration mode.

   ```
   enable
   configure terminal
   ipv6 nd raguard policy <policy-name>
   ```

2. Enable device role verification attached to the port. By default, router is selected.

   ```
   device-role {router | host}
   ```

3. Specify the IPv6 access list to verify IPv6 addresses.

   ```
   match ipv6 access-list <ipv6-access-list-name>
   ```

4. Remove RA-guard filtering for the sender's IPv6 addresses.

   ```
   no match ipv6 access-list <ipv6-access-list-name>
   ```

   OR

   ```
   default match ipv6 access-list <ipv6-access-list-name>
   ```

5. Specify the IPv6 prefix list to verify advertised prefixes.

   ```
   match ra prefix-list <ipv6-access-list-name>
   ```

6. Remove RA-guard filtering for the advertised prefixes.

   ```
   no match ra prefix-list <ipv6-access-list-name>
   ```

   OR

   ```
   default match ra prefix-list <ipv6-access-list-name>
   ```

7. Enable verification of the sender MAC address against the configured mac-access-list.

   ```
   match mac-access-list <mac-access-list-name>
   ```

8. Remove the source MAC address-based RA-guard filtering.

   ```
   no match mac-access-list <mac-access-list-name>
   ```

   OR

   ```
   default match mac-access-list <mac-access-list-name>
   ```

9. Enable managed address configuration flag verification in the advertised RA packet.

```
managed-config-flag <none |on | off>
```

10. Enable advertised hop count limit verification.

```
hop-limit {maximum | minimum} <0-255>
```

11. Enable the advertised default router-preference parameter value verification.

```
router-preference maximum {none | high | low | medium}
```

Variable definitions

Use the data in the following table to use the **raguard** configuration mode commands.

Variable	Description
match ipv6 access-list <*ipv6-access-list-name*>	Verifies sender's IPv6 address in the inspected messages against the configured authorized device source access list. **Note:** Inspection is not done if the access-list is not attached. If the list is attached and if it does not match any ip-prefix in the list, then the RA packet is dropped. To change this behavior, add a dummy ip-prefix "0::0/0" with the Allow option. The default value changes from Drop to Allow.
{no | default} match ipv6 access-list <*ipv6-access-list-name*>	Removes the sender's IPv6 address-based RA-guard filtering.
match ra prefix-list <*ipv6-access-list-name*>	Verifies the advertised prefixes in the inspected messages against the configured authorized prefix list. **Note:** Inspection is not done if the access-list is not attached. If the list is attached and if it does not match any ip-prefix in the list, then the RA packet is dropped. To change this behavior, add a dummy ip-prefix "0::0/0" with Allow option. The default value changes from Drop to Allow.
{no | default} match ra prefix-list <*ipv6-access-list-name*>	Removes the advertised prefix-based RA-guard filtering
match mac-access-list <*mac-access-list-name*>	Verifies sender's source MAC address against the configured mac-access-list. **Note:** Inspection is not done if the access-list is not attached.

Table continues…

Variable	Description
	If the list is attached and if it does not match any MAC in the list, then the RA packet is dropped. To change the behavior, add a dummy MAC “0:0:0:0:0:0” to the list with Allow option. The default value changes from Drop to Allow.
{no | default} match mac-access-list <*mac-access-list-name*>	Removes the source MAC address-based RA-guard filtering for the specified MAC address access list names.
managed-config-flag <*none* | *on* | *off*>	Verifies managed address configuration flag in the advertised RA packet. By default, the value is none and check is bypassed.
hop-limit {maximum | minimum} <*0–255*>	Verifies the advertised hop count limit. The limit value range is from 0 to 255. While changing the minimum or maximum value, ensure the maximum value is greater than the minimum value. By default, the minimum and maximum limit are 0. In this case, the hop-limit check is bypassed.
router-preference maximum {none | high | low | medium}	Verifies if the advertised default router-preference parameter value is lower than or equal to a specified limit. By default, the value is none and the check is bypassed.

Displaying RA-guard configuration

About this task

Displays configured RA-guard policy information.

Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display configured RA-guard policy information.

   ```
   show ipv6 nd raguard policy <policy-name>
   ```

Example

```
Switch(config)#show ipv6 nd raguard policy
Ra guard policy name :rag
Device role : Router
Source ip ACL policy : None
Ip prefix ACL policy : None
Source MAC ACL policy : None
Managed config : None
Router preference : None
Minimum hop limit : 0
Maximum hop limit : 0
```

Variable definitions

Use the data in the following table to use the **`show ipv6 nd raguard policy`** command.

Variable	Description
<policy-name>	Displays the RA-guard policy for the specified policy-name. By default, all the configured RA-guard policies are displayed.

ND-inspection configuration

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes neighbor discovery messages in order to build a trusted Source Binding Table (SBT) database; IPv6 neighbor discovery messages that do not conform are dropped.

The SBT learns the neighbor source address connected to the FHS switch dynamically or statically. These neighbors source addresses can be dynamically learned in different ways. Depending on the security level, SBT blocks unwanted messages such as Router Advertisements (RA) or Dynamic Host Configuration Protocol (DHCP) replies. This database, or binding table is used by various IPv6 guard features to validate the link-layer address (LLA), the IPv4 address, or the IPv6 address of the neighbors to prevent spoofing and redirect attacks.

Enabling or disabling ND-inspection

Before you begin

Enable FHS globally.

About this task

Enables ND-inspection globally. By default, ND-inspection is disabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable ND-inspection globally.

   ```
   ipv6 nd inspection enable
   ```

3. Disable ND-inspection.

   ```
   no ipv6 nd inspection enable
   ```

   OR

   ```
   default ipv6 nd inspection enable
   ```

Note:

When ND-inspection is deleted, all the corresponding dynamically-learned SBT entries are also deleted.

Managing entries in SBT

About this task

The Source Binding Table (SBT) learns the neighbor source address connected to the FHS switch dynamically or statically.

Neighbor source IP address are learned on the ports where ND-inspection is enabled. A maximum of 1024 dynamic source IP address are allowed to be learned.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Add a static entry to the SBT.

   ```
   ipv6 neighbor binding vlan <vlan-id> <ipv6-address> interface
   <interface-type> <port> <mac-address>
   ```

3. Delete a static or dynamic entry from SBT.

   ```
   no ipv6 neighbor binding vlan <vlan-id> <ipv6-address> interface
   <interface-type> <port> <mac-address>
   ```

4. Specify the maximum number of dynamic entries that can be inserted in the SBT.

   ```
   ipv6 neighbor binding max-entrie <1 - 1024>
   ```

5. Clear all the dynamically-learned SBT entries.

   ```
   ipv6 neighbor binding clear
   ```

6. Change the default SBT entry from 1024 to 512.

   ```
   default ipv6 neighbor binding max-entries
   ```

Variable definitions

Use the data in the following table to use the **`ipv6 neighbor binding`** command.

Variable	Description
vlan <*vlan-id*> <*ipv6-address*> interface <*interface-type*> <*port*> <*mac-address*>	Adds a static entry to the SBT. The IPv6 address 0::0 and Link-Layer MAC 0:0:0:0:0:0 are not allowed.

Table continues…

Variable	Description
	Note: The static entry replaces the dynamic entry (matching the source IP address). If there is an existing static SBT entry (matching the source IP address) and if you try to add a static SBT entry with a different MAC address or port, then those entries are not overwritten. The same SBT entry can be added in a different VLAN.
max-entrie *<1 - 1024>*	Specifies the maximum number of dynamic entries that are allowed to be inserted in the SBT. By default, the maximum number of dynamic entries that can be entered is 512. The value of dynamic entries ranges from 1 to 1024. The maximum number of static entries is 100 and this configuration excludes the static entry of 100. If there are more entries in the SBT than the configured maximum entries, then those configurations are not allowed until the SBT is cleared
clear	Clears all the dynamically-learned SBT entries. The SBT static entries are not cleared and the learned information, such as DHCP and other learned information, is not cleared.

Managing SBT entry lifetime

About this task

Incomplete, Reachable, Stale, and Down are the four states for an SBT entry. You can modify the lifetime of these states.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Specify the maximum Reachable lifetime for a dynamically-learned SBT entry.

   ```
   ipv6 neighbor binding reachable-lifetime [<30 – 86400 seconds> | infinite]
   ```

3. Change the Reachable lifetime to the default value. The default value is 300 seconds.

   ```
   default ipv6 neighbor binding reachable-lifetime
   ```

4. Specify the maximum Stale lifetime for a dynamically-learned SBT entry.

```
ipv6 neighbor binding stale-lifetime [ <30 – 86400 seconds> |
infinite]
```

5. Change the Stale lifetime to the default value. The default value is 86400 seconds.

   ```
   default ipv6 neighbor binding stale-lifetime
   ```

6. Specify the maximum Down lifetime for a dynamically-learned SBT entry.

   ```
   ipv6 neighbor binding down-lifetime [ <30 – 86400 seconds> |
   infinite]
   ```

7. Change the Down lifetime to the default value. The default value is 86400 seconds.

   ```
   default ipv6 neighbor binding down-lifetime
   ```

Variable definitions

Use the data in the following table to use the **`ipv6 neighbor binding`** command.

Variable	Description
reachable-lifetime [<*30 – 86400 seconds*> | *infinite*]	Specifies the maximum REACHABLE lifetime for a dynamically-learned SBT entry. After time-out, the entry moves from REACHABLE to a STALE state, or if the interface is down before this timer expires, then the state moves to a DOWN state. In this state, if the switch receives any ND packets with the matching entry in the SBT, then without validation the state moves to REACHABLE. Similarly, when the switch receives any ND packets matching the entry in the SBT, then this aging timer is refreshed. By default, the REACHABLE lifetime is 300 seconds. In the case of the `infinite` option, the SBT entry state never moves from the REACHABLE state to the other state. If the timer value is changed from infinite to a finite value, then the timer restarts and expires after the finite value in seconds. **Note:** The granularity of the timer is five seconds.
stale-lifetime [<*30 – 86400 seconds*> | *infinite*]	Specifies the maximum STALE lifetime for a dynamically-learned SBT entry. In this state, if the switch receives any ND message matching the information as the SBT entry, then validation is not done on that packet; instead, this entry directly moves to a REACHABLE state. After this timer expiry, this entry is deleted from the SBT By default, the STALE lifetime is 86400 seconds.

Table continues…

Variable	Description
	In the case of the `infinite` option, the SBT entry state is never deleted. If the timer value is changed from infinite to a finite value, then the timer restarts and expires after the finite value in seconds. **Note:** The granularity of the timer is 5 seconds.
down-lifetime [<*30 – 86400 seconds*> | *infinite*]	Specifies the maximum DOWN lifetime for a dynamically-learned SBT entry. In this state, if the switch receives any ND message matching the information as the SBT entry, then validation is not done on that packet; instead, this entry directly moves to a REACHABLE state. After this timer expiry, this entry is deleted from the SBT. By default, the DOWN lifetime is 86400 seconds. In the case of the `infinite` option, the SBT entry state is never deleted. If the timer value is changed from infinite to a finite value, then the timer restarts and expires after the finite value in seconds. **Note:** The granularity of the timer is 5 seconds.

Clearing ND-inspection statistics

About this task

Clears the ND-inspection statistics.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Clear the ND-inspection statistics and SBT entry drop status.

   ```
   ipv6 nd inspection clear stats [<port-number>]
   ```

3. Clear ND-inspection statistics globally.

   ```
   ipv6 fhs nd inspection stats clear
   ```

   Note:

   The SBT entry overflow statistics are also deleted.

Variable definitions

Use the data in the following table to use the **`ipv6 nd inspection clear stats`** command.

Variable	Description
<port-number>	Clears the ND-inspection statistics as well as SBT entry drop status. If port number is mentioned, then only the statistics for that particular port is cleared.

Enabling or disabling ND-inspection on an interface

About this task

Enables or disables the ND-inspection on an interface.

Procedure

1. Enter Interface Configuration mode:

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

2. Enable the ND-inspection on an interface.

   ```
   ipv6 nd inspection [dynamic-learning enable]
   ```

3. Disable the ND-inspection on an interface.

   ```
   no ipv6 nd inspection [dynamic-learning enable]
   ```

   OR

   ```
   default ipv6 nd inspection [dynamic-learning enable]
   ```

Variable definitions

Use the data in the following table to use the **`ipv6 nd inspection`** command.

Variable	Description
ipv6 nd inspection [dynamic-learning enable]	Enables the ND-inspection on an interface. The option `dynamic-learning` enables the FHS module to learn the neighbor source IP address in the SBT table. By default, ND-inspection is disabled and dynamic-learning is enabled. **Note:** ND-inspection is not done on the packets if the port belongs to the trunk.
[no] [default] ipv6 nd inspection [dynamic-learning enable]	Disables the ND inspection on an interface. The option `dynamic-learning` prevents the FHS module from learning the SBT entries dynamically on

Table continues…

Variable	Description
	the configured port. In this case, ND packets are forwarded only if static SBT entries are configured. In the case of disabling ND-inspection or dynamic-learning, all the corresponding dynamic SBT entries are learned on the port that must be deleted.

Displaying ND-inspection SBT entries

About this task

Display SBT entries and other timer values.

Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display SBT entries and timer values.

```
show ipv6 neighbor binding [vlan <vlan-id> | interface <type>
<number> | ipv6 <ipv6-address>]
```

Example

```
Switch(config)#show ipv6 neighbor binding
Binding Table has 2 entries, 2 dynamic
Reachable-timer: 300 sec, Stale-timer: 86300 sec, Down-timer 86300 sec
Codes: S - Static, ND - Neighbor Discovery, DH - DHCP
Preflevel values in Hex (prlvl):
0001:Access 0002:MAC & LLA match 0008:DAD Learnt 0010:DHCP Learnt
0020:Learnt from Non-ND-inspect Port(Trusted-port)
Type IPv6-Addr LL-Addr
================================================================
port vlan prlvl state Age (sec)
================================================================
ND 2001:DB8::/32 00:50:56:84:00:20
1/8 1 0003 REACH 86
ND 2001:DB8::/32 00:50:56:84:00:1e
3/14 1 0003 REACH 60
```

Variable definitions

Use the data in the following table to use the **`show ipv6 neighbor binding`** command.

Variable	Description
[vlan <*vlan-id*> | interface <*type*> number | ipv6 <*ipv6-address*>	Displays SBT entries and other timer values.

IPv6 Source Guard configuration using CLI

This section describes how you configure IPv6 Source Guard using the Command Line Interface (CLI).

Important:

You should not enable IPv6 Source Guard on trunk ports.

Note:

When you try to enable source guard on a port which does not have sufficient number of filters available, an error is returned and operation is failed.

Before you begin

Before you configure IPv6 Source Guard, you must ensure that FHS and ND Inspection are enabled globally and on port.

Configuring IPv6 Source Guard on an interface using CLI

Configure IPv6 Source Guard to add a higher level of security to the desired port by preventing IP spoofing. When you enable IPv6 Source Guard on an interface, filters are installed for IPv6 addresses which are already learned on that interface.

Before you begin

Enable FHS and ND Inspection globally and on port before you enable IPv6 Source Guard.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. Configure IPv6 Source Guard on interface.

   ```
   [no] [default] ipv6 source-guard [max-allowed-addr <2-10>]
   ```

3. Verify the settings.

   ```
   show ipv6 source-guard interface
   ```

Example

The following example shows the output for **show ipv6 source-guard interface**.

```
switch#show ipv6 source-guard interface 1-8
Unit/Port Source Guard Mode    Number of IPv6              Address
                               address allowed       overflow count
---------   -----------------  --------------------      ---------------
1/1          Disabled               5                          0
1/2          Disabled               5                          0
1/3          Enabled                10                         0
1/4          Disabled               5                          0
1/5          Enabled                5                          2
1/6          Enabled                3                          1
1/7          Disabled               5                          0
1/8          Disabled               5                          0
```

Variable definitions

The following table defines parameters for the `ipv6 source-guard` command.

Variable	Description
max-allowed-addr <2–10>	Configures the maximum number of IPv6 addresses allowed to transmit data through the FHS switch.
interface	Interface types
[no]	Disables IPv6 Source Guard to allow all IP traffic to go through without being filtered. Disabling the feature removes the filters for allowed IPv6 addresses and all hosts would be allowed to send data.
[default]	Sets the maximum addresses allowed to send data to default. The default value of max-allowed-addr is 5. **Note:** For setting the max-allowed-addr to default, the IPv6 source guard needs to be disabled on the interface.

Clearing the IPv6 Source Guard Overflow counters using CLI

Overflow counters consists of IPv6 addresses, which are not added to IPv6 Source Guard due to lack of filter resources. The following procedure describes how to clear the overflow counters for each specified interface or all interfaces.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. Clear the overflow counters.

   ```
   ipv6 source-guard overflow-count clear
   ```

3. Verify the settings.

   ```
   show ipv6 source-guard interface
   ```

Example

The following example shows the output for **show ipv6 source-guard interface** command.

```
switch#show ipv6 source-guard interface 1-8
Unit/Port Source Guard Mode    Number of IPv6              Address
                               address allowed       overflow count
---------   -----------------  --------------------      ---------------
1/1          Disabled               5                          0
1/2          Disabled               5                          0
```

```
1/3          Enabled              10                   0
1/4          Disabled             5                    0
1/5          Enabled              5                    2
1/6          Enabled              3                    1
1/7          Disabled             5                    0
1/8          Disabled             5                    0
```

Viewing IPv6 source bindings using CLI

Use this procedure to view IPv6 address bindings for all or given ports which are allowed by the IPv6 Source Guard.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display the IPv6 addresses allowed for each or given port.

   ```
   show ipv6 source-guard binding [interface <port-num>]
   ```

3. Display the binding entry for the given IPv6 address.

   ```
   show ipv6 source-guard binding <ipv6 address>
   ```

Example

The following example shows the output for the command **show ipv6 source-guard binding interface**.

```
switch#show ipv6 source-guard binding interface 1/3, 1/6
Unit/Port     IPv6 Address
1/3          2001:DB8:89ab:cdef:0123:4567:89ab:cdef
1/3          fe80::210:94ff:fe00:550b
1/6          2001:DB8:89ab:cdef:0123:4567:89ab:ghij
```

IPv6 FHS configuration using EDM

This section describes how to configure IPv6 First Hop Security (FHS) on the switch and protect the network by mitigating the various types of attacks such as address spoofing, remote address resolution cache exhaustion (denial of service attacks), and others, using Enterprise Device Manager (EDM).

Note:

FHS does not solve all cases of denial of services like blocking flooding of the IPv6 messages.

Configuring FHS Globals

About this task

Use this procedure to enable FHS to enable DHCPv6-guard, RA-guard, or ND-inspection policy globally, and to configure the lifetime for these policies.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **Globals** tab.
4. Configure FHS globals.
5. On the toolbar, click **Apply** to save the changes.
6. On the toolbar, click **Refresh** to update the results.

Variable definitions

The following table describes the Globals tab fields.

Variable	Description
Admin	Enables or disables the FHS policy.
RAGuardAdmin	Enables or disables the RA–guard policy.
DHCPv6GuardAdmin	Enables or disables the DHCPv6–guard policy.
NDInspectAdmin	Enables or disables ND–inspection policy.
MaxDynSBTEntries	Specifies the maximum dynamic SBT entries. The value range is from 0 to 1024. The default value for the maximum dynamic SBT entry is 512.
SBTReachLifeTime	Specifies the maximum REACHABLE lifetime for a dynamically-learned SBT entry. The value range is from 0 (infinite) or 30 to 864000 seconds. The default value for the SBT REACHABLE lifetime is 300 seconds. After time-out, the entry moves from REACHABLE to STALE state or if the interface is down before this timer expires, then the state moves to DOWN state. In this state, if the switch receives any ND packets with the matching entry in the SBT, then without validation the state moves to the REACHABLE. Similarly, when the switch receives any ND packets matching the entry in the SBT, then this aging timer is refreshed.
SBTStaleLifeTime	Specifies the maximum STALE lifetime for a dynamically learnt SBT entry.

Table continues…

Variable	Description
	The value range is from 0 (infinite) or 30 to 86400 seconds. The default value for the SBT STALE lifetime is 86400 seconds. In this state, if the switch receives any ND message matching the information as the SBT entry, then validation is not done on that packet; rather, this entry directly moves to the REACHABLE state. After this timer expiry, this entry is deleted from the SBT.
SBTDownLifeTime	Specifies the maximum DOWN lifetime for a dynamically-learned SBT entry. The value range is from 0 to 86400 seconds. The default value for the SBT DOWN lifetime is 86400 seconds. In this state, if the switch receives any ND message matching the information as the SBT entry, then validation is not done on that packet; rather, this entry directly moves to the REACHABLE state. After this timer expiry, this entry gets deleted from the SBT
SBTTblOverFlow	Specifies SBT overflow.

IPv6 access list configuration

An IPv6 access list is created to verify the sender's IPv6 address in the inspected messages. You can configure, view, or delete an IPv6 access list.

Creating IPv6 access list

About this task

Use this procedure to create an FHS IP access list or add IP prefixes to the existing IP access list

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **IPv6 Access List** tab.
4. On the toolbar, click **Insert**.
5. Configure the parameters for the IPv6 access list.
6. Click **Insert**.

Variable definitions

The following table describes the IP Access List tab fields.

Variable	Description
Name	Specify the IP access list name to create the IP access list.
Prefix	Specify the IP prefix for adding it to the IP access list.
PrefixMaskLen	Specify the prefix mask length for adding it to the IP access list. The value range is from 0 to 128. By default, the value is 0.
MaskLenFrom	Specify the start mask length for providing the IP range. The value range is from 0 to 128. By default, the value is 0.
MaskLenTo	Specify the end mask length for providing the IP range. The value range is from 0 to 128. By default, the value is 0.
AccessType	Select the access type to allow or deny the entry. By default, the access type is allow.

Viewing IPv6 access list

About this task

Use this procedure to display the IPv6 access list.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **IPv6 Access List** tab.

Variable definitions

The following table describes the IP Access List tab fields.

Variable	Description
Name	Specify the IP access list name to create the IP access list.
Prefix	Specify the IP prefix for adding it to the IP access list.
PrefixMaskLen	Specify the prefix mask length for adding it to the IP access list. The value range is from 0 to 128. By default, the value is 0.
MaskLenFrom	Specify the start mask length for providing the IP range. The value range is from 0 to 128. By default, the value is 0.

Table continues…

Variable	Description
MaskLenTo	Specify the end mask length for providing the IP range. The value range is from 0 to 128. By default, the value is 0.
AccessType	Select the access type to allow or deny the entry. By default, the access type is allow.

Deleting the IPv6 access list

About this task

Use this procedure to delete the created IPv6 access list.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **IPv6 Access List** tab.
4. Select a row from the IPv6 access list to delete.
5. Click **Delete**.

MAC access list configuration

A MAC access list is created to verify the sender's MAC address in the inspected messages. You can view, create, or delete a MAC access list.

Creating MAC access list

About this task

Use this procedure to create a MAC access list or add a MAC address to the existing MAC access list.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **MAC Access List** tab.
4. On the toolbar, click **Insert**.
5. Configure the parameters for the MAC access list.
6. Click **Insert**.

Variable definitions

The following table describes the MAC Access List tab fields.

Variable	Description
Name	Specify a name to create a MAC access list.
Mac	Specify the MAC address to add the address to the MAC access list.
AccessType	Specify allow or deny. By default, the access type is allow.

Viewing a MAC access list

About this task

Use this procedure to display a configured MAC access list.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **MAC Access List** tab.

Variable definitions

The following table describes the MAC Access List tab fields.

Variable	Description
Name	Specify a name to create a MAC access list.
Mac	Specify the MAC address to add the address to the MAC access list.
AccessType	Specify allow or deny. By default, the access type is allow.

Deleting a MAC access list

About this task

Use this procedure to delete the created MAC access list.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **MAC Access List** tab.
4. Select a row from the MAC access list to delete.
5. Click **Delete**.

DHCPv6-guard policy configuration

Configure the DHCP-DHCPv6 guard policy to block DHCP reply and advertisement messages that originate from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. You can view, create, or delete a DHCPv6 guard policy.

Creating DHCPv6-guard policy

About this task

Use this procedure to create the DHCPv6-guard policy to block DHCP reply and advertisement messages that originate from unauthorized DHCP servers and relay agents.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **DHCPv6 Guard Policy** tab.
4. On the toolbar, click **Insert**.
5. Configure the parameters for the DHCPv6-guard policy.
6. Click **Insert**.
7. On the toolbar, click **Refresh** to update the results.

Variable definitions

The following table describes the DHCPv6 Guard Policy tab fields.

Variable	Description
PolicyName	Specify the policy name to create or modify DHCPv6-guard policy.
DeviceRole	Select client or server to enable verification of the role of the device attached to the port. By default, no device is selected.
ServerAccessListName	Enables verification of the sender's IPv6 address in the inspected messages from the configured authorized device source access-list specified. **Note:** If the access-list is not attached, the inspection does not occur. If the list is attached and it does not match any IP prefixes in the list, the switch drops the DHCPv6 packet. To change this behavior, add a dummy ip-prefix 0.0.0.0/0 with the Allow option, which changes the default drop to default Allow.

Table continues…

Variable	Description
ReplyPrefixListName	Enables verification of the advertised prefixes in DHCP reply messages from the configured authorize prefix list. If not configured, this check is bypassed. An empty prefix list is treated as a permit. **Note:** If the access-list is not attached, the inspection does not occur. If the list is attached and it does not match any IP prefixes in the list, the switch drops the DHCPv6 packet. To change this behavior, add a dummy ip-prefix 0.0.0.0/0 with the Allow option, which changes the default drop to default Allow.
PrefLimitMin	Enables verification if the advertised preference (in reference option) is greater than the specified limit. If not specified, this check does not occur. The value range is from 0 to 255.
PrefixLimitMax	Enables verification if the advertised preference (in preference option) is less than the specified limit. If not specified, this check does not occur. The value range is from 0 to 255. **Note:** If both the maximum and minimum limit is 0, this preference check is ignored.

Viewing a DHCPv6-guard policy

About this task

Use this procedure to display configured DHCPv6-guard policies.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **DHCPv6 Guard Policy** tab.

Variable definitions

The following table describes the DHCPv6 Guard Policy tab fields.

Variable	Description
PolicyName	Specify the policy name to create or modify DHCPv6-guard policy.

Table continues…

Variable	Description
DeviceRole	Select client or server to enable verification of the role of the device attached to the port. By default, no device is selected.
ServerAccessListName	Enables verification of the sender's IPv6 address in the inspected messages from the configured authorized device source access-list specified. **Note:** If the access-list is not attached, the inspection does not occur. If the list is attached and it does not match any IP prefixes in the list, the switch drops the DHCPv6 packet. To change this behavior, add a dummy ip-prefix 0.0.0.0/0 with the Allow option, which changes the default drop to default Allow.
ReplyPrefixListName	Enables verification of the advertised prefixes in DHCP reply messages from the configured authorize prefix list. If not configured, this check is bypassed. An empty prefix list is treated as a permit. **Note:** If the access-list is not attached, the inspection does not occur. If the list is attached and it does not match any IP prefixes in the list, the switch drops the DHCPv6 packet. To change this behavior, add a dummy ip-prefix 0.0.0.0/0 with the Allow option, which changes the default drop to default Allow.
PrefLimitMin	Enables verification if the advertised preference (in reference option) is greater than the specified limit. If not specified, this check does not occur. The value range is from 0 to 255.
PrefixLimitMax	Enables verification if the advertised preference (in preference option) is less than the specified limit. If not specified, this check does not occur. The value range is from 0 to 255. **Note:** If both the maximum and minimum limit is 0, this preference check is ignored.

Deleting a DHCPv6–guard policy

About this task

Use this procedure to delete the created DHCPv6-guard policy.

Note:

If this policy is already attached to an interface, then this policy cannot be deleted.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **DHCPv6 Guard Policy** tab.
4. Select a row from DHCPv6 Guard policies to delete.
5. Click **Delete**.

RA-guard policy configuration

Configure IPv6 RA-guard to block or reject unwanted or rogue RA guard messages that arrive at the network device platform. You can view, create, or delete RA-guard policy.

Creating RA-guard policy

About this task

Use this procedure to create a RA-guard policy to block or reject unwanted or rogue RA guard messages that arrive at the network device platform.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **RA Guard Policy** tab.
4. On the toolbar, click **Insert**.
5. Configure the parameters for the RA-guard policy.
6. Click **Insert**.
7. On the toolbar, click **Refresh** to update the results.

Variable definitions

The following table describes the RA Guard Policy tab fields.

Variable	Description
PolicyName	Specify the name of the RA-guard policy to be created or modified.
DeviceRole	Select router or host to enable the device role verification attached to the port. By default, no device is selected.

Table continues…

Variable	Description
Ipv6AccessListName	Specify the IPv6 access list name to verify the sender's IPv6 address in the inspected messages against the configured authorized device source access list. **Note:** Inspection is not done if the access-list is not attached. If the list is attached and if it does not match any ip-prefix in the list, then the RA packet is dropped. To change this behavior, add a dummy ip-prefix "0::0/0" with the Allow option. The default value changes from drop to Allow.
Ipv6PrefixListName	Specify the IPv6 prefix list name to verify the advertised prefixes in the inspected messages against the configured authorized prefix list. **Note:** Inspection is not done if the access-list is not attached. If the list is attached and if it does not match any ip-prefix in the list, then the RA packet is dropped. To change this behavior, add a dummy ip-prefix "0::0/0" with Allow option. The default value changes from drop to Allow.
MacListName	Specify the MAC list name to verify the sender's source MAC address against the configured MAC access list. **Note:** Inspection is not done if the access-list is not attached. If the list is attached and if it does not match any MAC in the list, then the RA packet is dropped. To change the behavior, add a dummy MAC "0:0:0:0:0:0" to the list with Allow option. The default value changes from drop to Allow.
ManagedConfigFlag	Select managed configuration flag to verify managed address configuration in the advertised RA packet. By default, none is selected and this check does not occur.
RouterPrefMax	Select the router preference maximum to verify the if the advertised default router preference parameter value is lower than or equal to a specified limit.

Table continues…

Variable	Description
	By default, none is selected and this check does not occur.
HopLimitMin	Specify the minimum hop limit to verify the advertised hop count limit. The value range is from 0 to 255 By default, minimum hop limit is 0 and the hop-limit check does not occur.
HopLimitMax	Specify the maximum hop limit to verify the advertised hop count limit. The value range is from 0 to 255 By default, maximum hop limit is 0 and the hop-limit check does not occur.

Variable definitions

The following table describes the RA Guard Policy tab fields.

Variable	Description
PolicyName	Specify the name of the RA-guard policy to be created or modified.
DeviceRole	Select router or host to enable the device role verification attached to the port. By default, no device is selected.
Ipv6AccessListName	Specify the IPv6 access list name to verify the sender's IPv6 address in the inspected messages against the configured authorized device source access list. **Note:** Inspection is not done if the access-list is not attached. If the list is attached and if it does not match any ip-prefix in the list, then the RA packet is dropped. To change this behavior, add a dummy ip-prefix "0::0/0" with the Allow option. The default value changes from drop to Allow.
Ipv6PrefixListName	Specify the IPv6 prefix list name to verify the advertised prefixes in the inspected messages against the configured authorized prefix list. **Note:** Inspection is not done if the access-list is not attached.

Table continues…

Variable	Description
	If the list is attached and if it does not match any ip-prefix in the list, then the RA packet is dropped. To change this behavior, add a dummy ip-prefix “0::0/0” with Allow option. The default value changes from drop to Allow.
MacListName	Specify the MAC list name to verify the sender’s source MAC address against the configured MAC access list. **Note:** Inspection is not done if the access-list is not attached. If the list is attached and if it does not match any MAC in the list, then the RA packet is dropped. To change the behavior, add a dummy MAC “0:0:0:0:0:0” to the list with Allow option. The default value changes from drop to Allow.
ManagedConfigFlag	Select managed configuration flag to verify managed address configuration in the advertised RA packet. By default, none is selected and this check does not occur.
RouterPrefMax	Select the router preference maximum to verify the if the advertised default router preference parameter value is lower than or equal to a specified limit. By default, none is selected and this check does not occur.
HopLimitMin	Specify the minimum hop limit to verify the advertised hop count limit. The value range is from 0 to 255 By default, minimum hop limit is 0 and the hop-limit check does not occur.
HopLimitMax	Specify the maximum hop limit to verify the advertised hop count limit. The value range is from 0 to 255 By default, maximum hop limit is 0 and the hop-limit check does not occur.

Viewing RA-guard policy

About this task

Use this procedure to display configured RA-guard policies.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **RA Guard Policy** tab.

Variable definitions

The following table describes the RA Guard Policy tab fields.

Variable	Description
PolicyName	Specify the name of the RA-guard policy to be created or modified.
DeviceRole	Select router or host to enable the device role verification attached to the port. By default, no device is selected.
Ipv6AccessListName	Specify the IPv6 access list name to verify the sender's IPv6 address in the inspected messages against the configured authorized device source access list. **Note:** Inspection is not done if the access-list is not attached. If the list is attached and if it does not match any ip-prefix in the list, then the RA packet is dropped. To change this behavior, add a dummy ip-prefix "0::0/0" with the Allow option. The default value changes from drop to Allow.
Ipv6PrefixListName	Specify the IPv6 prefix list name to verify the advertised prefixes in the inspected messages against the configured authorized prefix list. **Note:** Inspection is not done if the access-list is not attached. If the list is attached and if it does not match any ip-prefix in the list, then the RA packet is dropped. To change this behavior, add a dummy ip-prefix "0::0/0" with Allow option. The default value changes from drop to Allow.
MacListName	Specify the MAC list name to verify the sender's source MAC address against the configured MAC access list.

Table continues…

Variable	Description
	Note: Inspection is not done if the access-list is not attached. If the list is attached and if it does not match any MAC in the list, then the RA packet is dropped. To change the behavior, add a dummy MAC “0:0:0:0:0:0” to the list with Allow option. The default value changes from drop to Allow.
ManagedConfigFlag	Select managed configuration flag to verify managed address configuration in the advertised RA packet. By default, none is selected and this check does not occur.
RouterPrefMax	Select the router preference maximum to verify the if the advertised default router preference parameter value is lower than or equal to a specified limit. By default, none is selected and this check does not occur.
HopLimitMin	Specify the minimum hop limit to verify the advertised hop count limit. The value range is from 0 to 255 By default, minimum hop limit is 0 and the hop-limit check does not occur.
HopLimitMax	Specify the maximum hop limit to verify the advertised hop count limit. The value range is from 0 to 255 By default, maximum hop limit is 0 and the hop-limit check does not occur.

Deleting a RA-guard policy

About this task

Use this procedure to delete the created RA-guard policy.

Note:

If this policy is already attached to an interface, then this policy cannot be deleted.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **RA Guard Policy** tab.
4. Select a row from RA Guard policies to delete.

5. Click **Delete**.

Port policy mapping configuration

This feature allows you to map the port with FHS, DHCPv6-guard, or RA-guard policy. You can view, create or delete the mappings.

Creating port to policy mapping

About this task

Use this procedure to map a port to a RA-guard or DHCPv6-guard policy and to clear the ND-inspection, DHCPv6-guard or RA-guard statistics.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **Port Policy Mapping** tab.
4. On the toolbar, click **Insert**.
5. Configure the parameters for the port policy mapping.
6. Click **Insert**.
7. On the toolbar, click **Refresh** to update the results.

Variable definitions

The following table describes the Port Policy Mapping tab fields.

Variable	Description
Ports	Specify the ports.
DHCPv6GuardPolicyName	Enter already-created DHCPv6-guard policy name to map it with the port.
RAGuardPolicyName	Enter already-created RA-guard policy name to map it with the port.
NDAdmin	Enable ND-inspection for the selected ports.

Viewing port policy mapping

About this task

Use this procedure to display port policy mapping information.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.

3. On the work area, click the **Port Policy Mapping** tab.

Variable definition

The following table describes the Port Policy mapping tab fields.

Variable	Description
IfIndex	Specifies the port.
DHCPv6GuardPolicyName	Specifies the DHCPv6-guard policy name associated with the port.
RAGuardPolicyName	Specifies the RA-guard policy name associated with the port.
NDAdmin	Specifies whether ND-inspection is enabled or disabled.
SBTDynLearnAdmin	Specifies if dynamic learning is enabled or disabled on a port. If dynamic learning is disabled, the ND packets are forwarded only through static SBT entries on those ports. By default, SBT dynamic learning is enabled. **Note:** Dynamic learning is not supported for ND packets with IPv6 any-cast address. A static SBT configuration is required.
TotalDHCPv6PktRcv	Specifies total number of DHCPv6 packets received on the DHCPv6-guard enabled interface.
TotalDHCPv6PktDropped	Specifies total number of DHCPv6 packets dropped due to DHCPv6-guard filtering.
TotalRAPktRcv	Specifies total number of RA packets received on the RA-guard enabled interface.
TotalRAPktDropped	Specifies total number of RA packets dropped due to RA-guard filtering.
TotalNDPktRcv	Specifies total number of ND packets received on the ND-inspection enabled interface.
TotalNDPktDropped	Specifies total number of ND packets dropped on the ND-inspection enabled interface.
ClearDHCPGuardStats	Specifies the DHCPv6-guard statistics cleared for the port number.
ClearRAGuardStats	Specifies the RA-guard statistics cleared for the port number.
ClearNDInspectStats	Specifies the ND-inspection statistics cleared for the port number.

Deleting port policy mapping

About this task

Use this procedure to delete the created port policy mapping.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **Port Policy Mapping** tab.
4. Select a row from Port Policy Mapping to delete.
5. Click **Delete**.
6. Click **Apply**.

Source Binding Table configuration

The Source Binding Table (SBT) learns the Neighbor source IP address on the ports where ND-inspection is enabled. The maximum number of dynamic source IP addresses allowed to be learned is 1024.

You can view, create or delete an SBT.

Configuring the SBT

About this task

Use this procedure to add a static or dynamic entry to the SBT.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **Source Binding Table** tab.
4. On the toolbar, click **Insert**.
5. Configure the parameters for the SBT.
6. Click **Insert**.
7. On the toolbar, click **Refresh** to update the results.

Variable definitions

The following table describes the Source Binding Table tab fields.

Variable	Description
InterfaceIndex	Specify the ports.

Table continues…

Variable	Description
Vlan	Enter the VLAD ID.
SrcIp	Enter the source IP address attached to the particular port or VLAN.
LinkLayerAddress	Specify the IPv6 address for learning the neighbor link layer address.

Viewing the SBT

About this task

Use this procedure to display all dynamically-learned neighbor source IP addresses and the statically-configured source IP address entries in the SBT.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **Source Binding Table** tab.

Variable definitions

The following table describes the Source Binding Table tab fields.

Variable	Description
InterfaceIndex	Specify the ports.
Vlan	Specifies the VLAN ID.
Srclp	Specifies the source IP address.
LinkLayerAddress	Specifies the link layer address.
LearnType	Specifies whether the source IP is learned statically or dynamically
LearnPriority	Specifies the learning priority for the source IP address attached to the particular port or VLAN.
LearnState	Specifies the SBT entry state.
LearnAge	Specifies the learning age for the source IP address attached to the particular port or VLAN.

Deleting the SBT

About this task

Use this procedure to delete the created SBT.

Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **FHS**.
3. On the work area, click the **Port Policy Mapping** tab.

4. Select a row from Port Policy Mapping to delete.
5. Click **Delete**.

IPv6 Source Guard configuration

IPv6 Source Guard is an extension to the IPv6 First Hop Security feature which works in conjunction with Neighbor Discovery Inspection and DHCPv6 Guard to ensure traffic forwarded is from valid hosts on the network.

Configuring IPv6 Source Guard

Configure IPv6 Source Guard to add a higher level of security to the desired port by preventing IP spoofing. When you enable IPv6 Source Guard on an interface, filters are installed for IPv6 addresses which are already learned on that interface.

Note:

Extreme Networks recommends that you do not enable IPv6 Source Guard on trunk ports.

Note:

An error appears and the operation fails if IPv6 Source Guard is enabled on port which does not have sufficient filters.

Before you begin

Enable FHS and ND Inspection globally and on port before you enable IPv6 Source Guard.

About this task

Use the following procedure to configure one or more ports for IPv6 Source Guard.

Procedure

1. From the Device Physical View, select a port, or use CTRL+click to select more than one port.
2. From the navigation tree, double-click IPv6.
3. In the IPv6 tree, click IPv6.
4. In the work area, click the Source Guard tab.
5. In the port row, double-click the cell in the **InterfaceState** column.
6. Select a value from the list: true or false.
7. Double-click the **MaxAddr** for a port.
8. Type the maximum number of IPv6 addresses allowed to transmit data from the switch.
9. Double-click the cell in the **ClearOverflowCount**.
10. Select a value from the list: true or false.

11. Optionally, to configure parameters for multiple ports, you can use the Make Selection section as below.
12. In the work area, in the Make Selection section of the Multiple Port Configuration pane, click the Switch/Stack/Ports ellipsis (...) to open the Port Editor dialog.
13. In the Port Editor window, click the ports you want to configure.

    Note:

    If you want to configure all ports, click **All**.
14. Click **OK** to return to the Make Selection pane.

    The ports you selected appear in the Switch/Stack/Ports box.
15. To change the configuration of the selected ports, in the Multiple Port Configuration pane, double-click the cell beneath the column heading that represents the parameter you want to change and do one of the following:
    - If applicable, select a value from a drop-down list.
    - Otherwise, type a value in the cell.
16. In the Make Selection pane, click **Apply Selection**.

    The changes appear in the table.
17. **(Optional)** Click **Clear Selection** to clear Multiple Port Configurations or click **Hide Non-Editable** to display only those parameters that are editable in the Multiple Port Configuration pane for the selected ports.
18. Click **Apply**.

Source Guard field descriptions

Use the data in the following table to configure IPv6 Source Guard.

Name	Description
IfIndex	Specifies a unique value assigned to each interface.
InterfaceState	Specifies the state of the interface. By default, the value is false.
MaxAddr	Specifies the maximum number of IPv6 addresses allowed to transmit data through the switch. By default, the value is 5. **Note:** To reset the value to default, the IPv6 Source Guard must be disabled on the interface.
OverflowCount	Specifies the number of IPv6 addresses which are not added to IPv6 Source Guard due to lack of filter resources.

Table continues…

Name	Description
ClearOverflowCount	Specifies whether the overflow counters must be cleared. By default, the value is false.

Viewing IPv6 Source Guard binding

About this task

Use this procedure to view IPv6 address bindings for ports allowed by IPv6 Source Guard.

Procedure

1. From the navigation tree, double-click IPv6.
2. In the IPv6 tree, click IPv6.
3. In the IPv6 work area, click the Source Guard Binding tab.

IPv6 Source Guard Binding field descriptions

Use the data in the following table view IPv6 Source Guard Binding.

Name	Description
IfIndex	Specifies a unique value assigned to each interface.
Ipv6Addr	Specifies binding entry for the IPv6 address

Chapter 13: MAC Address-Based Security

This chapter provides conceptual information and procedures to configure MAC address-based security using Command Line Interface (CLI) and Enterprised Device Manager (EDM).

MAC address-based security

The Media Access Control (MAC) address-based security feature is based on 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 destination MAC addresses the system uses to drop all packets that contain one of the specified MAC addresses as the destination address regardless of the ingress port, source address intrusion, or VLAN membership.

  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 source addresses and specify the source addresses authorized to connect to the switch or stack. There are three ways to populate this list:

  - Manual configuration

    When MAC address-based security is configured, the ports each MAC source address can access is specified. The options for allowed port access include: single port, multiple ports specified in a list or single trunk. A list can include a single port, 1/6 for example, or multiple ports, 1/1-4 for example. Manually added MAC addresses are referred to as being static.

  - MAC address security learning

    When activating MAC address learning on ports, security is temporarily disabled and all learned MAC addresses will be added to the list. When learning is deactivated, security is enabled and only the MAC addresses in the list are allowed to connect through the port.

  - MAC address-based security auto-learning

    Auto-learning populates the list without user intervention. The user sets a maximum number of allowed MAC addresses (1-25) for a specific port, and the switch only passes traffic from the addresses learned by the switch up to the maximum value.

Optional actions for the switch to perform if the software detects a source address security violation can be configured. Actions include sending an SNMP trap, turn on destination address filtering for the specified source addresses, disabling the port, or a combination of these options.

You can configure specified ports to exclude them from participating in MAC-based security using the MAC Security Port Lockout feature.

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: single port, multiple ports specified in a list or single trunk, 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 Command Line Interface (CLI) 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.

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.

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.

Delayed MAC authentication

Because of simultaneous EAP and Non-EAP authentication (with Non-EAP being faster), the Delayed MAC Authentication features allows a global delay timer, ranging from 0 to 20 seconds to be configured. The purpose of this feature is to give priority to another means of authentication other than Non-EAP through Radius.

When traffic is seen from a new MAC, the switch does not immediately try to authenticate it as Non-EAP through Radius. These pending MACs are displayed as a part of the enhancement to track all MACs on EAP ports and to classify them as authenticated or not authenticated. When a new MAC is learned on the port, the switch waits the configured delay time before Non-EAP traffic is authenticated through the RADIUS server.

If EAP authentication is initiated, the switch does not try to authenticate as Non-EAP until the EAP authentication is completed and the MAC is aged and relearned.

Track all MACs per port

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

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

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

Displaying all MACs

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display information on MACs for EAP sessions:

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

3. Display the summary of authenticated clients:

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

Example

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

```
Switch(config)#show eapol sessions

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

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

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

-------------------------- Unauthorized Clients ----------------------------
Unit/Port Client MAC Address Type           Radius Status
--------- ------------------ -------------- ------------------------------
1/15      1E:7C:B2:0F:00:00  Intruder       Reject
1/15      1E:7C:B2:0F:00:01  Intruder       Reject
1/15      1E:7C:B2:0F:00:02  Intruder       Reject
```

```
1/15      1E:7C:B2:0F:00:03  Intruder       Reject
1/15      1E:7C:B2:0F:00:04  Intruder       Reject
Total number of DHCP authenticated phones: 1
Total number of EAP authenticated clients: 2
Total number of non-EAP authenticated clients: 3
Total number of unauthenticated clients: 5


Switch(config)#show eapol summary

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


Switch(config)#show eapol summary verbose

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

Variable definitions

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

Variable	Value
port <portmask>	Specifies the numeric slot/port format. Range: 1/1 to 8/50 or ALL If no port is specified, the default is ALL. If no parameter is specified, the default is show everything. If “non-eap” is without other parameters, all types of non-eap authenticated macs are shown, except when MHSA under no-limit flag is enabled. When “unauthenticated” is not followed by parameters, all unauthenticated macs are shown.
dhcp-phones	Displays MACs of DHCP Phones.
eap	Displays authenticated EAPOL sessions.
non-eap	Displays authenticated non-EAPOL clients.

Table continues…

Variable	Value
radius	Displays non-EAPOL clients authenticated by RADIUS.
local	Displays locally authenticated non-EAPOL clients.
adac-lldp	Displays non-EAPOL clients authenticated through ADAC.
adac-mac-range	Displays neap sessions with macs in the adac mac range list.
held	Displays unauthenticated clients held by RADIUS.
mhsa	Displays non-EAP sessions for MHSA.
unauthenticated	Displays unauthenticated EAPOL and non-EAPOL clients.
intruder	Displays intruder MACs.
guest-vlan	Displays unauthenticated clients in Guest VLAN.
fail-open-vlan	Displays MACs of clients in Fail Open VLAN.
mhsa-no-limit	Displays non-EAP sessions for MHSA when no-limit is enabled.
interface <portlist>	Specifies the interfaces for which to display information. Select a port or a list of ports for which to display information.
verbose	Displays detailed output.

Configuring MAC Address-based Security

The following CLI 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 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 Ethernet Routing Switch 4900 and 5900 Series .

Note:

MAC security settings you have configured are applied only when MAC security is globally enabled on switch. By default, MAC security is disabled. Use the `mac-security enable` command to globally enable MAC security.

Displaying MAC address security settings

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display MAC address security settings:

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

Example

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

Switch#show mac-security mac-address-table
Number of addresses: 0

Port Allowed MAC Address   Type
---- ------------------- ---------

Security List Allowed MAC Address   Type
------------- ------------------- ---------

Trunk Allowed      MAC Address       Type
 --------------- ------------------- ---------
4
```

Variable definitions

Use the data in the following table to use the **`show mac-security`** command.

Parameter	Description
config	Displays general BaySecure configuration.
mac-address-table [address <macaddr>]	Displays contents of BaySecure table of allowed MAC addresses: • address — specifies a single MAC address to display; enter the MAC address
mac-da-filter	Displays MAC DA filtering addresses.

Table continues…

Parameter	Description
	Packets can be filtered from up to 10 MAC DAs or MAC SAs.
port <portlist>	Displays the BaySecure status of all ports.
security-lists	Displays port membership of all security lists.

Configuring MAC address security options

About this task

Configure the switch settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure MAC address security options:

   ```
   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}]
   ```

Variable definitions

Use the data in the following table to use the **`mac-security`** command.

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: • 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;

Table continues…

Parameter	Description
	a single port, a range of ports, several ranges, all ports, or no ports can be entered.
learning {enable|disable}	Specifies MAC address learning: • enable — enables learning by ports • disable — disables learning by ports
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.

Adding addresses to MAC security address table

About this task

Use the following procedure to assign either a specific port or a security list to the MAC address. This removes any previous assignment to the specified MAC address and creates an entry in the BaySecure table of allowed MAC addresses.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Add addresses to MAC security address table:

   ```
   mac-security mac-address-table address <H.H.H> {port <portlist> |
   security-list <1-128>}
   ```

Variable definitions

Use the data in the following table to use the **`mac-security mac-address-table`** command.

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

Assigning a list of ports to a security list

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Assign a list of ports to a security list:

   ```
   mac-security security-list <1–128> [add|remove] <portlist>
   ```

Variable definitions

Use the data in the following table to use the **`mac-security security-list`** command.

Variable	Value
<1–128>	Enter the number of the security list that you want to use.
<portlist>	Enter a list or range of port numbers.

Disabling MAC source address-based security

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable MAC security:

   ```
   no mac-security [security-list <1–128>]
   ```

Clearing the MAC address security table

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Clear the MAC address security table:

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

Variable definitions

Use the data in the following table to use the **`no mac-security mac-address-table`** command.

Variable	Value
address <H.H.H>	Enter the MAC address in the form of H.H.H
port <portlist>	Enter a list or range of port numbers.
security-list <1–32>	Enter the security list number.

Clearing the port membership of a security list

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Clear the port membership of a security list:

   ```
   no mac-security security-list <1-128>
   ```

Variable definitions

Use the data in the following table to use the **`mac-security security-list`** command.

Variable	Value
<1–128>	Enter the number of the security list that you want to clear.

Configuring MAC security for specific ports

About this task

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

Procedure

1. Enter Interface Configuration mode:

   ```
   enable

   configure terminal

   interface ethernet <port number>
   ```

2. Configure MAC security for specific ports:

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

   Note:

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

Variable definitions

Use the data in the following table to use the **`mac-security`** command.

Variable	Value
port <portlist>	Specifies the port numbers.
auto-learning|disable|enable|learning	Directs the specific port: • • auto-learning — configures MAC Auto- Learning • disable — disables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is performed • enable —enables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is performed • learning — disables BaySecure on the specified port and adds these port to the list of ports for which MAC address learning is performed

Filtering packets from specified MAC DAs

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Filter packets from specified MAC DAs:

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

Variable definitions

Use the data in the following table to use the **`mac-security mac-da-filter`** command.

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

Configuring MAC address autolearning

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

Configuring MAC address auto-learning aging time

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure MAC address auto-learning settings:

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

Variable definitions

Use the data in the following table to use the **`mac-security auto-learning aging-time`** command.

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

Variable	Value
	RANGE: 0 to 65535

Disabling MAC address auto-learning aging time

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable MAC address auto-learning aging-time:

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

Configuring MAC address auto-learning aging time to default

About this task

Use the following procedure to configure MAC address auto-learning aging time to default to configure the aging time for the MAC addresses automatically learned in the MAC security table. The default value is 60 minutes.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure MAC address auto-learning aging time to default:

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

Viewing the current Sticky MAC address mode

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the current Sticky MAC address mode:

   ```
   show mac-security config
   ```

Example

```
Switch>enable
Switch#show mac-security config
MAC Address Security: Disabled
```

```
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time:  60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Disabled
Learn by Ports: NONE
```

Enabling Sticky MAC address mode

Before you begin

You should disable autosave using the **`no autosave enable`** command when you enable Sticky MAC address.

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable Sticky MAC address mode:

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

Disabling Sticky MAC address mode

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable Sticky MAC address mode:

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

   OR

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

Enabling MAC security lock-out mode

About this task

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

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. Enable MAC security lock-out mode:

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

Disabling MAC security lock-out mode

About this task

Disable the lockout of specific ports from MAC-based security.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface ethernet <port number>
   ```

2. Disable MAC security lock-out mode:

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

   OR

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

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

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.

Chapter 14: MACsec

This chapter provides conceptual information on MACsec and procedures to configure MACsec using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

MACsec fundamentals

Note:

MACsec is not supported on ERS 4900 Series switches.

MACsec is based on the IEEE 802.1ae standard that allows authorized systems in a network to transmit data confidentially and to protect against data transmitted or modified by unauthorized devices.

MACsec enabled hosts encrypt and decrypt every frame exchanged between them using a MACsec key. The source MACsec host encrypts data frames and destination MACsec host decrypts the frames, ensuring delivery of the frame in its original condition to the recipient host. This ensures secure data communication.

MACsec is a link layer security standard which provides connectionless data integrity and optional confidentiality on a frame by frame basis. MACsec provides administrators additional options for securing their networks. It allows the administrator to secure those physical links identified as potential security concerns without regard to application or data type. It can protect against invalid network operations by preventing Ethernet frame snooping, injection, or modification between MACsec enabled devices. Because it is applied on a hop by hop basis, standard packet administrative functions such as QOS, filters, content inspection, and routing are unaffected.

You can configure MACsec on a physical port or on a trunk group level, which includes: Distributed MultiLink Trunking (DMLT), or Link aggregate group (LAG).

You configure a pre-shared key on either end of the MACsec link. The pre-shared key is an interface parameter, not a switch-wide parameter.

Note:

MACsec encrypts all packets. If you configure MACsec on one or more MultiLink Trunking (MLT) port members on one side, you must configure MACsec on the same port members on the other side. If you do not do this, the port can physically be up, but any overlying protocols can be down. You do not have to provision MACsec on all MLT port members, but if you

configure MACsec on an MLT port member on one side, you must also provision MACsec on the corresponding MLT port on the other side.

One way to detect a mismatch of MACsec configuration is to use Virtual Link Aggregation Protocol (VLACP) on the links.

MACsec provides security at the data link layer or the physical layer. It provides enhancements at the MAC service sub layer for its operation and services to the upper layer.

MACsec is an interface level feature and is disabled by default.

MACsec keys

MACsec provides industry-standard security through secure point-to-point Ethernet links. The point-to-point links are secured after matching security keys.

Security keys are of two types:

- connectivity association key (CAK), which is a configured *pre-shared key*. If you enable MACsec using the static connectivity association key (CAK) security mode.

  Important:

  The switch currently supports the configuration of a pre-shared key to enable MACsec using the static connectivity association key (CAK) security mode.

  The CAK must be identical across both ends of MACsec links.

- secure association key (SAK), which is a configured *static secure association key*. If you enable MACsec using the static secure association key (SAK) security mode. SAKs are short-lived keys derived from the CAK or pre-configured for a particular secure channel (SC). MACsec uses a timer to refresh these keys so that the key, as well the session, is secure.

  MACsec uses derived keys to encrypt or decrypt data at each end of the MACsec links.

Integrity Check Verification

MACsec ensures data integrity using Integrity Check Verification (ICV). MACsec introduces an 8 or 16 byte SecTag after the Ethernet header, and an 8 or 16 byte calculated ICV after the Encrypted Payload. MACsec computes the ICV for the entire frame, starting from the Ethernet header, SecTag until the Checksum. The receiving side recalculates the ICV after data decryption and verifies if the received ICV and computed ICV match. If the ICVs do not match, it indicates that data is modified, and MACsec drops the frame.

Connectivity associations (CA) and secure channels (SC)

You configure MACsec in connectivity associations. You can enable MACsec after you attach a connectivity association to an interface. To use the static CAK security mode to enable MACsec, you must create, and configure connectivity associations on both ends of the link.

A connectivity association (CA) is a logical representation of a MACsec domain within a network. Each connectivity association is associated with a connectivity association key (CAK). MACsec links are associated with a CA to establish end-to-end MACsec communication. Every MACsec enabled interface is a member of one connectivity association. Switch ports are members of a connectivity association, and can only be a member of one connectivity association.

A secure channel (SC) is a unidirectional channel that connects two endpoints of MACsec. A secure channel is a long-term relationship that persists through the sequence of secure associations. A secure association (SA) is a short-lived relationship within an SC. MACsec identifies each security association by AN, and supported Secure association key (SAK), which is derived from the CAK. The secure association key is used on both ends of MACsec links to encrypt and decrypt the frames. SAKs are frequently refreshed for security reasons. Periodically changing SAs allows the use of fresh keys without terminating the SC relationship.

You configure connectivity associations. Secure channels and secure associations are internally created in the hardware.

MACsec 2AN and 4AN mode

MACsec 2AN mode implementations use two security associations (SA) for each secure channel (SC) and symmetric keys on both MACsec endpoints. In 2AN mode the same key is used for both egress and ingress SAs.

MACsec 4AN mode generates four Secure Associations Keys (SAK) per secure channel. Each SA on each direction is secured with a different key. 4AN mode uses enhanced hashing algorithm to derive eight SAKs, and uses asymmetric keys on both ends. You can use the macsec connectivity-association command to configure different (asymmetric) transmit keys for each endpoint by using the key-parity keyword. If you do not specify a value for key-parity, the connectivity association is created in 2AN mode.

In both 2AN and 4AN modes the keys are derived from the same CAK.

Macsec components

MACsec has three major components:

- Security entity (SecY) — SecY is the entity that operates the MACsec protocol within the system. You configure a secure community association (CA) to meet the requirements of MACsec for connectivity between stations that attach to an individual LAN. Unidirectional

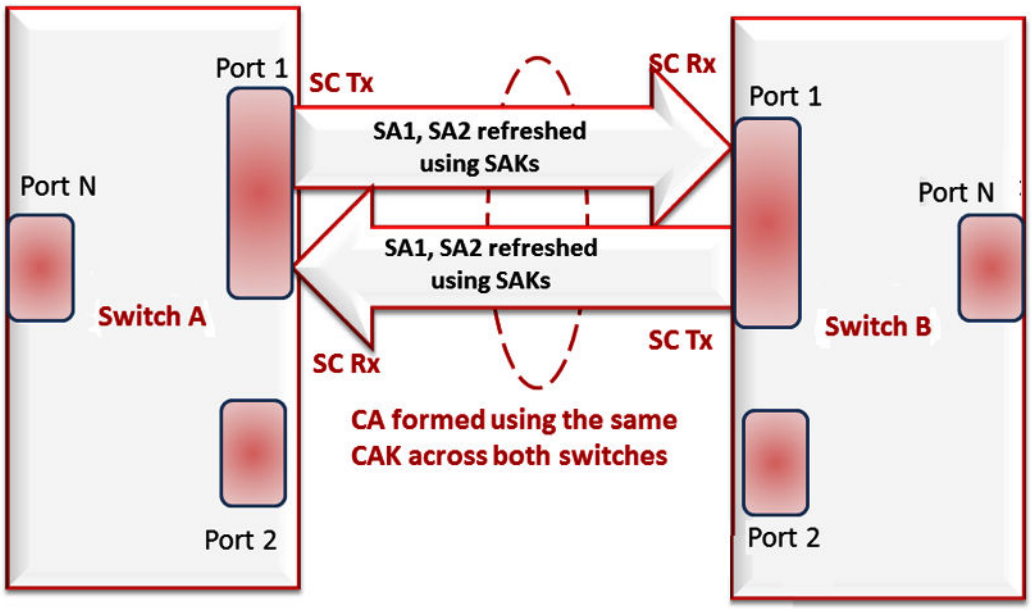
secure channels (SC) support each CA. Each SC supports secure transmission of frames through the use of symmetric key cryptography from one of the systems to all the others in the CA.

Each SecY transmits frames conveying secure MACsec service requests on a single SC, and receives frames conveying secure service indications on separate SCs, one for each of the other SecYs that participate in the secure CA.

A connectivity association (CA) is a logical representation of a MACsec domain within a network. Each connectivity association is associated with a connectivity association key (CAK). MACsec links are associated with a CA to establish end-to-end MACsec communication. Every MACsec enabled interface is a member of one connectivity association. Switch ports are members of a connectivity association, and can only be a member of one connectivity association.

A secure channel (SC) is a unidirectional channel that connects two endpoints of MACsec. A secure channel is a long-term relationship that persists through the sequence of secure associations. An SC is a unidirectional point to multipoint communication, and can persist through Secure Association Key (SAK) changes. A sequence of Secure Associations (SAs) support each SC and allow for the periodic use of fresh keys without terminating the relationship. A single secret key or a set of keys support each SA, where the cryptographic operations used to protect one frame require more than one key. An SCI identifies each SC. An SCI is comprised of a unique 48-bit universally administered MAC address, identifying the system to which the transmitting SecY belongs, concatenated with a 16-bit port number, identifying the SecY within that system.

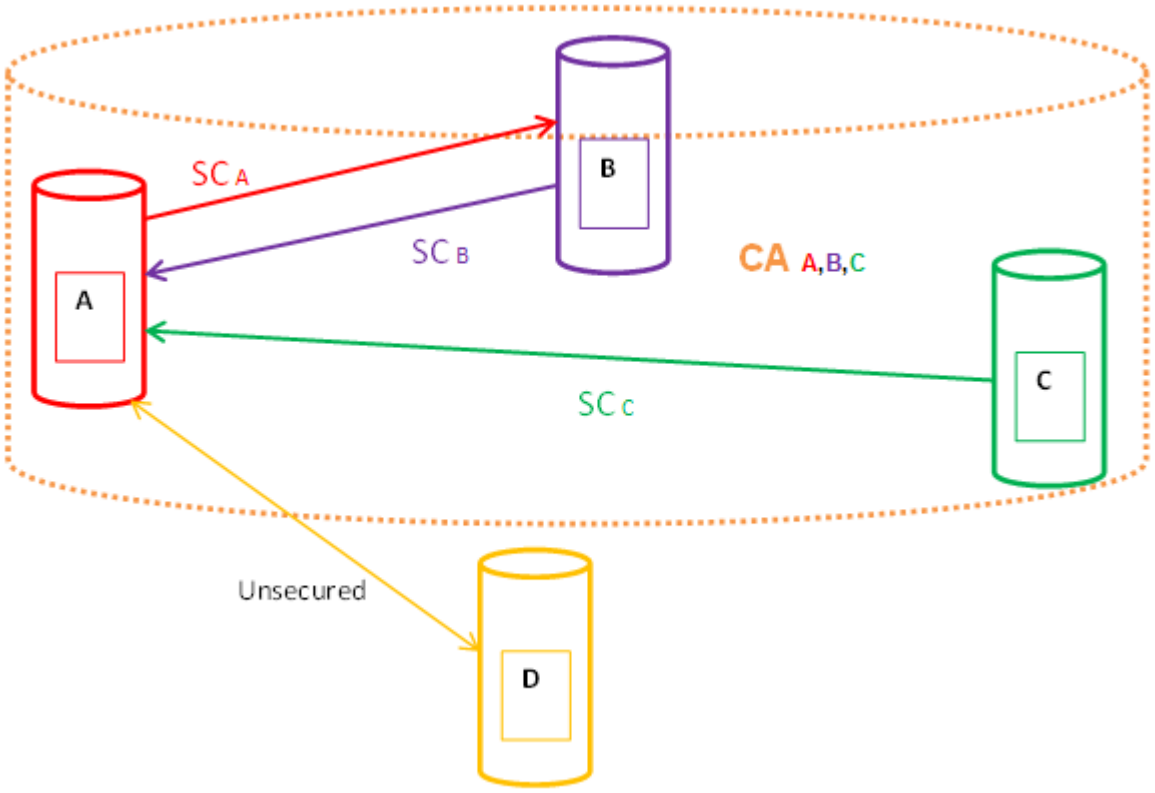
The SCI concatenated with a two-bit AN identifies each SA. The Secure Association Identifier (SAI) created allows the receiving SecY to identify the SA, and the SAK used to decrypt and authenticate the received frame. The AN, and hence the SAI, are only unique for the SAs that can be used or recorded by participating SecYs at any instant.



- Key agreement entity (KaY) — The KaY in MACsec is responsible for CAK and SAK computations, distributions, and maintenance of those keys. CAK is a global key, which is persistent until the CA exists. When you configure the CAK, ensure that it is identical across MACsec links. SAK are short-lived keys derived from the CAK, or pre-configured for a particular SC. MACsec uses a timer to refresh these keys so that the key, as well the session, is secure.
- Integrity check verification (ICV) or Cryptographic entity — The Cryptographic entity provides integrity check protection and validation for frames transmitted or received through the SecY layer. The ICV is calculated for the frame SA/DA, SecTag, User Payload, and CRC. The calculated ICV is appended at the end-of-frame, recalculated at the receiver side of MACsec link and validated to see if they are equal. This is called Integrity Check Verification (ICV). The frames that pass the integrity check are further processed, while the system drops the frames that fail the integrity check.

  MACsec configuration provides options to encrypt user payload or send in the clear. The option to start the encryption from N bytes after the Ethernet header also exists.

In the following figure, CA connects switches A, B, and C by their respective SC and SAK. Station D cannot participate in the secure communication between A, B, or C as station D does not know the SAK.



Macsec operation

As shown in the following figure, a host that connects to Switch A sends an Ethernet frame to a host that connects to Switch B. Switch A encrypts the frame, excluding the Ethernet header and optionally the 802.1Q header. Switch A also appends MACsec information like SecTag and ICV to the encrypted payload and transmits the frame using normal frame transmission. This process ensures data confidentiality.

On receiving the frame, Switch B decrypts the frame. Switch B recalculates the ICV using a MACsec key and the SecTag present in the frame. If the ICV present in the received frame matches the recalculated ICV, the switch processes the frame. If the two ICVs do not match, the switch discards the frame. This process ensures data origin authenticity and data integrity. The encryption and decryption algorithms follow the AES-GCM-128 standard.

The MACsec key between switches A and B are statically pre-configured.

MACsec Performance

To monitor MACsec performance, view the performance statistics. For information on the supported statistics, see Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series.

MACsec support limitations

MACsec support has the following limitations:

- Only Point-to-point operation mode is supported and is limited to a single Connectivity Association applied to a physical port.
- MACsec Key Agreement is implemented in a limited form. The master keys are not derived from the 802.1x EAPoL exchanged, as described in IEEE 802.1x-2010, but are statically assigned by the administrator. This is the Pre Shared Key mode described in IEEE 802.1x-2010.

Note:

MACsec use on access ports is not supported on the 5928MTS-uPWR model.

MACsec statistics

MACsec is an 802.1AE IEEE standard that allows authorized systems in a network to transmit data confidentially and to take measures against data transmitted or modified by unauthorized devices.

The switch supports the following statistics that provide a measure of MACsec performance.

Note:

If encryption is enabled, the following MACsec statistics are not incremented:

- *Octets Validated* for secure-channel inbound statistics
- *Octets Protected* for secure-channel outbound statistics

Table 18: General MACsec statistics

Statistics	Description
TxUntaggedPkts	Specifies the number of transmitted packets without the MAC security tag (SecTAG), with MACsec disabled on the interface.
TxTooLongPkts	Specifies the number of transmitted packets discarded because the packet length is greater than the Maximum Transmission Unit (MTU) of the Common Port interface.
RxUntaggedPkts	Specifies the number of received packets without the MAC security tag (SecTAG), with MACsec not operating in strict mode.
RxNoTagPkts	Specifies the number of received packets without the MAC security tag (SecTAG), with MACsec operating in strict mode.
RxBadTagPkts	Specifies the number of received packets discarded with an invalid SecTAG or with a zero value Packet Number (PN)/invalid Integrity Check Value (ICV).
RxUnknownSCIPkts	Specifies the number of packets received with an unknown Secure Channel Identifier (SCI) and with MACsec not operating in strict mode
RxNoSCIPkts	Specifies the number of packets received with an unknown Secure Channel Identifier (SCI) and with MACsec operating in strict mode.
RxOverrunPkts	Specifies the number of packets discarded because the number of received packets exceeded the cryptographic performance capabilities.

Table 19: Secure-channel inbound MACsec statistics

Statistics	Description
PortId	Specifies the port.
Late Packets	Specifies the number of packets received that have been discarded for this Secure Channel (SC) with Replay Protect enabled.
InvalidPkts	Specifies the summation of all packets received that were not valid for this SC, with MACsec operating in check mode.

Table continues…

Statistics	Description
Delayed Packets	Specifies the summation of packets for this SC, with the Packet Number (PN) of the packets lower than the lower bound replay protection PN.
Unchecked Packets	The total number of packets for this SC that: • were encrypted and had failed the integrity check • were not encrypted and had failed the integrity check • were received when MACsec validation was not enabled
Octets Validated	Specifies the number of octets of plaintext recovered from received packets that were integrity protected but not encrypted.
Octets Decrypted	Specifies the number of octets of plaintext recovered from received packets that were integrity protected and encrypted.

Table 20: Secure-channel outbound MACsec statistics

Statistics	Description
PortId	Specifies the port.
Octets Protected	Specifies the number of plain text octets that are integrity protected but not encrypted on the transmitting SC.
Octets Encrypted	Specifies the number of plain text octets that are integrity protected and encrypted on the transmitting SC.

MACsec configuration using CLI

This section describes how to configure MACsec using CLI.

Configuring a connectivity association

The MACsec connectivity association must exist and be configured before it is applied to one or more ports. A connectivity association is configured for manual mode. The connectivity association must be unassigned (for example, inactive) to any port in order to be configured or reconfigured. Live configuration is not supported.

Note:

Only single channel mode is supported. The key parity must be different on the link ends. One keygen must be odd and the other even.

If you do not specify the key parity, the operating mode is 2AN with 2 keys per SC. If you specify the key parity, the operating mode is 4AN with 4 keys per SC.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure a connectivity association (CA):

   ```
   [no] macsec connectivity-association WORD<5-15> connectivity-
   association-key WORD<10-32> [key-parity {even | odd}]
   ```

3. Enter Ethernet Interface Configuration mode:

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

4. Associate a port with CA:

   ```
   connectivity-association <ca-name>
   ```

5. Enable MACsec on the port:

   ```
   macsec enable
   ```

Example

Configure a connectivity association and enable MACsec on a port:

```
Switch>enable
Switch#configure terminal
Switch(config)#macsec connectivity-association caname1 connectivity-association-
key1029384756abcdef key-parity even|odd
Switch(config)#interface ethernet 2
Switch(config-if)#macsec connectivity-association caname1
```

Variable definitions

Use the data in the following table to use the **macsec** command.

Variable	Definition
connectivity-association *WORD<5–15>*	Specifies a connectivity-association name. It is a 5 to 15 character alphanumeric string.

Table continues…

Variable	Definition
connectivity-association-key *WORD<10–32>*	Specifies the hexadecimal value of the connectivity-association key (CAK). A 32 character string is recommended.
key-parity {even | odd}	Chooses even or odd generated keys.

Configuring MACsec encryption on a port

Use the following procedure to enable or disable encryption on a MACsec capable port. The default is disabled.

About this task

If you disable encryption, MACsec forwards traffic in clear text. You can view that data that is not encrypted in the Ethernet frame that travels across the link. Even if you disable encryption the MACsec header applies to the frame and integrity checks make sure that traffic has not been tampered with.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. At the prompt, enter the following command:

   ```
   macsec encryption enable
   ```

3. To disable encryption, enter the following command:

   ```
   no macsec encryption enable
   ```

Example

```
Switch>enable
Switch#configure terminal
Switch(config)#interface ethernet 2
Switch(config-if)#macsec encryption enable
```

Configuring the confidentiality offset on a port

The encryption offset option provides a way to start encryption after a few bytes following the Ethernet header. The encryption offset facilitates traffic flow inspection and classification on intermediate devices by not encrypting the Network Layer header for IPv4 or IPv6. For instance, if you configure the offset to 30, the IPv4 header and the TCP/UDP header are not encrypted. If you configure the offset to 50, the IPv6 header and the TCP/UDP header is not encrypted.

The default is disabled.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. At the prompt, enter the following command:

   ```
   macsec confidentiality-offset <30|50>
   ```

3. To enable encryption, enter the following command:

   ```
   macsec encryption enable
   ```

4. To disable the confidentiality offset on the port, enter the following command:

   ```
   no macsec confidentiality-offset
   ```

Example

```
Switch>enable
Switch#configure terminal
Switch(config)#interface ethernet 2
Switch(config-if)#macsec encryption enable
Switch(config-if)#macsec confidentiality-offset 30
```

Variable definitions

Use the data in the following table to use the **`macsec confidentiality-offset`** command.

Variable	Definition
offset <*30*|*50*>	Specifies the encryption offset to 30 or 50 bytes from the Sec Tag.

Configuring MACsec replay-protect on a port

Use the following procedure to set the anti-replay protect window size. This option provides a limit to out of order reception.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. At the prompt, enter the following command:

   ```
   macsec replay-protect enable window-size <window_size>
   ```

Variable definitions

Variable	Definition
window-size <window_size>	Sets the window size value.

Viewing the MACsec connectivity association details

Use the following procedure to the MACsec connectivity association (CA) details.

Note:

This command displays the MACsec connectivity association (CA) details, including the MD5 hashed value of the CA key.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter the following command:

   ```
   show macsec connectivity-association <ca-name>
   ```

Example

```
Switch>enable
Switch#show macsec connectivity-association ca333

================================================================================
                    MACSEC Connectivity Associations Info
================================================================================
Connectivity             Connectivity
AN_Mode /                       Port
Association          Name Association Key Hash          TxKeyParity              Members
--------------------------------------------------------------------------------
--------------------------------------------
ca333           1304a8fcc51296e7229683ff6882424a       4AN / Even               1/97
```

Viewing MACsec status

About this task

This command displays the status for the following:

- MACsec status
- MACsec encryption status
- The associated Connectivity Association (CA) name

Note:

If you do not specify a port number, the information on all MACsec capable interfaces is displayed.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the MACsec status:

   ```
   show macsec status <ports>
   ```

Example

```
Switch>enable
Switch>show macsec status
```

Clearing MACsec stats

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Clear MACsec stats:

   ```
   macsec clear-stats [port <ports>]
   ```

3. Enter Ethernet Interface Configuration mode:

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

4. Clear MACsec stats on ports:

   ```
   macsec clear-stats port <ports>
   ```

Viewing the MACsec connectivity association details

Use the following procedure to the MACsec connectivity association (CA) details.

Note:

This command displays the MACsec connectivity association (CA) details, including the MD5 hashed value of the CA key.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter the following command:

   ```
   show macsec connectivity-association <ca-name>
   ```

Example

```
Switch>enable
Switch#show macsec connectivity-association ca333

================================================================================================
                    MACSEC Connectivity Associations Info
================================================================================================
Connectivity             Connectivity
AN_Mode /                       Port
Association          Name Association Key Hash          TxKeyParity               Members
------------------------------------------------------------------------------------------------
------------------------------------------------
ca333           1304a8fcc51296e7229683ff6882424a       4AN / Even                1/97
```

Viewing MACsec statistics

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View MACsec statistics:

   ```
   show macsec statistics [<port>]
   ```

3. View the secure-channel inbound MACsec statistics:

   ```
   show macsec statistics <port> secure-channel inbound
   ```

4. View the secure-channel outbound MACsec statistics:

   ```
   show macsec statistics <port> secure-channel outbound
   ```

Example

Display general MACsec statistics, inbound MACsec statistics, and outbound MACsec statistics:

```
Switch(config)#show macsec statistics 2/1 secure-channel inbound
2017-11-10 16:45:12 GMT+03:00    UTC time: 2017-11-10 13:45:12


================================================================================
                 MACSEC Port Inbound Secure Channel Statistics

================================================================================
            Late        Delayed        Unchecked     Octets          Octets
PortId     Packets      Packets        Packets       Validated       Decrypted
--------------------------------------------------------------------------------
2/1         0            0              0             0               0
```

```
witch(config)#show macsec statistics 2/1 secure-channel outbound
2017-11-10 16:53:56 GMT+03:00    UTC time: 2017-11-10 13:53:56


================================================================================
                 MACSEC Port Outbound Secure Channel Statistics
```

```
================================================================================
          Octets          Octets
PortId    Protected       Encrypted
--------------------------------------------------------------------------------
2/1        0              0
```

Variable definitions

Use the data in the following table to use the **`show macsec statistics`** command.

Variable	Definition
<port>	Specifies the port for which to display MACsec statistics.

MACsec configuration using EDM

This section describes how to configure MACsec using Enterprise Device Manager (EDM).

Configuring connectivity associations

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > Chassis**.
2. Click **Chassis**.
3. In the Chassis window, click the **MACsec** tab.
4. Click **Insert**.
   a. In the **AssociationName** field, type the connectivity-association name.
   b. In the **AssociationKey** field, type the value of the connectivity-association key.

      Note:

      The connectivity-association key appears as an MD5-hashed text in the MAC security table.

   c. Click **Insert** to save the configuration.
5. Click **Apply**.

Field descriptions

Use the data in the following table to use the **`MACsec`** tab.

Name	Definition
AssociationName	Specifies a name for each connectivity association configured on the device.
AssociationKey	Specifies a pre-shared, connectivity association key associated with each connectivity association configured on the device.
AssociationPortMembers	Specifies the set of ports for which this connectivity association is associated.
AssociationTxKeyParity	Specifies the key parity for 4AN mode- Default is none (mode 2AN) • even — choose even keys generated • odd — choose odd keys generated

Associating a port with a connectivity association

Procedure

1. In the Device Physical View, click on the port that you want to associate with the connectivity association.
2. In the navigation tree, expand the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **MACsec** tab.
5. In the **CAName** field, type the connectivity-association name.
6. In the **OffsetValue** field, select the value of confidentiality offset to be achieved.
7. Select **EncryptionEnable** to enable encryption for the frames transmitted on ports.
8. Select **MACsec Enable** to enable MACsec on the port.
9. Select **Replay Protect** to enable MACsec port protection from replay-attacks.
10. If **Replay Protect** is enabled, enter a value <5–500> in the Replay Protect Window Size field.
11. Click **Apply** to save the configuration.

Field definitions

Name	Definition
CAName	Specifies the name of the connectivity association attached to the port or interface.
OffsetValue	Offsets MACsec encryption in an IPv4 TCP/UDP header or IPv6 TCP/UDP header.

Table continues…

Name	Definition
	The confidentiality offset provides a way to start encryption after a few bytes following the Ethernet header. The confidentiality offset facilitates traffic flow inspection and classification on intermediate devices by not encrypting the Network Layer header for IPv4 or IPv6. For instance, if you configure the offset to 30, the IPv4 header and the TCP/UDP header are not encrypted. If you configure the offset to 50, the IPv6 header and the TCP/UDP header is not encrypted.
EncryptionEnable	Specifies the encryption status per port. Use this field to enable or disable encryption for each MACsec capable port.
Macsec Enable	Enables or disables MACsec on the port.

Viewing MACsec interface statistics

Procedure

1. In the Device Physical View tab, select the port for which you need to view the MACsec interface statistics
2. In the navigation tree, click **Edit > Chassis**.
3. Click the **MACsec Interface Stats** tab.

Note:

Use the **Clear Stats** button to the clear MACsec interface statistics. The Clear Stats button is available to clear single-port as well as multiple-port MACsec interface statistics.

Field definitions

The following table describes the fields in the **MacSec Interface Stats** tab.

Name	Definition
TxUntaggedPkts	Specifies the number of transmitted packets without the MAC security tag (SecTAG), with MACsec disabled on the interface.
TxTooLongPkts	Specifies the number of transmitted packets discarded because the packet length is greater than the maximum transmission unit (MTU) of the common port interface.

Table continues…

Name	Definition
RxUntaggedPkts	Specifies the number of received packets without the MAC security tag (SecTAG), with MACsec not operating in strict mode.
RxNoTagPkts	Specifies the number of received packets without the MAC security tag (SecTAG), with MACsec operating in strict mode.
RxBadTagPkts	Specifies the number of received packets discarded with an invalid SecTAG, or with a zero value packet number (PN), or invalid Integrity Check Value (ICV).
RxUnknownSCIPkts	Specifies the number of packets received with an unknown secure channel identifier (SCI), and with MACsec not operating in strict mode.
RxNoSCIPkts	Specifies the number of packets received with an unknown secure channel identifier (SCI), and with MACsec operating in strict mode.
RxOverrunPkts	Specifies the number of packets discarded because the number of received packets exceeded the cryptographic performance capabilities.

Viewing secure channel (SC) inbound statistics

Procedure

1. In the Device Physical View tab, select the port for which you need to view the SC inbound statistics
2. In the navigation tree, expand the following folders: **Edit > Port > General**.
3. Click the **SC Inbound Stats** tab.

Note:

Use the **Clear Stats** button clear single-port secure channel inbound statistics. The Clear Stats button is available to clear single-port, as well as multiple-port MACsec interface statistics.

Field definitions

The following table describes the fields in the **SC Inbound Stats** tab.

Name	Definition
UnusedSAPkts	Specifies the summary of received unencrypted packets on all SAs of this secure channel, with MACsec not in strict mode.
NoUsingSAPkts	Specifies the summary of received packets that were discarded along with either encrypted packets or

Table continues…

Name	Definition
	packets that were received with MACsec operating in strict mode.
LatePkts	Specifies the number of packets received that have been discarded for this secure channel (SC) with Replay Protect enabled. **Note:** The current release does not support Replay Protect
NotValidPkts	Specifies the summary of packets that were discarded in all SAs of the SC because they were not valid with one of the following conditions: • MACsec was operating in strict mode. • The packets received were encrypted but contained erroneous fields.
InvalidPkts	Specifies the summary of all packets received that were not valid for this SC, with MACsec operating in check mode.
DelayedPkts	Specifies the summary of packets for this SC, with the packet number (PN) of the packets lower than the lower bound replay protection PN. **Note:** The current release does not support Replay Protect.
UncheckedPkts	The total number of packets for this SC that: • Were encrypted and had failed the integrity check. • Were not encrypted and had failed the integrity check. • Were received when MACsec validation was not enabled.
OKPkts	Specifies the number of octets of plaintext recovered from received packets that were integrity protected but not encrypted.
OctetsDecrypted	Specifies the number of octets of plaintext recovered from received packets that were integrity protected and encrypted.

Viewing secure channel (SC) outbound statistics

Procedure

1. In the Device Physical View tab, select the port for which you need to view the SC outbound statistics
2. In the navigation tree, expand the following folders: **Edit > Port > General**.
3. Click the **SC Outbound Stats** tab.

Note:

Use the **Clear Stats** button clear single-port secure channel outbound statistics. The Clear Stats button is available to clear single-port, as well as multiple-port MACsec interface statistics.

Field definitions

The following table describes the fields in the **SC Outbound Stats** tab.

Name	Definition
ProtectedPkts	Specifies the number of integrity protected but not encrypted packets for this transmitting SC.
EncryptedPkts	Specifies the number of integrity protected and encrypted packets for this transmitting SC.
OctetsProtected	Specifies the number of plain text octets that are integrity protected but not encrypted on the transmitting SC.
OctetsEncrypted	Specifies the number of plain text octets that are integrity protected and encrypted on the transmitting SC.

Chapter 15: Secure AAA server communication

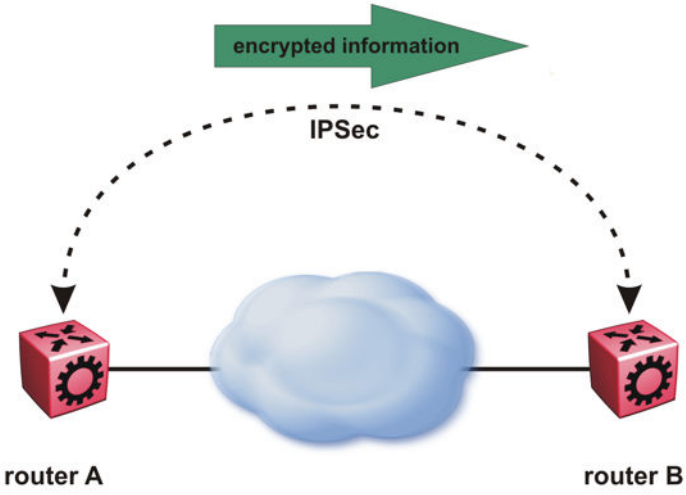
This chapter provides conceptual information on Secure AAA server communication and procedures to configure Secure AAA server communication using Command Line Interface (CLI).

Secure AAA server communication

An AAA server program deals with requests for access to computer resources and provides authentication, authorization, and accounting (AAA) services. The switch communicates with AAA servers using Remote Authorization Dial-in User Service (RADIUS). It is not sufficient to protect authentication information with only RADIUS. To provide additional security to the traffic in the communication channel, this release adds support for IP Security (IPsec) for the AAA server communication.

IPsec provides the ability to secure RADIUS servers against unwanted traffic by filtering on specific network adapters, by allowing or blocking specific protocols and enabling the server to selectively allow traffic from specific source IP addresses.

The following diagram shows the communication between AAA client and AAA server. The IPsec module on the client encrypts the packets to the AAA server and decrypts the packets from the AAA server. Similarly, the IPsec module on the server encrypts or decrypts the packets to or from the client.



To implement secure AAA server communication, the software supports the following:

- IPsec with Internet Key Exchange (IKE) protocol.
- IPv4 implementation of IPsec, is mainly for protocols involved in communication with AAA servers, that is, RADIUS. UDP and TCP protocols are supported but it is recommended to only apply IPsec to the RADIUS protocol.
- Digital signature as authentication method for IKE, in addition to the pre-shared key authentication method.
- Automatic and manual keying for session establishment. IKE is the default automated key management protocol for IPsec.
- IKEv1 protocol

IP security

Internet Protocol Security (IPsec) ensures the authenticity, integrity, and confidentiality of data at the network layer of the Open System Interconnection (OSI) stack.

IPsec secures the AAA server communication using packet filtering and cryptography. Cryptography provides user authentication, ensures data confidentiality and integrity, and enforces trusted communication.

Internet Key Exchange protocol

Internet Key Exchange (IKE) protocol sets up a Security Association (SA) in IPsec. SA is the relationship between two network devices that define attributes such as authentication mechanism, encryption and hash algorithms, exchange mode, and key length for secured communications. SA should be agreed to by both the devices.

The IKE protocol is based on Internet Security Association and Key Management Protocol (ISAKMP) which helps in building a secured connection between two or more hosts using the following concepts:

- authentication
- encryption

- key management
- security association (SA)
- policy

IKE uses a key exchange mechanism based on the Diffie-Hellman encryption key exchange protocol. IKE provides periodic automatic key renegotiation, pre-shared and public key infrastructures, and anti-replay defence. It is layered on top of the UDP protocol and uses UDP port 500 to exchange information between peers.

IKE phases

A switch negotiates with a peer using IKE in two phases.

- In phase 1, the switch negotiates the IKE SA to protect the negotiations that take place in phase 2. The SAs negotiated in phase 1 are bi-directional, and are applicable to traffic originating in both directions.
- In phase 2, the peers negotiate and establish the SAs for IPsec and session keys through quick mode. A Diffie-Hellman key exchange is done to achieve perfect forward secrecy, which ensures that the compromise of a single key does not permit access to data other than that protected by that compromised key. The SAs in phase 2 are uni-directional. They are used according to the direction of the traffic. The quick mode is initiated by either of the peer endpoints irrespective of who initiated phase 1.

IKE modes

There are two modes of exchanging messages in Phase 1:

- Main mode

  This is a secure mode of exchanging messages. It allows protection of the confidentiality of the peers during negotiation. This mode provides more flexibility in proposals compared to aggressive mode. As the main mode requires a total of 6 messages to be exchanged between peers, it is more time consuming.

- Aggressive mode

  This mode is less secure than the main mode. It does not protect the confidentiality of the peers. However, it requires only a total of 3 messages to be exchanged for phase 1, which makes this mode faster than the main mode. The number of total message exchange is reduced in this mode because some messages are embedded in other messages.

The mode of message exchange in phase 2 is called quick mode. In this mode a total of 3 messages are exchanged between the peers. This mode is used to establish IPsec SA. The negotiations in the quick mode are protected during the phase 1 negotiations in main mode.

IKE policies

A combination of security parameters used during the IKE SA negotiation is called a policy. The policies must be configured on both the peers and at least one of the policies should match on both ends to have a successful negotiation for. If a policy is not configured on both peers or if a policy does not match on both ends, an SA cannot be setup and data cannot be exchanged.

The following are the attributes of an IKE policy:

- Encryption — This is the cryptographic algorithm that is sent in the proposal by the initiator or responder during the phase 1 negotiation. This cryptographic algorithm is used to encrypt phase 2 negotiation messages. The supported encryption algorithms are:
  - DES
  - 3ES
  - AES
- Hash function — This function is used as part of the authentication mechanism during the authentication of peers in phase 1. It is always used with the authentication algorithm. The supported values are:
  - MD5
  - SHA1
  - SHA256
- Authentication — This process authenticates the peers. Following are the supported

  authentication modes:
  - Digital Signatures — The digital signatures use digital certificate which is signed by the certificate authority (CA) for authentication.
  - Pre-shared keys (PSK) — The PSKs are shared out-of-band between the peers before hand. Using PSK in main mode exchange limits identifying the peer to an IP address (and not host name).
- Diffe-Hellman (DH) Group — This is an algorithm used by two peers that are unknown to each other to establish a shared secret key. This key that is decided during phase 1 is used to encrypt subsequent message exchanges during phase 2 to establish security associations (SA) and security policies (SP) for IPsec sessions. The supported DH Groups are as follows:
  - Group 1 (MODP768)
  - Group 2 (MODP1024)
  - Group 14 (MODP2048)
- Lifetime — This is a time and data limit agreed by peers to protect an SA from getting compromised. It ensures that the peers renegotiate the SAs just before the lifetime value expires, that is, when the time limit is reached.
- Dead-peer detection – This is a process in which the switch waits for a response from peer for a limited number of seconds before declaring the peer as dead. It is a keep-alive mechanism required to perform IKE peer fail-over and to reclaim lost resources by freeing up SAs that are no longer in use.

IKE authentication

The security gateway of a peer must authenticate the security gateway of the peer it intends to communicate with. This ensures that IKE SAs are established between the peers. The switch supports the following two authentication methods:

- Digital certificates (using RSA algorithms)

  For digital certificate authentication, the initiator signs the message interchange data using the private key. The responder uses the public key of the initiator to verify the signature. The public

key is exchanged by messages containing an X.509v3 certificate. This certificate provides an assurance that the identity of a peer, as represented in the certificate, is associated with a particular public key.

- Pre-shared keys

  Pre-shared key authentication, the same secret must be configured on both security gateways before the gateways can authenticate each other.

Signature authentication

The switch receives the digital signature of its peer in a message exchange. The switch verifies the digital signature by using the public key of the peer. The certificate of the peer, received during the IKE negotiation, contains the public key. To ensure that the peer certificate is valid, the switch verifies its digital signature by using the certificate authority (CA) public key contained in the root CA certificate. The switch and its IKE peer require at least one common trusted root CA for authentication to work.

When IKE is configured to use digital certificates for authentication, the certificates are retrieved from the trusted certificate store in the switch, based on the provided distinguished name. The certificates received from the peer are verified with the public key.

Secure AAA server communication and IKE limitations

This section describes the limitations associated with secure AAA server communication feature.

- IKE version 2 is not supported in this release.
- AAA server protection is provided only for SSH/CLI/WEB/Telnet/Console Access Protection.
- FQDN (Fully Qualified Domain Names) is not supported to identify endpoints. This is because the user configures the IP address for the AAA servers in the switch.
- XAUTH (2-factor authentication) is not supported.
- Domain of Interpretation is not supported other than for IPsec.
- NAT Traversal is not supported.
- Custom IKE messages and vendor ID for the messages are not supported.
- IKE fragmentation is not supported.

Internet Protocol Security

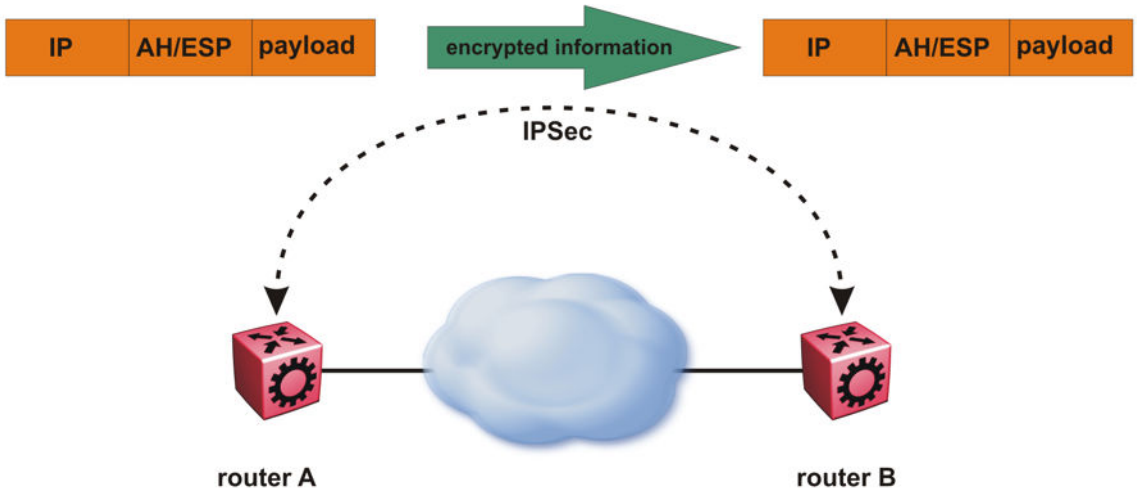
The following sections describe Internet Protocol Security (IPsec) and its configuration.

IPsec

Internet Protocol Security (IPsec) ensures the authenticity, integrity, and confidentiality of data at the network layer of the Open System Interconnection (OSI) stack.

The IPsec feature is a set of security protocols and cryptographic algorithms that protect communication in a network. Use IPsec in scenarios where you need to encrypt packets between two hosts, or two routers, or a router and a host.

The following figure displays the movement of traffic using IPsec.



The IPsec feature uses security ciphers and encryption algorithms like AES, DES, and 3DES to ensure confidentiality of data, and keyed MAC for authenticity of data. The encryption algorithms require shared keys to secure the communication. The IPsec feature supports both IPv4 and IPv6 interfaces.

To configure IPsec, you create an IPsec policy, and then link the IPsec policy to an interface. You also link each IPsec policy to an IPsec security association. The IPsec policies define the amount of security applied to specific traffic on a specific interface.

The IPsec feature supports the following security protocols:

- Encapsulating security payload (ESP)
- Authentication header (AH)

The device restricts IPsec encryption to control traffic through the CPU. The IPsec feature processes either the ingress, the egress, or both the egress and ingress control packets to and from the CPU.

Important:

The device restricts IPsec to transport mode only.

The device checks every ingress or egress packet for the IPsec base protocol, either AH or ESP. The base protocol interacts with the security policy database (SPD) and security association

database (SADB) to check the level of security to apply to the packet. The device consults the SPD for both ingress and egress traffic. For egress traffic, the device consults the SPD to determine if IPsec needs to apply security considerations. For ingress traffic, the device consults the SPD to determine whether the traffic received with IPsec encapsulation complies with the policies defined in the system.

Authentication header

The authentication header (AH) authenticates IP traffic and ensures you connect with who you want to connect. The authentication header can detect if data is altered in transit and protect against replay attacks. The authentication header does not encrypt traffic.

The authentication header provides a small header that precedes the payload with the use of the security parameters index (SPI) and sequence number. The authentication header provides:

- IP datagram sender authentication by HMAC or MAC
- IP datagram integrity assurance by HMAC or MAC
- Replay detection and protection by sequence number

The IPsec feature inserts the AH header after the IP header in transport mode. Transport mode with AH authenticates only the payload of the IP packet. The device only supports transport mode.

The device does not support tunnel mode. Tunnel mode authenticates the entire IP packet, including the IP header and data, to provide a secure hop between two hosts, two routers, or a router and a host.

The following figures show an original IP packet and an IP packet with an AH header.

Figure 19: Original IP packet

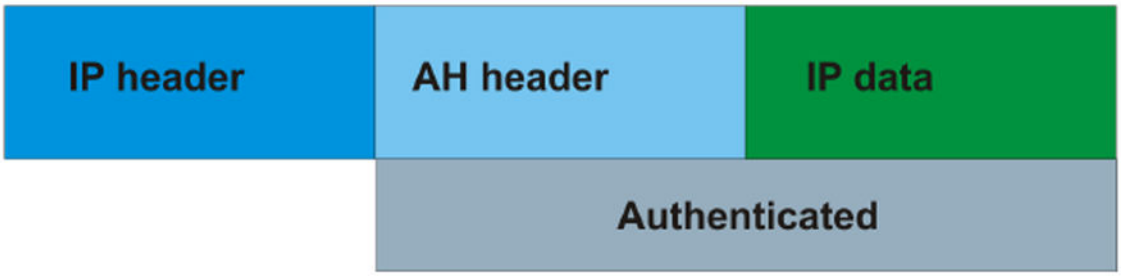


Figure 20: AH in transport mode

Encapsulating security payload

The encapsulating security payload (ESP) encrypts traffic with use of encryption algorithms, such as 3DES, AES-CBC, and AES-CTR. The security association specifies the algorithm and key used in ESP.

The encapsulating security payload can protect origin authenticity, integrity, and confidentiality of packets. ESP supports encryption-only and authentication-only configurations. The IPsec feature inserts the ESP header after the IP header and before the next layer protocol header in transport mode. Transport mode with ESP encrypts or authenticates only the payload of the IP packet. The device only supports transport mode in this release.

The device does not support tunnel mode in this release. Tunnel mode encrypts or authenticates the entire IP packet, including the IP header and data, to provide a secure hop between two hosts, two routers, or a router and a host.

The following figures show an original IP packet and a corresponding IP packet with ESP payload.

Figure 21: Original IP packet

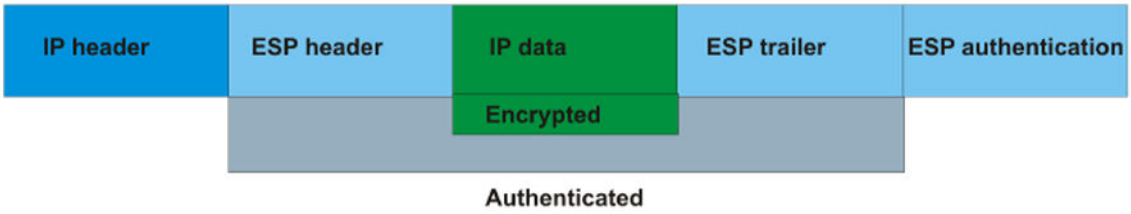


Figure 22: ESP in transport mode

IPsec modes

The IPsec feature security protocols use two different modes to protect the entire IP payload or the upper layer protocols:

- Transport mode
- Tunnel mode

The device only supports transport mode for this release. The device uses transport mode to protect the upper layer protocols. In transport mode, IPsec adds an IPsec header between the IP header and upper layer protocol header.

This release does not support tunnel mode. Under tunnel mode IPsec protects the whole IP packet. In tunnel mode, IPsec inserts the IPsec header between another IP datagram IP header and inner IP header.

Security association

A security association (SA) is a group of algorithms and parameters used to encrypt and authenticate the flow of IP traffic in a particular direction. An SA contains the information IPsec needs to process an IP packet. IPsec identifies SAs by:

- Security Parameter Index (SPI)
- Protocol value (either AH or ESP)
- Destination address to which the SA applies

Creation of a security association

Typically SAs exist in pairs; one in each direction, either inbound or outbound.

You can create SAs manually or dynamically. After you create an SA manually, the SA has no defined lifetime and the SA exists until you manually delete the SA.

After the device creates the SA dynamically, the SA can have a lifetime value that IPsec peers negotiate through use of a key management protocol. If the device uses the key excessively unauthorized access can occur. You must define the IPsec lifetime and other configurable parameters manually.

Security associations reside in the Security Association Database (SADB), which maintains a list of active SAs. The IPsec feature uses outbound SAs to secure the outgoing traffic and inbound SAs to process the incoming traffic. The device checks every ingress or egress packet for the IPsec base protocol, either AH or ESP. The base protocol interacts with the security policy database (SPD) and security association database (SADB) to check the level of security to apply to that packet.

The IPsec feature restricts SAs to the source and destination address of the connected router.

Security policy

Use IPsec to create IPsec security policies that define the levels of security for different types of traffic. You can use IPsec security policies to create rules to filter traffic with IPsec. IPsec policies determine what IP traffic to secure. An IPsec security policy typically consists of:

- An IP filter
- Security algorithms for authentication and key exchange
- An action

Creation of a security policy

You can configure IPsec on IPv4 and IPv6 interfaces. First, create and configure an IPsec policy, and then add and enable the policy on an interface.

After you enable IPsec, the device encrypts all control traffic on the interface based on the policy. You have to specify individual policies to target a particular interface address or multiple addresses. By default, this implementation does not work on a subnet.

The Security Policy Database (SPD) maintains the IPsec security policies. The device checks every ingress or egress packet for the IPsec base protocol, either AH or ESP. The base protocol interacts with the security policy database (SPD) and security association database (SADB) to check the level of security to apply to that packet.

The IPsec feature only adds policies if the local address in the policy specified matches an interface IP address.

The IPsec feature restricts the policy match local address to one of the interface addresses of the router.

IPsec limitations

This section describes the limitations associated with IPsec.

- The device supports IPsec mainly for protocols involved in communication with AAA servers, that is, RADIUS. UDP and TCP protocols are supported but it is recommended to only apply IPsec to the RADIUS protocol.
- The device only supports IPsec transport mode. IPsec does not support tunnel mode.

- The IPsec feature implementation is available only in software. Hardware implementation is not available. Only control packets to and from the CPU are subject to IPsec. IPsec implements IPsec policies in the software on the control path.
- The device does not support address ranges facility for an IPsec policy.
- No fast-path support exists for IPsec.

Digital certificates

This section provides information on the digital certificate framework and certificate management on ERS 4900 and ERS 5900.

A digital certificate is an electronic document that identifies subject, proves the ownership of public key, and is digitally signed by a certification authority (CA) that certifies the validity of the information in the certificate. A digital certificate is valid for only a specific period of time.

The following applications use digital certificates:

- SSL
- IKE

In order to be certified, a switch performs the following tasks:

- generates a certificate signing request
- has a certification authority sign the certificate
- validates the certificate
- renews the certificate before it expires

Subject

An administrator must configure the subject parameters, such as common name, e-mail, organization name, organization unit, locality, state and country. This information is added in the certificate signing request.

Key pair

Only 2048 bit RSA key pairs are supported. The system can generate or import up to 5 key pairs, but only one key pair can be associated with a trustpoint CA at any given time.

TrustPoint CA

Trustpoints allow you to manage and track CAs and certificates. A trustpoint is a representation of a CA or identity pair and contains the identity of the CA, CA-specific configuration parameters, the subject certificate, an association with a key pair and the list of applications that will use the identity pair. An administrator can configure up to 5 trustpoints.

Challenge password

A password is required for Simple Certificate Enrollment Protocol (SCEP) operations, such as the enrollment and renewal of identity certificate. This password is given offline by the CA during end entity registration. The administrator provides this password during enroll and renew operations.

UsePost

There are different types of CAs like EJBCA, Win2012, and others. The usePost parameter allows you to choose the style of HTTP request. The value for usePost parameter can be set True or False.

TrustStore

The truststore allows you to manage trusted CA certificates. Applications will trust leaf certificates signed by any of the CAs from the truststore. By default, trustpoint CA certificates are also added in the truststore.

Certificate enrollment

In order to enroll a trustpoint, the administrator must provide the name of the CA as it is on the server and the URL of the server. The enrollment involves generating a certificate signing request, therefore, subject information and key pair association are also required. Before enrollment, the CA must be authenticated. The authentication procedure retrieves CA and RA certificates from the server and presents root CA certificate fingerprints to the administrator for verification.

Certificate renewal

The certificate renewal must be done by the administrator before it expires. A warning message is logged 15 days before expiration. The system does not allow certificate renewal request if an active certificate is not available. If the renewal is successful, the existing certificate will be replaced.

Certificate revocation or removal

The certificate can be removed from the device at any point of time. The system does not allow certificate revocation request if an active certificate is not available. The administrator is responsible for communicating to the CA to revoke the certificate.

Offline certificate management

Offline certificate management supports the switches that cannot communicate with the Certificate Authority to obtain the identity certificate online by certificate enrollment operation.

A trustpoint CA is used to generate the certificate signing request needed to obtain the offline identity certificate. Root CA certificate and all intermediate CA certificates of the certificate chain must also be installed in the trustpoint because they are used to validate the identity certificate. The subject and key of the identity certificate must match the ones on the device.

Self-signed certificates

The administrator can use a trustpoint CA to generate a self-signed certificate if one is required. In order to generate a self-signed certificate, the administrator must configure subject information and associate a key pair with the trustpoint.

Configuring Secure AAA Communication using CLI

Use the procedures in this section to configure Secure AAA Communication using CLI.

IKE configuration using CLI

The following section provides procedures to configure IKE.

Configuring an IKE Phase 1 profile

About this task

Use the following procedure to configure an IKE Phase 1 profile.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create an IKE phase 1 profile:

   ```
   ike profile <name>
   ```

3. Configure the IKE phase 1 profile hash algorithm:

   ```
   ike profile <name> hash-algo <md5|sha|sha256|any>
   ```

4. **(Optional)** To configure the default Hash Algorithm, enter the following command:

   ```
   default ike profile <name> hash-algo
   ```

5. Configure the IKE phase 1 profile encryption algorithm:

   ```
   ike profile <name> encrypt-algo <desCbc|3DesCbc|aesCbc|any>
   ```

6. **(Optional)** To configure the default encryption algorithm, enter the following command:

   ```
   default ike profile <name> encrypt-algo
   ```

7. Configure the IKE phase 1 profile Diffie-Hellman group:

   ```
   ike profile <name> dh-group <modp768|modp1024|modp2048|any>
   ```

8. **(Optional)** To configure the default DH Group enter the following command:

   ```
   default ike profile <name> dh-group
   ```

9. Configure the IKE phase 1 encryption key length:

   ```
   ike profile <name> encrypt-key-len <128|192|256>
   ```

10. **(Optional)** To configure the default encryption key length, enter the following command:

    ```
    default ike profile <name> encrypt-key-len
    ```

11. Configure the IKE phase 1 lifetime, in seconds:

    ```
    ike profile <name> lifetime-sec <0-4294967295>
    ```

12. **(Optional)** To configure the default lifetime in seconds, enter the following command:

```
default ike profile <name> lifetime-sec
```

13. **(Optional)** Delete the IKE Phase 1 profile:

```
no ike profile <name>
```

Variable definition

Use the data in the following table to use the **`ike profile`** commands.

Variable	Value
profile *<name>*	Specifies the IKE profile name.
hash-algo *<md5|sha|sha256|any>*	Specifies the type of hash algorithm. The default value is sha256. To set this option to the default value, use the default operator with the command.
encrypt-algo *<desCbc|3DesCbc|aesCbc|any>*	Specifies the type of encryption algorithm. The default value is 3DesCbc. To set this option to the default value, use the default operator with the command.
dh-group *<modp768|modp1024|modp2048|any>*	Specifies the Diffie-Hellman (DH) group. DH groups categorize the key used in the key exchange process, by its strength. The key from a higher group number is more secure. The default value is mod1024. To set this option to the default value, use the default operator with the command.
encrypt-key-len *<128|192|256>*	Specifies the length of the encryption key.
lifetime-sec *<0-4294967295>*	Specifies the lifetime value in seconds. The lifetime ensures that the peers renegotiate the SAs just before the expiry of the lifetime value, to ensure that Security Associations are not compromised. The default value is 86400 seconds. To set this option to the default value, use the default operator with the command.

Configuring an IKE Phase 1 policy

Use the following procedure to create an IKE Phase 1 policy.

About this task

An IKE policy establishes Security Associations (SA) and message exchanges with IKE peers to successfully set up secured channels.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Create an IKE Phase 1 policy:

```
ike policy <policy_name> laddr <local_address> raddr
<remote_address>
```

3. Configure the Admin state:

```
ike policy <policy_name> enable
```

4. **(Optional)** Delete the IKE Phase 1 policy:

   ```
   no ike policy <policy_name>
   ```

5. **(Optional)** Disable an IKE P1 Policy:

   ```
   no ike policy <policy_name> enable
   ```

6. **(Optional)** Configure the default Admin state:

   ```
   default ike policy <policy_name> enable
   ```

7. **(Optional)** Configure the default profile name:

   ```
   default ike policy <policy_name> profile
   ```

Variable definition

Use the data in the following table to use the **`ike policy <policy_name> laddr`** command to create

Variable	Value
policy *<policy_name>*	Specifies the name of the IKE Phase 1 policy.
laddr *<local_address>*	Specifies the local IPv4 or IPv6 address.
raddr *<remote_address>*	Specifies the remote IPv4 or IPv6 address.

Configuring the profile for IKE Phase 1 policy

Use the following procedure to configure the IKE Phase1 profile for the IKE Phase 1 policy.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the profile name to be used for IKE Phase 1 policy:

   ```
   ike policy <name> profile <name>
   ```

Variable definition

Use the data in the following table to use the **`ike policy <name> profile <name>`** command.

Variable	Value
policy *<name>*	Specifies the name of the IKE Phase 1 policy.
profile *<name>*	Specifies the name of the IKE Phase 1 profile to be used for the policy.

Configuring IKE Phase 2 perfect forward secrecy

Use the following procedure to configure IKE Phase 2 perfect forward secrecy (PFS).

About this task

A Diffie-Hellman key exchange is done to achieve perfect forward secrecy. This ensures that the compromise of even a single key does not permit access to data other than that protected by that key.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the IKE Phase 2 perfect forward secrecy:

   ```
   ike policy <policy_name> p2-pfs <enable|disable> [use-ike-group
   <enable|disable>] [dh-group <modp768|modp1024|modp2048|any>]
   ```

3. **(Optional)** Disable Phase 2 perfect forward secrecy:

   ```
   no ike policy <1-32> p2-pfs
   ```

4. **(Optional)** Configure the default Phase 2 perfect forward secrecy:

   ```
   default ike policy <string> p2-pfs [use-ike-group] [dh-group]
   ```

Variable definition

Use the data in this table to use the **`ike policy <policy_name> p2-pfs`** command.

Variable	Value
policy <*policy_name*>	Specifies the name of the IKE Phase 1 policy.
p2–pfs	Enables the Phase 2 perfect forward secrecy.
dh-group <*modp768*|*modp1024*|*modp2048*|*any*>	Configures the Diffie-Hellman (DH) group to be used for Phase 2 perfect forward secrecy (PFS). The default value is mod1024. To set this option to the default value, use the default operator with the command.
use-ike-group <*enable*|*disable*>	Specifies whether to use the IKE Phase 1 DH group for Phase 2 PFS or not to use it.

Configuring the IKE authentication method

Use the following procedure to configure the IKE authentication method.

About this task

As part of the IKE protocol, one security gateway must authenticate another security gateway to make sure that IKE SAs are established with the intended party. The switch supports two authentication methods:

- Digital certificates
- Pre-shared keys

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. Configure the IKE authentication method:

```
ike policy WORD<1-32> auth-method <digital-certificate|pre-shared-
key>
```

Variable definition

Use the data in the following table to use the **`ike policy WORD<1–32> auth-method`** command.

Variable	Value
policy *WORD<1–32>*	Specifies the name of the IKE Phase 1 policy.
auth-method <*digital-certificate|pre-shared-key*>	Specifies the authentication method.

Configuring the revocation check method

Use the following procedure to configure the revocation check method as CRL, OCSP, or none.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. Configure the revocation check method:

```
ike policy <policy_name> auth-method digital-certificate
[revocation-check-method {OCSP | CRL | none}]
```

Variable definitions

The following table describes variables that you use with the **`ike policy <policy_name> auth-method digital-certificate`** command.

Variable	Definition
<policy_name>	Specifies the policy name.
revocation-check-method {OCSP | CRL | none}	Specifies the revocation check method as CRL, OCSP, or none.

Configuring the IKE pre-shared key

Use the following procedure to configure the IKE pre-shared key.

About this task

As part of the IKE protocol, one security gateway must authenticate another security gateway to make sure that IKE SAs are established with the intended party. The switch supports two authentication methods:

- Digital certificates
- Pre-shared keys

With pre-shared key authentication, the same secret must be configured on both security gateways before the gateways can authenticate each other.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the authentication method:

   ```
   ike policy <policy_name> {pre-shared-key <pre-shared-key>}
   ```

Variable definition

Use the data in the following table to use the **`ike policy <policy_name> pre-shared-key`** command.

Variable	Value
policy *<policy_name>*	Specifies the name of the IKE Phase 1 policy.
pre-shared-key *<pre-shared-key>*	Specifies the pre-shared key.

Configuring dead-peer detection timeout

Use the following procedure to configure the dead-peer detection (DPD) timeout for the IKE Phase 1 policy.

About this task

Dead Peer Detection (DPD) timeout is the interval for which the system sends messages to a peer to confirm its availability.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the DPD timeout:

   ```
   ike policy <policy_name> dpd-timeout <0-4294967295>
   ```

3. **(Optional)** To configure the default DPD timeout, enter the following command:

```
default ike policy <policy_name> dpd-timeout
```

Variable definition

Use the data in the following table to use the **`ike policy <policy_name> dpd-timeout`** command.

Variable	Value
policy *<policy_name>*	Specifies the name of the IKE Phase 1 policy.
dpd-timeout *<0–4294967295>*	Specifies the dead peer detection timeout in seconds for the IKE Phase 1 policy.

Displaying IKE policies

Use the following procedure to display the configured IKE policies

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display all IKE policies:

   ```
   show ike policy
   ```

3. Display a specific IKE policy:

   ```
   show ike policy <name>
   ```

Example

The following example displays sample output for the `show ike policy` command:

```
Switch(config)#show ike policy

================================================================================================
==========
                                    IKE Policy

================================================================================================
==========
Policy                Addr
 Name                 Type Local Address              Remote Address
------------------------------------------------------------------------------------------------
----------
ikepolicy             IPv4 192.0.2.2                  192.0.2.4


================================================================================================
==========
                                    IKE Policy

================================================================================================
==========
Policy                Profile
Revocation-Check
 Name                 Name                          Auth-Method    Pre-Shared Key
Method

------------------------------------------------------------------------------------------------
```

```
----------
ikepolicy             ikeprofile                  pre-shared-key
ikekey


================================================================================================
==========
                                  IKE Policy

================================================================================================
==========
Policy                   DPD       Admin  Oper          Use IKE
 Name                   Timeout     State  State P2 PFS  DH Grp  DH Group IntfId
------------------------------------------------------------------------------------------------
----------

ikepolicy              300        enable  up    disable enable  modp1024 10700
```

Variable definition

Use the data in the following table to use the **`show ike policy`** command.

Variable	Value
policy <*name*>	Specifies the name of the policy to be displayed.

Displaying IKE profiles

Use the following procedure to display the configured IKE profiles:

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display all IKE profiles:

   ```
   show ike profile
   ```

3. Display a specific ike profile:

   ```
   show ike profile <name>
   ```

Example

```
Switch(config)#show ike profile

================================================================================================
==========
                                  IKE Profile

================================================================================================
==========
                                 Hash    Encrypt    DH      Exchange   Lifetime
Name                             Algo     Algo     Group    Mode       seconds
------------------------------------------------------------------------------------------------
----------
DFLT_IKE_PROFILE                 sha256 aesCbc  modp1024 main       86400
ikeprofile                       sha256 aesCbc  modp2048 main       86400
```

Variable definition

Use the data in the following table to use the **`show ike profile`** command.

Variable	Value
profile *<name>*	Specifies the name of the profile to be displayed.

Displaying IKE security association

Use the following procedure to display the configured IKE Phase 1 security associations (SA).

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display all the security associations:

   ```
   show ike sa
   ```

3. Display security associations by policy name:

   ```
   show ike sa WORD<1-32>
   ```

4. Display security associations at the local address:

   ```
   show ike sa WORD<1-32> laddr <A.B.C.D>
   ```

5. Display security associations at the remote address:

   ```
   show ike sa WORD<1-32> laddr <A.B.C.D> raddr <A.B.C.D>
   ```

Example

```
Switch(config)#show ike sa

================================================================================================
==========
                            IKE Security Association

================================================================================================
==========
Policy          Addr                                                        Initiator/
 Name           Type Local Address              Remote Address              Responder
------------------------------------------------------------------------------------------------
----------


================================================================================================
==========
                         IKE Phase 1 Security Association

================================================================================================
==========
               DPD        Hash   Encrypt   DH     Lifetime
Name           Timeout    Algo   Algo     Group   seconds    Status

------------------------------------------------------------------------------------------------
----------
```

Variable definition

Use the data in the following table to use the **show ike sa** command.

Variable	Value
sa *WORD<1–32>*	Specifies the IKE security association identifier.
laddr <A.B.C.D>	Specifies the local IPv4 or IPv6 address.
raddr <A.B.C.D>	Specifies the remote IPv4 or IPv6 address.

IPsec configuration using CLI

The following section provides procedures to configure Internet Protocol Security (IPsec).

Creating an IPsec security association

Use the following procedure to create an IPsec security association. A security association (SA) is a group of algorithms and parameters used to encrypt and authenticate the flow of IP traffic in a particular direction. An SA contains the information IPsec needs to process an IP packet.

About this task

You cannot delete or modify a security association if the security association links to a policy. To modify a parameter in the security association or to delete the security association, you must first unlink the security association from a policy.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create an IPsec security association:

   ```
   ipsec security-association <sa-id>
   ```

3. **(Optional)** Delete an IPsec security association:

   ```
   no ipsec security-association <sa-id>
   ```

Variable definitions

The following table describes variables that you use with the **ipsec security-association** command.

Variable	Definition
<sa-id>	Specifies the security association identifier.

Configuring an IPsec security association

Use the following procedure to configure an IPsec security association (SA).

About this task

Before you begin

Create an IPsec security association to configure.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the IPsec security association key-mode:

   ```
   ipsec security-association <sa-id> key-mode <manual|automatic>
   ```

3. Configure the IPsec security association mode:

   ```
   ipsec security-association <sa-id> mode <tunnel|transport>
   ```

4. Configure the IPsec security association encapsulation protocol:

   ```
   ipsec security-association <sa-id> encap-proto <AH|ESP>
   ```

5. Configure the IP security association security parameters index:

   ```
   ipsec security-association <sa-id> spi <spi_value>
   ```

   For IPsec to function, each peer must have the same SPI value configured on both peers for a particular policy.

6. Configure the IPsec security association encryption algorithm:

   ```
   ipsec security-association <sa-id> encrypt-algo < algorithm
   name>[encrypt-key <key_value > [KeyLength <1-256>]]
   ```

   The encryption algorithm parameters are only accessible if you configure the encapsulation protocol to ESP.

7. Configure the IPsec security association authentication algorithm:

   ```
   ipsec security-association <sa-id> auth-algo < algorithm name>]
   [auth-key < key_value >] [KeyLength <1-256>
   ```

8. Configure the IPsec security association lifetime value:

   ```
   ipsec security-association <sa-id> lifetime <seconds<value>|
   bytes<value>
   ```

Variable definitions

The following table describes variables that you use with the **`ipsec security-association`** command.

Variable	Definition
auth-algo < algorithm name>] [auth-key < key_value >] [KeyLength <1-256>	Specifies the authorization algorithm, which includes one of the following values: • AES-XCBC-MAC • MD5 • NULL • SHA1 • SHA2 The default authentication algorithm name is MD5. The parameter auth-key specifies the authentication key. The KeyLength parameter specifies a string value of 1 to 256 characters in length. The default KeyLength is 128. The KeyLength values are as follows: 3DES is 48, AES-CBC is 32, 48, or 64, AES-CTR is 32.
encap-proto <AH|ESP>	Specifies the encapsulation protocol: • AH—Specifies authentication header. • ESP—Specifies encapsulation security payload. If you configure the encapsulation protocol as AH, you cannot configure the encryption algorithms and other encryption related attributes. You can only access the encryption algorithm parameters if you configure the encapsulation protocol to ESP. The default value is ESP.
encrypt-algo < algorithm name>[encrypt-key <key_value > [KeyLength <1-256>]]	Specifies the encryption algorithm value as one of the following: • 3DES • AES-CBC • AES-CTR • NULL—Only use the NULL parameter to debug. Do not use this parameter in any other circumstance. The default encryption algorithm is AES-CBC. You can only access the encryption algorithm parameters if you configure the encapsulation protocol to ESP. The EncrptKey specifies the encryption key. The KeyLength specifies the key length value in a string from 1 to 256 characters. The default KeyLength is 128. The KeyLength values are as

Table continues…

Variable	Definition
	follows: 3DES is 48, AES-CBC is 32, 48, or 64, AESCTR is 32.
key-mode <manual|automatic>	Specifies the key-mode as one of the following: • automatic • manual The default is manual.
lifetime <seconds<value>|bytes<value>	Specifies the lifetime value in seconds or kilobytes. The default lifetime value in seconds is 1. The default value in bytes is 1.
mode <tunnel|transport>	Specifies the mode value as one of the following: • transport—Transport mode encapsulates the IP payload and provides a secure connection between two end points. This release only supports transport mode. • tunnel—Tunnel mode encapsulates the entire IP packet and provides a secure tunnel. This release does not support tunnel mode. The default is transport mode.
spi <1-4294967295>	Specifies the security parameters index (SPI) value, which is a unique value. SPI is a tag IPsec adds to the IP header. The tag enables the system that receives the IP packet to determine under which security association to process the received packet. For IPsec to function, each peer must have the same SPI value configured on both peers for a particular policy. The default value is 0.

Creating an IPsec policy

Use the following procedure to configure an IPsec policy. An IPsec policy defines the level of security for different types of traffic.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create an IPsec policy:

   ```
   ipsec policy <Policy_ID>
   ```

3. **(Optional)** Delete an IPsec policy:

```
no ipsec policy <Policy_ID>
```

Variable definitions

The following table describes variables that you use with the **`ipsec policy`** command.

Variable	Definition
<Policy_ID>	Specifies the IPsec policy name.

Configuring an IPsec policy

Use the following procedure to configure an IPsec policy. An IPsec policy defines the level of security for different types of traffic.

About this task

You cannot delete or modify a policy if the policy links to a security association, or if the policy links to a port or VLAN interface. If you need to modify a policy you must first unlink the policy from the security association, and the port or VLAN interface.

Before you begin

Create an IPsec policy.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the remote address:

   ```
   ipsec policy <Policy_ID> raddr <ipv4_or_ipv6_address>
   ```

3. **(Optional)** Configure the local address:

   ```
   ipsec policy <Policy_ID> laddr <ipv4_or_ipv6_address>
   ```

   The `laddr` parameter is an optional parameter that you can configure to have multiple local addresses for each remote address.

4. Configure the protocol:

   ```
   ipsec policy <Policy_ID> protocol {udp <sport|any> <dport|any>|
   tcp<sport|any><dport|any>}
   ```

5. Configure the policy action:

   ```
   ipsec policy <Policy_ID> action <permit | drop>
   ```

Example

Configure the remote address to 192.0.2.2 and local address to 192.0.2.3. Configure the protocol to UDP, any port as the source port and port 1812 as the destination port. Configure the policy to permit.

```
Switch(config)#ipsec policy newpolicy
Switch(config)#ipsec policy newpolicy laddr 192.0.2.2
```

```
Switch(config)#ipsec policy newpolicy raddr 192.0.2.3
Switch(config)#ipsec policy newpolicy protocol udp sport any dport 1812
Switch(config)#ipsec policy newpolicy action permit
```

Variable definitions

The following table describes variables that you use with the **`ipsec policy`** command.

Variable	Definition
action <permit | drop>	Specifies the action the policy takes. The default is permit.
raddr <ipv4_or_ipv6_address>	Specifies the remote address. This is a remote IP address regardless of the policy direction.
laddr <ipv4_or_ipv6_address>	Specifies the local address. The laddr parameter is an optional parameter that you can configure to have multiple local addresses for each remote address. This is a local IP address regardless of the policy direction.
protocol {udp <sport|any> <dport|any>|tcp<sport|any><dport|any>}	Specifies the protocol, as one of the following: • TCP • UDP sport — Specifies the source port for TCP and UDP. You can specify any to configure any port as the source port. dport — Specifies the destination port for TCP and UDP. You can specify any to configure any port as the destination port. The default protocol is TCP any.

Enabling an IPsec policy

Use the following procedure to enable an IPsec policy. An IPsec policy defines the level of security for different types of traffic.

Before you begin

Create an IPsec policy.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable an IPsec policy:

   ```
   ipsec policy <Policy_ID> admin  enable
   ```

3. **(Optional)** Disable an IPsec policy:

```
no ipsec policy <Policy_ID> admin  enable
```

Variable definitions

The following table describes variables that you use with the **ipsec policy** command.

Variable	Definition
Policy_ID	Specifies the IPsec policy name.
admin enable	Enables the policy.

Linking the IPsec security association to an IPsec policy

Use the following procedure to link the security association to an IPsec policy.

About this task

You cannot delete or modify a security association if the security association links to a policy. To modify a parameter in the security association, or to delete the security association, you must first unlink the security association from the policy. You can only unlink a security association from a policy if the policy does not link to an interface. If a policy links to an interface, you must first unlink the policy from the interface, and then unlink the policy from the security association.

Before you begin

The IPsec security association and IPsec policy must exist.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Link the IPsec security association to the IPsec policy:

   ```
   ipsec policy <Policy_ID> security-association <sa-id>
   ```

3. Unlink the IPsec security association to the IPsec policy:

   ```
   no ipsec policy <Policy ID> security-association <sa-id>
   ```

Example

Link the IPsec security association named `newsa` to the IPsec policy named `newpolicy`:

```
Switch(config)# ipsec policy newpolicy security-association newsa
```

Variable definitions

The following table describes variables that you use with the **ipsec policy <Policy_ID> security-association <sa-id>** command.

Variable	Definition
<Policy_ID>	Specifies the policy ID.
security-association <sa-id>	Specifies the security association ID.

Enabling IPsec on an IPv4 interface

Use the following procedure to enable IPsec on an IPv4 interface or on the out of band management interface.

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <1-4094>
   ```

2. Enable IPsec on an interface:

   ```
   ip ipsec enable
   ```

   OR

   ```
   default ip ipsec enable
   ```

3. Enable IPsec on the out of band management interface:

   ```
   ip mgmt ipsec enable
   ```

   OR

   ```
   default ip mgmt ipsec enable
   ```

4. **(Optional)** Disable IPsec on the out of band management interface:

   ```
   no ip mgmt ipsec enable
   ```

Enabling IPsec on an IPv6 interface

Use the following procedure to enable IPsec on an IPv6 interface or on the out of band management interface.

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <1-4094>
   ```

2. Enable IPsec on an interface:

   ```
   ipv6 ipsec enable
   ```

   OR

   ```
   default ipv6 ipsec enable
   ```

3. Enable IPsec on the out of band management interface:

   ```
   ipv6 mgmt ipsec enable
   ```

OR

```
default ipv6 mgmt ipsec enable
```

4. **(Optional)** Disable IPsec on the out of band management interface:

```
no ipv6 mgmt ipsec enable
```

Linking an IPsec policy to an IPv4 interface

Use the following procedure to link an IPsec policy to an interface, and configure a policy direction. By default, the direction is both.

Before you begin

- You must enable IPsec on the interface first, and then you link the IPsec policy to the IPv4 interface.

About this task

You cannot delete or modify an IPsec policy if the policy links to a port or VLAN interface. If you need to modify the policy, first unlink the policy from the port or VLAN interface.

Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <1-4094>
```

2. Link the IPsec policy to the IPv4 interface:

```
ip ipsec policy <policy_name> dir <both|in|out>
```

3. **(Optional)** Unlink the IPsec policy to an interface:

```
no ip ipsec policy <policy_name> dir <both|in|out>
```

Example

Link the IPsec policy newpolicy to the interface VLAN 100:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface vlan 100
Switch:1(config-if)#ip ipsec policy newpolicy dir both
```

Variable definition

Use the data in the following table to use the **`ipsec policy dir`** command.

Variable	Value
<policy_name>	Specifies the policy ID.
dir <both|in|out>	Specifies the direction you want to protect with IPsec: • both—Specifies both ingress and egress traffic.

Table continues…

Variable	Value
	• in—Specifies ingress traffic. • out—Specifies egress traffic. The default is both.

Linking an IPsec policy to an IPv6 interface

Use the following procedure to link an IPsec policy to an interface, and configure a policy direction. By default, the direction is both.

Before you begin

- You must enable IPsec on the interface first, and then you link the IPsec policy to the IPv6 interface.

About this task

You cannot delete or modify an IPsec policy if the policy links to a port or VLAN interface. If you need to modify the policy, first unlink the policy from the port or VLAN interface.

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <1-4094>
   ```

2. Link the IPsec policy to the IPv4 interface:

   ```
   ipv6 ipsec policy <policy_name> dir <both|in|out>
   ```

3. **(Optional)** Unlink the IPsec policy to an interface:

   ```
   no ipv6 ipsec policy <policy_name> dir <both|in|out>
   ```

Example

Link the IPsec policy newpolicy to the interface VLAN 100:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface vlan 100
Switch:1(config-if)#ipv6 ipsec policy newpolicy dir both
```

Displaying IPsec information on an interface

Use this procedure to display IPsec information on a VLAN or management interface.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display IPsec status on a VLAN interface:

```
show ipsec interface vlan <vid>
```

3. Display IPsec status on the management interface:

```
show ipsec interface mgmt
```

Variable definitions

The following table describes variables that you use with the **`show ipsec interface`** command.

Variable	Definition
<vid>	Specifies the VLAN ID for which to display IPsec information.

Displaying configured IPsec policies

Use this procedure to display configured IPsec policies.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display all policies available:

```
show ipsec  policy all
```

3. Display interfaces linked to the policy:

```
show ipsec  policy interface <policy_name>
```

4. Display a specific IPsec policy:

```
show ipsec  policy name <policy_name>
```

Displaying IPsec security association information

Use the following procedure to display IPsec security association information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display all IPsec security associations:

```
show ipsec sa all
```

3. Display a specific IPsec security association:

```
show ipsec sa name WORD<1-32>
```

4. Display all security association policies:

```
show ipsec sa-policy
```

5. Display all security association policies linked to an VLAN interface:

```
show ipsec interface vlan <1-4059>
```

Example

Display information on IPsec security association policies:

```
Switch:1>enable
Switch:1#show ipsec sa all
================================================================================
                        IPSEC Security Association Table
================================================================================
sa-name: ospf1
key-Mode: manual
Encap protocol: ESP
SPI Value: 9
Encrypt Algorithm: 3dec-cbc
Encrypt-key: 52fb29f723b0800870dc83e3
Encrypt-key-Len: 24
Auth Algorithm: hmac-md5
Auth-key: 123456789abcdef0
Auth-key-Len: 16
Mode: transport
Lifetime-Sec: 1000
Lifetime-Byte: 20000

Switch:1#show ipsec sa name ospf1

================================================================================
                        IPSEC Security Association Table
================================================================================
sa-name: ospf1
key-Mode: manual
Encap protocol: ESP
SPI Value: 9
Encrypt Algorithm: 3dec-cbc
Encrypt-key: 52fb29f723b0800870dc83e3
Encrypt-key-Len: 24
Auth Algorithm: hmac-md5
Auth-key: 123456789abcdef0
Auth-key-Len: 16
Mode: transport
Lifetime-Sec: 1000
Lifetime-Byte: 20000

Switch:1#show ipsec sa-policy

================================================================================
                                SA POLICY TABLE
================================================================================
 Policy Name       Security Association
--------------------------------------------------------------------------------
 ospf1             ospf1
--------------------------------------------------------------------------------
```

Variable definition

Use the data in the following table to use the **`show ipsec sa`** command.

Variable	Value
all	Displays all security associations.
name *WORD<1–32>*	Displays a specific security association based on name

Use the data in the following table to use the **show ipsec sa-policy** command.

Variable	Value
sa-policy	Displays all security associations linked to a specific policy.

Displaying IPsec statistics

Use the following procedure to display IPsec statistics.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display the IPsec statistics on a VLAN interface:

   ```
   show ipsec statistics vlan <vlan_ID>
   ```

3. Display the system global IPsec statistics:

   ```
   show ipsec statistics system
   ```

4. Display IPsec statistics on the management interface:

   ```
   show ipsec statistics mgmt <slot>
   ```

Example

Displaying the IPsec statistics on a VLAN interface:

```
Switch(config)#show ipsec statistics system

================================================================================================
==========
                            IPSEC Global Statistics

================================================================================================
==========
InSuccesses           = 0
InSPViolations        = 0
InNotEnoughMemories   = 0
InAHESPReplays        = 0
InESPReplays          = 0
InAHFailures          = 0
InESPFailures         = 0
OutSuccesses          = 0
OutSPViolations       = 0
OutNotEnoughMemories  = 0
generalError          = 0
InAHSuccesses         = 0
InESPSuccesses        = 0
OutAHSuccesses        = 0
OutESPSuccesses       = 0
OutKBytes             = 0
OutBytes              = 0
InKBytes              = 0
InBytes               = 0
TotalPacketsProcessed= 0
TotalPacketsByPassed  = 0
OutAHFailures         = 0
OutESPFailures        = 0
InMD5Hmacs            = 0
```

```
InSHA1Hmacs          = 0
InAESXCBCs           = 0
InAnyNullAuth        = 0
In3DESCBCs           = 0
InAESCBCs            = 0
InAESCTRs            = 0
InAnyNullEncrypt     = 0
OutMD5Hmacs          = 0
OutSHA1Hmacs         = 0
OutAESXCBCs          = 0
OutInAnyNullAuth     = 0
Out3DESCBCs          = 0
OutAESCBCs           = 0
OutAESCTRs           = 0
OutInAnyNullEncrypt  = 0
```

Displaying the system global IPsec statistics:

```
Switch:1>enable
Switch:1#show ipsec statistics system

================================================================================
                            IPSEC Global Statistics

================================================================================
InSuccesses          = 0
InSPViolations       = 0
InNotEnoughMemories  = 0
InAHESPReplays       = 0
InESPReplays         = 0
InAHFailures         = 0
InESPFailures        = 0
OutSuccesses         = 0
OutSPViolations      = 0
OutNotEnoughMemories = 0
generalError         = 0
InAHSuccesses        = 0
InESPSuccesses       = 0
OutAHSuccesses       = 0
OutESPSuccesses      = 0
OutKBytes            = 0
OutBytes             = 0
InKBytes             = 0
InBytes              = 0
TotalPacketsProcessed= 0
TotalPacketsByPassed = 0
OutAHFailures        = 0
OutESPFailures       = 0
InMD5Hmacs           = 0
InSHA1Hmacs          = 0
InAESXCBCs           = 0
InAnyNullAuth        = 0
In3DESCBCs           = 0
InAESCBCs            = 0
InAESCTRs            = 0
InAnyNullEncrypt     = 0
OutMD5Hmacs          = 0
OutSHA1Hmacs         = 0
OutAESXCBCs          = 0
OutInAnyNullAuth     = 0
Out3DESCBCs          = 0
OutAESCBCs           = 0
OutAESCTRs           = 0
OutInAnyNullEncrypt  = 0
```

Variable definition

Use the data in the following table to use the **`show ipsec statistics`** command.

Variable	Value
profile <*profile_name*>	Specifies the name of the profile to be displayed.
vlan <*vlan_ID*>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
mgmt <*slot*>	Identifies the interface as a management interface.

Configuring Digital Certificates

The following section provides procedures to configure Digital Certificates.

Configuring device subject parameters

About this task

Use this procedure to configure the device subject parameters to identify the device, such as the name, Email ID, company, department, and location.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the subject parameters of the device:

   ```
   certificate subject {[common-name WORD<0-64>] [e-mail WORD<0-254>]
   [unit WORD<0-64>] [organization WORD<0-64>] [locality WORD<0-128>]
   [province WORD<0-128>] [country WORD<2>]}
   ```

3. **(Optional)** Delete a subject parameter:

   ```
   no certificate subject {[common-name] [e-mail] [unit] [organization]
   [locality] [province] [country]}
   ```

4. **(Optional)** Configure the default subject parameters of the device:

   ```
   default certificate subject
   ```

5. Verify configuration:

   ```
   show certificate subject
   ```

Example

Configuring subject parameters:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)# certificate subject common-name Self e-mail example@company.com unit
Engineering organization Company locality SanFrancisco province California country US
```

The following sample output shows an example of the **`show certificate subject`** command.

```
Switch#show certificate subject
Common-name           :
E-mail                :
Organizational unit   :
Organization          :
Locality              :
State/Province        :
Country               :
Include IP address    : false
```

Variable definitions

Use the data in the following table to use the **`Certificate Subject`** command.

Variable	Value
common-name WORD<0–64>	Specifies the name of the subject sending the Certificate Signing Request to the Certificate Authority.
e-mail WORD<0-254>	Specifies the Email address of the subject sending the Certificate Signing Request to the Certificate Authority.
unit WORD<0-64>	Specifies the organizational unit of the subject sending the Certificate Signing Request to the Certificate Authority.
organization WORD<0-64>	Specifies the organization of the subject sending the Certificate Signing Request to the Certificate Authority.
locality WORD<0-128>	Specifies the locality of the subject sending the Certificate Signing Request to the Certificate Authority.
province WORD<0-128>	Specifies the province of the subject sending the Certificate Signing Request to the Certificate Authority.
country WORD<2>	Specifies the country of the subject sending the Certificate Signing Request to the Certificate Authority.

Generating key pair

About this task

Use the following procedure to generate the private and public key pair for the specific cryptography type.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Generate the key pair:

   ```
   certificate key name WORD<1-45> generate
   ```

3. **(Optional)** Delete a key pair:

   ```
   no certificate key name WORD<1-45>
   ```

4. **(Optional)** Configure the default key pair:

   ```
   default certificate key name WORD<1-45>
   ```

5. Verify configuration:

   ```
   show certificate key [WORD<1-45> | detail]
   ```

Configuring a trustpoint CA

About this task

Use this procedure to configure the certificate authority and perform related actions. You can configure only one CA in a device at a time.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the trustpoint by getting CA specific configuration parameters and perform related actions:

   ```
   certificate ca IPSEC [action {caauth | enroll | generate-selfsigned-
   cert | get-crl | remove | renew}] [ca-url WORD<1-1000>][common-name
   WORD<1-64>] [export] [import] [key-name WORD<1-45>][regenerate-key-
   on-re-enroll] [use-for <ike | ssl-server >][use-post <true|false>]
   [validity <7-1185>]
   ```

   a. Configure the trustpoint and associate it with the generated key pair:

      ```
      certificate ca IPSEC {[common-name WORD<1-64>] [key-name WORD<1-
      45>] [ca-url WORD<1-1000>] [use-post <true|false>]}
      ```

   b. Configure trustpoint, authenticate the trustpoint CA by getting the certificate of the CA, and store the CA certificate locally:

      ```
      certificate ca IPSEC action caauth
      ```

   c. Generate certificate signing request to obtain identity certificate from configured trustpoint CA, get the digital certificate, and store it locally, associating with the trustpoint CA:

      ```
      certificate ca IPSEC action enroll
      ```

   d. Generate certificate renew request for given trustpoint CA, get the new digital certificate, and store it locally by replacing the old certificate with the new one:

```
certificate ca IPSEC action renew [validity-days <7-1185>]
[challenge-password <0-128>]}
```

e. Release the locally stored certificate associated with the trustpoint CA post revocation.

```
certificate ca IPSEC action remove
```

f. Get the Certificate Revocation List from the CDP and store into a file.

```
certificate ca IPSEC action get-crl
```

g. Generate a self-signed subject certificate:

```
certificate ca IPSEC action generate-self-signed-cert
```

3. Generate a new key pair before each re-enrollment:

```
certificate ca IPSEC regenerate-key-on-re-enroll
```

4. Specify the feature to use this identity:

```
certificate ca IPSEC use-for [[ike] | [ssl-server]]
```

5. Set the HTTP request type to support the type of CA:

```
certificate ca IPSEC use-post <false | true>
```

6. **(Optional)** Delete a trustpoint CA:

```
no certificate ca IPSEC [[common-name] | [key-name] | [ca-url] |
[use-post] | [use-for] [action]]
```

7. **(Optional)** Configure default trustpoint CA:

```
default certificate ca IPSEC
```

8. Verify configuration:

```
show certificate ca NAME [file WORD<1-512>| detail | chain]
```

Variable definition

Use the data in the following table to use the **`certificate ca`** command.

Variable	Value
ca WORD<1–45>	Specifies the name of the certificate authority. It should be alphanumeric and case-sensitive. The maximum length should be 45 characters.
common-name WORD<1–64>	Specifies the name of the owner of the device or user.
key-name WORD<1–45>	Specifies the key pair generated by the command that was first associated with the CA trustpoint.
ca-url WORD<1–1000>	Specifies the trusted CA url.
use-post <false | true>	Specifies the HTTP request style. The default value is True. For example, True for EJBCA and False for Win2012 CA.

Table continues…

Variable	Value
use-for <ike | ssl-server>	Specifies the name of the feature that uses this identity.
export	Export CA related files.
import	Import CA related files.
regenerate-key-on-re-enroll	Generates a new key pair before each re-enrollment.
action caauth	Authenticates the trustpoint CA by getting the certificate of the CA and stores the CA certificate locally.
action enroll	Generates certificate signing request to obtain identity certificate from configured trustpoint CA, gets the digital certificate, and stores it locally, associating with the trustpoint CA.
action generate-self-signed-cert	Generates a self-signed subject certificate.
action renew	Generates certificate renewal request for given trustpoint CA, gets the digital certificate, and stores it locally by replacing the old certificate with the new one.
action remove	Releases the locally stored certificate associated with the trustpoint CA post revocation.
action get-crl	Gets the Certificate Revocation List from the CDP and stores into a file.
validity <7–1185>	Specifies the number of days for which the certificate will remain valid. The default value is 365 days.

Moving or copying a certificate

About this task

Use this procedure to move or copy a certificate or CRL.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   certificate move [ca WORD<1-45>] [file WORD<1-512>] [trust-store]
   ```

   OR

   ```
   certificate copy [ca WORD<1-45>] [file WORD<1-512>] [trust-store]
   ```

Exporting a CSR

About this task

Use this procedure to export a CSR to SFTP or USB.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command:

```
certificate ca WORD export csr sftp filename <sftp_filename>
[address <sftp_address>] username <username>
```

OR

```
certificate ca WORD export csr usb filename <usb_filename> [unit
<1-8>]
```

Variable definition

Use the data in the following table to use the **`certificate export csr`** command.

Variable	Value
sftp	Specifies to export the CSR on an SFTP storage.
usb	Specifies to export the CSR on a USB storage.
WORD<1-256>	Specifies the filename.

Installing offline certificates

About this task

Use this procedure to install offline subject and CA certificates.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Import root CA/intermediate/subject certificates/CRL:

```
certificate ca WORD import sftp filename <sftp_filename>
[address<sftp_address>] username <username>
```

OR

```
certificate ca WORD import usb filename <usb_filename> [unit <1-8>]
```

3. **(Optional)** Import key-pair:

```
certificate key WORD import sftp filename <sftp_filename>
[address<sftp_address>] username <username>
```

OR

```
certificate key WORD import usb filename <usb_filename> [unit <1-8>]
```

4. Import PKCS12 container:

```
certificate ca WORD import encrypted sftp filename <sftp_filename>
[address<sftp_address>] username <username>
```

OR

```
certificate ca WORD import encrypted usb filename <usb_filename>
[unit <1-8>]
```

Importing a key pair

Use the following procedure to import a key pair from ramdisk.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   certificate key <name> import ramdisk filename <filename>
   ```

Variable definitions

Use the data in the following table to use the **`certificate key import ramdisk`** command.

Variable	Value
<name>	Specifies the certificate key pair name.
<filename>	Specifies the source filename.

Exporting a key pair

Use the following procedure to export a key pair to ramdisk.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   certificate key <name> export ramdisk filename <filename>
   ```

Variable definitions

Use the data in the following table to use the **`certificate key export ramdisk`** command.

Variable	Value
<name>	Specifies the certificate key pair name.
<filename>	Specifies the destination filename.

Import files into a certificate authority

Use the following procedure to import specified certificate authority related files from ramdisk.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   certificate ca <name> import ramdisk filename <filename>
   ```

Variable definitions

Use the data in the following table to use the **`certificate ca import ramdisk filename`** command.

Variable	Value
<name>	Specifies the Certificate Authority name.
<filename>	Specifies the remote filename to import.

Exporting files from a certificate authority to ramdisk

Use the following procedure to export a certificate local file or a Certificate Signing Request (CSR) file to ramdisk.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   certificate ca <name> export {file <filename> | csr} ramdisk
   filename <filename>
   ```

Variable definitions

Use the data in the following table to use the **`certificate ca <name> export`** command.

Variable	Value
<name>	Specifies the certificate key pair name.
file *<filename>*	Specifies the filename to export to ramdisk.
csr *<filename>*	Specifies to export the device Certificate Signing Request.

Importing trusted CA certificates from ramdisk

Use the following procedure to import trusted CA certificates from ramdisk.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   certificate trust-store import ramdisk filename <filename>
   ```

Variable definitions

Use the data in the following table to use the **`certificate trust-store import ramdisk`** command.

Variable	Value
filename *<filename>*	Specifies the filename to import from ramdisk.

Exporting trusted CA certificates to ramdisk

Use the following procedure to export trusted CA certificates to ramdisk.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   certificate trust-store export ramdisk filename <filename>
   ```

Variable definitions

Use the data in the following table to use the **`certificate trust-store export ramdisk`** command.

Variable	Value
filename *<filename>*	Specifies the filename to export to ramdisk.

Configuring Secure AAA Communication using EDM

Use the procedures in this section to configure Secure AAA Communication using EDM.

IKE configuration using EDM

The following section provides procedures to configure IKE.

Creating an IPsec phase 1 profile using EDM

Use the following procedure to create and configure an IKE Phase 1 profile.

Procedure

1. From the navigation tree, click **Security**.
2. Click the **Profile** tab.
3. Click **Insert**.
4. In the **Name** field, type a profile name.
5. Complete the remaining optional configuration to customize the profile.
6. Click **Insert**.

Field descriptions

Use the data in the following table to use the **Profile** tab.

Name	Description
Name	Specifies the name of the IKE profile.
HashAlgorithm	Specifies the authorization algorithm, which includes one of the following values: • md5 • sha • sha256 • any The default is sha256.
EncryptionAlgorithm	Specifies the encryption algorithm value as one of the following: • desCbc • tripleDesCbc • aesCbc • any The default is aesCbc.
EncrypKeyLen	Specifies the key length value in a string from 1 to 256 characters. The default is 256.

Table continues…

Name	Description
DHGroup	Specifies the Diffie-Hellman (DH) group as one of the following options: • modp768 • modp1024 • modp2048 • any The default value is mod2048.
ExchangeMode	Specifies the IKE Phase 1 negotiation mode. The default value is main.
LifetimeSeconds	Specifies the lifetime value in seconds. The lifetime determines the traffic that can pass between IPsec peers using a security association before that security association expires. The default lifetime value in seconds is 86400.

Configuring IKE Phase 1 policy

Use the following procedure to create and configure an IKE Phase 1 policy.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **IKE**.
3. Click the **Policy** tab.
4. Click **Insert**.
5. For the **LocalAddrType** field, select the type of address of the local peer.
6. In the **LocalAddr** field, type the address of the local peer.
7. In the **RemoteAddr** field, type the address of the remote peer.
8. In the **Name** field, type the name for the policy.

   Name must be assigned when creating the policy. When the policy is created, the name cannot be changed.
9. Complete the remaining optional configuration to customize the policy.
10. Click **Insert**.

Field descriptions

Use the data in the following table to use the **Policy** tab.

Variable	Value
LocalAddrType	Specifies whether the local address is an IPv4 or IPv6 address.

Table continues…

Variable	Value
LocalAddr	Specifies the address of the local peer.
RemoteAddrType	Specifies whether the remote address is an IPv4 or IPv6 address.
RemoteAddr	Specifies the address of the remote peer.
Name	Specifies the name given to the policy. The name should be assigned while creating the policy. You cannot change the name after the policy is created.
ProfileName	Specifies the name of the profile that should be used for this policy.
ProfileVersion	Specifies the profile version used for the policy.
PeerName	Specifies the peer name.
AuthenticationMethod	Specifies the proposed authentication method for the Phase 1 security association. The default authentication method is pre-shared key.
PSKValue	Specifies the value of the Pre-Shared Key if the authentication method is set to PSK.
DPDTimeout	Specifies the Dead Peer Detection timeout in seconds. Default value is 300 seconds.
P2PFS	Specifies whether or not the perfect forward secrecy (PFS) is used when refreshing keys. To use PFS, select enable. The default value is disable.
P2PfsUseIkeGroup	Specifies the IKE Phase 1 DH Group for Phase 2 PFS.
P2PfsDHGroup	Specifies the DH Group used for Perfect Forward Secrecy.
AdminState	Enable or disable the policy.
OperStatus	Displays the policy status.
RevocationCheckMethod	Specifies the revocation method used for IKE.

Displaying IKE Phase 1 security association

Use the following procedure to view the IKE Phase 1 security association.

Procedure

1. From the navigation tree, click **Security**.
2. Click **IKE**.
3. Click the **SA** tab.

Field descriptions

Use the data in the following table to use the **SA** tab.

Name	Description
Id	Specifies the profile ID.

Table continues…

Name	Description
LocalIfIndex	Specifies the Interface Index of the local address. Only port and vlan interfaces are supported.
LocalAddrType	Specifies whether the local address is an IPv4 or IPv6 address.
LocalAddr	Specifies the address of the local peer.
RemoteAddrType	Specifies whether the remote address is an IPv4 or IPv6 address.
RemoteAddr	Specifies the address of the remote peer.
Name	Specifies the name given to the SA.
AuthenticationMethod	Specifies the proposed authentication method for the Phase 1 security association. The default authentication method is pre-shared key.
DPDTimeout	Specifies the Dead Peer Detection timeout in seconds.
HashAlgorithm	Specifies the hash algorithm negotiated for this IKE Phase 1 SA.
EncryptionAlgorithm	Specifies the encryption algorithm negotiated for this IKE Phase 1 SA.
EncryptKeyLen	Specifies the encryption key length negotiated for this IKE Phase 1 SA.
DHGroup	Specifies the Diffie-Hellman group negotiated for this IKE Phase 1 SA
ExchangeMode	Specifies the IKE Phase 1 SA mode.
LifetimeSeconds	Specifies the amount of time for which an IKE Phase 1 SA can remain valid during IKE Phase 1 negotiation. A value of 0 means no the SA always remains valid.
Status	Specifies whether the SA is active or inactive.
Initiator	Specifies whether specifies the whether the SA is created by an initiator or a responder.

IPsec configuration using EDM

The following section provides procedures to configure Internet Protocol Security (IPsec).

Creating an IPsec policy

Use the following procedure to configure an IPsec policy for an IPv4 or an IPv6 interface. An IPsec policy defines the level of security for different types of traffic.

Procedure

1. From the navigation tree, click **Security**.
2. Click the **Policy** tab.
3. Click **Insert**.
4. In the **Name** field, type a policy name.
5. Complete the remaining optional configuration to customize the policy.

6. Click **Insert**.

Field descriptions

Use the data in the following table to use the **Policy** tab.

Name	Description
Name	Specifies the name of the IPsec policy name.
DstAddressType	Specifies the IP address type.
DstAddress	Specifies the remote address. This field accepts IPv4 and IPv6 address, depending on the selected source address type.
SrcAddressType	Specifies the IP address type.
SrcAddress	Specifies the local address. The local address is optional that you can configure to have multiple local addresses for each remote (destination) address. This field accepts IPv4 and IPv6 address, depending on the selected source address type.
SrcPort	Specifies the key length value in a string from 1 to 256 characters. The default is 256.
DstPort	Specifies the destination port for TCP and UDP. Leave this field empty to configure any port as the destination port. The default value is 1
AdminFlag	Enables or disables the policy. The default is disabled.
L4Protocol	Specifies the protocol, as one of the following: tcp udp The default is TCP.
Action	Specifies the action the policy takes. The default is to permit the packet.

Creating an IPsec security association

Use the following procedure to create an IPsec security association. A security association (SA) is a group of algorithms and parameters used to encrypt and authenticate the flow of IP traffic in a particular direction. An SA contains the information IPsec needs to process an IP packet.

You cannot delete or modify a security association if the security association links to a policy. To modify a parameter in the security association or to delete the security association, you must first unlink the security association from a policy.

You can only unlink a security association from a policy if the policy does not link to an interface. If a policy links to an interface, you must first unlink the policy from the interface, and then unlink the policy from the security association.

Procedure

1. From the navigation tree, click **Security**.

2. Click the **SecurityAssociation** tab.
3. Click **Insert**.
4. In the **Name** field, type a name to identify the SA.

   Note:

   For IPsec to function, each peer must have the same SPI value configured for a particular policy.
5. Complete the remaining optional configuration.
6. Click **Insert**.

Field descriptions

Use the data in the following table to use the **Security Association** tab.

Name	Description
Name	Specifies the name of the security association.
Spi	Specifies the security parameters index (SPI) value, which is a unique value. SPI is a tag IPsec adds to the IP header. The tag enables the system that receives the IP packet to determine under which security association to process the received packet. For IPsec to function, each peer must have the same SPI value configured for a particular policy. The default value is 0.
HashAlgorithm	Specifies the authorization algorithm, which includes one of the following values: • sha • aesXcbc • md5 • null—Only use the null parameter to debug. Do not use this parameter in any other circumstance. • sha2 The default authentication algorithm name is md5.
EncryptionAlgorithm	Specifies the encryption algorithm value as one of the following: • des3Cbc • aes128Cbc • aesCtr • null—Only use the null parameter to debug. Do not use this parameter in any other circumstance.

Table continues…

Name	Description
	The default encryption algorithm is aes128Cbc. You can only access the encryption algorithm parameters if you configure the encapsulation protocol to ESP
AuthMethod	Specifies the encapsulation protocol: • ah—Specifies authentication header. • esp—Specifies encapsulation security payload. If you configure the encapsulation protocol as ah, you cannot configure the encryption algorithms and other encryption related attributes. You can only access the encryption algorithm parameters if you configure the encapsulation protocol to es. The default value is esp.
Mode	Specifies the mode value as one of the following: • transport—Transport mode encapsulates the IP payload and provides a secure connection between two end points. This device only supports transport mode.
KeyMode	Specifies the key mode as one of the following: • manual • auto The default is manual.
EncryptKeyName	Specifies the encryption key.
EncryptKeyLength	Specifies the numbers of bits used in the encryption key. The key length values are as follows: • des3Cbc is 48 • aes128Cbc is 32, 48, 64 • aesCtr is 32
HashKeyName	Specifies the authentication key.
HashKeyLength	Specifies the numbers of bits used in the hash key. The key length values are as follows: • aesXcbc is 32 • md5 is 32 • sha1 is 40
LifetimeSeconds	Specifies the lifetime value in seconds. The lifetime determines the traffic that can pass between IPsec peers using a security association before that security association expires. The default lifetime value in seconds is 0, which is infinite.

Table continues…

Name	Description
LifetimeBytes	Specifies the lifetime value in bytes. The lifetime determines the traffic that can pass between IPsec peers using a security association before that security association expires. The default lifetime value in bytes is 4294966272.

Linking the IPsec security association to an IPsec policy

Use the following procedure to link the security association to an IPsec policy.

You cannot delete or modify a security association if the security association links to a policy. To modify a parameter in the security association, or to delete the security association, you must first unlink the security association from the policy. You can only unlink a security association from a policy if the policy does not link to an interface. If a policy links to an interface, you must first unlink the policy from the interface, and then unlink the policy from the security association.

Before you begin

The IPsec security association and IPsec policy must exist.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **IPSec**.
3. Click the **Policy SA Link** tab.
4. Click **Insert**.
5. In the **PolicyName** field, type the IPsec policy name.
6. In the **SAName** field, type the security association name.
7. Click **Insert**.

Field descriptions

Use the data in the following table to use the **Policy SA Link** tab.

Name	Description
PolicyName	Specifies the name of the IPsec policy.
SAName	Specifies the name of the security association.

Linking an IPsec policy to an interface

Use the following procedure to link an IPsec policy to an interface, and configure a policy direction. By default, the direction is both.

You cannot delete or modify an IPsec policy if the policy links to a port or VLAN interface. If you need to modify the policy, first unlink the policy from the port or VLAN interface.

Before you begin

You must enable IPsec on the interface first, and then you link the IPsec policy to the interface.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **IPSec**.
3. Click the **Interface Policy** tab.
4. Click **Insert**.
5. In the **Name** field, type the name of the IPsec policy.
6. In the **IfIndex** field, select the port.
7. Click **Ok**.
8. Complete the remaining optional configuration.
9. Click **Insert**.

Field descriptions

Use the data in the following table to use the **Interface Policy** tab.

Name	Description
Name	Specifies the name of the IKE profile. Specifies the IPsec policy name
IfIndex	Links a policy to either a port, VLAN, loopback, or management interface.
IfEnabled	Shows if the IPsec is enabled on the interface and if the administrative state of the policy is enabled.
IfDirection	Specifies the direction you want to protect with IPsec: • inbound—Specifies ingress traffic. • outbound—Specifies egress traffic. • bothDirections—Specifies both ingress and egress traffic. The default is bothDirections.

Enabling IPsec on an IPv4 interface

Use the following procedure to enable IPsec on an IPv4 interface.

Note:

If you downgrade your software, the current IPsec configurations are no longer supported. You must boot with the factory default settings for IPsec, and then reconfigure the IPsec features.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **IPSec**.
3. Click the **IPv4 Interfaces** tab.

4. In the **IpsecEnable** column, double-click in the **IpsecEnable** field, and select **true** from the drop-down box.
5. Click **Apply**.

Field descriptions

Use the data in the following table to use the **IPv4 Interfaces** tab.

Name	Description
Interface	Specifies the interface.
IpsecEnable	Specifies if IPsec is enabled on that particular interface.

Enabling IPsec on an IPv6 interface

Use the following procedure to enable IPsec on an IPv6 interface.

Note:

If you downgrade your software, the current IPsec configurations are no longer supported. You must boot with the factory default settings for IPsec, and then reconfigure the IPsec features.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **IPSec**.
3. Click the **IPv6 Interfaces** tab.
4. In the **IpsecEnable** column, double-click in the **IpsecEnable** field, and select **true** from the drop-down box.
5. Click **Apply**.

Field descriptions

Use the data in the following table to use the **IPv6 Interfaces** tab.

Name	Description
Interface	Specifies the interface.
IpsecEnable	Specifies if IPsec is enabled on that particular interface.

Displaying IPsec interface statistics

Use this procedure to view IPsec statistics and counter values for each IPsec-enabled interface.

If you select an interface on the **Stats** tab, you can click **Graph** to graph particular statistics for that interface.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **IPSec**.

3. Click the **Interface Stats** tab.

Field descriptions

Use the data in the following table to use the **Interface Stats** tab.

Name	Description
IfIndex	Shows the interface index for which the statistic is captured.
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the AH replay check fails.
InESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the ESP replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.
InAhSuccesses	Specifies the number of ingress packets IPsec carries because the AH authentication succeeds.
OutAHSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
InESPSuccesses	Specifies the number of ingress packets IPsec carries since boot time because the ESP authentication succeeds.
OutESPSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutKBytes	Specifies the total number of kilobytes on egress.
OutBytes	Specifies the total number of bytes on egress.
InKBytes	Specifies the total number of bytes on ingress.
InBytes	Specifies the total number of bytes on ingress.
TotalPacketsProcessed	Specifies the total number of packets processed.
TotalPacketsByPassed	Specifies the total number of packets bypassed.

Table continues…

Name	Description
OutAHFailures	Specifies the number of egress packets IPsec discards since boot time because the AH authentication check fails.
OutESPFailures	Specifies the number of egress packets IPsec discards since boot time because the ESP authentication check fails
InMD5Hmacs	Specifies the number of inbound HMAC MD5 occurrences since boot time.
InSHA1Hmacs	Specifies the number of inbound HMAC SHA1 occurrences since boot time.
InAESXCBCs	Specifies the number of inbound AES XCBC MAC occurrences since boot time.
InAnyNullAuth	Specifies the number of inbound null authentication occurrences since boot time.
In3DESCBCs	Specifies the number of inbound 3DES CBC occurrences since boot time.
InAESCBCs	Specifies the number of inbound AES CBC occurrences since boot time.
InAESCTRs	Specifies the number of inbound AES CTR occurrences since boot time.
InAnyNulEncrypt	Specifies the number of inbound null occurrences since boot time. Used for debugging purposes.
OutMD5Hmacs	Specifies the number of outbound HMAC MD5 occurrences since boot time.
OutSHA1Hmacs	Specifies the number of outbound HMAC SHA1 occurrences since boot time.
OutAESXCBCs	Specifies the number of outbound AES XCBC MAC occurrences since boot time.
OutInAnyNullAuth	Specifies the number of outbound null authentication occurrences since boot time.
Out3DESCBCs	Specifies the number of outbound 3DES CBC occurrences since boot time.
OutAESCBCs	Specifies the number of outbound AES CBC occurrences since boot time.
OutAESCTRs	Specifies the number of outbound AES CTR occurrences since boot time.
OutInAnyNullEncrypt	Specifies the number of outbound null occurrences since boot time. Used for debugging purposes.

Displaying switch level statistics for IPsec-enabled interfaces

Use this procedure to view IPsec statistics and counter values at the switch level for all IPsec-enabled interfaces.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **IPSec**.
3. Click the **Global Stats** tab.

Field descriptions

Use the data in the following table to use the **Global Stats** tab.

Name	Description
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the AH replay check fails.
InESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the ESP replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
OutSuccesses	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
InESPFailures	Specifies the number of egress packets IPsec successfully carries since boot time
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation oc
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.
InAHSuccesses	Specifies the number of ingress packets IPsec carries because the AH authentication succeeds.
OutAHSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
InESPSuccesses	Specifies the number of ingress packets IPsec carries since boot time because the ESP authentication succeeds.
OutESPSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutKBytes	Specifies the total number of kilobytes on egress.
OutBytes	Specifies the total number of bytes on egress.
InKBytes	Specifies the total number of bytes on ingress.
InBytes	Specifies the total number of bytes on ingress.
TotalPacketsProcessed	Specifies the total number of packets processed.
TotalPacketsByPassed	Specifies the total number of packets bypassed.
OutAHFailures	Specifies the number of egress packets IPsec discards since boot time because the AH authentication check fails.
OutESPFailures	Specifies the number of egress packets IPsec discards since boot time because the ESP authentication check fails.
InMD5Hmacs	Specifies the number of inbound HMAC MD5 occurrences since boot time.

Table continues…

Name	Description
InSHA1Hmacs	Specifies the number of inbound HMAC SHA1 occurrences since boot time.
InAESXCBCs	Specifies the number of inbound AES XCBC MAC occurrences since boot time.
InAnyNullAuth	Specifies the number of inbound null authentication occurrences since boot time.
In3DESCBCs	Specifies the number of inbound 3DES CBC occurrences since boot time.
InAESCBCs	Specifies the number of inbound AES CBC occurrences since boot time.
InAESCTRs	Specifies the number of inbound AES CTR occurrences since boot time.
InAnyNulEncrypt	Specifies the number of inbound null occurrences since boot time. Used for debugging purpose
OutMD5Hmacs	Specifies the number of outbound HMAC MD5 occurrences since boot time.
OutSHA1Hmacs	Specifies the number of outbound HMAC SHA1 occurrences since boot time.
OutAESXCBCs	Specifies the number of outbound AES XCBC MAC occurrences since boot time.
OutInAnyNullAuth	Specifies the number of outbound null authentication occurrences since boot time
Out3DESCBCs	Specifies the number of outbound 3DES CBC occurrences since boot time.
OutAESCBCs	Specifies the number of outbound AES CBC occurrences since boot time.
OutAESCTRs	Specifies the number of outbound AES CTR occurrences since boot time
OutInAnyNullEncrypt	Specifies the number of outbound null occurrences since boot time. Used for debugging purposes.

Digital certificate configuration using EDM

The following section provides procedures to configure digital certificate configuration using EDM.

Configuring device subject parameters

Use this procedure to configure the device subject parameters to identify the device. The parameters include name, Email ID, company, department, and location of the subject.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **Certificate**.
3. Click the **Subject** tab.
4. In the **CommonName** field, type the name of the subject.
5. Complete the remaining optional configuration to customize the policy.
6. Click **Apply**.

Field descriptions

Use the data in the following table to use the **Subjects** tab.

Name	Description
CommonName	Specifies the name of the subject sending the Certificate Signing Request to the Certificate Authority.
EmailAddress	Specifies the Email address of the subject sending the Certificate Signing Request to the Certificate Authority.
OrganizationalUnit	Specifies the organizational unit of the subject sending the Certificate Signing Request to the Certificate Authority.
Organization	Specifies the organization of the subject sending the Certificate Signing Request to the Certificate Authority.
Locality	Specifies the organization of the subject sending the Certificate Signing Request to the Certificate Authority.
Province	Specifies the province of the subject sending the Certificate Signing Request to the Certificate Authority.
Country	Specifies the country of the subject sending the Certificate Signing Request to the Certificate Authority.
Fqdn	Specifies the domain name.
IncludeIpAddress	Specifies the subject contains IP address.

Generating key pair

Use the following procedure to generate the private and public key pair.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **Certificate**.
3. Click the **Key-Pair** tab.
4. Click **Insert** .
5. In the Name field, enter the of the name of the key-pair.
6. Click **Apply**.

Field descriptions

Use the data in the following table to use the **Key-Pair** tab.

Name	Description
Name	Specifies the name of the key-pair generated for the subject.
Type	Specifies the cryptography algorithm used to generate the key-pair.
Size	Specifies the size of the key-pair to be generated.
SHA1 Fingerprint	Displays SHA1 fingerprint of the key.

Configuring certificate authority

Use this procedure to configure the certificate authority (CA) and perform related actions. You can configure only one CA in a device at a time.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **Certificate**.
3. Click the **CA** tab.
4. Click **Insert** .
5. In the **Name** field, type a user-defined name of the CA.
6. In the **CommonName** field, type the common name of the CA..
7. In the **KeyName** field, type the name of the associated key pair.
8. Complete the remaining optional configuration to customize the policy.
9. Click **Apply**.

Field descriptions

Use the data in the following table to use the **CA** tab.

Name	Description
Name	Specifies the user-defined name referring to the Certificate Authority issuing the Digital Certificate.
CommonName	Specifies the Common Name of the Certificate Authority issuing the Digital Certificate.
KeyName	Specifies the name of the associated key pair.
CaUrl	Specifies the URL of the Certificate Authority issuing the Digital Certificate.
Action	Executes the action for SCEP procedure: • noop — Set action to none. • caauth — Execute caauth procedure for authenticating the CA • enroll — Execute enroll procedure for obtaining subject certificate from the CA. • renew — Execute renew procedure for subject certificate. • remove — Execute remove procedure of the subject certificate. • getCrl — Ask the CRL from the CA. • genSelfSign — Generate the self signed certificate. • getCaCert — Import root and RA certificates from CA.

Table continues…

Name	Description
ActionChallengePassword	Specifies the challenge password required to perform the SCEP operation.
Authenticated	Specifies whether or the Certificate Authority is authenticated.
LastActionStatus	Specifies the status of the last action: • none - No action is performed yet. • success - Execution of the action triggered is completed successfully. • failed - Execution of the action triggered has failed. • inProgress - Execution of the action triggered is in progress.
LastActionFailureReason	Specifies the reason of failure for the last action performed by the Certificate Authority.
SubjectCertificateValidityDays	Specifies the number of days for which subject certificate will remain valid. The default value is 365 days.
UsePost	Specifies the HTTP request type: URL or POST. TRUE for EJBCA and FALSE for Win2012 CA
UseFor	Specifies which applications use the CA.
RegenerateKeyOnEnroll	Specifies whether or not a new key pair is generated before each re-enroll.
CaChainComplete	Specifies if the CA contains a complete chain.

Viewing the certificate details

Use this procedure to:

- display the configured key details for given key name.
- display the digital certificate for the given certificate index or list all the certificate details from the local store if the certificate index is not specified.
- display the CA details for given trustpoint CA name or list all the CA details from the local store if the CA name is not specified.

Procedure

1. From the navigation tree, click **Security**.
2. In the Security tree, click **Certificate**.
3. Click the **Certificate** tab.

Field descriptions

Use the data in the following table to use the **CA** tab.

Name	Description
AssociatedContextType	Displays the associated context type of the certificate.
AssociatedContextName	Displays the associated context name of the certificate.
FileName	Displays the filename of the certificate.
Type	Displays the certificate file type, such as rootCa, interCa or subjectCert,crl.
ChainPosition	Displays the certificate position in the chain.
Sha1Hash	Displays Sha1 hash of the certificate.
Md5Hash	Displays MD5 hash of the certificate.
VersionNumber	Displays the certificate version.
SerialNumber	Displays the certificate serial number.
IssuerName	Displays the certificate issuer common-name.
ValidStartPeriod	Displays the date from which the certificate is valid.
ValidEndPeriod	Displays the date to which the certificate is valid.
CertificateSignatureAlgorithm	Displays the certificate signature algorithm.
CertificateSignature	Displays the certificate signature hash.
Subject	Displays the certificate subject.
SubjectPulickKeyAlgorithm	Displays the certificate encryption
SubjectPublicKey	Displays the certificate public key hash.
HasBasicContstraint	Displays whether the certificate contains or not basic constraints
HasKeyUsage	Displays the hash key usage.
IsCa	Displays if the certificate is the root CA.
KeyUsage	Displays the certificate key usage.
Status	Displays the status of the certificate. It can be active or revoked.
CdpUrl	Displays the certificate CDP url used for CRL revocation method.
OcspUrl	Displays the certificate OCSP url used for OCSP revocation method.
ExtendedKeyUsage	Displays the certificate extended key usage.

Chapter 16: RADIUS-based Network Security

This chapter provides conceptual information and procedures to configure RADIUS-based Network Security using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

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.

You should configure two RADIUS servers so that if one server is unreachable, the switch attempts 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 switch 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.

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 CLI.

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.

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 if ICMP reachability messages from the switch to the RADIUS server, you can configure the switch to use dummy RADIUS requests. You can configure both a username and a password for the dummy account using CLI. Because the switch interprets either Request Accept or Request Reject responses as a confirmation for reachability, you do not have to add the credentials on server in order to test for server reachability. Extreme Networks recommends that you set up a dummy account with a user name and password on the RADIUS server to avoid the generation of error messages indicating invalid user logins, if RADIUS server reachability is enabled.

If the **use-radius** option is configured, the username and password for the dummy RADIUS packet can also be configured using CLI.

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

The switch regularly checks each RADIUS Server (for example, Global, EAP and NEAP servers, in that order) for reachability. For each of these RADIUS servers, the switch performs the following:

- If the primary server is reachable, the server status is updated to *reachable* and further authentication will use this server. As long as the primary server is reachable, the secondary server will not be tested for reachability.
- If the primary server is not reachable but the secondary server is reachable, the current status of the secondary server is updated to *reachable* and further authentication will use this server
- If both primary and secondary servers are unreachable, the current server status is updated to *unreachable* and no further authentication occurs until the next successful reachability check.

You can configure the intervals between two consecutive reachability checks. The default values are as follows:

- one minute, if the last check result was *unreachable*
- three minutes, if the last check result was *reachable*

A server is marked as unreachable after a number of retries and timeouts. The default number of retries is three and the default timeout value is 20 seconds, but you can also configure these values in CLI.

The use-radius method is usually better for testing reachability. Testing using ICMP packets may mark the server as reachable after a successful response from a ping, but the RADIUS Service may not be started on the server side.

RADIUS authentication delay

RADIUS authentication delay prevents authentication issues caused by bursts of re-authentication requests sent to the RADIUS Server.

In scalability setups, there are situations when the RADIUS Servers cannot respond to all these requests. Even if the RADIUS Server responds to all re-authentication requests, the switch may be unable to process all of them.

RADIUS authentication delay introduces a delay between authentications when a burst is detected. The switch limits the RADIUS requests it sends to 50 packets per second. The re-authentication period for EAP and NEAP clients is limited to a period of minimum 60 seconds.

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 server priority in MHSA mode

In MHSA mode, if you configure EAP RADIUS servers, they will be used in the following priority order:

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

In MHSA mode, if you configure NEAP RADIUS servers, they will be used in the following priority order:

- NEAP RADIUS server – primary
- NEAP RADIUS server – secondary

In MHSA mode, if you do not configure EAP RADIUS servers or NEAP RADIUS servers, Global RADIUS servers are used in the following priority order:

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

RADIUS server priority in MHMA-MV mode

Since MHMA-MV 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-MV mode

The following diagram illustrates a network that includes the following:

- a switch with a port configured for MHMA-MV
- the MHMA-MV 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

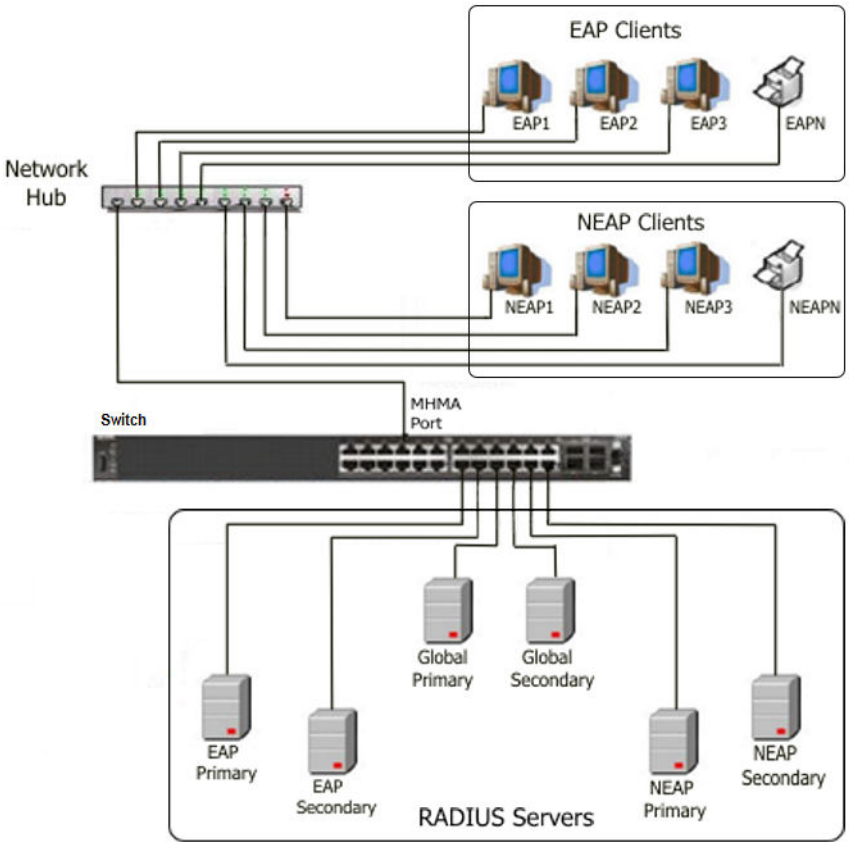


Figure 23: EAP and non-EAP RADIUS servers in MHMA-MV mode

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

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.

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 enabled by default.

RADIUS authentication fallback to secondary server

With this enhancement, each time a request to the primary RADIUS server times out after the expiration of all the configured retries, the switch queries the secondary RADIUS server as well. The fallback query respects the configured number of retries, and it is sent only if the secondary RADIUS server is configured. The switch sends the fallback query regardless of the secondary server being known to be reachable or not.

Configuring RADIUS authentication

You can configure and manage RADIUS authentication using CLI 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:

When both in band and out of band IP addresses are configured and RADIUS use management IP is enabled, the switch chooses the IP address that is closer to the destination network as source for the RADIUS request. This information is taken from the routing table. For example, if the RADIUS server is in a subnet that appears in the routing table as being reachable using the in-band configuration, then the in-band address will be used to send the RADIUS requests. If

the device has a management route configured for the subnet containing the RADIUS server the OOB address will be used.

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 21: 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.
NAS-Port	This is equal to the unit number in a stack if the customer uses the console port. If the connection is

Table continues…

RADIUS attribute	Definition
	virtual, you should set this value 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. • 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 CLI and EDM.

RADIUS Management Accounting with TACACS+ support

RADIUS Management Accounting provides the ability to send RADIUS accounting packets for management events such as user login/logout or session time-outs for a logged in user. When enabled, this feature allows TACACS+ related messages to be transmitted to the RADIUS server.

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.

RFC 4675 RADIUS Attributes: Egress-VLANID and Egress-VLAN-NAME

This feature introduces support for two standard RADIUS attributes defined in RFC 4675: *Egress-VLANID* and *Egress-VLAN-NAME*. Using these attribute you can control the 802.1Q tagging for traffic egressing a port where RADIUS authentication was performed for a connected EAP or non-EAP client.

You must configure the preferred tagging option and the VLAN name or ID on the RADIUS server. Egress-VLANs are standard attributes, therefore the RADIUS Server should support them by default and offer the ability to configure them. Each attribute contains two parts, the first indicating whether frames on the VLAN egress must be tagged or untagged, and the second specifying the VLAN name or VLAN ID.

The switch applies the VLAN received in the Egress-VLAN attributes to the port where the client was authenticated via RADIUS and then sets the tagging rules (tagged or untagged) accordingly.

The switch does not operate a PVID change due to either one of these attributes. If you need any PVID modification, you must also send attributes that modify the PVID, such as Tunnel-Private-Group-ID or Fabric Attach ISID.

The switch does not automatically create the VLANs specified in these attributes. If you need the VLANs to be auto-created, include attributes that support VLAN auto-creation, such as Tunnel-Private-Group-ID or Fabric Attach ISID. The switch processes last the Egress-VLAN attributes when decoding the RADIUS packet, therefore the switch will first create the VLANs then set the propper tagging for them. You can also create in advance the VLANs on the switch.

Untagged devices such as PCs, or laptops should use the Tunnel-Private-Group-ID attribute, which controls the ingress VLAN. Tagged devices such as phones should use Egress VLAN attribute. For configuring an untagged VLAN for both ingress and egress, Tunnel-Private-Group-ID attribute must be used, while Egress VLAN attributes may be necessary.

The Egress VLAN attributes introduce a new *Hybrid* tagging mode that supports multiple tagged and multiple untagged VLANs on a port. Use the **`show vlan interface info`** command to display the tagging on a VLAN interface. The output of the **`show vlan interface verbose`** command is also updated to indicate whether a VLAN is tagged or untagged.

Feature configuration

In order to use the Egress VLAN attributes, you must enable the *Radius assigned VLAN* and *NEAP use RADIUS assigned VLAN* features. Enter the following CLI commands to enable these features:

- eapol multihost use-radius-assigned-vlan
- eapol multihost non-eap-use-radius-assigned-vlan

Limitations

Because ADAC also sets a custom tagging on the ports where it is enabled, the switch does not process Egress-VLAN attributes on ADAC-enabled EAP ports.

In this release, RFC 5176 Change of Authorization (CoA) is not available for the Egress-VLAN attributes.

RADIUS dynamic authorization extension (RFC 5176)

With RADIUS dynamic authorization extension (RFC 5176), you can enable a third party device to dynamically change VLANs on switches or close user sessions.

The RADIUS dynamic authorization extension devices include the following:

- Network Access Server (NAS) — the switch that authenticates each EAP/NEAP client at a RADIUS server.
- RADIUS server sends disconnect, reauthentication and Change of Authorization (CoA) requests to the NAS. A CoA command modifies user session authorization attributes, disconnect command ends a user session and a reauthentication command reauthenticates 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).
- EAP/NEAP client — the device that requires authentication and uses the switch services.

Important:

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

The switch can receive reauthentication, 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)

RADIUS dynamic authorization extension functions when either of the RADIUS VLAN assignment features are active on a port.

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 RADIUS dynamic authorization extension feature, 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 reauthentication, disconnect or CoA commands if the commands addresses a port on which RADIUS 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. You should 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, you should configure proxies to confirm that NAS identification attributes match the source IP address of the RADIUS UDP packet.

RADIUS dynamic authorization extension complies with the following standards and RFCs:

- IEEE 802.1X standard (EAP)
- RFC 2865–RADIUS
- RFC 5176–Dynamic Authorization Extensions to RADIUS

RFC 5176 Disconnect and CoA support for NEAP clients

This feature adds support for processing of RFC 5176 Disconnect and Change of Authorization (CoA) RADIUS requests for Non-EAP clients.

To enable the feature on a specific port or list of ports, you must perform the following actions:

- globally enable EAP
- enable EAP per-port
- enable dynamic authorization extension per-port

- configure the RADIUS dynamic client

Disconnect request processing

When the feature is operational, after receiving a RADIUS Disconnect-Request packet, the switch disconnects authenticated NEAP users on a port and removes the requested client session.

If the requested user session is found and all attributes specified in the RADIUS server request exist on the required port, the switch performs the following operations for that session:

- removes the requested client session from the specified port
- performs port VLAN restore operations if the port does not have other sessions
- removes the port from any existing RADIUS assigned VLAN

If all the above operations perform successfully, the switch sends the *Disconnect-ACK* disconnect response to the RADIUS dynamic client. If the user session is not found or the switch is unable to disconnect the client session, the switch sends the *Disconnect-NAK* response to the RADIUS dynamic client, including the cause of the problem.

CoA command processing

When the feature is operational, after receiving a RADIUS CoA-Request packet, the switch dynamically changes port assignment for a specific port to a specific VLAN.

If the requested user session is found and a valid VLAN ID is specified for the port, the switch performs the following operations:

- if the specified port is assigned to a VLAN different than the one specified in the RADIUS request, the port is removed from that VLAN and assigned to the VLAN specified in the RADIUS request
- depending on the configured EAP mode, the switch can change the port PVID to the new VLAN value

If the above operations perform successfully, the switch sends a CoA-ACK response to the RADIUS dynamic client.

If the requested user session is not found, the VLAN specified in the request is not port-based or if errors are encountered while processing the CoA request, the switch sends a CoA-NAK response to the RADIUS dynamic client, including the cause of the problem.

Note:

CoA requests for NEAP clients with Guest VLAN enabled will reauthenticate the clients.

RADIUS authentication configuration using CLI

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

Configuring switch RADIUS server settings

Before you begin

- Configure at least one RADIUS server.
- Physically connect the RADIUS server to your network.

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure RADIUS server account information on the switch :

   ```
   [no] [default] radius server host {<A.B.C.D> |<WORD>} [acct-enable]
   [acct-port <port>] [key{key}] [port <port>] [retry <1-5>]
   [secondary] [timeout <1-60>] [used-by <eapol| non-eapol>]
   ```

3. Configure the RADIUS server authentication type:

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

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

Table continues…

Variable	Value
	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 10 seconds.
used-by <eapol | non-eapol>	Specifies the RADIUS server as an EAP RADIUS Server or a Non-EAP (NEAP) RADIUS Server. • eapol—configures the RADIUS server to process EAP client requests only. • non-eapol—configures the RADIUS server to process Non-EAP client requests only.

Enabling or disabling RADIUS password fallback

About this task

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.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable RADIUS password fallback:

```
radius-server password fallback
```

OR

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

3. Disable RADIUS password fallback:

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

Viewing RADIUS information

About this task

Use this procedure to display RADIUS server configuration information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display RADIUS configuration status:

```
show radius-server
```

Example

```
Switch>enable
Switch#show radius-server
RADIUS Global Server
----------------------------------------------------------------
Primary Host           : 0.0.0.0
Secondary Host         : 0.0.0.0
Port                   : 1812
Time-out               : 2
Key                    : ***************
Radius Accounting      : Disabled
Radius Accounting Port : 1813
Radius Retry Limit     : 3
Current Status         : None Reachable
Time Until Next Check  : 40

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
Current Status         : None Reachable
Time Until Next Check  : 40

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
Current Status         : None Reachable
Time Until Next Check  : 40

Other Settings
----------------------------------------------------------------
Password Fallback      : Enabled
RADIUS Encapsulation   : PAP
```

Configuring RADIUS server reachability

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure the reachability of the RADIUS server:

   ```
   [default] radius reachability {check {eap | non-eap} [global] | mode
   {use-icmp | use-radius [username <username> password <password>}
   [timeout <1-60>][retry <1-5>] [bad-timer <30-600>] [good-timer
   <30-600>] | bad-timer <30-600> | good-timer <30-600> | retry <1-5>}
   ```

Variable definitions

Use the data in the following table to use the **`radius reachability`** command.

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

Table continues…

Variable	Value
timeout <1–60>	Sets the time-out period. Range is 1 to 60 seconds.
retry <1–5>	Specifies the number of retry attempts. Range is from 1 to 5.
bad-timer <30–600>	Sets the interval between checks when the RADIUS server is unreachable. Range is 30 to 600 seconds.
check	Initiates an immediate check to determine the reachability of the RADIUS server.
eap	Checks the EAP RADIUS server reachability.
global	Checks the Global RADIUS server reachability.
non-eap	Checks the Non-EAP RADIUS server reachability.
good-timer <30–600>	Sets the interval between checks when the RADIUS server is reachable. Range is 30 to 600 seconds.

Viewing the RADIUS server reachability method

About this task

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

Procedure

1. Logon to the User EXEC mode in CLI.
2. Display the configured RADIUS server reachability method:

   ```
   show radius reachability
   ```

Example

```
Switch>show radius reachability
RADIUS reachability: USE ICMP
RADIUS reachability timeout: 2
RADIUS reachability retry: 3
RADIUS reachability bad timer: 60
RADIUS reachability good timer: 180
```

RADIUS dynamic authorization extension (RFC 5176) configuration using CLI

You can configure RADIUS dynamic authorization extension (RFC 5176) for a third party device to dynamically change VLANs on switches or close user sessions.

Configuring RADIUS dynamic authorization extension (RFC 5176)

Before you begin

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

Important:

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

About this task

Configure RADIUS dynamic authorization extension (RFC 5176) to enable the RADIUS server to send a change of authorization (CoA), disconnect or reauthentication command to the Network Access Server (NAS).

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure RADIUS dynamic authorization extension:

   ```
   radius dynamic-server client A.B.C.D [ secret] [ port <1024-65535> ]
   [ enable ] [process-disconnect-requests] [process-change-of-auth-
   requests] [process-reauthentication-requests]
   ```

Variable definitions

Use the data in the following table to use the **`radius dynamic-server client`** 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.
process-reauthentication-requests	Enables reauthentication request processing.

Table continues…

Variable	Value
secret	Configures the RADIUS Dynamic Authorization Client secret word.

Disabling RADIUS dynamic authorization extension (RFC 5176)

About this task

Disable RADIUS dynamic authorization extension (RFC 5176) to prevent the RADIUS server to send a change of authorization (CoA) or disconnect command to the Network Access Server (NAS).

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable RADIUS dynamic authorization extension:

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

Variable definitions

Use the data in the following table to use the **`no radius dynamic-server client`** command.

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

Viewing RADIUS dynamic authorization extension (RFC 5176) configuration

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Configure View RADIUS dynamic authorization client configuration:

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

Variable definitions

Use the data in the following table to use the **show radius dynamic-server client <A.B.C.D.>** command.

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

Viewing RADIUS dynamic authorization extension (RFC5176) statistics

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View RADIUS dynamic authorization client configuration:

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

Variable definitions

Use the data in the following table to use the **show radius dynamic-server statistics client <A.B.C.D.>** command.

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

Enabling dynamic authorization extension (RFC 5176) on EAP ports

About this task

Enable dynamic authorization extension (RFC 5176) on EAP ports for the ports to process CoA and disconnect requests from the RADIUS server.

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable
   ```

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

2. Enable RADIUS dynamic authorization extension (RFC 5176) on an EAP port

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

3. Enable RADIUS dynamic authorization extension (RFC 5176) on a specific EAP port or a list of EAP ports:

```
eapol port <LINE> radius-dynamic-server enable
```

Variable definitions

Use the data in the following table to use the **`eapol port <LINE> radius-dynamic-server enable`** command.

Variable	Value
<LINE>	Specify an individual port or list of ports.

Disabling RADIUS dynamic authorization extension (RFC 5176) on EAP port

About this task

Disable RADIUS dynamic authorization extension (RFC 5176) on EAP ports to discontinue the ports from processing CoA and disconnect requests from the RADIUS server.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. Disable RADIUS dynamic authorization extension (RFC 5176) on an EAP port:

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

3. Disable RADIUS dynamic authorization extension (RFC 5176) on a specific EAP port or a list of EAP ports:

```
no eapol port <LINE> radius-dynamic-server enable
```

Variable definitions

Use the data in the following table to use the **`no eapol port <LINE> radius-dynamic-server enable`** command.

Variable	Value
<LINE>	Specify an individual port or list of ports.

Enabling RADIUS dynamic authorization extension (RFC 5176) default on EAP ports

About this task

Enable RADIUS dynamic authorization extension (RFC 5176) default on EAP ports to return the ports to the default configuration for processing CoA and disconnect requests from the RADIUS server.

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable

   configure terminal

   interface Ethernet <port>
   ```

2. Enable RADIUS dynamic authorization extension (RFC 5176) default on an EAP port:

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

3. Enable RADIUS dynamic authorization extension (RFC 5176) default on a specific EAP port or a list of EAP ports:

   ```
   default eapol port <LINE> radius-dynamic-server enable
   ```

Variable definitions

Use the data in the following table to use the **`default eapol port <LINE> radius-dynamic-server enable`** command.

Variable	Value
<LINE>	Specify an individual port or list of ports.

RADIUS accounting configuration using CLI

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 on page 438.

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

About this task

Use this procedure to enable RADIUS accounting for a Global, EAPOL, or non-EAPOL RADIUS server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable RADIUS accounting for a Global RADIUS server:

   ```
   radius server host [<ipaddr> | <ipv6addr>] acct-enable
   ```

3. Enable RADIUS accounting for an EAPOL RADIUS server:

   ```
   radius server host [<ipaddr> | <ipv6addr>] used-by eapol acct-enable
   ```

4. Enable RADIUS accounting for a non-EAPOL RADIUS server:

   ```
   radius server host [<ipaddr> | <ipv6addr>] used-by non-eapol acct-
   enable
   ```

Variable definitions

Use the data in the following table to use the **`radius server host`** command.

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

About this task

Use this procedure to disable RADIUS accounting for a Global, EAPOL, or non-EAPOL RADIUS server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable RADIUS accounting for a Global RADIUS server:

   ```
   no radius server host [<ipaddr> | <ipv6addr>] acct-enable
   ```

3. Disable RADIUS accounting for an EAPOL RADIUS server:

   ```
   no radius server host [<ipaddr> | <ipv6addr>] used-by eapol acct-enable
   ```

4. Disable RADIUS accounting for a non-EAPOL RADIUS server:

   ```
   no radius server host [<ipaddr> | <ipv6addr>] used-by non-eapol acct-enable
   ```

Variable definitions

Use the data in the following table to use the **`no radius server host`** command.

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

About this task

Use this procedure to set RADIUS accounting for a Global, EAPOL, or non-EAPOL RADIUS server to default.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Set RADIUS accounting for a Global RADIUS server to default:

   ```
   default radius server host [<ipaddr> | <ipv6addr>] acct-enable
   ```

3. Set RADIUS accounting for an EAPOL RADIUS server to default:

   ```
   default radius server host [<ipaddr> | <ipv6addr>] used-by eapol acct-enable
   ```

4. Set RADIUS accounting for a non-EAPOL RADIUS server to default:

   ```
   default radius server host [<ipaddr> | <ipv6addr>] used-by non-eapol acct-enable
   ```

Variable definitions

Use the data in the following table to use the **default radius server host** command.

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

About this task

Use this procedure to enable or disable RADIUS interim accounting updates and configure the interval timeout period for the updates. You can also set these parameters to default values.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure RADIUS interim accounting updates.

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

3. Disable RADIUS interim accounting updates.

   ```
   no radius accounting interim-updates [enable] [use-server-interval]
   ```

4. Set RADIUS interim accounting updates to default values.

   ```
   default radius accounting interim-updates [enable] [interval] [use-
   server-interval]
   ```

Variable definitions

The following table defines parameters that you can enter with the **radius accounting interim-updates** command.

Variable	Value
default	Sets specified parameter(s) to their default values.
no	Disables the specified parameter(s).
enable	Enables or disables RADIUS accounting interim updates for the switch. DEFAULT: disabled

Table continues…

Variable	Value
interval <seconds>	Specifies the time interval (in seconds) before RADIUS accounting interim updates times out. DEFAULT: 600
use-server-interval	Enables or disables the use of the RADIUS server applied timeout interval for interim updates. DEFAULT: enabled

Viewing RADIUS interim accounting updates information

About this task

Displays information about RADIUS interim accounting updates configuration.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display RADIUS interim accounting updates information.

   ```
   show radius accounting interim-updates
   ```

Example

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

Changing the RADIUS password

Before you begin

- You must have at least one configured and reachable RADIUS server in your network.
- You must have enabled RADIUS encapsulation MS-CHAPv2

About this task

Changes the RADIUS password once connected to the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Change RADIUS password.

```
cli password change
```

Example

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no radius-server encapsulation ms-chap-v2
Switch(config)#cli password change
% Enable radius MSCHAPV2 encapsulation first.
Switch(config)#radius-server encapsulation ms-chap-v2
Switch(config)#cli password change
Changing password for user: rw
Enter old password        : ******
Enter New Password        : *********
Re-enter New Password     : *********
```

RADIUS Request use Management IP configuration using CLI

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

Enabling the RADIUS Request to use Management IP address

Perform this procedure to enable the RADIUS requests to use the Management VLAN IP address.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable RADIUS Request to use the Management IP address.

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

3. Verify the settings.

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

Disabling the RADIUS Request to use the Management IP address

Follow this procedure to disable the RADIUS requests to use the Management VLAN IP address.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Disable the RADIUS Request to use the Management IP address.

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

3. Verify the settings.

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

Setting the RADIUS Request use the Management IP address to default mode

Follow this procedure to set the RADIUS Request to use the Management IP address to default mode.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Set the RADIUS Request to use the Management IP address to default mode.

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

3. Verify the settings.

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

RADIUS security configuration

Use the following procedures to configure RADIUS security for the switch.

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

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.
6. 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.
7. In the RADIUS section, click a **Reachability** radio button.
8. In the RADIUS section, type the reachability user name in the **ReachabilityUserName** dialog box.
9. In the RADIUS section, type the reachability password in the **ReachabilityPassword** dialog box.
10. In the RADIUS section, type the reachability password again to confirm in the **Confirm ReachabilityPassword** dialog box.
11. In the RADIUS Encapsulation section, click an **EncapsulationProtocol** radio button.
12. On the toolbar, click **Apply**.

Variable definitions

Use the data in the following table configure RADIUS security and encapsulation for the switch

Variable	Value
RADIUS	
UseMgmtIp	When selected, RADIUS uses the system management IP address as the source address for RADIUS requests.

Table continues…

Variable	Value
PasswordFallbackEnabled	When selected, enables RADIUS password fallback.
DynAuthReplayProtection	When selected, enables RADIUS replay protection.
RADIUS Reachability	
Mode	Specifies the RADIUS server reachability mode. Values include: • useRadius—uses dummy RADIUS requests to determine reachability of the RADIUS server. • useIcmp—uses ICMP packets to determine reachability of the RADIUS server (default).
UserName	Specifies a user identification name for RADIUS reachability.
Password	Specifies a user password for RADIUS reachability.
Confirm Password	Re-enter the user password for verification.
Timeout	Specifies the timeout period. DEFAULT: 10 seconds
Retry	Specifies the number of retry attempts. DEFAULT: 3
BadTimer	Specifies the interval between checks when the RADIUS server is unreachable. DEFAULT: 60 seconds
GoodTimer	Specifies the interval between checks when the RADIUS server is reachable. DEFAULT: 180 seconds
RADIUS Encapsulation	
EncapsulationProtocol	Specifies the type of encapsulation for the RADIUS packets. Values include: • 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

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

Use the data in this table to enable or disable RADIUS accounting and to configure RADIUS accounting interim updates.

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. • 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.

Note:

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

Procedure

1. From the navigation tree, double-click **Security**.

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 **Confirm SharedSecret(Key)** box.
12. To enable accounting, select 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

Use the data in this table to configure a Global RADIUS Server for processing client requests without designating separate EAP or Non-EAP requests.

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. **Important:** 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.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary Global RADIUS Server. Values include unknown, ipv4, and ipv6.
SecondaryRadiusServer	Specifies the IP address for the secondary Global RADIUS Server. The default address is 0.0.0.0. The secondary Global

Table continues…

Variable	Value
	RADIUS Server is used only if the primary Global RADIUS Server is unavailable or unreachable. **Important:** 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.
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 value is 10 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.
Confirm SharedSecret(key)	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.
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 1 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

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. Select 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

Use the data in this table to configure an EAP RADIUS Server for processing EAP client requests.

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. **Important:** 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.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary EAP RADIUS Server. Values include unknown, ipv4, and ipv6.
SecondaryRadiusServer	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. **Important:** 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.

Table continues…

Variable	Value
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 value is 10 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 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

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 time-out 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, select 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 definitions

Use the data in this table to configure a Non-EAP (NEAP) RADIUS Server for processing NEAP client requests only.

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. Important: **Important:** 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.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary NEAP RADIUS Server. Values include unknown, ipv4, and ipv6.
SecondaryRadiusServer	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. **Important:** 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.
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.

Table continues…

Variable	Value
RadiusServerTimeout	Specifies the timeout interval between each retry for service requests to the NEAP RADIUS Server. The default value is 10 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.
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 1 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

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.
DisconInvalidClientAddresses	Indicates the number of Disconnect-Request packets received from unknown addresses.

Table continues…

Variable	Value
CoAInvalidClientAddresses	Indicates the number of CoA-Request packets received from unknown addresses.

Viewing RADIUS Dynamic Server statistics using EDM

Use the following procedure to display RADIUS Dynamic Server statistical information.

Procedure

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 Dymanic Server client index.
ClientAddressType	Indicates the type of RADIUS Dymanic Server address. Values are ipv4 or ipv6.
ClientAddress	Indicates the IP address of the RADIUS Dymanic Server.
ServerCounterDiscontinuity	Indicates a count of RADIUS Dymanic Server discontinuity instances.

Creating a RADIUS dynamic authorization extension (RFC 5176) client using EDM

Use the following procedure to create an RADIUS Dynamic Authorization client for the switch.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **Radius**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.

4. Click **Insert**.

   The Insert RADIUS Dynamic Auth. Client dialog box displays.
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** check box.

   OR

   To disable the RADIUS Dynamic Authorization client, clear the **Enabled** check box.
8. In the **UdpPort** dialog box, type a port number.
9. To enable change of authorization request processing, select the **ProcessCoARequests** check box.

   OR

   To disable change of authorization request processing, clear the **ProcessCoARequests** check box.
10. To enable disconnect request processing, select the **ProcessDisconnectRequests** check box.

    OR

    To disable disconnect request processing, clear the **ProcessDisconnectRequests** check box.
11. To enable process re-authentication requests, select the **ProcessReAuthRequests** check box.

    OR

    To disable process re-authentication requests, clear the **ProcessReAuthRequests** check box.
12. In the **Secret** dialog box, type a shared secret word.
13. Click **Insert**.
14. 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.

Table continues…

Variable	Value
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.
ProcessReAuthRequests	Enables or disables process re-authentication requests.
Secret	Defines the secret word shared between the RADIUS Dynamic Authorization Client and the RADIUS server.

Deleting a RADIUS dynamic authorization extension (RFC 5176) client configuration using EDM

Use the following procedure to delete an existing RADIUS Dynamic Authorization client configuration.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **Radius**.
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 RADIUS dynamic authorization extension (RFC 5176) client configuration using EDM

Use the following procedure to display existing RADIUS Dynamic Authorization client configurations for the switch.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, click **Radius**.

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 configurations for the switch.

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.
ProcessReAuthRequests	Indicates whether process re-authentication requests is enabled or disabled.
Secret	Indicates the secret word shared between the RADIUS Dynamic Authorization Client and the RADIUS server.

Modifying the RADIUS dynamic authorization extension (RFC 5176) client configuration using EDM

Use the following procedure to edit an existing RADIUS Dynamic Authorization client configuration.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **Radius**.
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 the RADIUS dynamic client processing, or **false** to disable the RADIUS dynamic client processing.

7. Select a value from the list—**true** to enable RADIUS Dynamic Authorization client, or **false** to disable RADIUS Dynamic Authorization client for the VLAN.
8. In the client row, double-click the cell in the **UdpPort** column.
9. Edit the UDP port number as required.
10. In the client row, double-click the cell in the **ProcessCoARequests** column.
11. Select a value from the list—**true** to enable CoA request processing, or **false** to disable CoA request processing.
12. In the client row, double-click the cell in the **ProcessDisconnectRequests** column.
13. Select a value from the list—**true** to enable disconnect request processing, or **false** to disable disconnect request processing.
14. In the client row, double-click the cell in the **ProcessReAuthRequest** column.
15. Select a value from the list—**true** to enable reauthentication processing requests from a RADIUS dynamic client, or **false** to disable reauthentication processing requests from a RADIUS dynamic client.
16. On the toolbar, click **Apply**.

Variable definitions

Use the data in the following table to modify an existing RADIUS Dynamic Authorization client

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. • 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.
ProcessReAuthRequest	Enables or disables reauthentication request processing.
Secret	The RADIUS Dynamic Authorization Client secret word. This cell remains empty.

Changing the RADIUS dynamic authorization extension (RFC 5176) client secret word using EDM

Use the following procedure to change the existing RADIUS Dynamic Authorization client secret word.

Procedure

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **Radius**.
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**.

Graphing RADIUS Dynamic Server statistics using EDM

Use the following procedure to graph statistics for a RADIUS Dynamic Server client.

Procedure

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**.

Chapter 17: Secure Shell

The following sections describe how to use Secure Shell (SSH) to enable secure communications support over a network for authentication, encryption, and network integrity.

Secure Shell Protocol

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

The SSH protocol includes two versions: SSH1 and SSH2. The switch 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 CLI 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 banner

When the SSH banner is enabled, a message is displayed to the SSH clients before completing the SSH login, prior to entering the password. This ensures the awareness of the institution’s security policy. By default, the banner is not configured.

The SSH banner can be customized by downloading it on the switch from the TFTP server as a text file. For example, sshBanner.txt.

Note:

SSH banner feature is present only on SSH images.

SSH banner in stack

SSH banner is configured on all units in the stack. If the stack breaks, then all units in the stack use the recently configured SSH banner. When a stack is formed, the SSH initialization overrides the SSH banner of all units in the stack with the SSH banner of the base.

SSH retry

Using the SSH retry feature, you can control SSH configuration by setting number of retries from 1 to 100, or set the retries to the default value of 3. When the switch is in stack mode and you set the number of SSH retries, it is adopted by all the other switches in the stack.

Note:

The SSH retry feature is enabled only when SSH is enabled.

SSH clients

The switch supports the following SSH clients:

- 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 CLI.

The 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 exists, 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 CLI, enter a '~' followed by a period (~.). You can also use the CLI command 'ssh close-session' from a different CLI console.

Note:

When an SSH session is initiated to a host which is not IP reachable, the console is blocked until the timeout for trying to establish a TCP connection to the host expires. By design, a TCP connection attempt times out after 75 seconds if the connection is unsuccessful.

Note:

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 know 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 CLI, 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.

SSH rekeying

SSH rekeying is an SSHv2 feature that allows the SSH server or client to force a key exchange between server and client, while changing the encryption and integrity keys. After you enable SSH rekeying, key exchanges occur after the configured time interval. The default time-interval is 1 hour. You can configure this value, or enable or disable SSH rekeying.

SSH rekey is disabled by default when enhanced secure mode is disabled on switch, and enabled by default when enhanced secure mode is enabled.

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.

Secure Shell protocol configuration using CLI

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

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

Displaying SSH information using CLI

Use this procedure to display general SSH settings and information about all active SSH sessions.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Enter the following command:

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

Example

The following example displays sample output for the **`show ssh global`** command:

```
Switch(config)#show ssh global
Active SSH Sessions     :  0
Version                 :  Version 2 only
Port                    :  22
Authentication Timeout  :  60
DSA Authentication      :  True
RSA Authentication      :  True
```

```
Password Authentication :  True
X.509v3 Authentication  :  True
X.509v3 Username Overwrite  : False
X.509v3 Strip Domain    :  False
X.509v3 Use-Domain      :
Auth Retries            :  3
SSH Rekey               :  False
SSH Rekey-Interval      :  3600000
SSH Rekey-DataLimit     :  1
Auth Key TFTP Server    :  192.0.2.1
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys           :  Exist
RSA Host Keys           :  Exist
Enabled                 :  False
```

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

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

Variable definitions

Use the data in the following table to use the **show ssh** command.

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

Enabling SSH using CLI

Use this procedure to enable SSH in a non-secure mode. If the host keys do not exist, they are generated.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable SSH in a non-secure mode:

   ```
   ssh
   ```

3. Disable SSH for the switch:

   ```
   no ssh {dsa-auth | dsa-auth-key | dsa-host-key| pass-auth | rsa-auth
   | rsa-auth-key | rsa-host-key | x509v3-auth}
   ```

Variable definitions

Use the data in the following table to use the **ssh** command.

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.
pass-auth	Disables SSH password authentication.
rsa-auth	Disables SSH RSA authentication.
rsa-auth-key	Deletes the SSH RSA authentication key.
rsa-host-key	Deletes the SSH RSA host key.
x509v3–auth	Disables x509v3 authentication.

Generating a new SSH DSA host key using CLI

Use this procedure to generate a new SSH DSA host key for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Generate a new SSH DSA host key for the switch:

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

3. Delete the switch SSH DSA host key:

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

Generating a new SSH RSA host key using CLI

Use this procedure to generate a new SSH RSA host key in the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Generate a new SSH RSA host key in the switch:

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

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

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

Downloading DSA or RSA authentication keys using CLI

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Download the DSA or RSA authentication key into the switch:

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

Variable definitions

Use the data in the following table to use the **`ssh download-auth-key`** command.

Variable	Value
address <*A.B.C.D*> | <*WORD*>	Specifies the address of the TFTP server. • 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 CLI

Use this procedure to delete the SSH DSA authentication key in the switch.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Delete the SSH DSA authentication key in the switch:

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

Deleting the SSH RSA authentication key using CLI

Use this procedure to delete the SSH RSA authentication key in the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Delete the SSH RSA authentication key in the switch:

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

Enabling user log-on with an SSH DSA key using CLI

Use this procedure to enable user log-on with SSH DSA key authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable user log-on with SSH DSA key authentication with either of the following commands:

   ```
   ssh dsa-auth
   ```

   OR

   ```
   default ssh dsa-auth
   ```

3. Disable user log-on with SSH DSA key authentication:

   ```
   no ssh dsa-auth
   ```

Enabling user log-on with an SSH RSA key using CLI

Use this procedure to enable user log-on with SSH RSA key authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable user log-on with SSH RSA key authentication:

```
ssh rsa-auth
```

OR

```
default ssh rsa-auth
```

3. Disable user log-on with SSH RSA key authentication:

```
no ssh rsa-auth
```

Enabling user log-on with SSH password authentication using CLI

Use this procedure to enable user log-on using the SSH password authentication method.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable user log-on using the SSH password authentication method:

```
ssh pass-auth
```

OR

```
default ssh pass-auth
```

3. Disable user log-on using the SSH password authentication method:

```
no ssh pass-auth
```

Disabling SNMP and Telnet With SSH using CLI

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Disable SNMP and Telnet management interfaces permanently:

```
ssh secure [force]
```

Variable definitions

Use the data in the following table to use the **`ssh secure`** command.

Variable	Value
force	Skips the confirmation step.

Configuring the TCP port for SSH daemon using CLI

Use this procedure to configure the TCP port for the SSH daemon.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the TCP port for the SSH daemon:

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

Variable definitions

Use the data in the following table to use the **`ssh port`** command.

Variable	Value
<1-65535>	Specifies the number of the TCP port to use.

Configuring the default TCP port for the SSH daemon using CLI

Use this procedure to configure the default TCP port for the SSH daemon.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the default TCP port for the SSH daemon:

   ```
   default ssh port
   ```

Configuring the SSH timeout using CLI

Use this procedure to configure the SSH authentication timeout, in seconds.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the SSH authentication timeout:

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

Variable definitions

Use the data in the following table to use the **`ssh timeout`** command.

Variable	Value
<1-120>	Specifies the desired timeout value in seconds.

Configuring the SSH timeout to default using CLI

Use this procedure to configure the SSH authentication timeout to the default value of 60 seconds.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
default ssh timeout
```

Configuring and clearing the SSH banner

About this task

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

Note:

The maximum size of the SSH banner is 1564 characters.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the SSH banner:

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

3. Display the SSH banner:

```
show ssh banner
```

4. **(Optional)** Clear the SSH banner:

```
clear ssh banner
```

Example

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

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

Variable definitions

Use the data in the following table to use the **`ssh download-banner address`** command.

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

Configuring SSH retry

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure SSH entry retries:

```
ssh retries <1-100>
```

3. **(Optional)** Set SSH retries to default value:

```
default ssh retries
```

Enabling or disabling SSH rekey

About this task

Use this procedure to enable or disable SSH rekey. By default, SSH rekey is disabled when enhanced secure mode is disabled, and enabled when enhanced secure mode is enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable SSH rekey, enter the following command:

   ```
   ssh rekey
   ```

3. To disable SSH rekey, enter the following command:

   ```
   no ssh rekey
   ```

Configuring SSH rekey interval

About this task

Use this procedure to configure the SSH rekey datalimit.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the SSH rekey interval:

   ```
   ssh rekey-datalimit <1–6>
   ```

Variable definitions

Use the data in the following table to use the `ssh rekey-datalimit` command.

Variable	Definition
<1–6>	Specifies the SSH rekey data limit, in Gigabytes. The default data limit is 1 Gigabyte.

Configuring SSH rekey interval

About this task

Use this procedure to configure the SSH rekey interval.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the SSH rekey interval:

   ```
   ssh rekey-interval <1-6>
   ```

Variable definitions

Use the data in the following table to use the `ssh rekey-interval` command.

Variable	Definition
<1–6>	Specifies the SSH rekey interval, in hours. The default interval is 1 hour.

SSH x509v3 Authentication and SSH Server configuration

Use the procedures in this section to configure SSH x509v3 Authentication and SSH Server.

Configuring SSH X.509v3 Authentication

Use the following procedure to configure SSH X.509v3 authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command to enable SSH X.509v3 Authentication:

   ```
   ssh x509v3-auth
   ```

   Note:

   You cannot enable x509v3 authentication if there is no trustpoint configured for SSH.

3. Enter the following command to disable SSH X.509v3 Authentication:

   ```
   no ssh x509v3-auth
   ```

Note:

You cannot disable a trustpoint if SSH x509v3 authentication is configured.

Example

The following sample output displays when you try to enable x590v3 authentication without a trustpoint configured for SSH:

```
Switch(config)#ssh x509v3-auth
%Cannot modify settings
% No CA is configured for SSH Server.
```

The following sample output displays when you try to disable a trustpoint when SSH x509v3 authentication is configured:

```
Switch(config)#no certificate ca CAC use-for
% Cannot modify settings
% CA is currently used for SSH x509v3Auth
```

Displaying SSH X.509v3 Authentication

Use the following procedure to display SSH X.509v3 authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enter the following command:

   ```
   show ssh global
   ```

Example

```
Switch(config)#show ssh global
Active SSH Sessions     :  0
Version                 :  Version 2 only
Port                    :  22
Authentication Timeout  :  60
DSA Authentication      :  True
RSA Authentication      :  True
Password Authentication :  True
X.509v3 Authentication  :  True
X.509v3 Username Overwrite  : False
X.509v3 Strip Domain    :  False
X.509v3 Use-Domain      :
Auth Retries            :  3
SSH Rekey               :  False
SSH Rekey-Interval      :  3600000
SSH Rekey-DataLimit     :  1
Auth Key TFTP Server    :  192.0.2.1
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys           :  Exist
RSA Host Keys           :  Exist
Enabled                 :  False
```

Enabling Username Overwrite

Authorization is performed based on the username sent by the SSH Client. The username contains information from the client certificate—subject alternative name and principal name. The username is extracted from the Principal Name field contained in the certificate. The username can be local or remote on the RADIUS server.

Note:

If RADIUS is configured and is reachable, RADIUS is used with no fallback to local authorization; otherwise, local authorization is used. With RADIUS authorization, you are prompted to enter a password associated with the username when you try to pass the banner (Ctrl+y). If your username is configured with an empty password, press **Enter** in the password field.

About this task

Use the following procedure to overwrite the username sent by the SSH client.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   ssh x509v3-auth username overwrite
   ```

3. Enter the following command to return to default configuration:

   ```
   default ssh x509v3-auth username overwrite
   ```

   OR

   ```
   no ssh x509v3-auth username overwrite
   ```

Example

```
Switch#show ssh global
Active SSH Sessions     :  0
Version                 :  Version 2 only
Port                    :  22
Authentication Timeout  :  60
DSA Authentication      :  True
RSA Authentication      :  True
Password Authentication :  True
X.509v3 Authentication  :  True
X.509v3 Username Overwrite  :  True
X.509v3 Strip Domain    :  False
X.509v3 Use-Domain      :
Auth Retries            :  3
SSH Rekey               :  False
SSH Rekey-Interval      :  3600000
SSH Rekey-DataLimit     :  1
Auth Key TFTP Server    :  192.0.2.1
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys           :  Exist
```

```
RSA Host Keys           :  Exist
Enabled                 :  False
```

Specifying a Domain Name

When you enable this functionality, a locally configured domain is sent along with the username to the RADIUS server.

About this task

Use the following procedure to specify the domain name.

Before you begin

Enable username overwrite functionality.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   ssh x509v3-auth username use-domain <domain name>
   ```

3. Enter the following command to return to default configuration:

   ```
   default ssh x509v3-auth username use-domain
   ```

   OR

   ```
   no ssh x509v3-auth username use-domain
   ```

Example

```
Switch#show ssh global
Active SSH Sessions     :  0
Version                 :  Version 2 only
Port                    :  22
Authentication Timeout  :  60
DSA Authentication      :  True
RSA Authentication      :  True
Password Authentication :  True
X.509v3 Authentication  :  True
X.509v3 Username Overwrite  :  True
X.509v3 Strip Domain    :  True
X.509v3 Use-Domain      :  my.domain.com
Auth Retries            :  3
SSH Rekey               :  False
SSH Rekey-Interval      :  3600000
SSH Rekey-DataLimit     :  1
Auth Key TFTP Server    :  192.0.2.1
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys           :  Exist
RSA Host Keys           :  Exist
Enabled                 :  False
Enabled                 :  False
```

Enabling Strip Domain Name

If a domain is part of the username in the certificate principal name, you can strip the domain name so that it is not sent to the RADIUS server.

About this task

Use the following procedure to strip the domain name.

Before you begin

Enable username overwrite functionality.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   ssh x509v3-auth username strip-domain
   ```

3. Enter the following command to return to default configuration:

   ```
   default ssh x509v3-auth username strip-domain
   ```

   OR

   ```
   no ssh x509v3-auth username strip-domain
   ```

Example

```
Switch#show ssh global
Active SSH Sessions     :  0
Version                 :  Version 2 only
Port                    :  22
Authentication Timeout  :  60
DSA Authentication      :  True
RSA Authentication      :  True
Password Authentication :  True
X.509v3 Authentication  :  True
X.509v3 Username Overwrite  :  True
X.509v3 Strip Domain    :  True
X.509v3 Use-Domain      :
Auth Retries            :  3
SSH Rekey               :  False
SSH Rekey-Interval      :  3600000
SSH Rekey-DataLimit     :  1
Auth Key TFTP Server    :  192.0.2.1
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys           :  Exist
RSA Host Keys           :  Exist
Enabled                 :  False
```

Configuring the SSH Server

Use the following procedure to configure the SSH server and setup the trust point to be used. The key and CSR can be generated locally but this document describes the method of importing those files generated elsewhere. Online procedure can also be applied for obtaining digital certificates.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the following command to confirm Enhanced Secure Mode is enabled:

   ```
   show enhanced-secure-mode
   ```

   ```
   Switch(config)# show enhanced-secure-mode 2018-04-03 09:38:06 GMT
   +00:00 Enhanced Secure Mode: Enabled
   ```

3. Enter the following command to confirm the clock is synchronized:

   ```
   show clock
   ```

   ```
   Switch(config)# show clock System Clock time : 2018-04-03 10:14:43
   GMT+02:00 SNTP time : 2018-04-03 10:14:43 GMT+02:00Daylight saving
   recurring time is disabledDaylight saving time is disabledTime zone
   is set to 'Buc', offset from UTC is 02:00
   ```

4. Import the key contained in the switch subject certificate from USB / SFTP

   ```
   Switch(config)#certificate key CAC-server.key.pem import usb filename CAC-
   server.key.pemSwitch(config)#certificate key CAC-server.key.pem import sftp
   filename CAC-server.key.pem username sftp Enter SFTP server password:
   ```

   ```
   Switch(config)#show certificate key Name Type Size
   ---------------------------------------------- ----- ---- CAC-
   server.key.pem RSA 2048
   ```

5. Configure the certificate subject parameters:

   ```
   Switch(config)#certificate subject common-name CAC-server
   Switch(config)#certificate subject e-mail jsmith@extremenetworks.com
   Switch(config)#certificate subject unit BayPv
   Switch(config)#certificate subject organization Extreme Networks
   Switch(config)#certificate subject locality Buc
   Switch(config)#certificate subject province Buc
   Switch(config)#certificate subject country RO
   Switch(config)#sh certificate subject
   Common-name           : CAC-server
   E-mail                : jsmith@extremenetworks.com
   Organizational unit   : BayPv
   Organization          : Extreme Networks
   Locality              : Buc
   State/Province        : Buc
   Country               : RO
   Include IP address    : false
   FQDN                  :
   ```

6. Configure the trustpoint on the switch.

```
Switch(config)#certificate ca CAC common-name IPSEC key-name CAC-server.key.pem
Switch(config)#sh certificate ca CAC
Name                          : CAC
Common-name                   : IPSEC
KeyName                       : CAC-server.key.pem
CaUrl                         :
UsePost                       : false
SubjectCertValidityDays       : 365
Regenerate key on re-enroll   : false
Auto-renew                    : disabled
Use for                       :
CA contains a complete chain  : false
LastAction                    : no-op
LastActionStatus              : none
LastActionFailureReason       : OK
```

7. Import ROOT CA and subject certificates from USB/SFTP.

```
Switch(config)#certificate ca CAC import usb filename ca.cert.pem
Switch(config)#certificate ca CAC import usb filename CAC-server.pem
Switch(config)#certificate ca CAC import sftp filename ca.cert.pem username sftp
Enter SFTP server password:
Switch(config)#certificate ca CAC import sftp filename CAC-server.pem username sftp
Enter SFTP server password:

Switch#show certificate ca CAC
Name                          : CAC
Common-name                   : IPSEC
KeyName                       : CAC-server.key.pem
CaUrl                         :
UsePost                       : false
SubjectCertValidityDays       : 365
Regenerate key on re-enroll   : false
Auto-renew                    : disabled
Use for                       :
CA contains a complete chain  : true
LastAction                    : no-op
LastActionStatus              : none
LastActionFailureReason       : OK

Type          File name                   Not valid before   Not valid after
------------- --------------------------- ------------------ ------------------
rootCa        ca.cert.pem                 05/17/17 12:11:06  05/12/37 12:11:06
subjectCert   CAC-server.pem              03/29/18 15:32:39  04/08/19 15:32:39

Switch(config)#show certificate ca CAC file CAC-server.pem
2018-04-03 09:42:50 GMT+00:00
FileName                : CAC-server.pem
Associated context name : CAC
Associated context type : CA
File type               : subjectCert
Version number          : X.509 v3
Serial number           : 10:1E
Issuer name             : CO=RO, P=Buc, L=Buc, O=Extreme Networks, OU=BayPv,
CN=IPSEC, EM=jsmith@extremenetworks.com
Not valid before        : 03/29/18 15:32:39
Not valid after         : 04/08/19 15:32:39
Signature algorithm     : sha256withRSAEncryption
Signature               : 2B:34:8B:62:62:6F:2A:
73:52:A4:EC:E9:F0:B6:74:14:A5:B3:35:97:7F:9F:87:BB:A5:05:20:7A:23:31:71:BB:2A:3D:
14:6
5:3B:E3:E5:6B:96:90:B7:DA:68:0E:8E:19:CD:5B:D3:53:06:88:1A:81:97:65:B1:5C:2D:B1:DB:
```

```
60:9C:CE:8D:74:3D:28:58:51:EB:C5:EB:74:E2:5E:35:2
9:DB:BE:7C:FA:EC:93:08:A6:B5:2A:08:84:22:9F:77:CA:31:C9:6B:99:24:57:A2:EF:
13:C0:ED:E8:EB:2D:B8:BE:78:CD:28:6C:0A:91:5B:9D:97:75:79:A
A:CE:CB:EA:D2:42:24:2A:EB:83:35:69:AC:D0:32:16:66:DD:73:7E:CC:BF:AF:
61:60:07:D2:6A:E4:C7:98:18:26:E8:Switch:F3:99:1E:BB:5A:F1:57:31:19:7
E:0B:E8:8D:7A:A7:4F:C0:A6:F6:68:70:14:6F:98:1E:B1:EC:10:A1:86:14:BD:30:BE:A1:9D:
59:40:C1:A8:40:FE:03:36:FD:46:A0:26:74:CA:BA:24:B0:8
0:D0:1A:4E:74:EA:1B:0E:9E:E3:CC:12:D7:18:EC:42:66:33:FA:6B:1C:
53:15:28:17:89:1D:C5:05:3D:00:96:29:AB:9A:3E:B1:82:02:9F:80:44:8B:90:1
B:D6:3B:A4:55:CA:C7:C5:0E:EF:E1:B0:DC:AD:83:4C:0E:A4:5E:62:23:A6:D4:BA:
10:84:2C:FF:E2:A7:5F:A5:9C:60:CC:7F:19:36:AE:CD:FC:E6:4C:25:D
3:CE:16:23:81:AE:DD:14:90:E3:F7:C9:C6:3F:DC:27:70:DF:21:27:2B:78:F1:9B:F8:D7:6A:9F:
7D:4C:E2:73:BE:E9:11:A1:8D:21:55:75:B8:8F:D6:48:4
1:24:91:5D:0E:5C:6E:B5:64:01:96:D2:E6:DC:0C:4F:F4:E3:14:3B:AA:2E:31:47:11:C5:6E:1D:
04:04:F4:0E:7A:C7:3B:05:F6:B6:A2:FA:CB:F2:56:3B:2
B:D2:1F:0D:FA:37:08:45:47:E5:24:3D:3D:
51:F1:B7:AE:CF:F6:FE:A1:55:D3:65:5E:FF:C3:A2:42:9A:72:0B:2D:30:D0:AF:
2D:E5:21:F2:A5:5C:40:12:A
A:0C:9D:43:D4:5A:E5:F1:14:FA:44:D3:19:80:D4:C0:ED:61:0F:4F:91:B4:F6:A9:99:4F:3C:FB:
37:0A:AE:03:46:87:38:CA:B6:D8:49:B4:0A:94:BD:9D:6
9:AA:30:00:47:7E:0B:59:DE:FC:BC:D3:8C:01:77:FD:0B:DF:22:B5:52:6A:B7:2E:B3:BE:4F:
57:9B:7A:06:4C:5C:35:33:D1:91
Subject                 : CO=RO, P=Buc, L=Buc, O=Extreme Networks, OU=BayPv,
CN=IPSEC, EM=jsmith@extremenetworks.com
Public key algorithm    : rsaEncryption
Public key              : 30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:
01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:9D:F
8:C6:86:3A:12:95:D7:9C:58:9D:2E:6E:98:AC:CB:EC:2E:04:FA:60:FD:
6C:E8:07:E4:20:74:1D:C6:47:E4:2F:12:13:C6:18:A9:A0:05:80:29:96:78:F9:A
A:16:01:6B:82:D8:35:FF:D5:58:6B:B1:ED:C9:BE:75:20:91:8E:BA:26:45:67:6E:D6:15:BA:CC:
26:A5:F5:0A:E2:7A:13:34:0C:00:82:A7:9E:9E:45:BF:C
2:93:9D:5C:43:B5:E7:27:C6:9A:06:EB:35:2F:A7:16:D5:1F:A3:DA:D7:AF:E6:EC:3C:
07:56:C7:21:49:08:D4:D0:E0:78:45:63:C7:93:01:0C:CA:0B:B4:4
D:2A:4D:24:B1:A4:2F:CB:32:17:73:AE:D4:ED:9A:D6:5E:15:62:33:81:F3:19:E5:51:FF:52:DF:
7F:E1:D2:4D:2A:4E:91:A5:9D:D9:8A:CF:EF:D5:48:32:0
C:B1:BC:E5:EE:3B:49:94:73:1E:F9:40:CA:B2:FB:EA:11:74:19:89:89:82:98:E4:4C:BC:
35:76:08:2B:55:D9:67:C4:99:84:0E:1A:0C:CF:E2:A5:E0:F3:F
6:23:26:98:16:6E:99:AF:CC:68:6B:46:97:35:61:C1:96:91:3A:08:46:4D:72:91:B3:1E:
35:94:C3:31:D4:75:01:6D:02:03:01:00:01
Has basic constraint    : true
Has key usage           : true
Is CA                   : false
Key usage               :
Status                  : active
CDP url                 : http://192.0..2.1
OCSP url                : http://192.0.2.1:2561
Extended key usage      : TLS Web Server Authentication
```

8. Configure the trustpoint to be used for SSH-server.

```
Switch(config)#certificate ca CAC use-for ssh-server
Switch#show certificate ca CAC
Name                          : CAC
Common-name                   : IPSEC
KeyName                       : CAC-server.key.pem
CaUrl                         :
UsePost                       : false
SubjectCertValidityDays       : 365
Regenerate key on re-enroll   : false
Auto-renew                    : disabled
Use for                       : SSH-Server
CA contains a complete chain  : true
LastAction                    : no-op
LastActionStatus              : none
LastActionFailureReason       : OK
```

9. Import in the trust store root CA and Intermediate CA that signed the certificate from the card

```
certificate trust-store import sftp filename Self-signedTrustAnchorCertificate.cer
username sftp
certificate trust-store import sftp filename RSA2048IssuingCACertificate.cer
username sftp
show certificate trust-store
2018-04-05 11:53:35 GMT+00:00
Type          File name                    Not valid before   Not valid after
------------- ---------------------------- ------------------ ------------------
interCa       RSA2048IssuingCACertificate.cer 10/01/10 08:30:00  10/01/30
08:30:00
rootCa        Self-signedTrustAnchorCertificate.cer 10/01/10 08:30:00  10/01/30
08:30:00
```

Using an Idenity for SSH Server

Use the following procedure to use an identity for the SSH server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enter the following command:

   ```
   certificate ca <ca-name> use-for ssh-server
   ```

Example

```
Switch(config)#certificate ca IPSEC use-for ?
  ssh-server  Use as identity for SSH Server

Switch(config)#show certificate ca IPSEC
Name                          : IPSEC
Common-name                   : IPSEC-ICA
KeyName                       : TEST.key.der
CaUrl                         : http://10.100.94.41:8080/ejbca/publicweb/apply/scep/test/
pkiclient.exe
UsePost                       : true
SubjectCertValidityDays       : 365
Regenerate key on re-enroll   : false
Auto-renew                    : disabled
Use for                       : SSH-Server
CA contains a complete chain  : true
LastAction                    : enroll
LastActionStatus              : success
LastActionFailureReason       : OK
```

Clearing Idenity Usage for SSH Server

Use the following procedure to remove identity usage for the SSH server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enter the following command:

```
no certificate ca <ca-name> use-for
```

Secure Shell Client configuration

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

Opening and closing an SSH session involves three actions:

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

Configuring SFTP authentication for SSH Client using CLI

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the SFTP authentication method the SSH Client uses for transferring files:

```
sshc authentication {dsa | password | rsa}
```

3. Configure the SFTP authentication method SSH Client to the default of DSA:

```
default sshc authentication
```

OR

```
no sshc authentication
```

Variable definitions

Use the data in the following table to use the **`sshc authentication`** command.

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

Closing an SSH Client session using CLI

Use this procedure to close a specific SSH Client session.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Close a specific SSH Client session:

   ```
   sshc close-session <0-8>
   ```

Variable definitions

Use the data in the following table to use the **`sshc close-session`** command.

Variable	Value
<0–8>	Specifies the SSH Client session ID.

Generating an SSH client DSA host key using CLI

Use the following procedure to generate public and private DSA SSH client host keys for user access authentication.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Generate public and private DSA SSH client host keys for use access authentication:

   ```
   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.

3. Delete the public or private DSA host keys from NVRAM:

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

Variable definitions

Use the data in the following table to use the **sshc dsa-host-key** command.

Variable	Value
force	Creates a new DSA key, even in the presence of an existing DSA key.

Generating an SSH client RSA host key using CLI

Use the following procedure to generate public and private SSH client RSA host keys for user access authentication.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Generate public and private SSH client RSA host keys for user access authentication:

```
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.

3. Delete public and private RSA host keys from the NVRAM:

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

The RSA authentication state remains unchanged.

Variable definitions

Use the data in the following table to use the **sshc rsa-host-key** command.

Variable	Value
force	Creates a new RSA key, even in the presence of an existing RSA key.

Connecting SSH to a host using CLI

Use the following procedure to establish a SSH connection to a host.

About this task

You can use the following command from User EXEC or Privileged EXEC mode.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Establish an SSH connection to a host:

   ```
   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)?
   ```

   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.
   ```

Example

This example displays sample steps for connecting an SSH Client to a host.

```
Switch>enable
Switch#ssh 192.0.2.2
Switch#ssh 192.0.2.2 username laur
Switch#ssh 192.0.2.2 username RW port 22
```

Variable definitions

Use the data in the following table to use the **ssh** command.

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.

Displaying current SSH client sessions

Use the following procedure to display current SSH client sessions.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display current SSH client sessions:

   ```
   show sshc sessions
   ```

Example

The following example shows sample output for the **show sshc sessions** command.

```
Switch>enable
Switch#show sshc sessions
1 active SSH Session:
----------  ----------------------    ---------------------------
Session ID  Host IP Address           Connection time:
----------  ----------------------    ---------------------------
0               192.0.2.2                  1 minute
```

Displaying SSH client known hosts

Use this procedure to display information about the configuration of SSH client known hosts on the switch.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display information about the configuration of SSH client known hosts on the switch:

   ```
   show sshc known-hosts
   ```

Note:

The **show sshc known-hosts** command is present only on terminals with Read-Write access.

Example

The following example shows sample output for the **show sshc known-hosts** command.

```
Switch>enable
Switch#show sshc known-hosts
IP Address                SHA-256 Fingerprint
-----------------------   ------------------------------------------------
192.0.2.3                 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
-----------------------   ------------------------------------------------
192.0.2.2                 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 CLI

Use the following procedure to clear the public key of a known host.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Clear the public key of a known host:

   ```
   clear sshc known-host {<A.B.C.D> | <host_name> | <ipv6_address> |
   all}
   ```

Example

The following example displays a sample step for clearing the public key of a known host.

```
Switch>enable
Switch#configure terminal
Switch(config)#clear sshc known-host 192.0.2.2
```

Variable definitions

Use the data in the following table to use the **clear sshc known-host** command.

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 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 2001:db8:0:0:0:0:0:1
   ```

   For Switch #2 enter the following commands:

   ```
   ipv6 enable
   int vlan 1
   ipv6 interface enable
   ipv6 address 2001:db8:0:0:0:0:0:2
   ```

2. Establish a SSH connecting using the IPv6 address.
   - Establish a SSH connection from Switch #1 to Switch #2.
   - On Switch #1 :

     ```
     ssh 2001:db8:0:0:0:0:0:2 user RW
     ```

   - SSH from Switch #1 to Switch #2:
   - On Switch #2:

     ```
     ssh 2001:db8:0:0:0:0:0:1 user RO
     ```

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 CLI interface.

Procedure

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. • 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.
Retries	Specifies the number of SSH authentication retries configured on the switch. DEFAULT: 3
KeyAction	Specifies the SSH key action. • none • generateDsa • generateRsa • deleteDsa • deleteRsa
RsaAuth	Enables or disables SSH RSA authentication
DsaAuth	Enables or disables SSH DSA authentication.

Table continues…

Variable	Value
PassAuth	Enables or disables SSH password authentication.
RsaAuthKeyName	Indicates the RSA authentication key name.
DsaAuthKeyName	Indicates the DSA authentication key name.
RsaHostKeyStatus	Indicates the current status of the SSH RSA host key. Values include: • noSuchInstance_OID • notGenerated • generated • generating
DsaHostKeyStatus	Indicates the current status of the SSH DSA host key. Values include: • noSuchInstance_OID • notGenerated • generated • generating
TftpServerInetAddressType	Indicates the type of address stored in the TFTP server. Values include: • ipv4 • ipv6
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: • none • downloadSshDsaPublicKeys • deleteSshDsaAuthKey • downloadSshRsaPublicKeys • deleteSshRsaAuthKey
TftpResult	Displays the result of the last TFTP action request.
SshAuthKeyFilename	Specifies the SSH authentication key file to download.
UsbTargetUnit	Specifies the unit number of the USB port to use for file uploads and downloads. Values range from 0 to 10. Value 0 applies to the TFTP server. Values 1 to 8 apply to a USB port in a switch stack. Value 9 applies to a standalone switch.

Table continues…

Variable	Value
	Value 10 applies to the SFTP server.
Action	• none • dnldSshDsaAuthKeyFromUsb — when selected, specifies to download the SSH DSA authentication key using the USB port. • dnldSshRsaAuthKeyFromUsb — when selected, specifies to download the SSH RSA 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: • 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

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.
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

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	Specifies the action to take for the SSH Client host key. Values include: • 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. • generateDsaForce—generates a new, active DSA host key, even in the presence of an existing DSA key. • generateRsaForce—generates a new, active RSA host key, even in the presence of an existing RSA key.
KeyFileName	Specifies the a SSH Client host key file name.
TftpAction	Specifies the type of SSH Client authentication key to upload using TFTP. Values include: • 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.

Table continues…

Variable	Value
TftpServerInetAddressType	Indicates the type of address stored in the TFTP server. Values include: • ipv4 • ipv6
TftpServerInetAddress	Specifies the IP address of the TFTP server for TFTP operations.
UsbAction	Specifies the type of SSH Client authentication key to upload using USB. Values include: • 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.
UsbTargetUnit	Specifies the unit number of the USB port to use for file uploads and downloads. Values range from 0 to 10. Value 0 applies to the TFTP server. Values 1 to 8 apply to a USB port in a switch stack. Value 9 applies to a standalone switch. Value 10 applies to the SFTP server.
DsaKeySize	Specifies the DSA key size. In this release, the value is fixed and it is 1024.
RsaKeySize	Specifies the RSA key size. Values range from 1024 to 2048.
DsaHostKeyStatus	Indicates the current status of the SSH Client DSA host key. Values include: • notGenerated • generated • generating
RsaHostKeyStatus	Indicates the current status of the SSH Client RSA host key. Values include: • notGenerated • generated • generating
SFTP	
Port	Specifies the TCP port number for the SFTP file transfer. Values range from 1 to 65535.

Table continues…

Variable	Value
Authentication	Specifies the SSH authentication type. Values include: • DsaAuthentication • RsaAuthentication • PasswordAuthentication
SftpServerInetAddressType	Indicates the type of address stored in the SFTP server. Values include: • ipv4 • ipv6
SftpServerInetAddress	Specifies the IP address of the SFTP server for SFTP operations.
UserName	Specifies the user name.
SftpServerPassword	Specifies the SFTP server password.
Confirm SftpServerPassword	Confirms the SFTP server password.

Chapter 18: Simple Network Management Protocol

You can use the Simple Network Management Protocol (SNMP) to remotely collect management data and configure devices.

An SNMP agent is a software process that monitors the UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or modify.

Simple Network Management Protocol

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.

Switch support for SNMP

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

SNMPv3 support 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 can configure SNMPv3 using EDM or CLI.

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.

Setting SNMP v1, v2c, v3 Parameters

With the switch support for SNMPv3, you can configure SNMP using the new standards-based method of configuring SNMP communities, users, groups, views, and trap destinations.

The switch 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 switch software supports MD5 and SHA authentication, as well as AES and DES 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 and DES based privacy encryption. Export restrictions on SHA and DES necessitate support for domestic and non domestic executable images or defaulting to no encryption for all customers.

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: 40
- snmpNotifyTable: 20
- snmpTargetAddrTabel: 20
- snmpTargetParamsTable: 20

SNMP MIB support

The switch 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 switch, see Supported SNMP MIBs and traps on page 577.

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 switch supports both industry-standard SNMP traps, as well as private 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 switch, see *Supported SNMP MIBs and traps*.

You can use CLI or EDM to enable or disable SNMP traps for a series of features, such as:

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

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

- avFabricAttachDiscoveredElement
- avFabricAttachExpiredElement
- lldpRemTablesChange
- risingAlarm
- fallingAlarm
- vrrpTrapNewMaster
- vrrpTrapAuthFailure
- pethPsePortOnOffNotification
- pethMainPowerUsageOnNotification
- pethMainPowerUsageOffNotification
- ospfVirtIfStateChange
- ospfNbrStateChange
- ospfVirtNbrStateChange
- ospfIfConfigError
- ospfVirtIfConfigError
- ospfIfAuthFailure
- ospfVirtIfAuthFailure
- ospfIfStateChange
- entConfigChange
- coldStart
- warmStart
- linkDown
- linkUp

- authenticationFailure
- lldpXMedTopologyChangeDetected
- ntnQosPolicyEvolLocalUbpSessionFailure
- ntnQosPolicyEvolDosAttackDetected
- slaMonitorAgentExceptionDetected
- nnMstGeneralEvent
- nnMstErrorEvent
- nnMstNewRoot
- nnMstTopologyChange
- nnMstProtocolMigrationnnMstRegionConfigChange
- nnRstGeneralEvent
- nnRstErrorEvent
- nnRstNewRoot
- nnRstTopologyChange
- nnRstProtocolMigration
- bspeIpPhonePowerLimitNotification
- bspeIpPhonePowerPriorityNotification
- bsAdacPortConfigNotification
- bsAdacPortOperDisabledNotification
- bsveVrrpTrapStateTransition
- bsDhcpSnoopingBindingTableFull
- bsDhcpSnoopingTrap
- bsDhcpOption82MaxLengthExceeded
- bsDhcpSnoopingExtSaveEntryMACConflict
- bsDhcpSnoopingExtSaveEntryInvalidInterface
- bsDhcpSnoopingExtSaveEntryLeaseExpired
- bsDhcpSnoopingExtSaveEntryParsingFailure
- bsDhcpSnoopingExtSaveNTP
- bsDhcpSnoopingExtSaveUSBSyncSuccess
- bsDhcpSnoopingExtSaveTFTPSyncSuccess
- bsDhcpSnoopingExtSaveUSBSyncFailure
- bsDhcpSnoopingExtSaveTFTPSyncFailure

- bsDhcpSnoopingExtSaveUSBRestoreSuccess
- bsDhcpSnoopingExtSaveTFTPRestoreSuccess
- bsDhcpSnoopingExtSaveUSBRestoreFailure
- bsDhcpSnoopingExtSaveTFTPRestoreFailure
- bsDhcpSnoopingExtSaveEntryInvalidVlan
- bsDhcpSnoopingExtSaveSFTPSyncSuccess
- bsDhcpSnoopingExtSaveSFTPSyncFailure
- bsDhcpSnoopingExtSaveSFTPRestoreSuccess
- bsDhcpSnoopingExtSaveSFTPRestoreFailure
- bsDhcpSnoopingExtSaveEntryIfTrustedConflict
- bsDhcpSnoopingStaticEntryMACConflict
- bsaiArpPacketDroppedOnUntrustedPort
- bsSourceGuardReachedMaxIpEntries
- bsSourceGuardCannotEnablePort
- bsRadiusReachabilityServerDown
- bsRadiusReachabilityServerUp
- bspimeNeighborStateChanged
- bsDdiSfpTempAlarm
- bsDdiSfpTempWarn
- bsDdiSfpTempNormal
- bsDdiSfpVoltageAlarm
- bsDdiSfpVoltageWarn
- bsDdiSfpVoltageNormal
- bsDdiSfpBiasAlarm
- bsDdiSfpBiasWarn
- bsDdiSfpBiasNormal
- bsDdiSfpTxAlarm
- bsDdiSfpTxWarn
- bsDdiSfpTxNormal
- bsDdiSfpRxAlarm
- bsDdiSfpRxWarn
- bsDdiSfpRxNormal

- bsnesGloballyEnabled
- bsnesGloballyDisabled
- bsnesManuallyActivated
- bsnesManuallyDeactivated
- bsnesScheduleNotApplied
- bsnesScheduleApplied
- bsnesActivated
- bsnesDeactivated
- bsifnInstallationFailure
- bsStormControlBelowLowWatermark
- bsStormControlAboveHighWatermark
- bsLstInterfaceStatusChanged
- bsLstGroupOperStateChanged
- bsIpv6NDSBTTableFull
- bsIpv6NDNotificationsUntrustedPort
- rcnBpduReceived
- rcnIsisPlsbMetricMismatchTrap
- rcnIsisPlsbDuplicateSysidTrap
- rcnIsisPlsbLsdbUpdateTrap
- rcnIsisPlsbBvidMismatchTrap
- rcnIsisPlsbAdjStateTrap
- rcnIsisPlsbDuplicateNnameTrap
- rcnIsisPlsbMultiLinkAdjTrap
- bsnConfigurationSavedToNvram
- bsnEapAccessViolation
- bsnStackManagerReconfiguration
- bsnLacTrunkUnavailable
- bsnLoginFailure
- bsnTrunkPortDisabledToPreventBroadcastStorm
- bsnTrunkPortEnabledToPreventBroadcastStorm
- bsnLacPortDisabledDueToLossOfVLACPDU
- bsnLacPortEnabledDueToReceiptOfVLACPDU

- bsnStackConfigurationError
- bsnEapUbpFailure
- bsnTrialLicenseExpiration
- bsnEnteredForcedStackMode
- bsnEapRAVError
- bsnSystemUp365Days
- bsnUSBInsertion
- bsnUSBRemoval
- bsnSFPInsertion
- bsnSFPRemoval
- bsnStackProtection
- bsnRunScripts
- bsnAaaUserAccountNotUsed
- bsnAaaAlreadyConnected
- bsnAaaIncorrectLogOnThresholdExceeded
- bsnAaaMaxNoOfSessionsExceeded
- bsnAuditUnsentMessages
- bsnAuditRecordEventsFailure
- bsnAuditStartUpTrap
- bsnAuditShutDownTrap
- bsnAaaUserPasswordExpired
- rcnSlppGuardHoldDownExpired
- rcnSlppGuardPacketReceived
- s5EtrSbsMacTableFull
- s5EtrSbsMacTableClearedForPort
- s5EtrSbsMacTableCleared
- s5EtrSbsMacRemoved
- s5EtrNewSbsMacAccessViolation
- s5EtrMacAddressTablesThresholdReached
- s5CtrNewHotSwap
- s5CtrNewProblem
- s5CtrNewUnitUp

- s5CtrNewUnitDown
- s5CtrFanDirectionError
- s5CtrHighTemperatureError

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 DCHP Snooping External Save.

Configuring SNMP using CLI

This section provides procedures to configure and manage SNMP using CLI.

Viewing SNMP configuration

About this task

View SNMP configuration.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View SNMP configuration:

   ```
   show snmp-server
   ```

Example

```
Switch>enable
Switch#show snmp-server
Read-Only Community String: public
Read-Write Community String: private
Trap #1 IP Address:       0.0.0.0
        Community String:
```

```
Trap #2 IP Address:       0.0.0.0
        Community String:
Trap #3 IP Address:       0.0.0.0
        Community String:
Trap #4 IP Address:       0.0.0.0
        Community String:
AutoTopology: Enabled
```

Variable definitions

Use the data in the following table to use the **`show snmp-server`** command.

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.
view	Displays SNMP views.

Enabling and disabling SNMP authentication failure traps

About this task

Enable or disable the generation of SNMP authentication failure traps.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable the generation of SNMP authentication failure traps:

   ```
   snmp-server authentication-trap enable
   ```

3. Disable the generation of SNMP authentication failure traps:

   ```
   snmp-server authentication-trap disable
   ```

   OR

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

Restoring the SNMP authentication trap configuration to default

About this task

Restore the SNMP authentication trap configuration to the default settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Restore the SNMP authentication trap configuration to the default settings:

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

Configuring a single read-only or read-write community

About this task

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.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure a single read-only or a single read-write community:

   ```
   snmp-server community [word{notify-view|read-view|ro|rw|write-view}]
   ```

Variable definitions

Use the data in the following table to use the `snmp-server community` command.

Parameters and variables	Description
word [notify-view|read-view|ro|rw|write-view]	The following list describes the snmp-server community parameters: • 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. **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).

Creating community strings

About this task

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.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Create community strings:

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

Variable definitions

Use the data in the following table to use the **snmp-server community** command.

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.

Clearing SNMP server community

About this task

Clear the snmp-server community configuration.

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.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Clear the snmp-server community configuration:

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

Variable definitions

Use the data in the following table to use the **no snmp-server community** command.

Parameters and variables	Description
ro |rw|<community-string>	Changes the settings for SNMP: • 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).

Restoring the community string configuration to default

About this task

Restore the community string configuration to the default settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Restore the community string configuration to the default settings:

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

Variable definitions

Use the data in the following table to use the **`default snmp-server community [ro|rw]`** command.

Parameters and variables	Description
ro|rw	Restores the read-only community to Public, or the read-write community to Private.

Configuring SNMP sysContact value

About this task

Configure SNMP sysContact value.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure SNMP sysContact value:

   ```
   snmp-server contact
   ```

Variable definitions

Use the data in the following table to use the **`snmp-server contact`** command.

Parameters and variables	Description
text	Specifies the SNMP sysContact value.

Clearing or restoring the SNMP sysContact value to default

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To clear the sysContact value, enter the following command:

```
no snmp-server contact
```

OR

To restore the sysContact value to the default value:

```
default snmp-server contact
```

Enabling or disabling the SNMP server

About this task

Enable or disable the SNMP server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable or disable the SNMP server:

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

Disabling SNMP access

About this task

Disable SNMP access.

Important:

If you disable SNMP access you cannot use Enterprise Device Manager for the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable SNMP access:

   ```
   no snmp-server
   ```

Adding trap receivers to SNMPv3 traps

Before you begin

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

About this task

Use the following procedure to add a trap receiver to the SNMPv3 tables.

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.

Using the new standards-based SNMP method, you can create several entries in this table, and each can generate v1, v2c, or v3 traps.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Add trap receivers to SNMPv3 traps.

   ```
   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>]}
   ```

Variable definitions

Use the data in the following table to use the **`snmp-server host`** command.

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.
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: • auth: auth specifies SNMPv3 traps are sent using authentication and no privacy;

Table continues…

Parameters and variables	Description
	• 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.

Deleting trap receivers or restoring the SNMPv3 table to defaults

About this task

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

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Delete trap receivers using the proprietary method syntax:

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

3. Delete trap receivers using the standards-based method syntax:

   ```
   no snmp-server host <host-ip> [port <trap-port>] {v1|v2c|v3
   <community-string>]
   ```

4. Restore the table to defaults (to clear the table):

   ```
   default snmp-server host
   ```

Variable definitions

Use the data in the following table to use the **no smp-server host** command.

Parameters and variables	Description
<host-ip> [<community-string>]	In the proprietary method, enter the following variables: • 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.

Restoring trap receivers configured ports to default

About this task

Restore all trap receivers configured ports to the default port used for listening traps. The default port is 162.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Restore all trap receivers configured ports to the default port:

   ```
   default snmp-server port
   ```

Configuring or clearing the SNMP sysLocation value

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Configure the SNMP sysLocation value:

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

3. Clear the SNMP sysLocation value:

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

Variable definitions

Use the data in the following table to use the **[no] snmp-server location** command.

Parameters	Description
text	Specify the SNMP sysLocation value; enter an alphanumeric string of up to 255 characters.

Restoring the SNMP sysLocation to the default

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Restore sysLocation to the default value:

```
default snmp-server location
```

Configuring the SNMP sysName value

About this task

Use the following procedure to configure the SNMP sysName value.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the SNMP sysName value:

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

Variable definitions

Use the data in the following table to use the **snmp-server name>** command.

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.

Clearing the SNMP sysName value

About this task

Clear the sysName value.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Clear the sysName:

   ```
   no snmp-server name
   ```

   OR

   default snmp-server name

Enabling SNMP server notification control

About this task

Use this procedure to enable or disable SNMP traps for specific ports, or for all switch ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable SNMP traps for specific ports, or for all switch ports:

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

3. Disable SNMP traps for specific ports, or for all switch ports:

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

Variable definitions

Use the data in the following table to use the

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**.

Setting SNMP server notification control to default

About this task

Use this procedure to set SNMP traps to the default value (disabled).

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Set SNMP server notification control to default:

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

Variable definitions

Use the data in the following table to use the

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**.

Creating an SNMPv3 user

About this task

Use the following procedure to create 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

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Create an SNMPv3 user:

   ```
   snmp-server user [engine-id <engine-id>] <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>]] {aes|des} <password> [read-view <view-
   name>] [write-view <view-name>] [notify-view <view-name>]
   ```

Variable definitions

Use the data in the following table to use the **`snmp-server user`** command.

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: • 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: • view-name: specifies the viewname; enter an alphanumeric string that can contain at least some of the non alphanumeric characters.

Table continues…

Parameters	Description
notify-view <view-name>	Specifies the notify view to which the new user has access: • view-name: specifies the viewname; enter an alphanumeric string that can contain at least some of the non alphanumeric characters.
SHA	Specifies SHA authentication.
AES	Specifies AES privacy encryption.
DES	Specifies DES privacy encryption.
engine-id	Specifies the SNMP engine ID of the remote SNMP entity.

For authenticated access, you must specify the md5 or sha parameter. For authenticated and encrypted access, you must also specify the 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.

Removing an SNMPv3 user

About this task

Use the following procedure to delete a specified SNMPv3 user.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Delete a specified SNMPv3 user:

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

Variable definitions

Use the data in the following table to use the **`no snmp-server user`** command.

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.

Creating an SNMPv3 view

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Create an SNMPv3 view:

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

Variable definitions

Use the data in the following table to use the **`snmp-server view`** command.

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). 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: • 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) 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: • snmp-server view myview +system -sysDescr

Table continues…

Parameters and variables	Description
	And you use that view for the read-view of a user, then the user can read only the system group except for sysDescr. **Important:** There are ten possible OID values.

Removing an SNMPv3 view

About this task

Use the following procedure to delete an SNMPv3 view.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Delete an SNMPv3 view:

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

Variable definitions

Use the data in the following table to use the **`no snmp-server view`** command.

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 22: snmp-server host for old-style table command parameters and variables on page 531 describes the parameters and variables for the **`snmp-server host`** for old-style table command.

Table 22: 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 23: snmp-server host for new-style table command parameters and variables on page 531 describes the parameters and variables for the **snmp-server host** for new-style table command.

Table 23: 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: • **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.

Creating an initial set of configuration data for SNMPv3

About this task

Use the following procedure to create an initial set of configuration data for SNMPv3. This configuration data follows the conventions described in the SNMPv3 standard (in RFC 3414and 3415). The data consists of a set of initial users, groups, and views.

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create an initial set of configuration data:

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

Variable definitions

Use the data in the following table to use the **`snmp-server bootstrap`** command.

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.

SNMP configuration using EDM

This section describes the configuration options available for SNMP in EDM.

Viewing the SNMP configuration using EDM

Follow this procedure to display information about SNMP on your switch.

Procedure

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 24: 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.
TrpRcvrCurEnt	Indicates the current number of trap receiver entries.
TrpRcvrNext	Indicates the next trap receiver entry to be created.

Creating an SNMP user using EDM

User the following procedure to create an SNMP user.

Procedure

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 **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: • None • DES • 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: • volatile—entry does not persist if switch loses power • nonVolatile—entry persists if switch loses power

Viewing the user details using EDM

Use the following procedure to view information about an SNMP user.

Procedure

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 **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.
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

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

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

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

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 configure an SNMP host notification control.

Procedure

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 Host 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. • trap • inform
Version	Indicates the SNMP version as one of the following: • SNMPv1 • SNMPv2c • SNMPv3/USM
SecurityLevel	Indicates the minimum security level required to gain access rights
Community / User Name	Indicates that a secret alphanumeric name is assigned to the community string associated with the SNMP host. **Note:** The specific alphanumeric characters of the secret community string name are represented by asterisks (*).
Storage Type	Indicates the storage type as one of the following: • volatile: Entry does not persist if switch loses power. • nonVolatile: Entry persists if switch loses.

Configuring notifications (traps) from the list using EDM

Use the following procedure to enable and disable SNMP trap control.

Procedure

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

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Snmp 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. 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

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 definitions

Use the data in this table to enable or disable SNMP traps for specific ports, or for all switch ports.

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

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.
OutTooBigs	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is tooBig.
OutNoSuchNames	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is noSuchName.
OutBadValues	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is badValue.
OutGenErrs	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is genErr.
InBadVersions	The total number of SNMP messages delivered to the SNMP protocol for an unsupported SNMP version.
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.

Table continues…

Variable	Value
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 19: Secure Socket Layer Protocol

This chapter provides conceptual information and procedures to configre Secure Socket Layer (SSL) Protocol using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

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 (CLI 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 (CLI 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, Extreme Networks 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    : Extreme Networks
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
```

SHA-2 Support for SSL Certificates

In Release 7.1.0 or later, only the SHA-256 hash algorithm is supported to compute the SSL certificate signature. Support for SHA-1 is deprecated and trusting SHA-1 generated certificates is stopped.

Important:

When you upgrade from a release that uses SHA-1 based certificates to Release 7.1.0 or later, the old certificate is used with the upgraded software. In this case, SSL negotiation sessions fail because SHA-1 is not supported on Release 7.1.0 or later. To successfully negotiate an SSL session that uses SHA-1, you must first upgrade to a release that supports SHA-256 and then regenerate the SSL certificate.

For information about regenerating certificates, see Regenerating the SSL Certificate using CLI on page 547.

Configuring SSL using CLI

This section provides procedures to configure SSL to secure a Web management interface using CLI.

Enabling or Disabling SSL

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable SSL, enter the following command:

   ```
   ssl
   ```

   OR

   To disable SSL, enter the following command:

   ```
   no ssl
   ```

Creating or Deleting an SSL Certificate

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To create an SSL certificate, enter the following command:

   ```
   ssl certificate
   ```

   OR

   To delete an SSL certificate, enter the following command:

   ```
   no ssl certificate
   ```

Viewing the SSL Server Configuration

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ssl
   ```

Example

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

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

Variable Definitions

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

Field	Description
WEB Server SLL Secured	Displays whether or not the Web server uses an SSL connection
SSL server state	
Uninitialized	The server is not running.
Certificate Initialization	The server is generating a certificate during the initialization phase.
Active	The server is initialized and running.
SSL Certificate	
Generation in progress	Shows whether SSL is generating a certificate. The SSL server generates a certificate during server startup initialization, or the CLI user can regenerate a new certificate.
Saved in NVRAM	Shows whether an SSL certificate exists in the NVRAM. The SSL certificate is not present if the system is being initialized for the first time or the CLI user deleted the certificate.
Certificate file size	Displays the certificate file size in bytes.
RSA host key length	Displays the RSA host key length in bits.

Viewing the SSL Certificate

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ssl certificate
   ```

Example

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

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


RSA Host Key (length = 2048 bits):
b199777714196fad8575948047b2f15fcd944a6bbf897e634c3c2898665f457a
e93de38acf5733786bb76a6d21f001835f55c710ddd476c51a525da60f526b47
be8ef3aa2119046e54402da7b3180d6948a1bd4fbab740f231968b29dc55ceb6
194547a853847a02d05bf9ea8e918f456fe8490a7b64d0903417f917bc22569d
c3790bd3c59ddcee00bd4cd8b006cee26c0337065453badb192e934aae416244
315cdbb77bf4f69a1e3a48dee0e3d5554a05605f6d961500fb5f7279394845d7
99ce1b5b4ae4e5d4feca1a3435a778ee8680ab99aa907d18b98e1144fb731c5f
6c62054a3f3ac43a9ff25ccf5ce418a3d0f680c89f53d4829bd62dac60aed2c5
```

Regenerating the SSL Certificate

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

Before you begin

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   ```
   ssl certificate
   ```

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

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

```
show ssl
```

Note:

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

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

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

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

```
ssl reset
```

Example

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

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

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

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

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

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: • true—indicates that a valid certificate is created. • false—indicates that no valid certificate is created, or that the certificate is deleted.
CertificateControlStatus	Indicates the status of the most recent attempt to create or delete a certificate. The possible status messages are as follows: • 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. **Important:** You cannot reset the SSL server while creating the SSL certificate.

Chapter 20: Storm Control

This chapter provides conceptual information and procedures to configure Storm Control using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

Storm Control

This feature provides granular control of Broadcast, Multicast and Unicast traffic rates on a per-port basis. Broadcast, Multicast and Unicast traffic rates can be individually or collectively controlled on a switch or switch stack by setting the following:

- low-watermark and high watermark values in packets per second (pps)
- polling interval value
- action type
- SNMP traps

When a high watermark is exceeded, an action of None, Drop or Shutdown can be applied to the traffic type.

A defined action is reversed, or ceases, when the traffic rate in pps falls below the low-watermark setting. When an action of ‘drop’ is used, traffic is dropped when traffic exceeds the high-watermark and does not resume forwarding until the traffic rate falls below the low-watermark. When the action of ‘shutdown’ is used, the switch port is administratively shutdown when traffic exceeds the high-watermark and requires administrator intervention to re-enable the switch port to resume traffic forwarding.

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

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

Storm control configuration

This section describes the procedures to configure storm control using CLI.

Configuring storm control globally

Follow this procedure to configure storm control globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure storm control.

   ```
   storm-control [broadcast | multicast | unicast | all] [low-watermark
   <10-100000000>] [high-watermark <10-100000000>] [poll interval
   <5-300>][action] [none | drop | shutdown ]] [trap-interval <0-1000>]
   [enable]
   ```

3. Disable storm control.

   ```
   no storm-control [broadcast | multicast | unicast | all] enable
   ```

4. Restore default storm control settings.

   ```
   default storm-control [broadcast | multicast | unicast | all] [low-
   watermark] [high-watermark] [poll interval] [action] [trap-interval]
   ```

Variable definitions

The following table defines parameters that you enter with the **`storm-control`** command.

Variable	Description
action	Specifies the storm control action: • **drop**: Set storm control action to drop • **none**: • **shutdown**: Set storm control action to shut down
enable	Enables storm control.
high-watermark <10-100000000>	Specifies the high-watermark value in packets per second (pps). Range: 10 to 100000000 Default: 1000
low-watermark <10-100000000>	Specifies the low-watermark value in packets per second (pps). Range: 10 to 100000000 Default: 100
poll-interval<5-300>	Specifies the interval for watermark checking; the value varies in seconds. Range: 5 to 300

Table continues…

Variable	Description
	Default: 5
trap-interval<0-1000>	Specifies the interval for sending traps when the poll-intervals exceed. Range: 0 to 1000 **Note:** Value 0 means disabled (high watermark traps will not be repeated) Default: 0

Displaying storm control

Follow this procedure to display storm control configuration.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display storm control settings.

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

3. Display storm control settings for an interface or list of ports.

   ```
   show storm-control interface [Ethernet [<port_list>] | <port_list>]
   ```

Example

```
Switch#show storm-control all
Storm Control Status    High Wm    Low Wm    Poll    Action      Trap
--------------------    --------   --------  -----   ---------   ----
Unicast     Disabled    1000       100        5       none        0
Broadcast   Disabled    1000       100        5       none        0
Multicast   Disabled    1000       100        5       none        0
Switch#
Switch#show storm-control interface 1,2
Unit/Pt Storm Control Status    High Wm     Low Wm     Poll    Action      Trap
------- --------------------    -------     --------   -----   ---------   ----
1         Unicast   Disabled    1000        100        5       none        0
        Broadcast   Disabled    1000        100        5       none        0
        Multicast   Disabled    1000        100        5       none        0
2         Unicast   Disabled    1000        100        5       none        0
        Broadcast   Disabled    1000        100        5       none        0
        Multicast   Disabled    1000        100        5       none        0
```

Storm control configuration using EDM

Use the procedures in this section to configure storm control globally and for specific traffic types.

Configuring storm control globally

About this task

Use the following procedure to globally configure Storm Control using EDM

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree, click **Storm Control**.
3. In the work area, click the **Globals** tab.
4. Configure the Storm Control parameters as required.
5. On the toolbar, click **Apply**.

Variable definitions

Variable	Description
TrafficType	Indicates the different types of traffic for Storm Control Settings: • **unicast**: Indicates the unicast storm control settings • **broadcast**: Indicates the broadcast Storm Control settings • **multicast**: Indicates the multicast Storm Control settings
Enabled	Indicates the current setting for the port. Values include: • **true**: enables Storm Control on the port • **false**: disables Storm Control on the port
LowWatermark(pps)	Indicates the low-watermark value for the port in packets per second (pps). Range: 10 to 100000000 Default: 100
HighWatermark(pps)	Indicates the high-watermark value for the port in packets per second (pps). Range: 10 to 100000000 Default: 1000
PollInterval(secs)	Indicates the interval for watermark checking, the value varies in seconds. Range: 5 to 300

Table continues…

Variable	Description
	Default: 5
TrapInterval	Indicates the interval for sending traps when the poll-intervals exceed. Range: 0 to 1000 **Note:** Value 0 means disabled (high watermark traps will not be repeated) Default: 0
ActionType	Indicates the Storm Control action for the specified port: • **drop**: Set Storm Control action to drop • **none** • **shutdown**: Set Storm Control action to shutdown

Configuring broadcast storm control

About this task

Use the following procedure to configure the broadcast storm control settings.

Procedure

1. In the navigation tree double-click **Edit** to open the Edit tree.
2. In the Edit tree, click **Storm Control**.
3. In the work area, click the **Broadcast** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **Enabled** column.
6. Set a value from the drop-down list: **true** to enable Storm Control, or **false** to disable Storm Control for the specified port.
7. In the port row, double-click the cell in the **LowWatermark(pps)** column, and enter a value in the range `<10-100000000>`.
8. In the port row, double-click the cell in the **HighWatermark(pps)** column, and enter a value in the range `<10-100000000>`.
9. In the port row, double-click the cell in the **PollInterval(secs)** column, and enter a value in the range `<5-300>`.
10. In the port row, double-click the cell in the **TrapInterval** column, and enter a value in the range `<0-1000>`.
11. In the port row, double-click the cell in the **ActionType** column.

12. Set a value from the drop-down list: **none** to take no action, **drop**, or **shutdown** to shutdown Storm Control for the specified port.
13. On the toolbar, click **Apply**.

Variable definitions

Variable	Description
Index	Indicates the port number.
Enabled	Indicates the current setting for the port. Values include: • **true**: enables Storm Control on the port • **false**: disables Storm Control on the port
LowWatermark(pps)	Indicates the low-watermark value for the port in packets per second (pps). Range: 10 to 100000000 Default: 100
HighWatermark(pps)	Indicates the high-watermark value for the port in packets per second (pps). Range: 10 to 100000000 Default: 1000
PollInterval(secs)	Indicates the interval for watermark checking, the value varies in seconds. Range: 5 to 300 Default: 5
TrapInterval	Indicates the interval for sending traps when the poll-intervals are exceeded. Range: 0 to 1000 **Note:** Value 0 means disabled (high watermark traps will not be repeated) Default: 0
ActionType	Indicates the Storm Control action for the specified port: • **drop**: Set Storm Control action to drop • **none**: • **shutdown**: Set Storm Control action to shutdown

Configuring multicast storm control

About this task

Use the following procedure to configure the multicast storm control setting.

Procedure

1. In the navigation tree double-click **Edit** to open the Edit tree.
2. In the Edit tree, click **Storm Control**.
3. In the work area, click the **Multicast** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **Enabled** column.
6. Set a value from the drop-down list: **true** to enable Storm Control, or **false** to disable Storm Control for the specified port.
7. In the port row, double-click the cell in the **LowWatermark(pps)** column, and enter a value in the range <10–100000000>.
8. In the port row, double-click the cell in the **HighWatermark(pps)** column, and enter a value in the range <10–100000000>.
9. In the port row, double-click the cell in the **PollInterval(secs)column**, and enter a value in the range <5–300>.
10. In the port row, double-click the cell in the **TrapIntervalcolumn**, and enter a value in the range <0–1000>.
11. In the port row, double-click the cell in the **ActionType** column.
12. Set a value from the drop-down list: **none** to take no action, **drop** , or **shutdown** to shutdown Storm Control for specified port.
13. On the toolbar, click **Apply**.

Variable definitions

Variable	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
Enabled	Indicates the current setting for the port. Values include: • **true**: enables Storm Control on the port • **false**: disables Storm Control on the port

Table continues…

Variable	Description
LowWatermark(pps)	Indicates the low-watermark value for the port in packets per second (pps). Range: 10 to 100000000 Default: 100
HighWatermark(pps)	Indicates the high-watermark value for the port in packets per second (pps). Range: 10 to 100000000 Default: 1000
PollInterval(secs)	Indicates the interval for watermark checking, the value varies in seconds. Range: 5 to 300 Default: 5
TrapInterval	Indicates the interval for sending traps when the poll-intervals are exceeded. Range: 0 to 1000 **Note:** Value 0 means disabled (high watermark traps will not be repeated) Default: 0
ActionType	Indicates the Storm Control action for the specified port: • **drop**: Set Storm Control action to drop • **none** • **shutdown**: Set Storm Control action to shutdown

Configuring unicast storm control

About this task

Use the following procedure to configure the unicast storm control settings.

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree, click **Storm Control**.
3. In the work area, click the **Unicast** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **Enabled** column.

6. Set a value from the drop-down list: **true** to enable Storm Control, or **false** to disable Storm Control for the specified port.
7. In the port row, double-click the cell in the **LowWatermark(pps)** column, and enter a value in the range <10–100000000>.
8. In the port row, double-click the cell in the **HighWatermark(pps)** column, and enter a value in the range <10–100000000>.
9. In the port row, double-click the cell in the **PollInterval(secs)** column, and enter a value in the range <5–300>.
10. In the port row, double-click the cell in the **TrapIntervalcolumn**, and enter a value in the range <0–1000>.
11. In the port row, double-click the cell in the **ActionType** column.
12. Set a value from the drop-down list: **none** to take no action, **drop** , or **shutdown** to shutdown Storm Control for specified port.
13. On the toolbar, click **Apply**.

Variable definitions

Variable	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
Enabled	Indicates the current setting for the port. Values include: • **true**: enables Storm Control on the port • **false**: disables Storm Control on the port
LowWatermark(pps)	Indicates the low-watermark value for the port in packets per second (pps). Range: 10 to 100000000 Default: 100
HighWatermark(pps)	Indicates the high-watermark value for the port in packets per second (pps). Range: 10 to 100000000 Default: 1000
PollInterval(secs)	Indicates the interval for watermark checking, the value varies in seconds. Range: 5 to 300 Default: 5

Table continues…

Variable	Description
TrapInterval	Indicates the interval for sending traps when the poll-intervals are exceeded. Range: 0 to 1000 **Note:** Value 0 means disabled (high watermark traps will not be repeated) Default: 0
ActionType	Indicates the Storm Control action for the specified port: • **drop**: Set Storm Control action to drop • **none** • **shutdown**: Set Storm Control action to shutdown

Configuring port-based storm control

About this task

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

Procedure

1. From the Device Physical View, click one or more ports.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double-click **Chassis**.
4. In the Chassis tree, click **Ports**.
5. In the work area, click the **Storm Control** tab.

Variable definitions

Variable	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
Enabled	Indicates the current setting for the port. Values include: • **true**: enables Storm Control on the port • **false**: disables Storm Control on the port
LowWatermark(pps)	Indicates the low-watermark value for the port in packets per second (pps).

Table continues…

Variable	Description
	Range: 10 to 100000000 Default: 100
HighWatermark(pps)	Indicates the high-watermark value for the port in packets per second (pps). Range: 10 to 100000000 Default: 1000
PollInterval(secs)	Indicates the interval for watermark checking, the value varies in seconds. Range: 5 to 300 Default: 5
TrapInterval	Indicates the interval for sending traps when the poll-intervals are exceeded. Range: 0 to 1000 **Note:** Value 0 means disabled (high watermark traps will not be repeated) Default: 0
ActionType	Indicates the Storm Control action for the specified port: • **drop**: Set Storm Control action to drop • **none** • **shutdown**: Set Storm Control action to shutdown

Chapter 21: Terminal Access Controller Access Control System Plus

This chapter provides conceptual information and procedures to configure Terminal Access Controller Access Control System Plus (TACACS+) using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

TACACS+

The switch 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 CLI.

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 switch using the following methods:

- Connect the TACACS+ server through a local interface. Management PCs can reside on an out-of-band management port or serial port, or on the corporate network. The TACACS+ server is placed on the corporate network so that it can be routed to the switch.
- Connect the TACACS+ server through the management interface 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 564.

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 564.

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 = n0rt31
#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 24: 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 CLI terminal sessions within serial, Telnet, or SSH shells (from CLI management interface).

The accounting record includes the following information:

- user name
- date
- start, stop, 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 CLI to configure TACACS+ on the switch. You can also configure TACACS+ using Enterprise Device Manager.

For more information about configuring TACACS+ server information and TACACS+ authentication, authorization, and accounting using CLI, see TACACS+ configuration using CLI on page 565.

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.

TACACS+ configuration using CLI

This section describes how you configure TACACS+ to perform AAA services for system users.

Configuring switch TACACS+ server settings

About this task

Configures switch TACACS+ server settings to add a TACACS+ server to your system.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure switch TACACS+ server settings.

   ```
   tacacs server { [host <host_addr>] [secondary-host <sec_host_addr>]
   [key <key>] [port <1-65535>] }
   ```

3. Clear switch TACACS+ server settings.

   ```
   no tacacs server { [host] [secondary-host] [key] [port] }
   ```

4. Restore switch TACACS+ server settings to default.

   ```
   default tacacs server { [host] [secondary-host] [key] [port] }
   ```

Variable definitions

The following table defines parameters that you can enter with the **`tacacs server`** command.

Variable	Value
no	Disables or clears the TACACS+ server settings.
default	Restores the TACACS+ server settings to default values.
host <*host_addr*>	Specifies the IP address of the primary host you want to add or configure.
secondary-host <*sec_host_addr*>	Specifies the IP address of the secondary host. The secondary host is used only if the primary server does not respond.
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 identified 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 <*1–65535*>	Specifies the TCP port for TACACS+. DEFAULT: 49

Enabling remote TACACS+ services

Before you begin

- Configure a TACACS+ server on the switch

About this task

Enables remoteTACACS+ services to provide services to remove users over serial or Telnet conections.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable remote TACACS+ services for serial connections.

   ```
   cli password serial tacacs
   ```

3. Enable remote TACACS+ services for Telnet connections.

   ```
   cli password telnet tacacs
   ```

Enabling or disabling TACACS+ authorization

About this task

Enables or disables TACACS+ authorization globally on the switch.

TACACS+ authorization is disabled by default.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable TACACS+ authorization.

   ```
   tacacs authorization enable
   ```

3. Disable TACACS+ authorization.

   ```
   tacacs authorization disable
   ```

Configuring TACACS+ authorization privilege levels

About this task

Configures TACACS+ authorization privilege levels to specify the privilege levels to which TACACS+ authorization applies.

The default authorization level is NONE.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure TACACS+ authorization privilege levels.

   ```
   tacacs authorization { ALL | <level> | NONE }
   ```

Variable definitions

The following table defines parameters that you can enter with the **`tacacs authorization level`** command.

Variable	Value
ALL	Enables authorization for all privilege levels.
<level>	Specifies integer values in the range of 0–15, indicating the privilege levels for which authorization is enabled. You can enter a single level, a range of levels, or several levels. For any levels you do not specify, authorization does not apply, and users assigned to these levels can execute all commands.
NONE	Authorization is not enabled for privilege levels. All users can execute commands available on the switch.

Enabling or disabling TACACS+ accounting

About this task

Enables or disables TACACS+ accounting globally on the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Enable TACACS+ accounting.

```
tacacs accounting enable
```

3. Disable TACACS+ accounting.

```
tacacs accounting disable
```

Configuring the switch TACACS+ level

About this task

Configures the switch TACACS+ level to select a new level for a switch or use the last configured level.

The default switch TACACS+ level is 15.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure a new TACACS+ level for a switch.

```
tacacs switch level [<1-15>]
```

3. Use the last configured TACACS+ level for a switch.

```
tacacs switch back
```

Viewing TACACS+ information

About this task

Displays TACACS+ information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display TACACS+ information.

```
show tacacs
```

Example

```
Switch#show tacacs
Primary Host: 0.0.0.0
Secondary Host: 0.0.0.0
Port: 49
```

```
Key: ***************
TACACS+ authorization is disabled
Authorization is enabled on levels : 2-9
TACACS+ accounting is disabled
```

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

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. Web access is Read-Only (RO) for levels 1 to 14 and Read-Write-All (RW) for level 15.

Configuring the TACACS+ server

Adding a TACACS+ server using EDM

Use the following procedure to add TACACS+ server in the system.

Procedure

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 displays.
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

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.

Chapter 22: Configuration Examples

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

Extreme Networks Identity Engine Ignition Server TACACS+ configuration example

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

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

The example displays how to do the following:

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

For more information on the Ignition Server, see Identity Engines Ignition Server.

Before you begin

- Configure the Ignition Server appliance and set up its network settings. For more information, see Identity Engines Ignition Server Getting Started.
- Install the Ignition Dashboard on your Windows OS.
- Configure each authenticator (switch) to recognize the Ignition Server appliance as its TACACS + server.

- Configure your switch to send packets to the Ignition Server appliance with the appropriate IP address and port.
- Ensure licenses are up-to-date.

Procedure

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

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

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

      As an example:

      User Name: jsmith

First Name: John

Last Name: Smith

Password: test

Confirm password: test

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

      In this window you build your command set by adding commands to the list. You can build the command list manually or you can import a list. For more information on importing a command list, see Identity Engines Ignition Server.
   e. To manually add the commands, click **Add** in the New/Edit Device Command Set window.
   f. Click the **Simple Command Using Keywords and Arguments** box.
   g. In the **Command** field, type the command, and optionally its arguments.
   h. To allow the command to be used with any argument, select the **Allow** box.
   i. To allow only the specific command and arguments you have types, tick the **Deny** box.
   j. Click **OK** to add the command to the list.
   k. Continue to add the commands that you want.
5. If your TACACS+ policy uses privilege-level authorization, create the TACACS+ access policy to allow the TACACS+ Ignition Server to communicate with the switch.
   a. In the Ignition Server Dashboard, expand the following in the Configuration tree: **Site Configuration** > **Access Policies** > **TACACS+**.
   b. Select **default-tacacs-admin**.
   c. Click on the **Authorization Policy** tab and select the name of the policy you want to edit.
   d. Click **Edit** and the **Edit Authorization Policy** window appears.
   e. In the **Rules** section, select the rule you want to edit. In this case select level5, to which you have already added commands.

      The **Rules** list at the left lets you browse and sort the rules in your policy. Use the up and down arrow buttons at the right to set the rule sequence, and click a rule name in the list to edit that rule. The Selected Rule Details section lets you edit the rule you have selected.

f. In the Selected Rule Details section, under **Rule Name**, for this example, it reads `level5`.

g. Select **Rule Enabled**.

h. With level5 selected in the Rules list, go to the buttons to the right of the **Constraint** list and click **New**.

i. In the Action section, select **Allow**.

j. Select the **Command Sets** tab, in the Action section. Allow Commands in Set should read level-5, in this example, and under All Command Sets all the commands that are accessible under level5 should be listed.

k. Click **OK**.

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

IF User: user-id = level5 THEN Allow

Permit commands in Command Set: level-5

6. Configure the Ignition Server to connect to authenticators, which is the switch:

a. In the Ignition Server Dashboard, expand the following folders: **Site Configuration** > **Authenticators** > **default** and the Authenticator Summary window appears.

b. Click **New**, and the Authenticator Details window appears.

c. For this example, type `VSPswitch` under name.

d. To the right select **Enable Authenticator**.

e. Type the IP address for the switch, which is the authenticator. Use the primary CPU address or the management virtual address.

f. In the **Vendor** field, select **Nortel**.

g. In the **Device template** field, select **ers-switches-nortel**.

h. Select the **TACACS+ Settings** tab.

i. Select **Enable TACACS+ Access**.

j. In the **TACACS+ Shared Secret** field, type the key value you entered into the switch. In this example, the key is the word `secret`.

To connect using TACACS+, you must use the shared secret for each device. In your switch documentation, the shared secret can also be referred to as a specific key string or an encryption string.

k. Under **Access Policy**, select **default-tacacs-user**.

l. Click **OK**.

Configuration example: Linux freeware server

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

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

2. Open the configuration file tac_plus.cfg:

   ```
   $vi tac_plus.cfg
   ```

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

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

   - where

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

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

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

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

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

   The following is a sample config file.

   ```
   $vi tac_plus.cfg


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

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

4. Save the changes to the tac_plus.cfg file.

5. Run the TACACS+ daemon using the following command:

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

   where

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

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

Supported SNMP MIBs and traps

This section contains information about:

- Supported MIBs on page 577
- Supported traps on page 579

Supported MIBs

The following tables list supported SNMP MIBs.

Table 25: 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

Table continues…

MIB name	RFC	File name
SNMP-VIEW-BASED-ACM-MIB	3415	rfc3415.mib
SNMP-COMMUNITY-MIB	3584	rfc3584.mib

Table 26: 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
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 27: 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 (rcVlanIgmp 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

Table continues…

Application	Related MIBs	File name
	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
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 28: 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 (Extreme Networks 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	• 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.

Table continues…

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 lldpStatsRemTableLast ChangeTime 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.
nnMstRegionConfigChange	System-wide	The MST region configuration identifier changes.

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:

mac-max restricts the maximum number of EAP and NEAP clients allowed per port. The limit set by **mac-max** takes precedence over **eap-mac-max** or **non-eap-mac-max**. The default **mac-max** value is 1.

MHSA mode (with or without RADIUS VLAN)

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 PVID is kept as the one you manually configured for that port before EAP was enabled.
- an unauthenticated client is on the port -- the port is kept in the initial VLAN ID and the PVID is kept as the one you manually configured for that port before EAP was enabled.
- an authenticated client is on the port but it did not receive valid RADIUS attributes—the port is kept in the initial VLAN ID, and the PVID is kept as the one you manually configured for that port before EAP was enabled.
- an authenticated client is on the port and it has received valid RADIUS attributes—the port is moved to the RADIUS VLAN ID and it uses the RADIUS VLAN PVID.

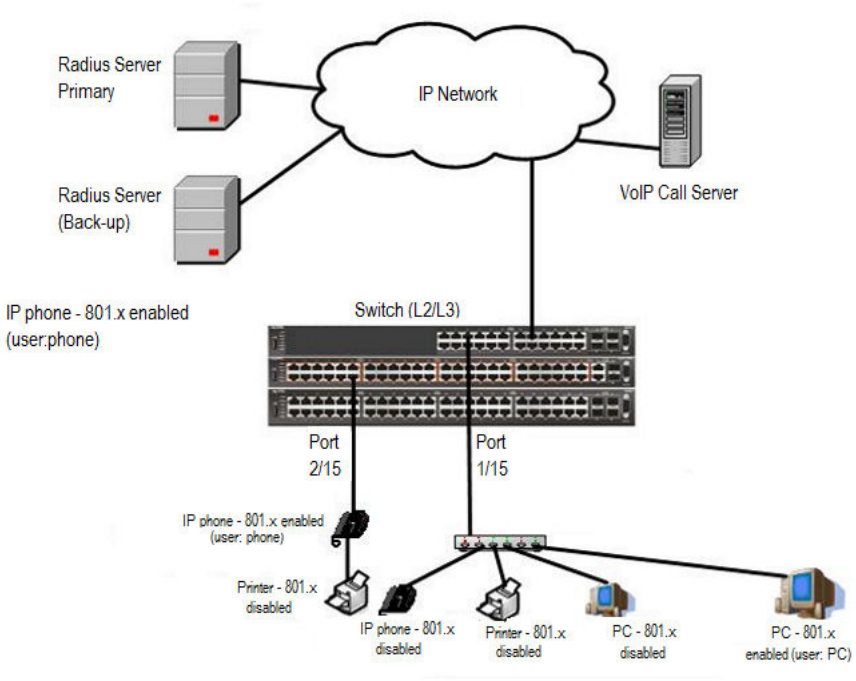


Figure 25: MHSA authentication mode (with or without RADIUS VLAN)

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

```
Switch(config)# ip address 192.0.2.1 netmask 255.255.255.0 default-gateway 192.0.2.2
Switch(config)# radius server host 192.0.2.3
Switch(config)# radius server host 192.0.2.4 secondary
Switch(config)# radius server host key
Enter key: RadiusKey
Enter key: RadiusKey
Switch(config)# vlan configcontrol automatic
Switch(config)# vlan create 50 type port
```

```
Switch(config)# vlan create 100 type port
Switch(config)# vlan create 200 type port
Switch(config)# vlan create 300 type port
Switch(config)# vlan members add 50 1/15
Switch(config)# vlan members add 100 2/15
```

2. Confirm the VLAN interface settings

```
Switch(config)# sho vlan interface info 1/15,2/15
```

```
           Filter    Filter
           Untagged  Unregistered
Unit/Port  Frames    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

```
Switch(config)#sho vlan interface info 1/15,2/15
```

```
                                                VLAN              VLAN
Unit/Port  VLAN      VLAN Name      VLAN       Name      VLAN      Name
--------   --------  --------       --------   ------    -------   ------
1/15       50        VLAN #50       --------   ------    -------   ------
2/15       100       VLAN #100      --------   ------    -------   ------
```

4. Confirm that you can reach the RADIUS server

```
Switch(convig)#ping 192.0.2.3
(Host is reachable)
```

5. Set the EAPOL status

```
Switch(config)#interface Ethernet 1/15,2/15
Switch(config-if)#eapol multihost auto-non-eap-mhsa-enable
Switch(config-if)#eapol multihost non-eap-mac-max 4
Switch(config-if)#eapol status auto
Switch(config-if)#exit
Switch(config)#eapol multihost auto-non-eap-mhsa-enable
Switch(config)#eapol enable
```

6. Confirm authentication for EAP/NEAP clients

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

```
                                                 Backend
           Client                                Auth
Unit/Port  MAC Address          Pae State        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
```

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

```
          Client
Unit/Port MAC Address              State                Vid       Pri
--------  --------                 --------             -------   -------
1/15      00:1C:9C:2B:CE:04        Auto-Learned For     N/A       N/A
                                   MHSA
2/15      00:1D:3E:4A:BC:01        Auto-Learned For     N/A       N/A
                                   MHSA
Total number of authenticated clients:  2
```

7. Confirm the VLAN interface settings

```
Switch(config)# show vlan interface info 1/15,2/15
```

```
          Filter    Filter
          Untagged  Unregistered
Unit/Port Frames    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 VIDs.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
                                                 VLAN              VLAN
Unit/Port VLAN      VLAN Name      VLAN          Name      VLAN    Name
--------  --------  --------       --------      ------    -------  -------
1/15      300       VLAN #300      --------      ------    -------  -------
2/15      200       VLAN #200      --------      ------    -------  -------
```

Alternate configuration

The following operation applies to **MHSA authentication mode 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. Confirm EAPOL MultiHost status.

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

```
                                                Backend
           Client                               Auth
Unit/Port  MAC Address          Pae State       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
```

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

```
           Client
Unit/Port  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
```

2. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 1/15,2/15
```

```
                    Filter
           Filter   Unregister
           Untagged ed
Unit/Port  Frames   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.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
                    VLAN                VLAN                VLAN
Unit/Port  VLAN     Name       VLAN     Name       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

The configuration example in this section applies to the following client port settings when:

- 802.1x is disabled on port—the port is kept in the initial VLAN ID, and the PVID is kept as the one you manually configured.

- EAP is enabled on port—the port is moved to the Guest VLAN and the PVID is set to Guest VLAN.
- an authenticated client is on the port but it did not receive RADIUS attributes or valid RADIUS attributes—the port is included in the initial VLAN ID, and the PVID is kept as the one you manually configured for that port before EAP was enabled.
- an authenticated client is on the port and it has received valid RADIUS attributes—the port is moved to the RADIUS VLAN ID and it uses the RADIUS VLAN as PVID.

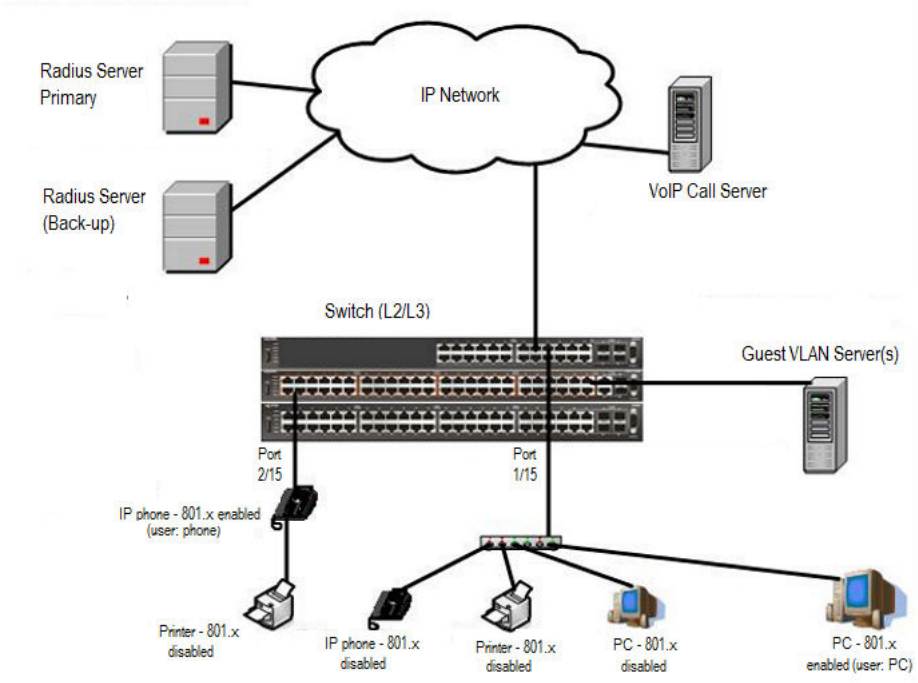


Figure 26: MHSA authentication mode (Guest VLAN option enabled) with or without RADIUS additional attributes

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
  - EAP is enabled 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
  - EAP is enabled 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

```
Switch(config)#ip address 192.0.2.1 netmask 255.255.255.0 default-gateway 192.0.2.2
Switch(config)#radius server host 192.0.2.3
Switch(config)#radius server host 192.0.2.4 secondary
Switch(config)#radius server host key
Enter key: RadiusKey
Enter key: RadiusKey
Switch(config)#vlan configcontrol automatic
Switch(config)#vlan create 20 type port
Switch(config)#vlan create 50 type port
Switch(config)#vlan create 100 type port
Switch(config)#vlan create 200 type port
Switch(config)#vlan create 300 type port
Switch(config)#vlan members add 50 1/15
Switch(config)#vlan members add 100 2/15
```

2. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 1/15,2/15
```

```
           Filter    Filter
           Untagged  Unregistered
Unit/Port  Frames    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 inteface VIDs.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
Unit/Port  VLAN      VLAN Name      VLAN       VLAN      VLAN      VLAN
--------   --------  --------      --------   Name      -------   Name
                                               ------              ------
1/15       50        VLAN #50       --------   ------    -------   ------
2/15       100       VLAN #100      --------   ------    -------   ------
```

4. Confirm that you can reach the RADIUS server.

```
Switch(config)#ping 192.0.2.3
(Host is reachable)
```

5. Set the EAPOL status.

```
Switch(config)#interface Ethernet 1/15,2/15
Switch(config-if)#eapol guest-vlan vid 20
Switch(config-if)#eapol guest-vlan enable
Switch(config-if)#eapol multihost auto-non-eap-mhsa-enable
Switch(config-if)#eapolmultihost non-eap-mac-max 4
Switch(config-if)#eapol status auto
Switch(config-if)#exit
Switch(config)#eapol multihost auto-non-eap-mhsa-enable
Switch(config)#eapol enable
```

6. Before EAP clients are authenticated, confirm the EAPOL MultiHost status

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

```
                                          Backend
           Client                         Auth
Unit/Port  MAC Address          Pae State  State     Vid       Pri
--------   --------             --------   ------    -------   -------
```

7. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 1/15,2/15
```

```
           Filter    Filter
           Untagged  Unregistered
 Unit/Port Frames    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.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
Unit/Port  VLAN      VLAN Name      VLAN       VLAN      VLAN      VLAN
--------   --------  --------       --------   Name      -------   Name
                                               ------              -------
1/15       20        VLAN #20       --------   ------    -------   -------
2/15       20        VLAN #20       --------   ------    -------   -------
```

9. After EAP clients are authenticated, confirm the EAPOL MultiHost status.

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

```
                                                Backend
           Client                               Auth
Unit/Port  MAC Address              Pae State   State     Vid       Pri
--------   --------                 --------    ------    -------   -------
1/15       00:50:BF:B8:09:AF        Authentic   Idle      N/A       N/A
                                    ated
2/15       00:1E:CA:FF:C2:94        Authentic   Idle      N/A       N/A
                                    ated
```

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

```
           Client
 Unit/Port MAC Address              State                Vid       Pri
 --------  --------                 --------             -------   -------
 1/15      00:1C:9C:2B:CE:04        Auto-Learned For     N/A       N/A
                                    MHSA
 2/15      00:1D:3E:4A:BC:01        Auto-Learned For     N/A       N/A
                                    MHSA
```

10. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 1/15,2/15
```

```
           Filter    Filter
           Untagged  Unregistered
Unit/Port  Frames    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.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
Unit/Port  VLAN      VLAN Name      VLAN       VLAN       VLAN       VLAN
--------   --------  --------       --------   Name       -------    Name
                                                ------                -------
1/15       300       VLAN #300      --------   ------     -------    -------
2/15       200       VLAN #200      --------   ------     -------    -------
```

Alternate configuration

The following operation applies to **MHSA authentication mode with Guest VLAN 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. Confirm EAPOL MultiHost status.

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

```
                                                Backend
           Client                               Auth
Unit/Port  MAC Address           Pae State      State      Vid        Pri
--------   --------              --------       --------   --------   -------
1/15       00:50:BF:B8:09:AF     Authentic      Idle       N/A        N/A
                                 ated
2/15       00:1E:CA:FF:C2:94     Authentic      Idle       N/A        N/A
                                 ated
```

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

```
           Client
Unit/Port  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
```

2. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 1/15,2/15
```

```
           Filter     Filter
           Untagged   Unregister
Unit/Port  Frames     ed         PVID       PRI        Tagging    Name
--------   --------   Frames     --------   --------   --------   -------
                      --------
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.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
                                                                    VLAN
Unit/Port  VLAN      VLAN Name    VLAN      VLAN Name    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

The configuration example in this section applies to the following client port settings when:

- 802.1x is disabled on port—the port is included in the initial VLAN ID, and the PVID is kept as the one you manually configured for that port before EAP was enabled.
- EAP is enabled on port—the port is moved to the Guest VLAN and the PVID is set to Guest VLAN.
- an authenticated client is on the port but it did not receive RADIUS attributes or valid RADIUS attributes—the port is included in the initial VLAN ID, and the PVID is set as the one you manually configured for that port before EAP was enabled.
- an authenticated client is on the port and it has received valid RADIUS attributes—the port is moved to the RADIUS VLAN ID and it uses the RADIUS VLAN PVID.
- RADIUS Server Unreachable (801.x enabled)—the port is moved to the Fail Open VLAN, and the port uses the Fail Open VLAN PVID.

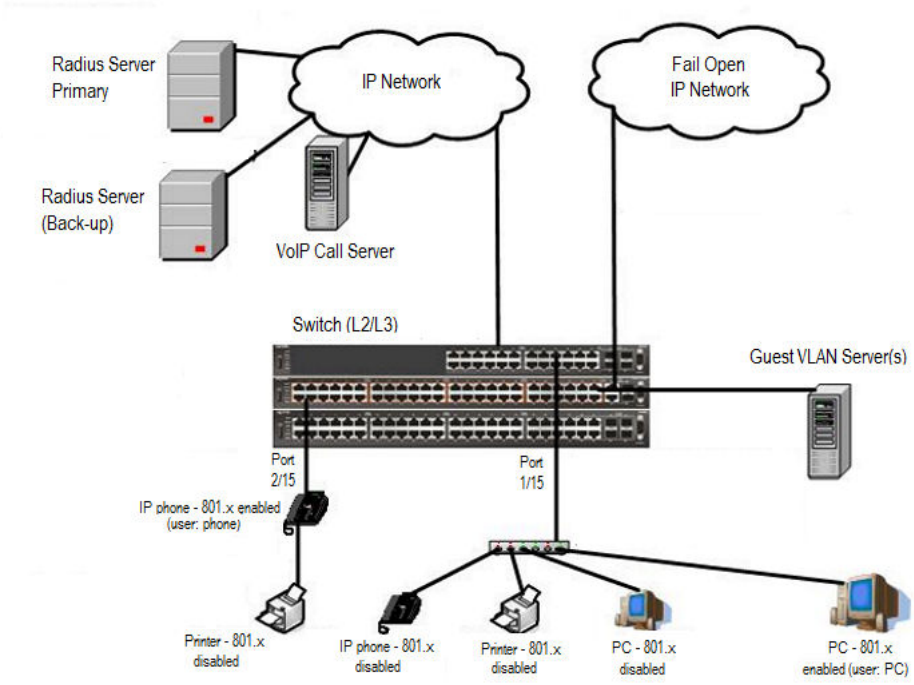


Figure 27: MHSA authentication mode (Guest VLAN and Fail Open VLAN options enabled) with or without RADIUS additional attributes

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
  - EAP is enabled 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
  - EAP is enabled 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

```
Switch(config)#ip address 192.0.2.1 netmask 255.255.255.0 default-gateway 192.0.2.2
Switch(config)#radius server host 192.0.2.3
Switch(config)#radius server host 192.0.2.4 secondary
Switch(config)#radius server host key
Enter key: RadiusKey
Enter key: RadiusKey
Switch(config)#vlan configcontrol automatic
Switch(config)#vlan create 20 type port
Switch(config)#vlan create 30 type port
Switch(config)#vlan create 50 type port
Switch(config)#vlan create 100 type port
Switch(config)#vlan create 200 type port
Switch(config)#vlan create 300 type port
Switch(config)#vlan members add 50 1/15
Switch(config)#vlan members add 100 2/15
```

2. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 1/15,2/15
```

```
           Filter    Filter
           Untagged  Unregistered
Unit/Port  Frames    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 inteface VIDs.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
                                                VLAN                VLAN
Unit/Port  VLAN      VLAN Name      VLAN        Name       VLAN     Name
--------   --------  --------       --------    ------     -------  ------
1/15       50        VLAN #50       --------    ------     -------  ------
2/15       100       VLAN #100      --------    ------     -------  ------
```

4. Confirm that you can reach the RADIUS server.

```
Switch(config)#ping 192.0.2.3
(Host is reachable)
```

5. Set the EAPOL status.

```
Switch(config)#eapol multihost fail-open-vlan vid 30
Switch(config)#eapol multihost fail-open-vlan enable
Switch(config)#interface Ethernet 1/15,2/15
Switch(config-if)#eapol guest-vlan vid 20
Switch(config-if)#eapol guest-vlan enable
Switch(config-if)#eapol multihost auto-non-eap-mhsa-enable
Switch(config-if)#eapol multihost non-eap-mac-max 4
Switch(config-if)#eapol status auto
Switch(config-if)#exit
Switch(config)#eapol multihost auto-non-eap-mhsa-enable
Switch(config)#eapol enable
```

6. Before EAP clients are authenticated, confirm the EAPOL MultiHost status.

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

```
                                                Backend
           Client                               Auth
Unit/Port  MAC Address              Pae State   State     Vid       Pri
--------   --------                 --------    ------    -------   -------
```

7. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 1/15,2/15
```

```
           Filter      Filter
           Untagged    Unregistered
Unit/Port  Frames      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.

```
Switch(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.

```
Switch(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
```

```
Switch(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.

```
Switch(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.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
                                                    VLAN                VLAN
Unit/Port  VLAN      VLAN Name      VLAN           Name        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.

```
Switch(config)#ping 192.0.2.3
(Host is not reachable)
Switch(config)#ping 192.0.2.4
(Host is not reachable)
```

14. After approximately 3 minutes, confirm the EAPOL MultiHost status again.

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

```
                                                  Backend
           Client                                 Auth
Unit/Port  MAC Address              Pae State     State     Vid       Pri
--------   --------                 --------      ------    -------   -------
```

15. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 1/15,2/15
```

```
           Filter     Filter
           Untagged   Unregistered
Unit/Port  Frames     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.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
                                                    VLAN                VLAN
Unit/Port  VLAN      VLAN Name      VLAN           Name        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.

```
Switch(config)#ping 192.0.2.3
(Host is reachable)
```

19. Confirm the EAPOL MultiHost status again.

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

```
                                                Backend
           Client                               Auth
Unit/Port  MAC Address          Pae State       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.

```
Switch(config)#show vlan interface info 1/15,2/15
```

```
           Filter    Filter
           Untagged  Unregistered
Unit/Port  Frames    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.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
                                                VLAN               VLAN
Unit/Port  VLAN      VLAN Name      VLAN        Name     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 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. After EAP clients are authenticated, confirm EAPOL MultiHost status.

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

```
                                          Backend
            Client                        Auth
Unit/Port   MAC Address         Pae State 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
```

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

```
            Client
Unit/Port   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
```

2. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 1/15,2/15
```

```
            Filter    Filter
            Untagged  Unregister
Unit/Port   Frames    ed          PVID      PRI       Tagging   Name
--------    --------  Frames      --------  --------  --------  -------
                      --------
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.

```
Switch(config)#show vlan interface vids 1/15,2/15
```

```
                      VLAN                  VLAN                  VLAN
Unit/Port   VLAN      Name      VLAN        Name      VLAN        Name
--------    --------  --------  --------    --------  --------    -------
1/15        50        VLAN #50  --------    --------  --------    -------
2/15        100       VLAN #100 --------    --------  --------    -------
```

MHMA-MV authentication mode with or without additional RADIUS attributes

In this mode, traffic from each EAP or Non-EAP user with a unique MAC address can be sent through a unique VLAN. This functionality is achieved by using MAC-based VLANs, which will send untagged traffic from the client to its associated VLAN.

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 PVID is kept as the one you manually configured.
- when 802.1X is enabled on the port:
  - EAP is enabled on the port—the port is included in the initial VLAN ID, and the PVID is kept as the one you manually configured for that port before EAP was enabled.
  - an EAP or Non-EAP authenticated client is on the port:
    - if no RADIUS attributes or invalid ones are received, the port is kept in the initial VLAN. The client MAC will be associated with the initial PVID.
    - if valid RADIUS attributes are received for the 802.1x client, the port is added to the RADIUS VLAN and kept in the initial VLANs. The PVID is kept as the initial one. The client MAC is associated with the RADIUS VLAN.
  - an authenticated Non-EAP static MAC client is on the port (client MAC was learned in the MAC address table)—the port is kept in the initial VLANs and the PVID is the initial one. The client MAC is associated with the PVID.
  - an authenticated Non-EAP DHCP client (IP Phone) is on the port and the client authenticate using a valid DHCP signature—in this case, the port remains in the initial VLAN and the PVID is the initial one. The DHCP client will be associated with the first EAP Voice VLAN configured, to send untagged traffic. But the client can also send tagged traffic, in the VoIP VLAN configured in the phone settings.

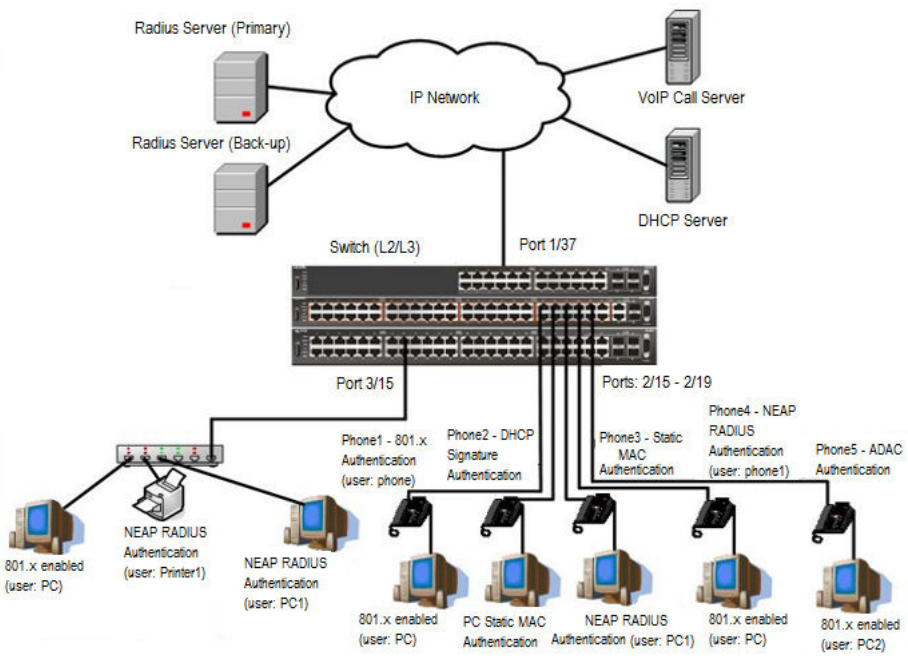


Figure 28: MHMA-MV authentication mode with or without additional RADIUS attributes

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:
     - 802.1x authenticated user Phone1connected
     - 802.1x 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
     - 802.1x 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

- 802.1x enabled user PC2 connected
- Initial VLAN ID = 50, 300
- PC RADIUS VLAN ID = none
- Phone ADAC VLAN ID = 201

• Port 3/15:

- 802.1x 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:

- 802.1x disabled - VLAN ID/PVID = 50,200/50
- EAP is enabled on the port - 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:

- 802.1x disabled - VLAN ID/PVID = 50,300/300
- EAP is enabled on the port - 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:
  - 802.1x disabled - VLAN ID/PVID = 50,200/50
  - EAP is enabled on the port - 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:
  - 802.1x disabled - VLAN ID/PVID = 50,200/50
  - EAP is enabled on the port - 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:
  - 802.1x disabled - VLAN ID/PVID = 50,300/300
  - EAP is enabled on the port - 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:

- 802.1x disabled - VLAN ID/PVID = 50/50
- EAP is enabled on the port - VLAN ID/PVID = 50/50
- Authenticated (at least one user authenticated from : PC, PC1, Printer1):
  - VLAN ID/PVID = 50/ 50 (No RADIUS attribute received/Invalid RADIUS attributes received)
  - VLAN ID/PVID = 300/ 300 (Valid RADIUS attributes received)
  - EAP port vid for PC client: 300
  - EAP port vid for printer NEAP client: 300
  - EAP port vid for NEAP PC client: 300

Configuration example

1. Configure the RADIUS servers and VLAN settings

```
Switch(config)#ip address 192.0.2.1 netmask 255.255.255.0 default-gateway 192.0.2.2
Switch(config)#radius server host 192.0.2.3
Switch(config)#radius server host 192.0.2.4 secondary
Switch(config)#radius server host key
Enter key: RadiusKey
Enter key: RadiusKey
Switch(config)#vlan configcontrol automatic
Switch(config)#vlan create 50 type port
Switch(config)#vlan create 200 type port
Switch(config)#vlan create 300 type port
Switch(config)#vlan members add 50 2/15-19,3/15
```

2. Confirm the VLAN interface settings.

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

```
                Filter      Filter
                Untagged    Unregistered
Unit/Port       Frames      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 inteface VIDs.

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

```
Unit/Port   VLAN        VLAN Name    VLAN        VLAN Name   VLAN        VLAN Name
--------    --------    --------     --------    ------      -------     ------
2/15        50          VLAN #50     --------    ------      -------     ------
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.

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

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

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

6. Confirm the VLAN interface settings.

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

```
          Filter      Filter
          Untagged    Unregistered
Unit/Port Frames      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 inteface VIDs.

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

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

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

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

9. Confirm the VLAN interface settings.

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

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

10. Confirm the VLAN inteface VIDs.

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

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

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

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

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

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

```
           Filter     Filter
           Untagged   Unregistered
Unit/Port  Frames     Frames       PVID      PRI       Tagging    Name
---------  --------   ---------    ------    -------   -------    -------

1/37       No         Yes          1         0         TagAll     Unit 1,
                                                                  Port 37
```

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

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

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

14. Configure ADAC.

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

Important:

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

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

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

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

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

```
Switch(config)#ping 192.0.2.3
(Host is reachable)

Switch(config)#ping 192.02.4
 (Host is reachable)
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

24. Set the EAPOL MultiHost status.

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

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

25. Enable ADAC.

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

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

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

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

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

27. Confirm the VLAN status.

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

```
Id      Name          Type     Protocol  User     Active  IVL/SVL  Mgmt
------  --------      ------   -----     PID      ------  ------   ------
                                         ------
1       VLAN #1       Port     None      0x0000   Yes     IVL      Yes

        Port Members: 1/2-34,1/39-50,2/1-14,2/20-26,3/1-14,3/16-26

50      VLAN #50      Port     None      0x0000   Yes     IVL      No

        Port Members: 1/1,1/35,2/15-19,3/15

200     VLAN #200     Port     None      0x0000   Yes     IVL      No

        Port Members: 1/36,2/15-18

201     Voice_VLAN    Port     None      0x0000   Yes     IVL      No

        Port Members: 1/37,2/19

300     VLAN #300     Port     None      0x0000   Yes     IVL      No

        Port Members: 1/37-38,2/15-19,3/15
```

28. Confirm the EAPOL MultiHost status.

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

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

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

```
                                                Backend
           Client                               Auth
Unit/Port  MAC Address          Pae State       State      Vid        Pri
--------   --------             --------        ------     -------    ------

2/15       00:19:E1:E5:52:92    Authenticated   Idle       50         0

2/15       00:50:BF:B8:09:AF    Authenticated   Idle       300        0

2/18       00:AB:CD:03:00:12                    Idle       3000       N/A

2/19       00:AB:CD:04:00:13    Authenticated   Idle       300        0

3/15       00:AB:CD:01:00:10    Authenticated   Idle       300        0

=========       Neap Phones     =============

2/16       00:19:E1:E6:09:B1

Total number of authenticated clients:  6
```

29. Confirm the VLAN interface settings.

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

```
           Filter      Filter
           Untagged    Unregistered
Unit/Port  Frames      Frames       PVID       PRI        Tagging     Name
--------   --------    --------     ------     -------    -------     -------

2/15       No          Yes          50         0          UntagPvid   Unit 2,
                                                           Only        Port 15

2/16       No          Yes          300        0          UntagPvid   Unit 2,
                                                           Only        Port 16

2/17       No          Yes          50         0          UntagPvid   Unit 2,
                                                           Only        Port 17

2/18       No          Yes          50         0          UntagPvid   Unit 2,
                                                           Only        Port 18

2/19       No          Yes          300        0          UntagPvid   Unit 2,
                                                           Only        Port 19

3/15       No          Yes          50         0          UntagAll    Unit 3,
                                                                       Port 15
```

30. Confirm the VLAN interface VIDs.

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

```
Unit/Port  VLAN       VLAN Name   VLAN       VLAN Name    VLAN       VLAN Name
--------   --------   ---------   --------   ------       -------    -------
2/15       50         VLAN #50    200        VLAN #200    300        VLAN #300
2/16       50         VLAN #50    200        VLAN #200    300        VLAN #300
2/17       50         VLAN #50    200        VLAN #200    300        VLAN #300
2/18       50         VLAN #50    200        VLAN #200    300        VLAN #300
2/19       50         VLAN #50    201        Voice_VLAN   300        VLAN #300
3/15       50         VLAN #50    300        VLAN #300    -------    -------
```

Alternate configuration

The following operation applies to **applies to MHMA-MV authentication mode without valid additional RADIUS attributes**, when the RADIUS server has no special attributes configured or the RADIUS server uses misconfigured attributes (not matching the device configuration).

This configuration example modifies EAP and NEAP client attributes on the RADIUS server, replacing VLAN ID 300 with VLAN ID 124, which is not configured on the device.

1. Enable EAPOL.

```
Switch(config)#eapol disable
Switch(config)#eapol enable
```

2. Confirm EAPOL MultiHost status.

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

```
           Client
Unit/Port  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            N/A        N/A
                                For IP
                                Telephony
3/15       00:AB:CD:01:00:20    Authenticated By RADIUS  50         0
3/15       00:AB:CD:01:00:21    Authenticated By RADIUS  50         0
Total number of authenticated clients:  7
```

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

```
                                                Backend
           Client                               Auth
Unit/Port  MAC Address          Pae State       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

                                Authenticated
3/15       00:AB:CD:01:00:10                    Idle       50        0
=========       Neap Phones       ===========
2/16       00:19:E1:E6:09:B1
Total number of authenticated clients:  6
```

3. Confirm the VLAN interface settings.

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

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

4. Confirm the VLAN interface settings.

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

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

5. Confirm the VLAN interface VIDs.

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

```
Unit/Port VLAN     VLAN Name  VLAN     VLAN Name  VLAN     VLAN Name
--------- -------- ---------- -------- ---------- -------- -------
2/15      50       VLAN #50   200      VLAN #200  -------- -------
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-MV authentication mode with Guest VLAN and Fail-Open VLAN enabled

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 kept in its initial VLANs and the PVID is the one you manually configured
- when 802.1X is enabled on the port:
  - EAP is enabled on the port—the port is included only in the Guest VLAN ID, and the port uses the Guest VLAN PVID
  - an EAP or a Non-EAP client authenticated via Radius is on the port with Guest VLAN enabled
    - if no RADIUS attributes or invalid RADIUS attributes are received for the client, the port is kept in the initial VLAN and in Guest VLAN. The PVID is the Guest VLAN ID. The client MAC is associated with the initial PVID. In this way, a guest will send untagged traffic in the Guest VLAN and an authenticated client will send traffic in the initial VLAN.

  - if valid RADIUS attributes are received for the client, the port is added to the RADIUS VLAN and the PVID is kept as the Guest VLAN ID. The port is also kept in the initial VLANs. The client MAC is associated with the RADIUS VLAN.

- an authenticated Non-EAP 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 its initial VLAN and the PVID is the Guest VLAN VID. The client is associated with the initial PVID for untagged traffic.
- an authenticated non-802.x DHCP client (IP Phone) is on the port and the client authenticate using a valid DHCP signature. In this case, the port remains in the initial VLAN and the PVID is the initial one. The DHCP client will be associated with the first EAP Voice VLAN configured, to send untagged traffic. But the client can also send tagged traffic, in the VoIP VLAN configured in the phone settings. The port is a member of any EAP VOIP VLAN that has been created and enabled.
- RADIUS Server Unreachable (802.1x enabled) - the port is copied to the Fail Open VLAN (the port is also kept in the VLANs manually configured before EAP enabling, in the Guest VLAN and in all RADIUS VLANs for authenticated clients). Authenticated clients send their traffic in their own associated VLANs (either manually configured before EAP enabling, or RADIUS-assigned). New unauthenticated clients will send traffic in the Fail Open VLAN.

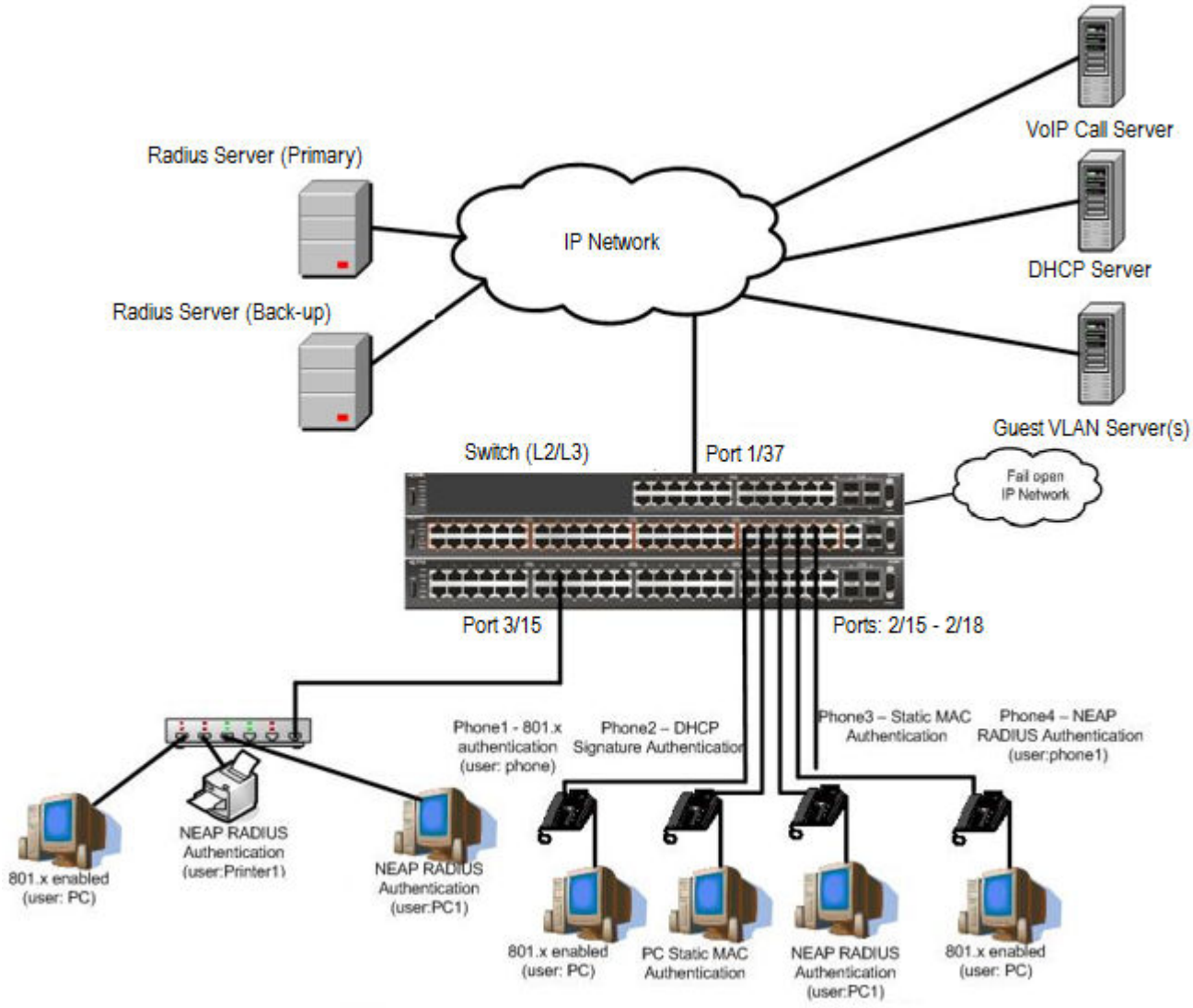


Figure 29: MHMA-MV authentication mode with Guest and Fail-Open VLANs with or without additional RADIUS attributes

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. Global FailOpen VLAN ID: 30
3. Configure all IP Phones to send tag traffic with proper VoIP VLAN ID.

4. 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

5. 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

```
Switch(config)#ip address 192.0.2.1 netmask 255.255.255.0 default-gateway 192.0.2.2
Switch(config)#radius server host 192.0.2.3
Switch(config)#radius server host 192.0.2.4 secondary
Switch(config)#radius server host key
Enter key: RadiusKey
Enter key: RadiusKey
Switch(config)#vlan configcontrol automatic
Switch(config)#vlan create 20 type port
Switch(config)#vlan create 30 type port
Switch(config)#vlan create 50 type port
Switch(config)#vlan create 200 type port
Switch(config)#vlan create 300 type port
Switch(config)#vlan members add 50 2/15-19,3/15
```

2. Confirm the VLAN interface settings.

```
Switch(config)#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 inteface VIDs.

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

```
Unit/Port  VLAN  VLAN Name  VLAN  VLAN Name  VLAN  VLAN Name
---------  ----  ---------  ----  ---------  ----  ---------
2/15       50    VLAN #50   ----  ------     ----  ------
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.

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

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

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

6. Confirm the VLAN interface settings.

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

```
          Filter     Filter
          Untagged   Unregistered
Unit/Port Frames     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 inteface VIDs.

```
Switch(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.

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

9. Confirm the VLAN interface settings.

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

```
          Filter     Filter
          Untagged   Unregistered
Unit/Port Frames     Frames       PVID       PRI      Tagging     Name
--------- ---------- ---------- ---------- ------ ------- -------

2/15      No         Yes        50         0        UntagPvid   Unit 2,
                                                     Only        Port 15
2/16      No         Yes        50         0        UntagPvid   Unit 2,
                                                     Only        Port 16
2/17      No         Yes        50         0        UntagPvid   Unit 2,
                                                     Only        Port 17
2/18      No         Yes        50         0        UntagPvid   Unit 2,
                                                     Only        Port 18
```

10. Confirm the VLAN inteface VIDs.

```
Switch(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).

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

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

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

```
           Filter     Filter
           Untagged   Unregistered
Unit/Port  Frames     Frames       PVID       PRI      Tagging    Name
--------   --------   --------     --------   ------   -------    -------

1/37       No         Yes          1          0        TagAll     Unit 1,
                                                                  Port 37
```

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

```
Switch(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 Extreme Networks recommends you verify RADIUS server logs for authentication request sent by device.

```
Switch(config)#ping 192.0.2.3
(Host is reachable)
Switch(config)#ping 192.0.2.4
(Host is reachable)
```

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

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

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

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

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

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

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

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

19. Set the EAPOL status for port 3/15.

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

20. Set the Guest and Fail-Open VLANs.

```
Switch(config)#eapol guest-vlan vid 20
Switch(config)#eapol guest-vlan enable
Switch(config)#eapol multihost fail-open-vlan vid 30
Switch(config)#eapol multihost fail-open-vlan enable
```

21. Set the EAPOL MultiHost status.

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

22. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 2/15-18,3/15
```

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

23. Confirm the VLAN interface VIDs.

```
Switch(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.

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

Before any clients authenticate on ports:

25. Confirm the VLAN interface settings.

```
Switch(config)#sho vlan interface info 2/15-18,3/15
```

```
          Filter     Filter
          Untagged   Unregistered
Unit/Port Frames     Frames       PVID       PRI      Tagging     Name
--------  --------   --------     --------   ------   -------     -------

2/15      No         Yes          20         0        UntagPvid   Unit 2,
                                                      Only        Port 15
2/16      No         Yes          20         0        UntagPvid   Unit 2,
                                                      Only        Port 16
2/17      No         Yes          20         0        UntagPvid   Unit 2,
                                                      Only        Port 17
2/18      No         Yes          20         0        UntagPvid   Unit 2,
                                                      Only        Port 18
3/15      No         Yes          20         0        UntagAll    Unit 3,
                                                                  Port 15
```

26. Confirm the VLAN interface VIDs.

```
Switch(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.

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

```
           Client
Unit/Port  MAC Address          State                  Vid        Pri
--------   --------             --------               -------    ------
2/16       00:19:E1:A2:4D:36    Authenticated          300        0
                                Locally
2/17       00:19:E1:E5:52:4A    Authenticated          50         0
                                Locally
2/17       00:AB:CD:02:00:20    Authenticated          300        0
                                By
                                RADIUS
2/18       00:19:E1:E2:40:46    Authenticated          50         0
                                By
                                RADIUS
3/15       00:AB:CD:01:00:20    Authenticated          300        0
                                By
                                RADIUS
3/15       00:AB:CD:01:00:21    Authenticated          300        0
                                By
                                RADIUS
Total number of authenticated clients:  6
```

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

```
                                          Backend
           Client                         Auth
Unit/Port  MAC Address          Pae State  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 MHSA mode with Guest VLAN, where Guest VLAN was available only until the first client was authenticated on the port.

28. Confirm the VLAN interface settings.

```
Switch(config)#show vlan interface info 2/15-18,3/15
```

```
          Filter     Filter
          Untagged   Unregistered
Unit/Port Frames     Frames       PVID       PRI     Tagging      Name
--------  --------   --------     --------   ------  -------      -------

2/15      No         Yes          20         0       UntagPvid    Unit 2,
                                                     Only         Port 15
2/16      No         Yes          20         0       UntagPvid    Unit 2,
                                                     Only         Port 16
2/17      No         Yes          20         0       UntagPvid    Unit 2,
                                                     Only         Port 17
2/18      No         Yes          20         0       UntagPvid    Unit 2,
                                                     Only         Port 18
3/15      No         Yes          20         0       UntagAll     Unit 3,
                                                                  Port 15
```

29. Confirm the VLAN interface VIDs.

```
Switch(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
           300       VLAN #300
2/16       20        VLAN #20   200       VLAN #200   300       VLAN #300
2/17       20        VLAN #20   50        VLAN #50    200       VLAN #200
           300       VLAN #300
2/18       20        VLAN #20   50        VLAN #50    200       VLAN #200
           300       VLAN #300
3/15       20        VLAN #20   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.

```
Switch(config)#ping 192.0.2.3
(Host is not reachable)

Switch(config)#ping 192.0.2.4
(Host is not reachable)
```

32. After around 3 minutes, verify the ports are copied in this VLAN and that new MACs send traffic in the FailOpen VLAN.

33. Connect both primary and secondary RADIUS servers back to the network.

34. After approximately 1 minute, attempt to reach the primary RADIUS server.

```
Switch(config)#ping 192.0.2.3
(Host is reachable)
```

35. Verify that the ports are no longer in Fail-Open VLAN and unauthenticated MACs send traffic in GuestVLAN.

Alternate configuration

The following operation applies to the **MHMA-MV authentication mode with Guest and Fail-Open VLANs 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.

```
Switch(config)#eapol disable
Switch(config)#eapol enable
```

2. Confirm EAPOL MultiHost status.

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

```
           Client
Unit/Port  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
```

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

```
                                          Backend
           Client                         Auth
Unit/Port  MAC Address          Pae State  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.

```
Switch(config)#show vlan interface info 2/15-18,3/15
```

```
          Filter     Filter
          Untagged   Unregistered
Unit/Port Frames     Frames       PVID       PRI        Tagging     Name
--------- --------   --------     --------   --------   --------    -------
2/15      No         Yes          20         0          UntagPvid   Unit 2,
                                                        Only        Port 15
2/16      No         Yes          20         0          UntagPvid   Unit 2,
                                                        Only        Port 16
2/17      No         Yes          20         0          UntagPvid   Unit 2,
                                                        Only        Port 17
2/18      No         Yes          20         0          UntagPvid   Unit 2,
                                                        Only        Port 18
3/15      No         Yes          20         0          UntagAll    Unit 3,
                                                                    Port 15
```

4. Confirm the VLAN interface VIDs.

```
Switch(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    --------  -------
```

5. Disconnect both primary and back-up RADIUS servers from the network (unplug cables from server side).

6. Attempt to reach the primary and back-up RADIUS servers.

```
Switch(config)#ping 192.0.2.3
(Host is not reachable)

Switch(config)#ping 192.0.2.4
(Host is not reachable)
```

7. After around 3 minutes, verify the ports are copied in this VLAN and that new MACs send traffic in the FailOpen VLAN.

8. Connect both primary and secondary RADIUS servers back to the network.

9. After approximately 1 minute, attempt to reach the primary RADIUS server.

```
Switch(config)#ping 192.0.2.3
(Host is reachable)
```

10. Verify that the ports are no longer in Fail-Open VLAN and unauthenticated MACs send traffic in GuestVLAN.

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 an 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.

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

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

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

3. Verify the MAC security configuration for the interfaces.

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

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.

```
Switch#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 an individual port:

(Port 1/6 is used for this example.)

1. Enable MAC security and auto-learning globally.

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

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

3. Verify the configuration by displaying the MAC security MAC address table.

```
Switch#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
--------                    --------                   -------
```

First Hop Security using example scenario

This appendix provides a configuration example for the overall deployment of the First Hop Security (FHS) feature.

FHS deployment scenario

In this example, consider there are four users (PC1, PC2, PC3, and PC4). a DHCP server, and an RA or DHCPv6-server Enabled Router connected to the FHS-enabled switch.

The following is the expected behavior:

- RA Enabled Router–Assigns IP subnet for PC1 user
- DHCPv6 Enabled Router–Assigns IP subnet for PC2 user
- DHCPv6-server–Assigns IP subnet for PC3 and PC4

The FHS-enabled switch can only protect the first hop host or network elements which are directly connected. In this scenario, the FHS-enabled switch can protect the hosts PC1, PC2, PC3, and PC4 from the host RTR-PC1 attack. On the other hand, this switch cannot protect the router from the attack caused by the host RTR-PC1. Similarly, an FHS-enabled switch can protect PC1, PC2, PC3, DHCPv6-server and the router from the host PC4 attack.

The following figure shows the FHS deployment scenario topology.

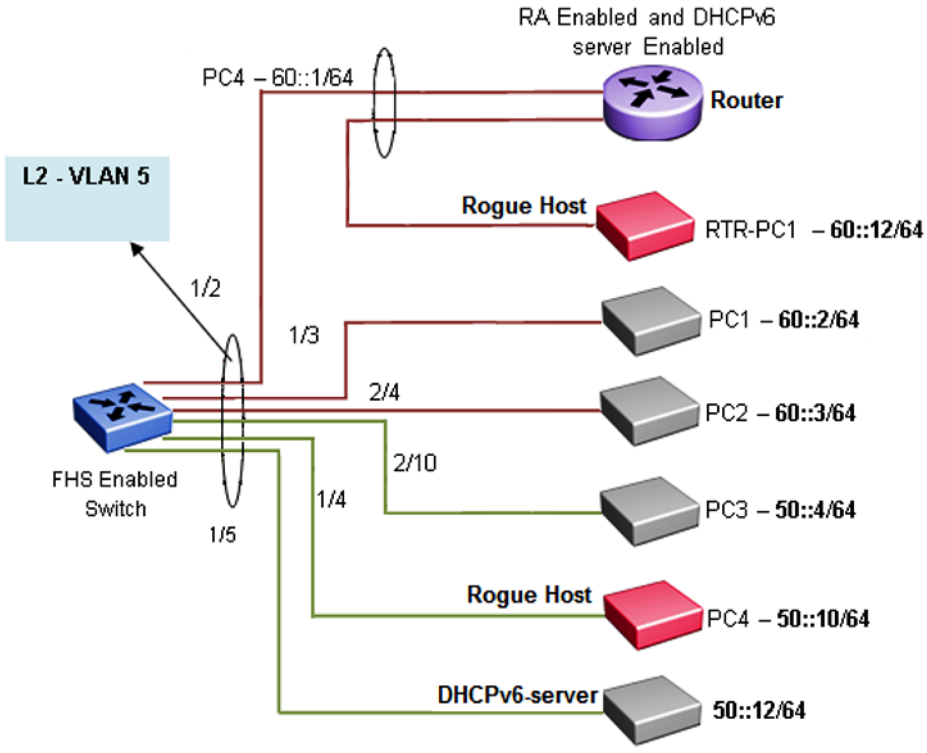


Figure 30: FHS deployment topology

By default, all the ports are trusted, until DHCP-guard or RA-guard policies are configured.

See the following procedures for configuring FHS RA-guard and DHCPv6-guard for the preceding topology.

Creating FHS IPv6 ACL

About this task

Filter IPv6 traffic by creating IPv6 Access Control Lists (ACLs) and applying them to the interfaces similar to the way that you create and apply IPv4 named ACLs.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create an IP ACL name (rtr_sip) to match the source IP address of the router connected to the interface 1/2.

   ```
   ipv6 fhs ipv6-access-list rtr_sip 60::1/128 mode allow
   ```

3. Create an IP ACL name (rtr_pip) to match the IP prefix generated by the router connected to the interface 1/2.

   ```
   ipv6 fhs ipv6-access-list rtr_pip 60::0/64 mode allow
   ```

4. Create an IP ACL name (svr_sip) to match the source IP of the DHCPv6-server connected to the interface 1/5.

   ```
   ipv6 fhs ipv6-access-list svr_sip 50::12/128 mode allow
   ```

5. Create an IP ACL name (svr_rip) to match the prefix generated by the DHCPv6-server connected to the interface 1/5.

   ```
   ipv6 fhs ipv6-access-list svr_rip 50::12/128 mode allow
   ```

Next steps

Create FHS MAC ACL.

Creating FHS MAC ACL

About this task

Filter the IPv6 traffic by creating a MAC access list with the ACL mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create an MAC ACL name (rtr_smac) to match the source MAC of router connected to the interface 1/2.

   ```
   ipv6 fhs ipv6-access-list rtr_smac 1:2:3:4:5:6 mode allow
   ```

Creating DHCPv6-guard policy for the Router

About this task

Create a DHCPv6–guard policy for the Router to provide Layer 2 security to DHCPv6 clients by protecting them against rogue DHCPv6 servers.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter DHCP Guard mode with the DHCP-guard policy name (rtr_dhcpg). The DHCP-guard policy for the interface is connected to a Router.

```
ipv6 dhcp guard policy rtr_dhcpg
```

3. Determine the device role as server so that this policy allows the DHCPv6 server reply message.

   ```
   device-role server
   ```

4. Configure the source IP access list to allow only a DHCPv6 server reply originating from the IP address 60::1/128 and check the preceding IPv6 ACL configuration for rtr_sip list.

   ```
   match server access-list rtr_sip
   ```

5. Verify the prefixes sent in the DHCPv6 server reply message so that the rtr_pip IPv6 ACL configuration allows only the prefix 60::0/64.

   ```
   match reply prefix-list rtr_pip
   ```

Creating DHPv6-guard policy for the DHCPv6-Server attached to the switch

About this task

Configure a DHCP-guard policy for the interface connected to a DHCPv6-server to verify the prefixes sent in the DHCPv6 server reply message.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the DHCP Guard mode using the DHCP-guard policy name (svr_dhcpg).

   ```
   ipv6 dhcp guard policy svr_dhcpg
   ```

3. Determine the device role as server so that this policy allows the DHCPv6 server reply message.

   ```
   device-role server
   ```

4. Configure the source IP access list to allow only DHCPv6 server reply originating from the IP address 50::12/128 by checking the preceding IPv6 ACL configuration for svr_sip list.

   ```
   match server access-list svr_sip
   ```

5. Verify the prefixes sent in the DHCPv6 server reply message so that svr_rip IPv6 ACL configuration allows only the prefix 50::0/64.

   ```
   match reply prefix-list svr_rip
   ```

Creating DHPv6-guard host policy for PC1, PC2, PC3, and PC4 attached to the switch

About this task

Create a DHPv6-guard host policy for PC1, PC2, PC3, and PC4 attached to the switch to determine PC1, PC2, PC3, and PC4 as host.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the DHCP Guard mode using the DHCP-guard policy name (host_dhcpg).

   ```
   ipv6 dhcp guard policy host_dhcpg
   ```

   Note:

   In this case, the DHCP-guard policy is configured for the interface connected to a PC1, PC2, PC3, and PC4.

3. Determine the device role as host so that this policy does not allow the DHCPv6 server reply message.

   ```
   device-role host
   ```

Creating RA-guard policy for the Router

About this task

Create an **rtr_rag** RA-guard policy for the Router and configure the source IP access list to allow only the RA packets originating from the source IP address **60::1/128**. This configuration verifies the prefixes sent in the RA packets.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the RA Guard mode and configure RA-guard policy (rtr_rag) for the interface connected to a Router.

   ```
   ipv6 nd raguard policy rtr_rag
   ```

3. Determine the device role as router so that this policy allows the RA packets from the ingress interface on which the policy is attached.

```
device-role router
```

4. Configure the source IP access list to allow only RA packets originating from the source IP address 60::1/128 and check the preceding IPv6 ACL configuration for rtr_sip list.

   ```
   match ipv6 access-list rtr_sip
   ```

5. Verify the prefixes sent in the RA packets so that the rtr_pip IPv6 ACL configuration allows only the prefix 60::0/64.

   ```
   match reply prefix-list rtr_pip
   ```

6. Verify the source MAC address of the received RA packet. Depending on the rtr_smac MAC access list configuration, the packet is allowed or denied.

   ```
   match mac-access-list rtr_smac
   ```

Creating RA-guard policy for the non-RA hosts

About this task

Create a **host_rag** RA-guard policy for the interface connected to PC1, PC2, PC3, PC4 and DHCPv6-Server. This policy determines the device role as router and allows RA packets from the ingress interface on which the policy is attached.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter RA Guard mode and configure the RA-guard policy name (host_rag) for the interface connected to PC1, PC2, PC3, PC4 and DHCPv6-Server.

   ```
   ipv6 nd raguard policy host_rag
   ```

3. Determine the device role as router so that this policy allows the RA packets from the ingress interface on which the policy is attached.

   ```
   device-role host
   ```

Attaching FHS policies to the interfaces

About this task

Attach the FHS policies to the interfaces.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Configure DHCP-guard and RA-guard policy on the interface (1/2) connected to the Router.

```
interface ethernet 1/2
ipv6 dhcp guard attach-policy rtr_dhcpg
ipv6 nd raguard attach-policy rtr_rag
```

3. Configure DHCP-guard and RA policy on the interface (1/5) connected to DHCPv6-Server.

```
interface ethernet 1/5
ipv6 dhcp guard attach-policy svr_dhcpg
ipv6 nd raguard attach-policy host_rag
```

4. Configure DHCP-guard and RA policy on the interface (1/3,2/4,2/10,1/4) connected to PC1, PC2, PC3, and PC4 correspondingly.

```
interface ethernet 1/3,1/4,2/4,2/10
ipv6 dhcp guard attach-policy host_dhcpg
ipv6 nd raguard attach-policy host_rag
```

Enabling ND-inspection on the interfaces with IPv6 address assigned by DHCPv6 server attached to the interface 1/5

About this task

Enable ND-inspection on the interfaces 1/3,1/4, 2/4, 2/10 with IPv6 address assigned by DHCPv6 server attached to the interface 1/5.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable IPv6 admin status.

```
ipv6 enable
```

3. Enable FHS globally.

```
ipv6 fhs enable
```

4. Enable ND inspection on the port 1/3, 1/4, 2/4, and 2/10.

```
interface ethernet 1/3,1/4,2/4,2/10
ipv6 nd inspection
```

5. Enable DHCP-guard policy on the port connected to the DHCPv6 server which assigns the IP address for the preceding ports. This ensures that the DHCP assigned IP address is taken into account while inspecting the ND packet.

```
interface fa 1/5

ipv6 dhcp guard attach-policy svr_dhcpg
```

RADIUS and SYSLOG server configuration examples for Enhanced Secure Mode

This section contains the following examples, which are applicable when enhanced secure mode is enabled:

- Radius switch and server configuration examples
- Syslog switch and server configuration examples
- Syslog messaging via RFC 3195

Configuration example: RADIUS configuration

Configuring the switch for RADIUS authentication

Use the following commands to configure the switch for RADIUS authentication.

1. Configure the RADIUS server IP address and shared secret.

```
Switch(config)#radius server host 192.0.2.1 key
Enter key:
```

2. Verify the RADIUS configuration.

```
Switch:#show radius-server

RADIUS Global Server
----------------------------------------------------------------
Primary Host           : 192.0.2.1
Secondary Host         : 0.0.0.0
Port                   : 1812
Time-out               : 10
Key                    : ***************
Radius Accounting      : Disabled
Radius Accounting Port : 1813
Radius Retry Limit     : 3
Current Status         : Reachable via Primary
Time Until Next Check  : 169

RADIUS EAP Server
----------------------------------------------------------------
Primary Host           : 0.0.0.0
Secondary Host         : 0.0.0.0
Port                   : 1812
Time-out               : 10
Key                    : ***************
Radius Accounting      : Disabled
```

```
Radius Accounting Port : 1813
Radius Retry Limit     : 3
Current Status         : None Reachable
Time Until Next Check  : 169

RADIUS Non-EAP Server
------------------------------------------------------------
Primary Host           : 0.0.0.0
Secondary Host         : 0.0.0.0
Port                   : 1812
Time-out               : 10
Key                    : ***************
Radius Accounting      : Disabled
Radius Accounting Port : 1813
Radius Retry Limit     : 3
Current Status         : None Reachable
Time Until Next Check  : 169

Other Settings
------------------------------------------------------------
Password Fallback      : Enabled
RADIUS Encapsulation   : PAP
```

3. Set the authentication method.

   By default the authentication method is set to local database – roles based access control (RBAC). You can also change the authentication method to remote authentication using a RADIUS server.

```
Switch:(config)#show cli password type

Console Password Type: Local Password
Telnet/WEB Password Type: Local Password

Switch:(config)#cli password serial radius
Switch:(config)#cli password telnet radius
```

4. Verify the configuration.

```
Switch:(config)#show cli password type

Console Password Type: RADIUS Authentication
Telnet/WEB Password Type: RADIUS Authentication
```

Configuring user account details – FreeRadius server on a UNIX machine

Use the following steps to modify the following configuration files to define the user account.

- clients.conf file for defining allowed client IP addresses and Radius shared secret.
- users file for defining the user accounts allowed to access the switch.

After defining the user accounts, only the authenticated user can connect to the network after the Network Authentication Server (NAS) validates the credentials.

1. Login as root on the UNIX machine.
2. Access Radius configuration files.

   By default, the configuration files are located at `/usr/local/etc/raddb` folder.
3. Edit clients.conf file to define client entries for a particular client IP or clients IP range.

Following is example. In this example, the client range is *ags1*, permitted IP address clients range is *192.0.2.1/16* subnet, and shared secret key is *bayproject*.

```
client ags1 {
ipaddr = 192.0.2.1
netmask = 16
secret = bayproject
shortname = ags1
}
```

4. Edit users file to define the user account entries that are allowed to access the switch.

   In the following example, the server is configured to allow security administrator, system administrator or application administrator.

```
appl_adm Auth-Type := Local, Cleartext-password := "MY!#xaxao_104274982"
Service-Type = Administrative-User,
Reply-Message := "Welcome appl_adm!",
NAS-Filter-Rule = 1
security_adm Auth-Type := Local, Cleartext-password := "MY!#xexez_104274982"
Service-Type = Administrative-User,
Reply-Message := "Welcome security_adm!",
NAS-Filter-Rule = 2
```

   Note:

   The NAS-Filter-Rule parameter is value 1 for application administrator role, value 2 for security administrator role or value 4 for system administrator.

5. Start the NAS server after completing the configuration changes to the FreeRadius server.

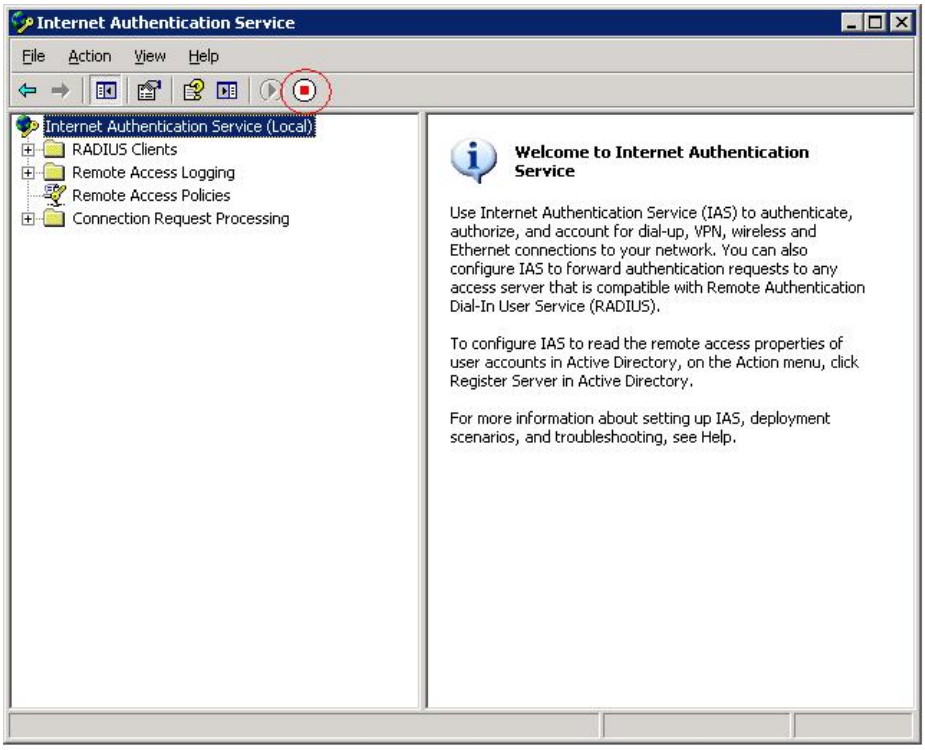
   `radiusd –X`

   As each user logs in, debugging traces can be inspected on the command screen.

Configuring RADIUS server running Windows Server 2003

Use the following steps to configure a RADIUS server running Windows 2003 Server.

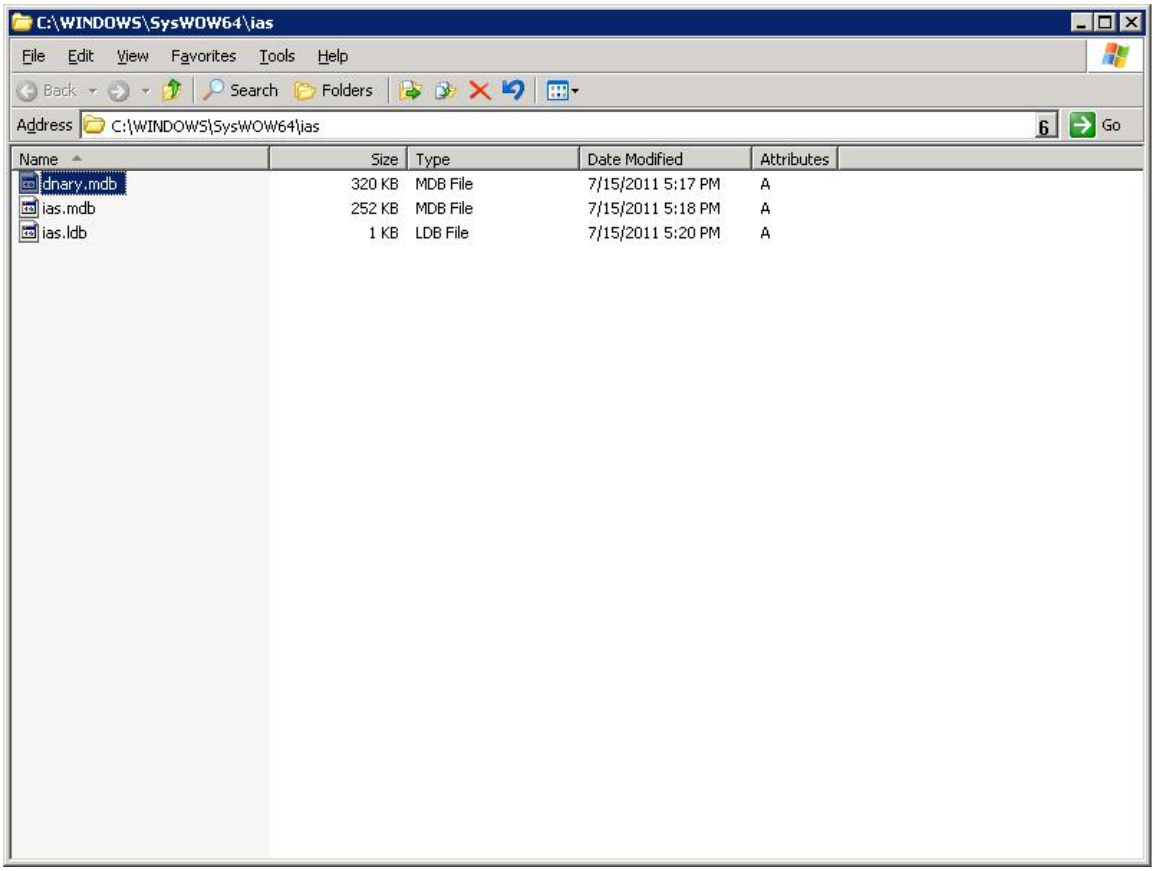
1. Go to **Start** > **Control Panel** > **Administrative Tools** > **Internet Authentication Service** and select **Internet Authentication Service (Local)**.
2. Click Stop button to stop the Internet Authentication Service.



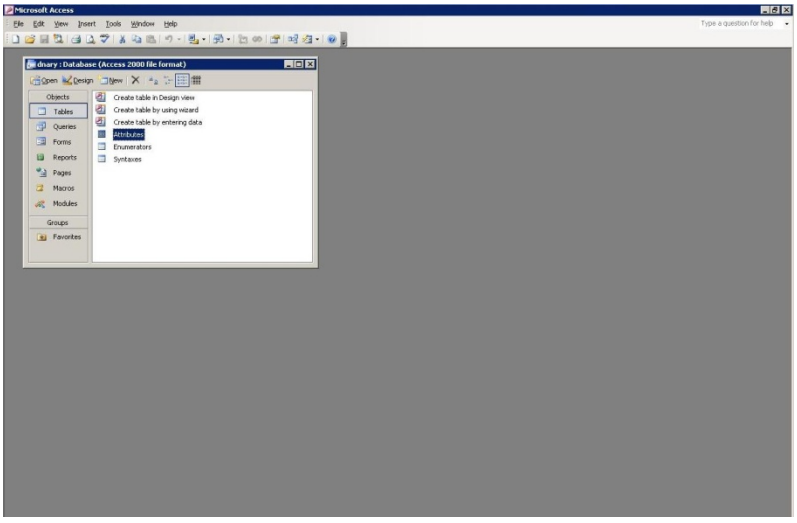
3. Go to location `C:\WINDOWS\SysWOW64\ias` and open dnary.mdb using Microsoft Access.

Note:

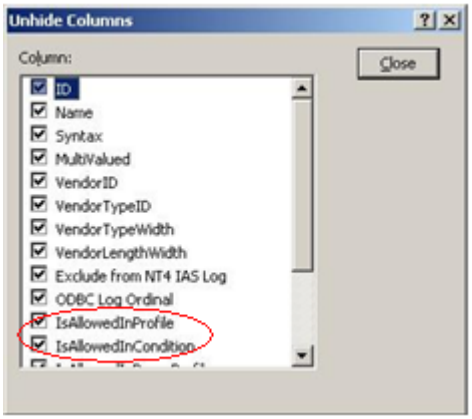
This folder location can be different.



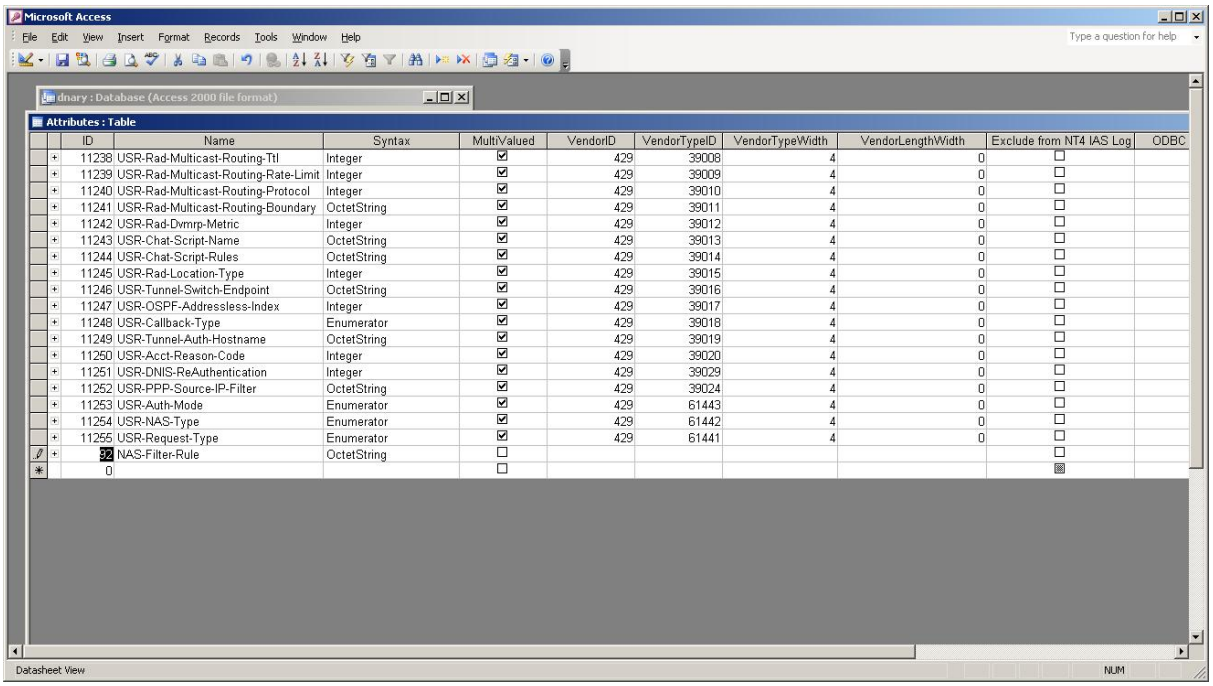
4. From the navigation tree, select **Tables** > **Attributes**.



5. Select **Format** > **Unhide columns**.
6. Select **IsAllowedInProfile** and **IsAllowedInCondition**.

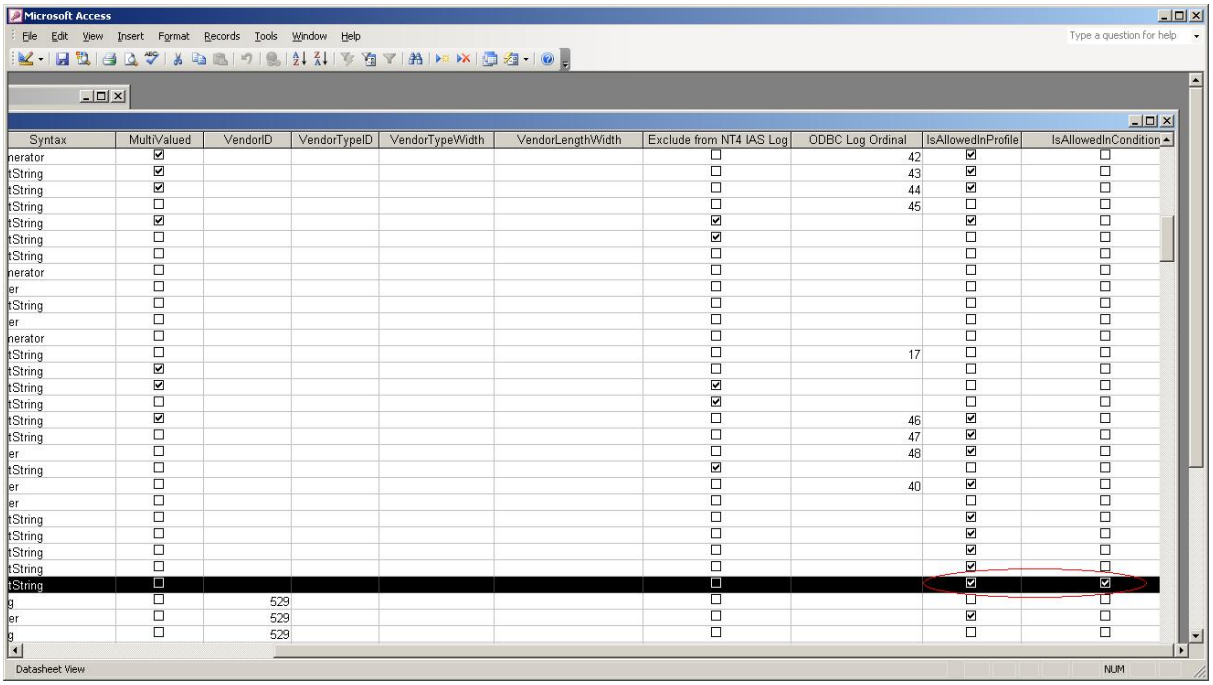


7. Click Insert and New Record and enter `92` in the ID column and `NAS-Filter-Rule` in the Name column.

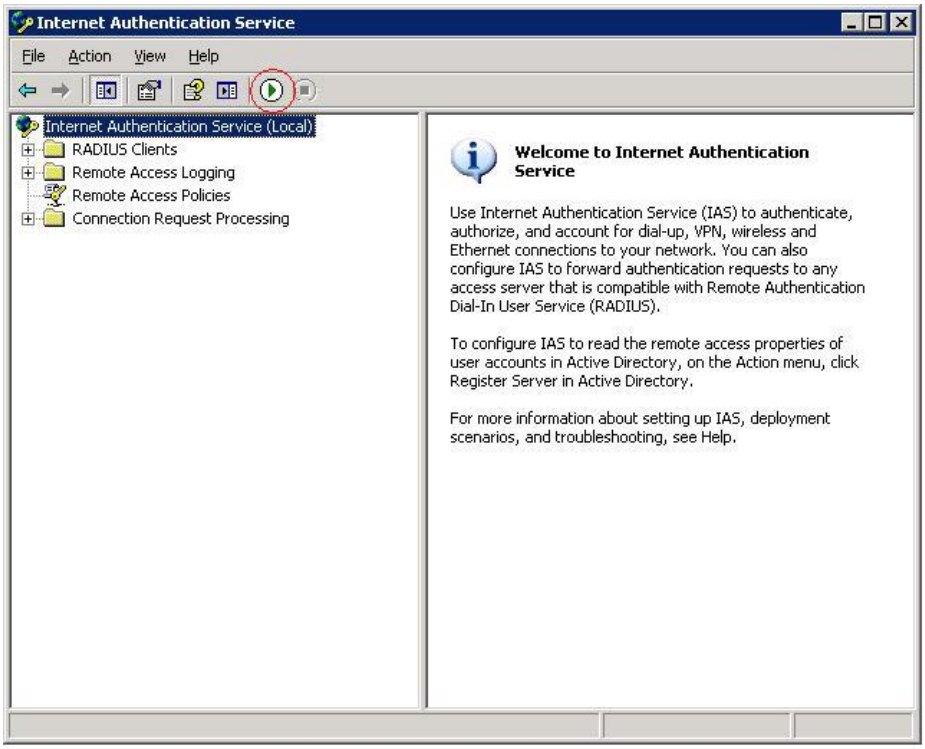


8. Select the two options.

   In the following example, IsAllowedInProfile and IsAllowedInCondition are selected.



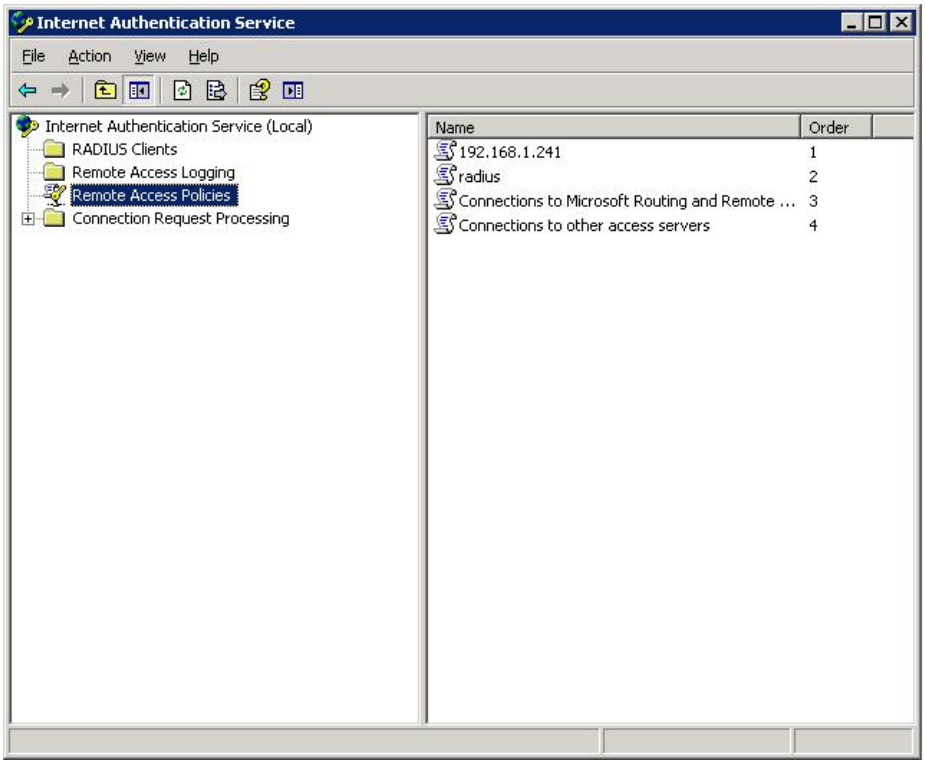
9. Save and close the database.
10. Click the Start button to start the Internet Authentication Service.



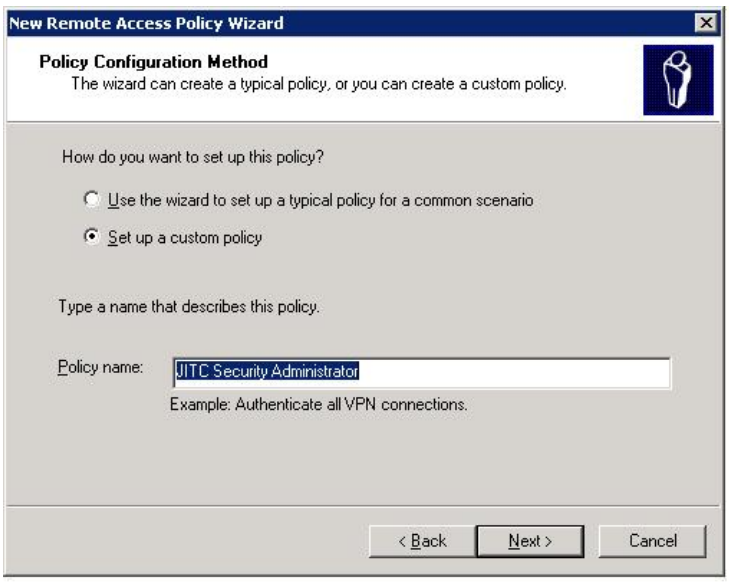
11. Restart the server.

Defining the RADIUS access policy using the NAS-Filter rule attribute on Windows 2003 Server

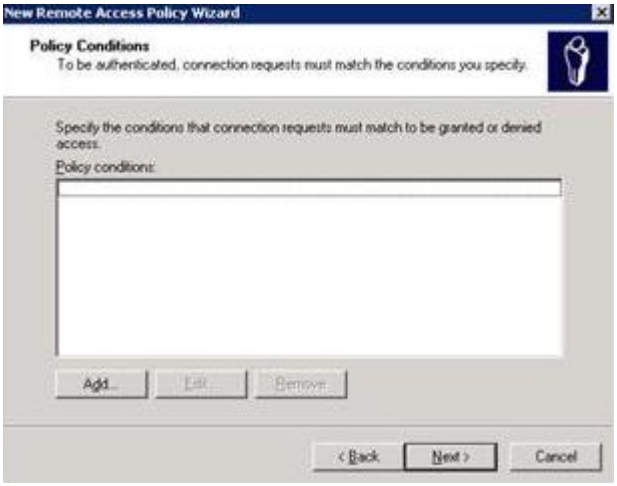
1. Go to **Start** > **Control Panel** > **Administrative Tools** > **Internet Authentication Service**.
2. Select **Remote Access Policies** and right-click to select **New Remote Access Policy**.



3. Select **Set up a custom policy** and in the Policy Name field, enter a name.

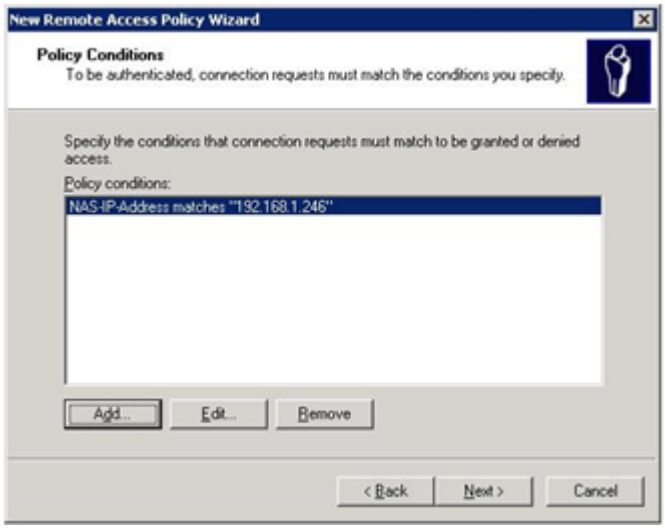


4. Click **Next**.
5. Click **Add.**

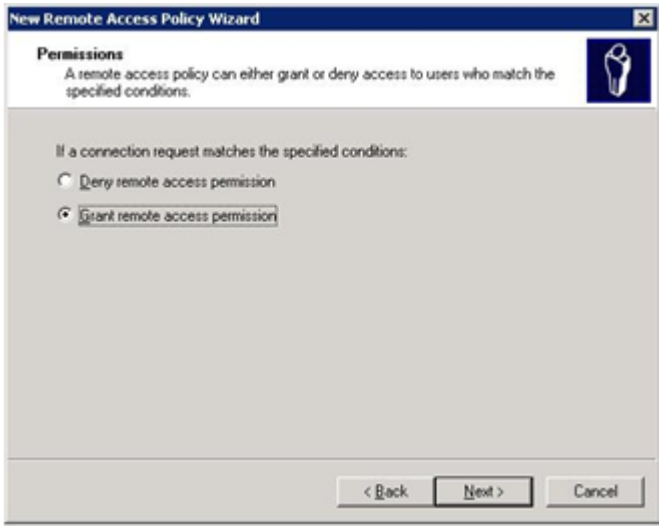


6. Select NAS-IP-Address and click **Add**.

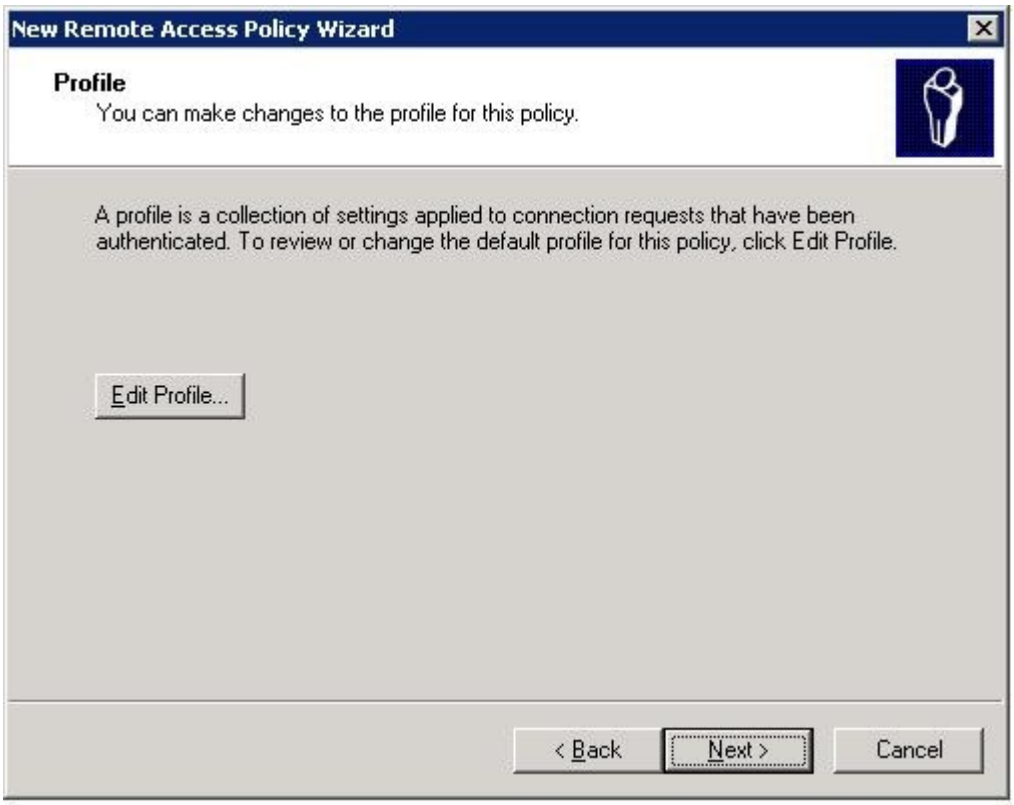
7. Configure the NAS IP address and click **Next**.



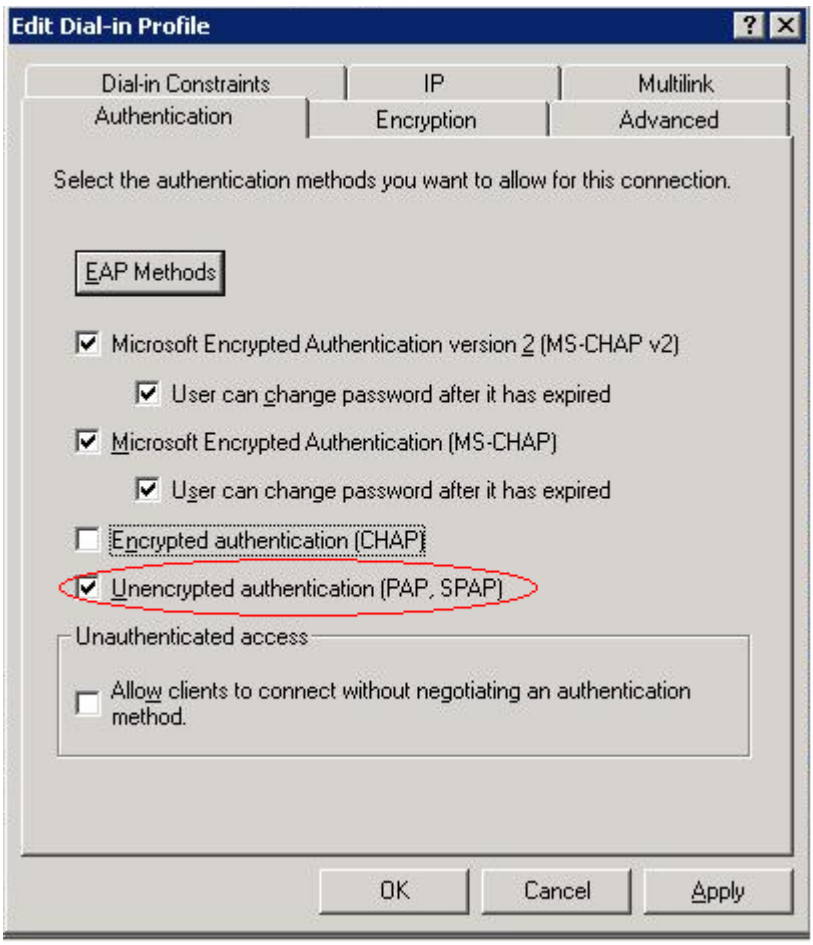
8. Select **Grant remote access permission** and click **Next**.



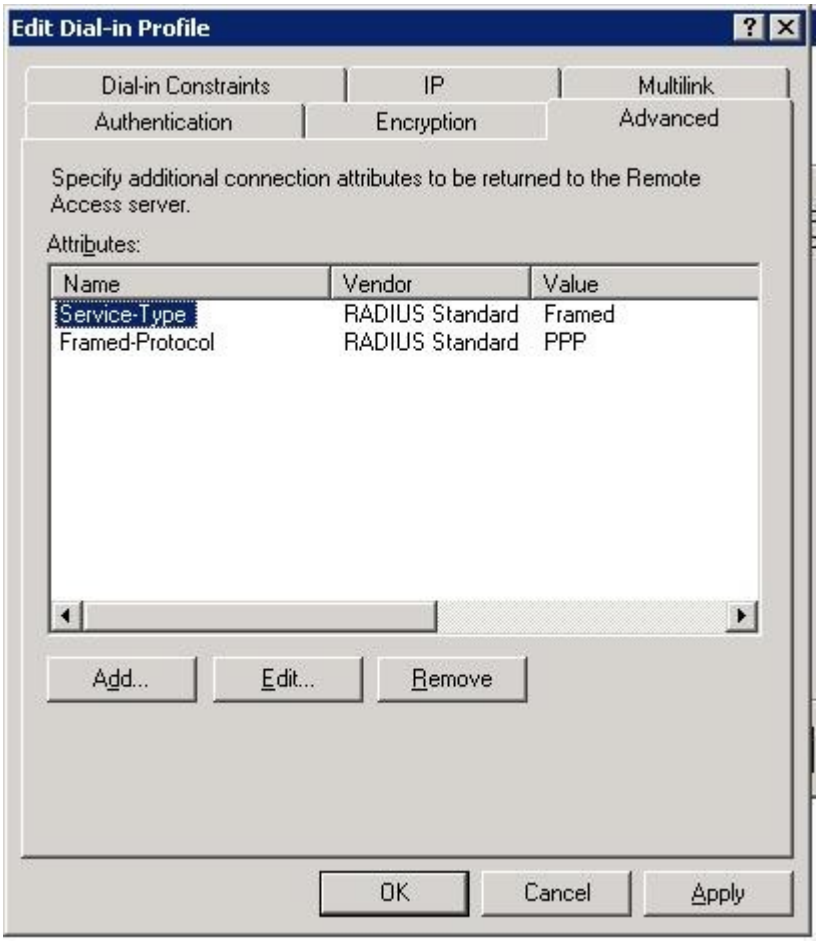
9. Click **Edit Profile**.



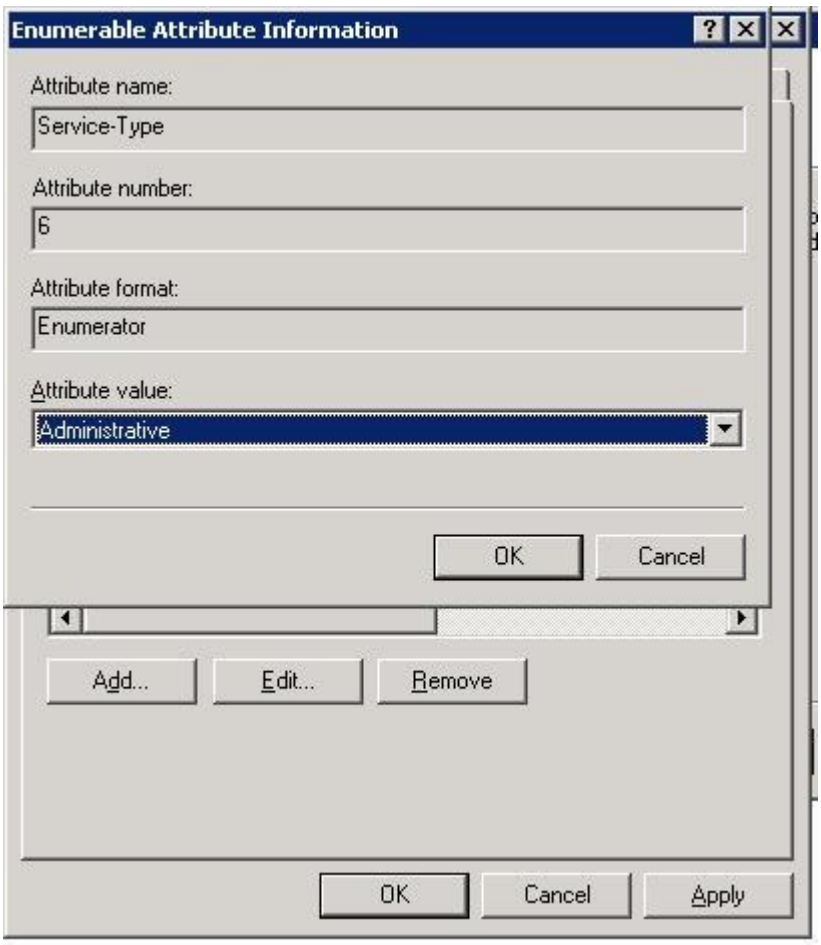
10. Select **Authentication** tab and then, select **Unencrypted authentication (PAP, SPAP)**.



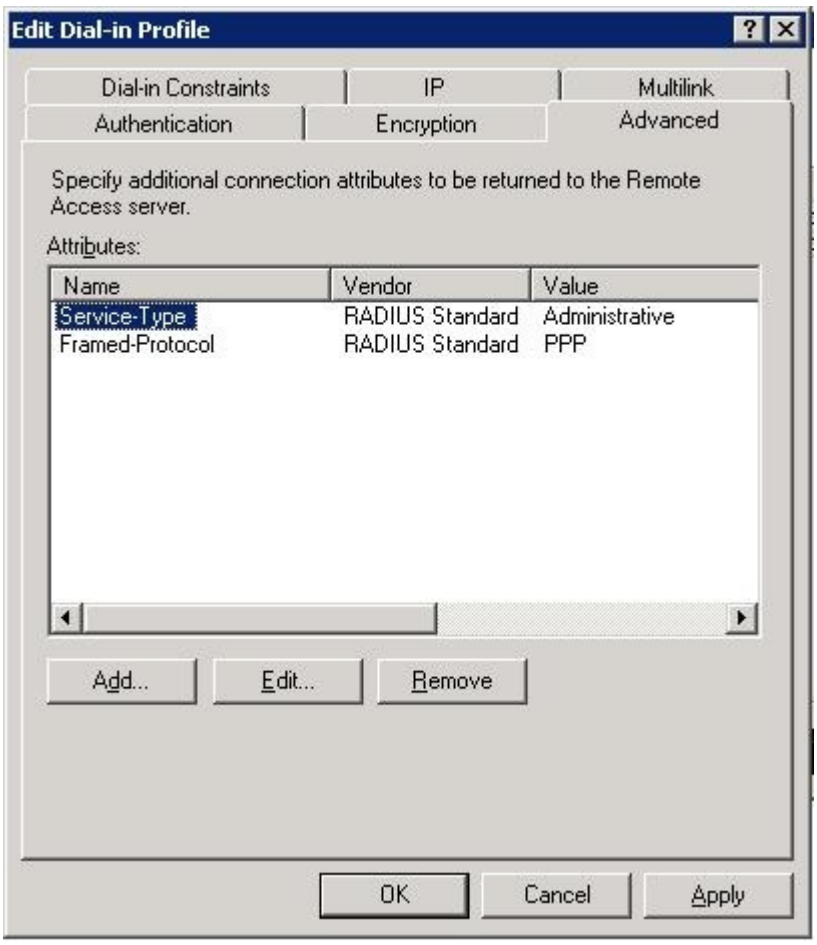
11. Select **Advanced** tab and then, double-click **Service-Type**.



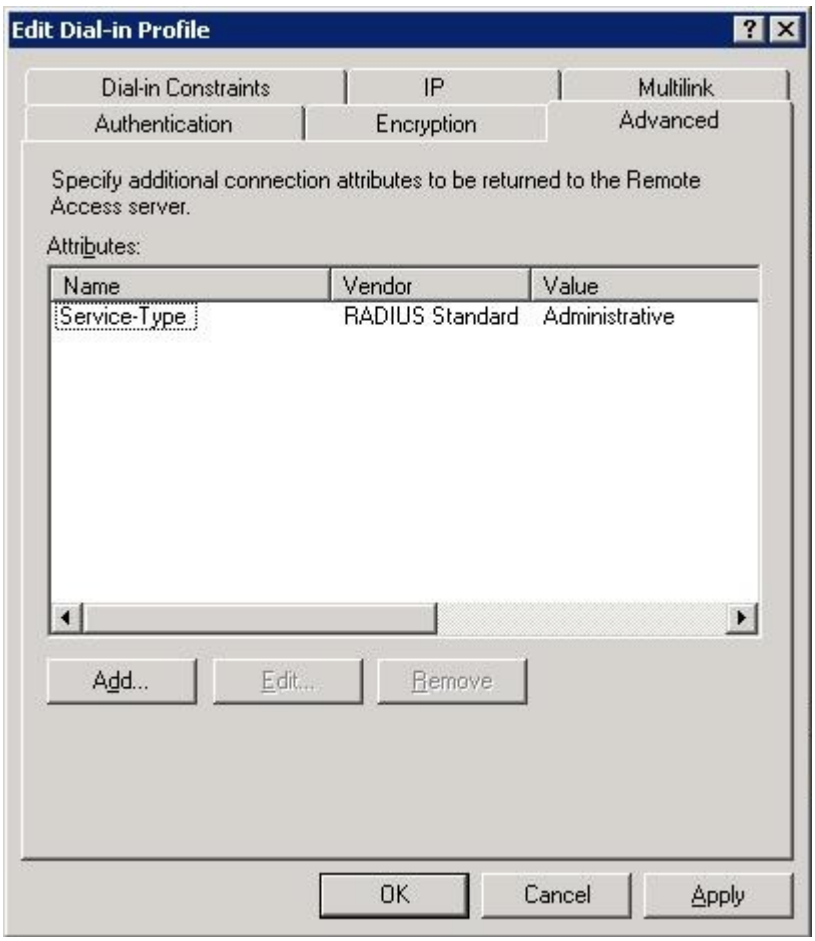
12. From the Attribute value drop-down, select Administrative.



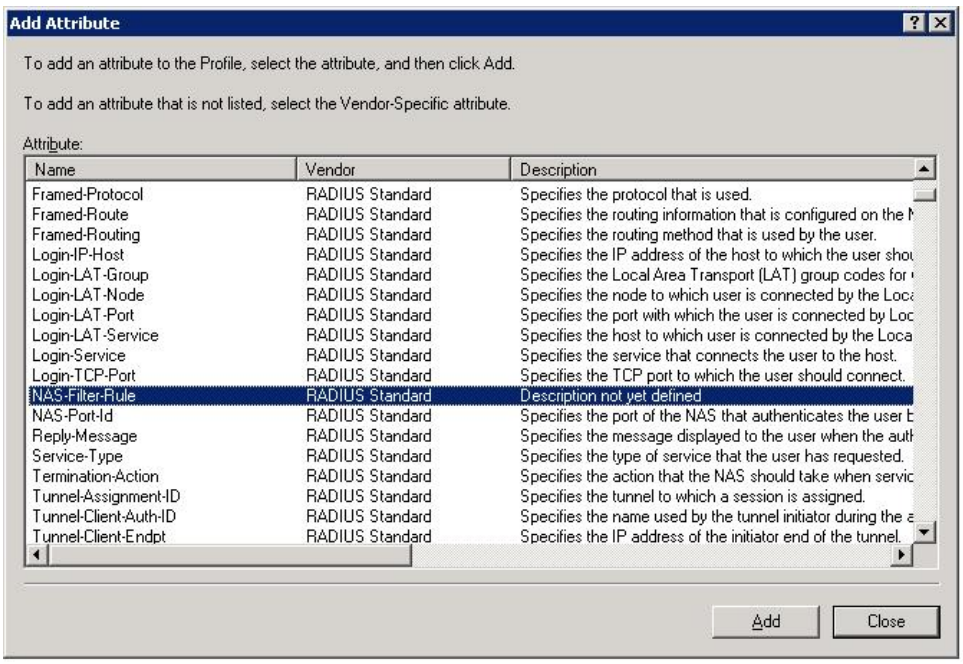
13. The Service-Type value is Administrative.



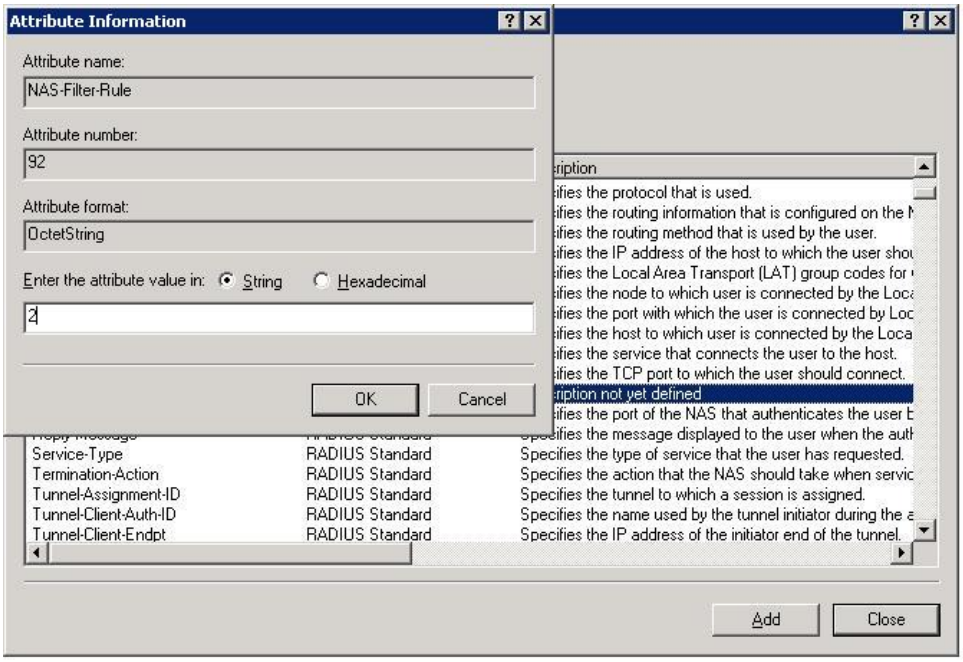
14. Remove the Framed-Protocol attribute.



15. Click **Add** and select NAS-Filter-Rule.



16. Click **Add**.
17. In the Enter the Attribute value field, select **String** and enter the value `2`.



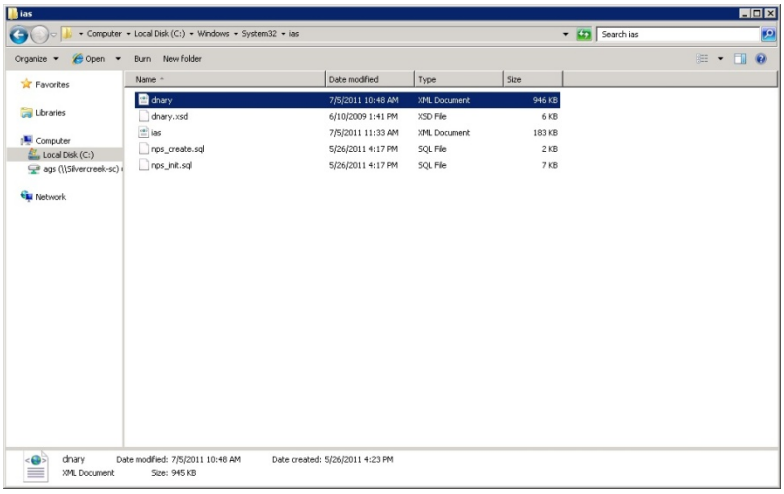
The access level used in this example is 2 to authenticate the Security-administrator. Repeat this procedure to add different access levels. The NAS-Filter Rule attribute is used to define a desired security access level based on RBAC implementation. The levels are:

- Application administrator NAS-Filter-Rule = 1
- System administrator NAS-Filter-Rule = 4
- Security administrator NAS-Filter-Rule = 2

Configuring RADIUS authentication on Windows 2008 Server

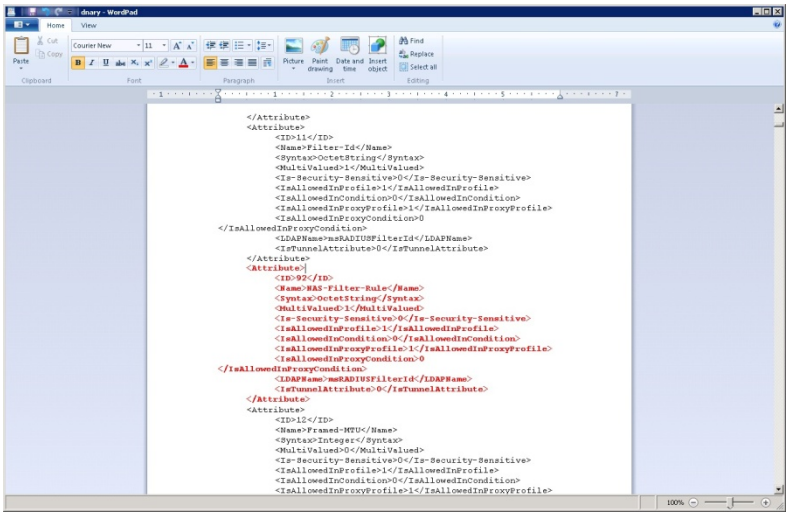
Use the following steps to define the attribute needed for RADIUS authentication on a Windows 2008 Server

1. Go to **Start** > **Computer** > **Windows** > **System32** > **ias**.



2. Open the file dnary.xml and insert the following between Attribute 11 and 12:

```
<Attribute>
        <ID>92</ID>
        <Name>NAS-Filter-Rule</Name>
        <Syntax>OctetString</Syntax>
        <MultiValued>1</MultiValued>
        <Is-Security-Sensitive>0</Is-Security-Sensitive>
        <IsAllowedInProfile>1</IsAllowedInProfile>
        <IsAllowedInCondition>0</IsAllowedInCondition>
        <IsAllowedInProxyProfile>1</IsAllowedInProxyProfile>
        <IsAllowedInProxyCondition>0</IsAllowedInProxyCondition>
        <LDAPName>msRADIUSNASFilterRule</LDAPName>
        <IsTunnelAttribute>0</IsTunnelAttribute>
    </Attribute>
```



3. Save the file and reboot Windows 2008 Server.

Configuring RADIUS server and RADIUS IETF new attribute information

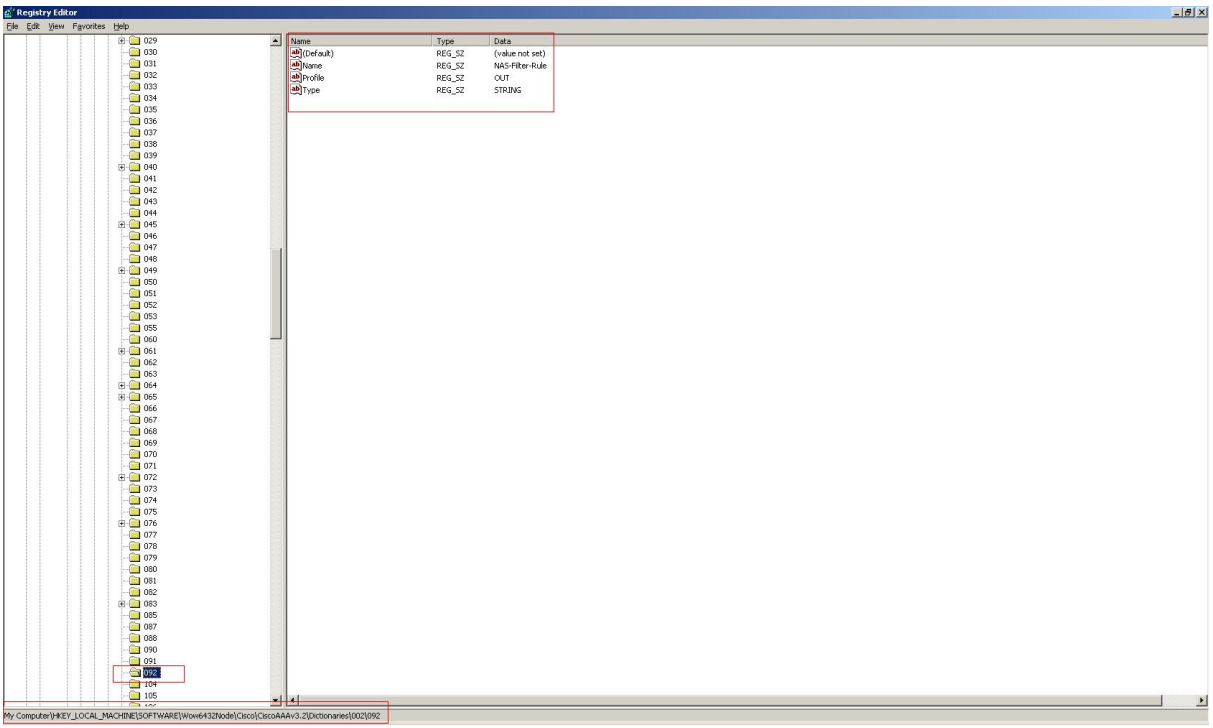
Use the following steps to configure RADIUS on Windows 2008 using Cisco Server ACS.

1. Using Windows Registry editor, add the type 092 attribute to the RADIUS IETF attributes list used by CiscoSecure ACS:
   a. Open Windows Registry editor using regedit run command.
   b. Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\CiscoAAAv3.2\Dictionaries\002 .`

      Note:

      Key location depends on the Windows version in use or CiscoSecure ACS version.

   c. Create a new key named 092 corresponding to the attribute value.
   d. For the newly created key, assign the following values:
      - Name: NAS-Filter-Rule
      - Type: STRINGProfile: OUT

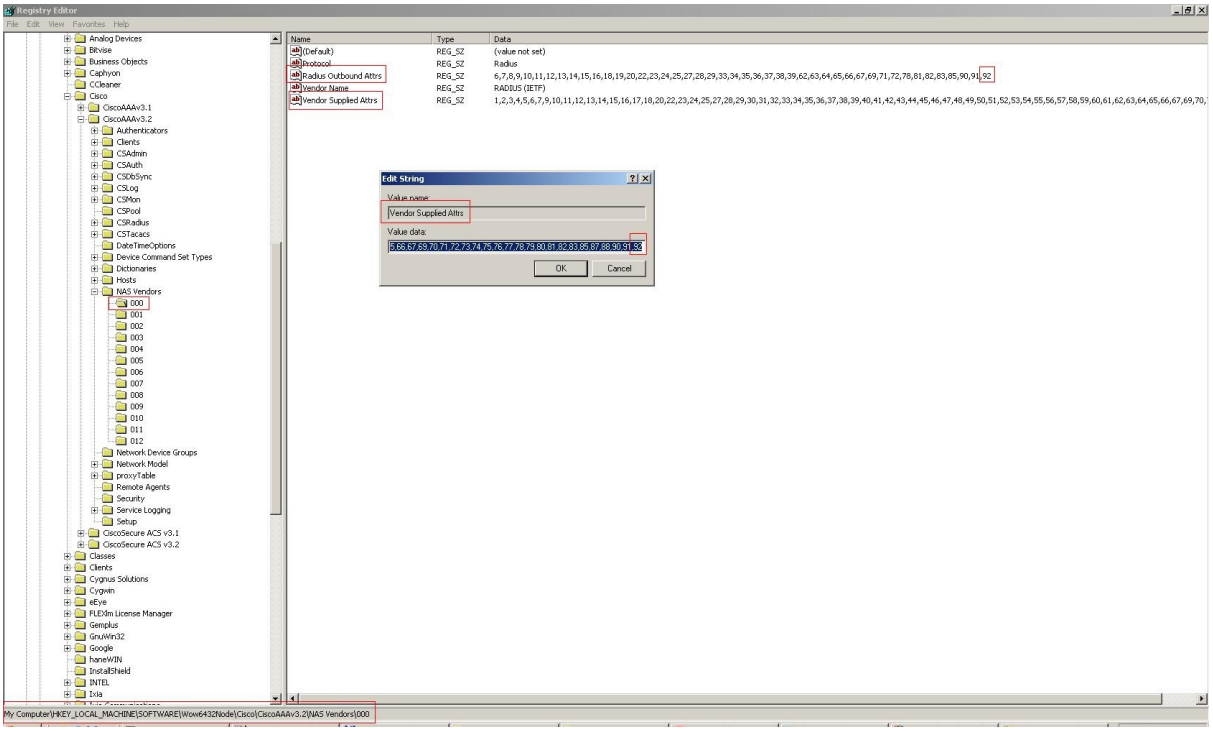


2. Using Windows Registry editor, make the newly added attribute available to the CiscoSecure ACS configuration interface:
   a. Open Windows Registry editor using regedit run command.
   b. Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\CiscoAAAv3.2\NAS Vendors\000`

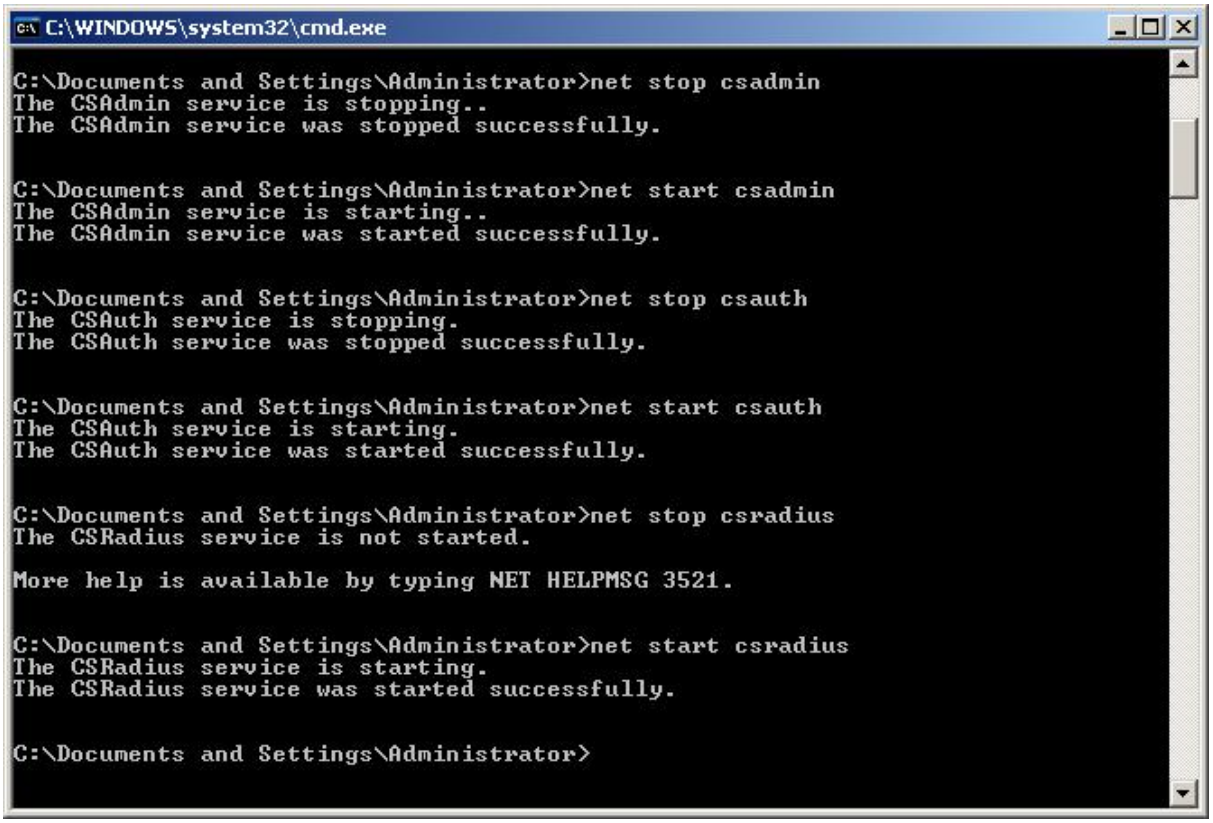
      Note:

      Key location depends on the Windows version in use or CiscoSecure ACS version.

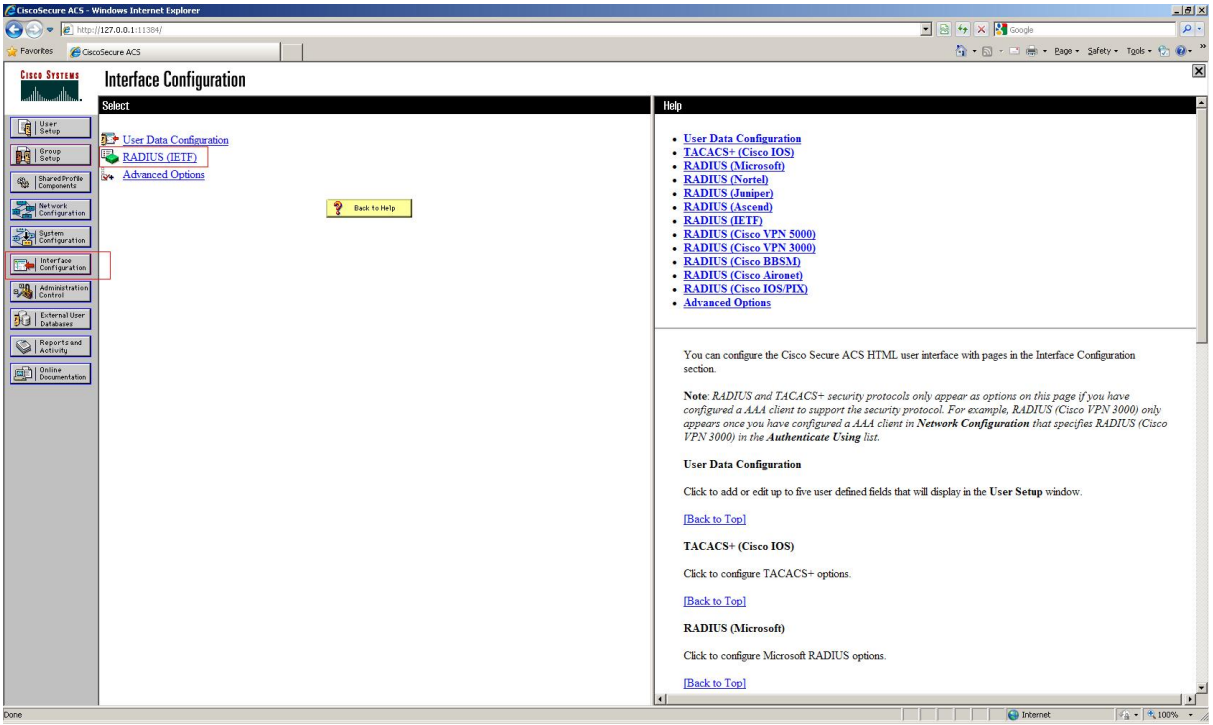
   c. In the Radius Outbound Attrs list and Vendor Supplied Attrs list make sure value 92 is added at the end.



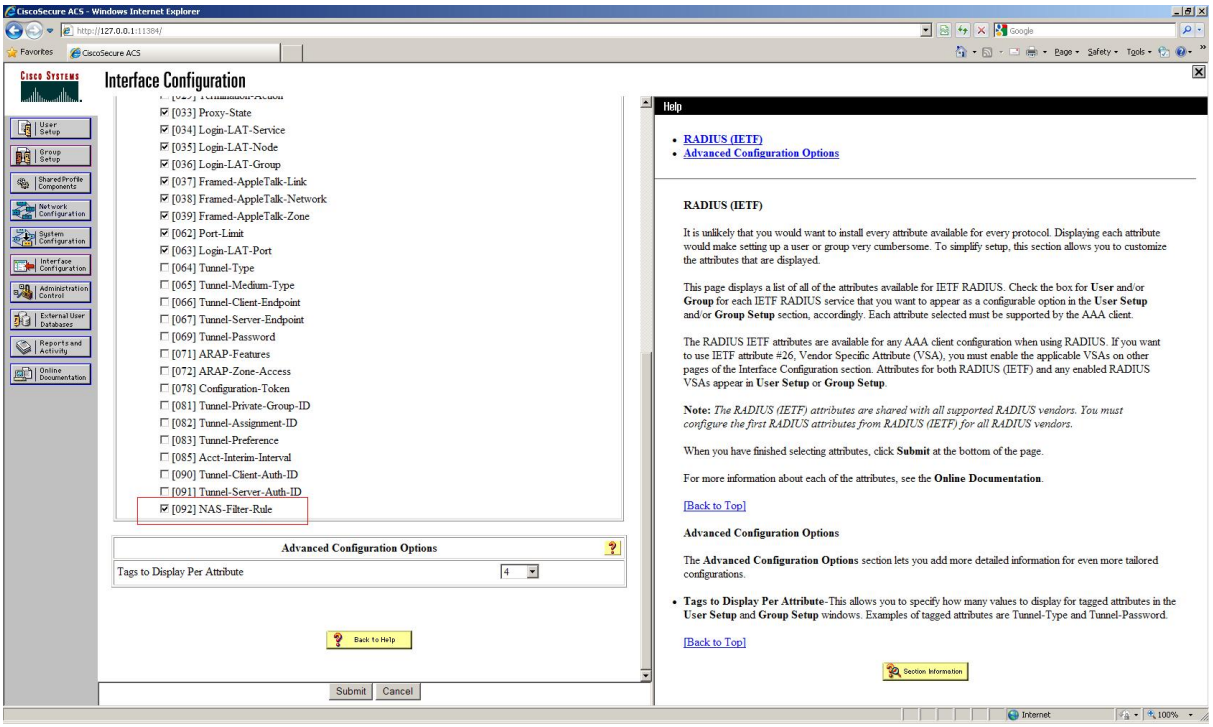
3. After modifying the registry, restart the CSAdmin, CSAuth and CSradius services. If the attribute is not available in CiscoSecure ACS configuration interface, restart the server machine.



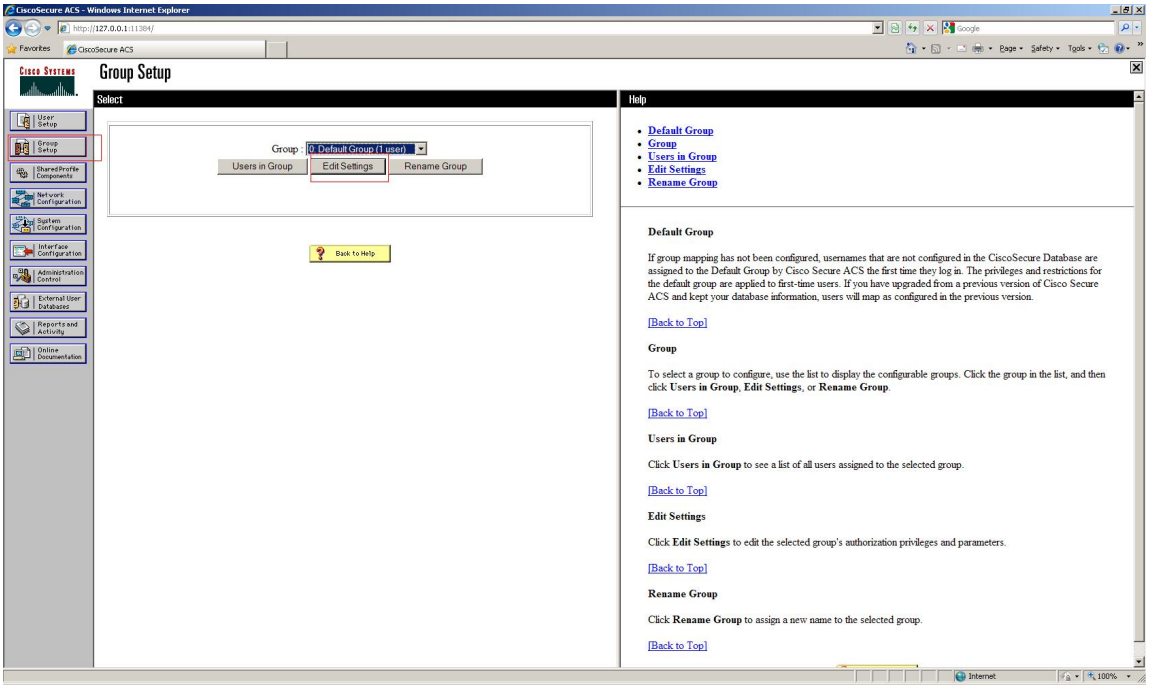
4. Select **Interface configuration** and then, select **RADIUS (IETF)** to make the newly added RADIUS IETF attribute available to the Group Setup parameters.



5. Select the attribute at the end of the list.

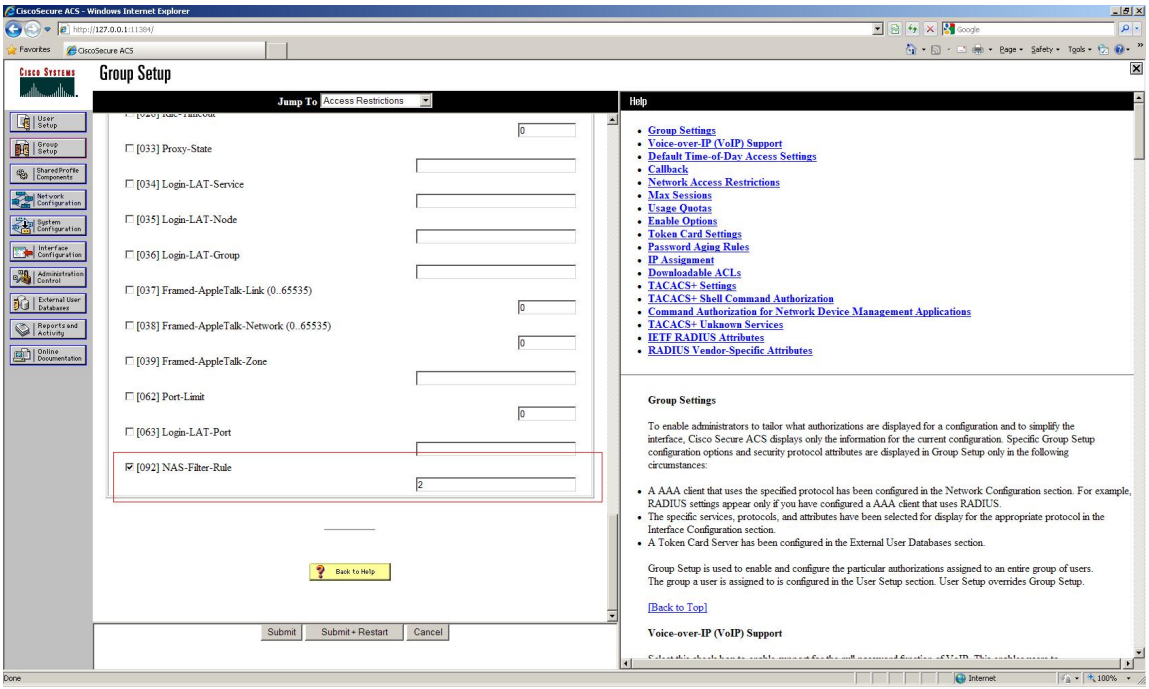


6. RADIUS attribute is available for any Group setup related to the user you want to configure to access the switch.
   a. Select **Group Setup** > **Select desired User Group** > **Edit Settings**.



b. Select **[092] NAS-Filter-Rule** attribute, and enter the access level to provide access to the user. Following are the access levels:

- Application administrator NAS-Filter-Rule = 1
- System administrator NAS-Filter-Rule = 4
- Security administrator NAS-Filter-Rule = 2



Configuration example: SYSLOG

Use the following procedure to configure the switch for Sslog.

1. Configure the remote Syslog server IP address and the remote logging level.

```
Switch:(config)#logging remote address 192.0.2.4 udp-transport
Switch:(config)#logging remote level debug
Switch:(config)#logging remote enable
```

Note:

The valid Syslog levels are alert, critical, debug, emergency, error, information, notice, and warning.

2. Verify the configuration.

```
Switch:(config)#show logging config

#show logg conf
Event Logging: Enabled
Volatile Logging Option: Overwrite
Event Types To Log: Critical, Warning, Informational
Event Types To Log To NV Storage: Critical, Warning
Remote Logging: Enabled
Primary Remote Server
```

```
        Address: 192.0.2.4
        Connection Type: UDP
        SSH Protect: Disabled
        SSH Protect TCP Port: 1025
Secondary Remote Server
        Address: 0.0.0.0
        Connection Type: TCP
        SSH Protect: Disabled
        SSH Protect TCP Port: 1025
Event Types To Log Remotely:
Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug
Facility: Local7
```

Configuration example: Secure Syslog

The following is an example for configuring secure Syslog messaging via RFC 3195 and remote port forwarding.

The following is the high-level configuration of RFC 3195 method of secure Syslog delivery:

- Security Administrator user is created (if it does not exist).
- The ERS switch is configured to send Syslog messages securely to a remote TCP port on the Syslog server.
- The PuTTY client on the Syslog server establishes a secure SSHv2 connection to the ERS switch through which the messaging passes.
- The PuTTY client then uses the port to forward the received Syslog messages to the WinSyslog server residing on the same PC for viewing and writing to file.

Prerequisites:

- Remote logging must be globally enabled.
- Event types to be logged remotely must be properly specified (usually at Informational level).
- The remote Syslog server machines must be reachable at the IP level.

Switch configuration

1. Verify if a Security Administrator account is present on the switch:

```
#show username

Lockout timeout: 1 min
Emergency account timeout: 30 days

Username:           application_adm
-----------------------------------------
Role name:          app_administrator
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled
```

```
Username:           security_adm
-------------------------------------------
Role name:          security_administrator
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled

Username:           system_adm
-------------------------------------------
Role name:          system_administrator
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled

Username:           emergency_adm
-------------------------------------------
Role name:          emergency_administrator
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled
```

If a Security Administrator account is not present on the switch, create one using

2. Configure the maximum number of concurrent sessions allowed if you want to use a Security Administrator account for both Syslog and normal operations.

```
Switch(config)#username security_admin max-number-of-sessions 9
```

3. Create a new Security Administrator account:

```
Switch:(config)#username add syslog_adm role security_administrator password
Switch:(config)#show username

Lockout timeout: 1 min
Emergency account timeout: 30 days

Username:           application_adm
-------------------------------------------
Role name:          app_administrator
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled
```

```
Username:           security_adm
-------------------------------------------
Role name:          security_administrator
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled

Username:           system_adm
-------------------------------------------
Role name:          system_administrator
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled

Username:           emergency_adm
-------------------------------------------
Role name:          emergency_administrator
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled

Username:           syslog_adm
-------------------------------------------
Role name:          security_administrator
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled
```

Note:

The switch enforces the change of the temporary default password for each new created account before you can use the account.

Configure Secure Syslog on the ERS switch

1. Enter Global Configuration mode and enter the following commands:

```
Switch(config)#logging remote address 192.0.2.2 tcp-transport ssh-protect tcp-port
1026
```

In this example, TCP port 1026 port is selected for secure forwarding and it is forwarded to the WinSyslog Server. The WinSyslog Server IP address is 192.0.2.2, where the SSH client with the remote port forwarder is configured.

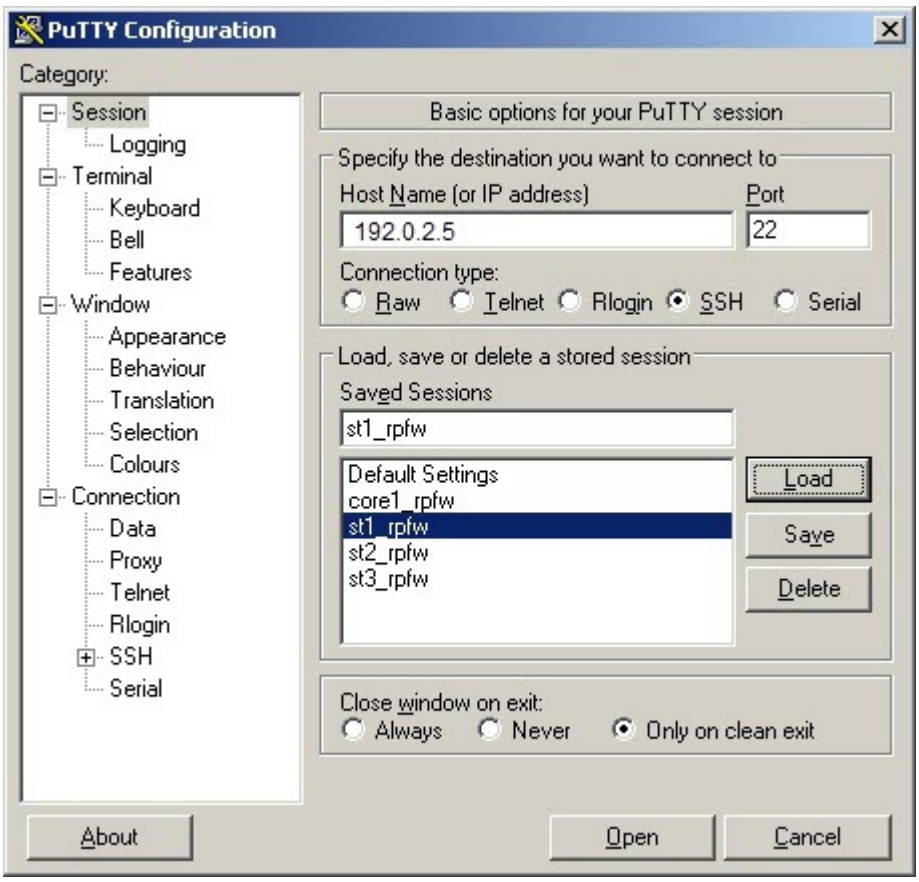
2. Configure the primary Syslog server.

```
Switch#show logging config
Event Logging: Enabled
Volatile Logging Option: Overwrite
Event Types To Log: Critical, Warning, Informational
Event Types To Log To NV Storage: Critical, Warning
Remote Logging: Enabled
Primary Remote Server
        Address: 192.0.2.2
        Connection Type: TCP
        SSH Protect: Enabled
        SSH Protect TCP Port: 1026
Secondary Remote Server
        Address: 0.0.0.0
        Connection Type: TCP
        SSH Protect: Disabled
        SSH Protect TCP Port: 1025
Event Types To Log Remotely:
Emergency, Alert, Critical, Error, Warning, Notice, Informational
Facility: Local7
```

3. Configure secondary remote Syslog server. The configuration command must be entered with secondary-address parameter instead of address.

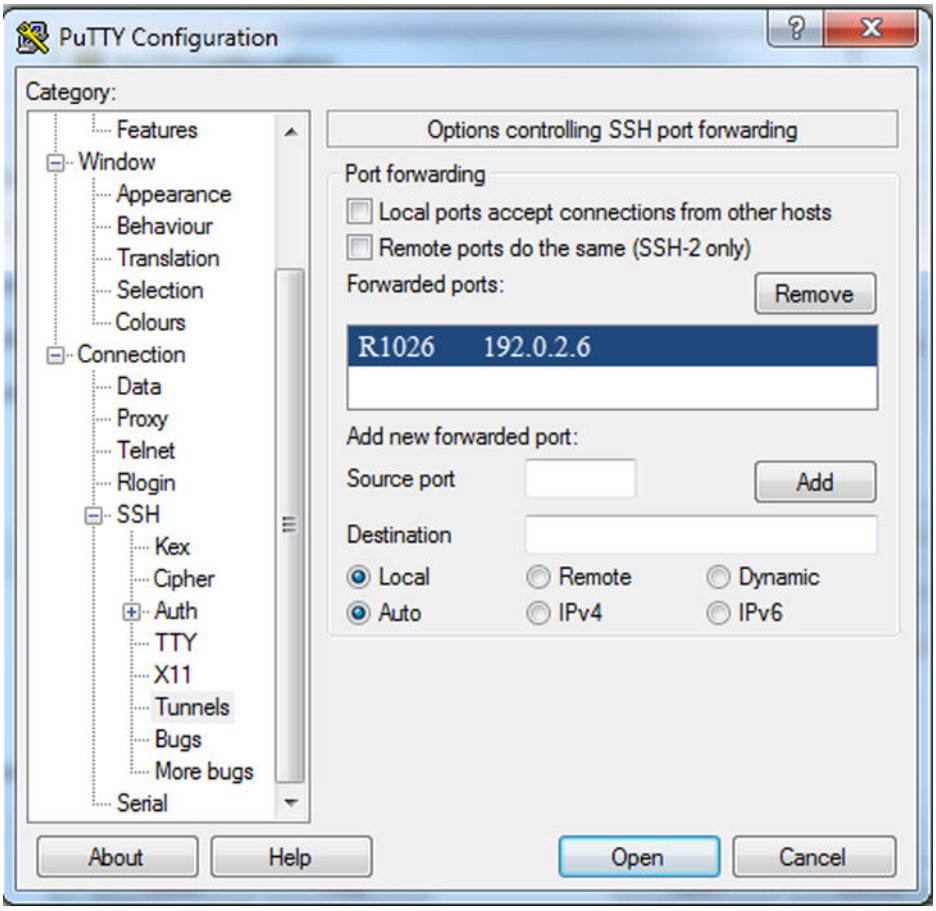
Configuring PuTTY

1. Open PuTTY and create a regular profile that points to the ERS on SSH port 22



2. Create the secure tunnel.

   Remote forwarder is configured within the SSH session. The administrator configures the remote port on the ERS (which was defined as the TCP secure forwarder port 1026) to this local PC's port where the RFC3195 WinSyslog server is listening, in this example TCP is 601.



a. In Port forwarding section, select **Local Ports accept connections from other hosts**.

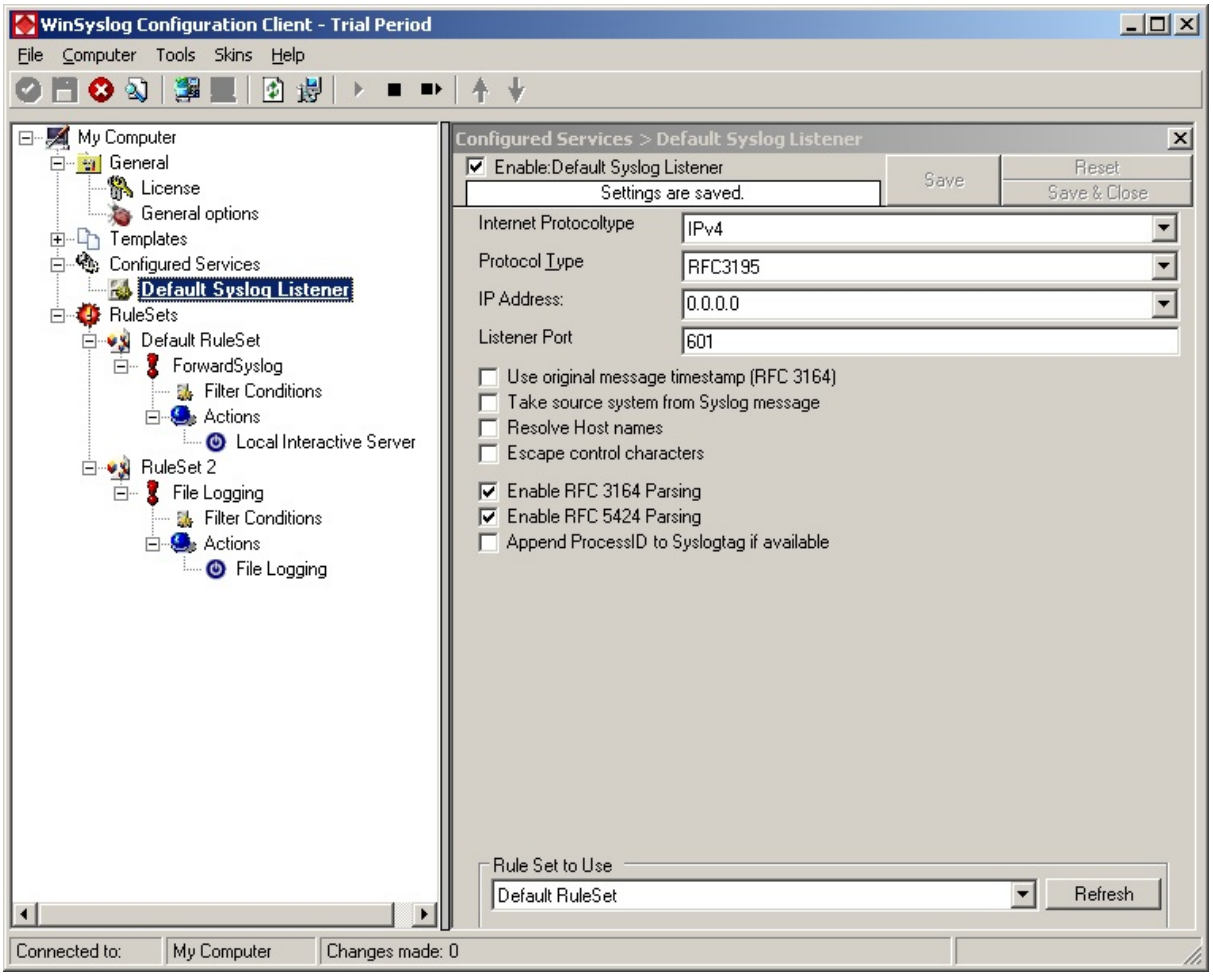
b. Ensure that Forwarding is set up for Remote not Local port forwarding.

c. Return to the beginning Session Screen and click **Save** to ensure that the Tunnel is saved to this profile.

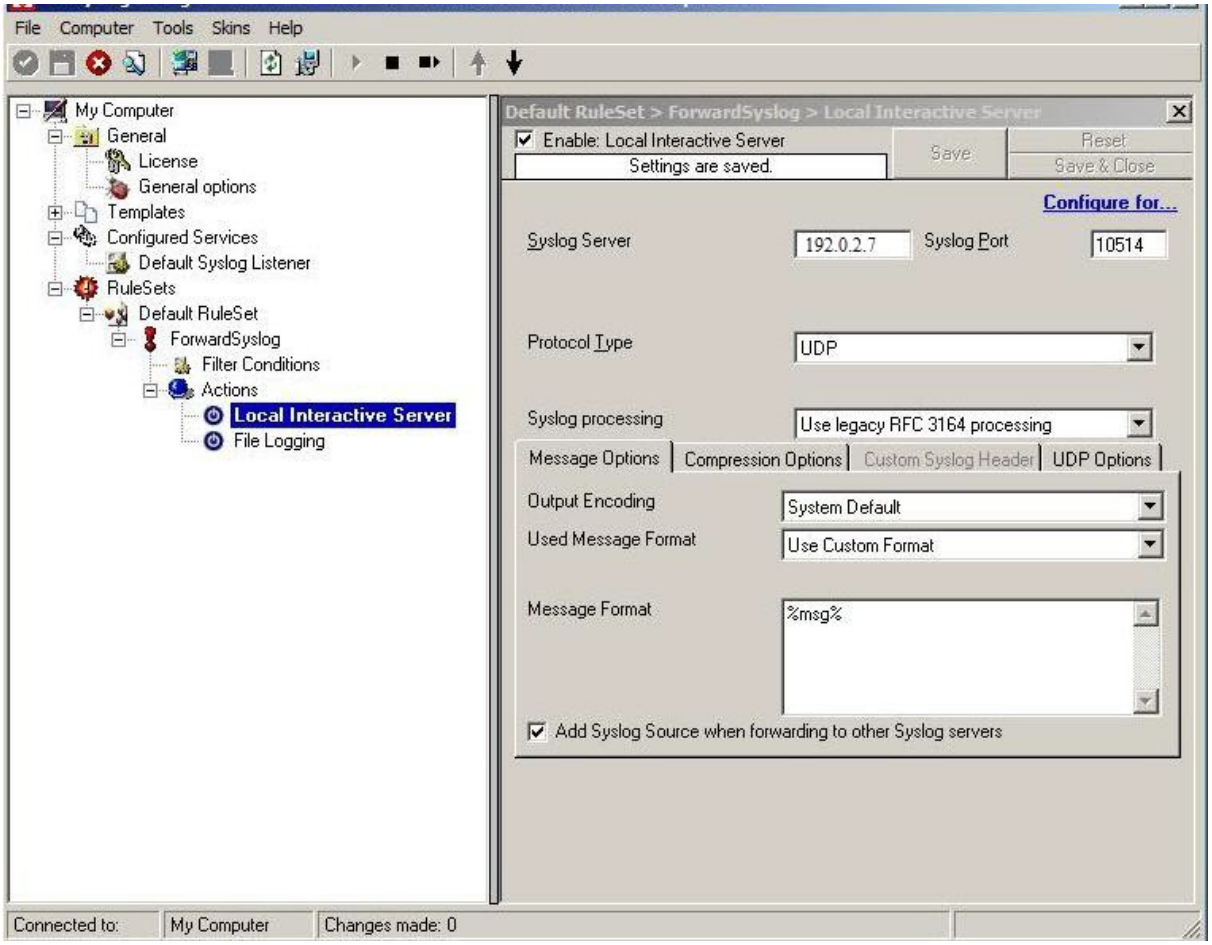
Configuring the WinSyslog server

The following section describes the setup of the WinSyslog server to support the RFC 3195 secure Syslog.

1. Go to **Start** > **My Computer** > **Configured Services** > **Default Syslog Listener**.



2. Select **Enable: Default Syslog Listener**.
3. From the Internet Protocoltype drop-down, select IPv4.
4. From the Protocol Type drop-down, select RFC3165.
5. From the IP Address drop-down, select 0.0.0.0.
6. From the Listener Port drop-down, select 601.
7. Select **Enable RFC 3164 Parsing** and **Enable RFC 5424 Parsing**.
8. From the My Computer navigation tree, expand Rule Sets/Default RuleSet options.
9. Select **Local Interactive Server**.

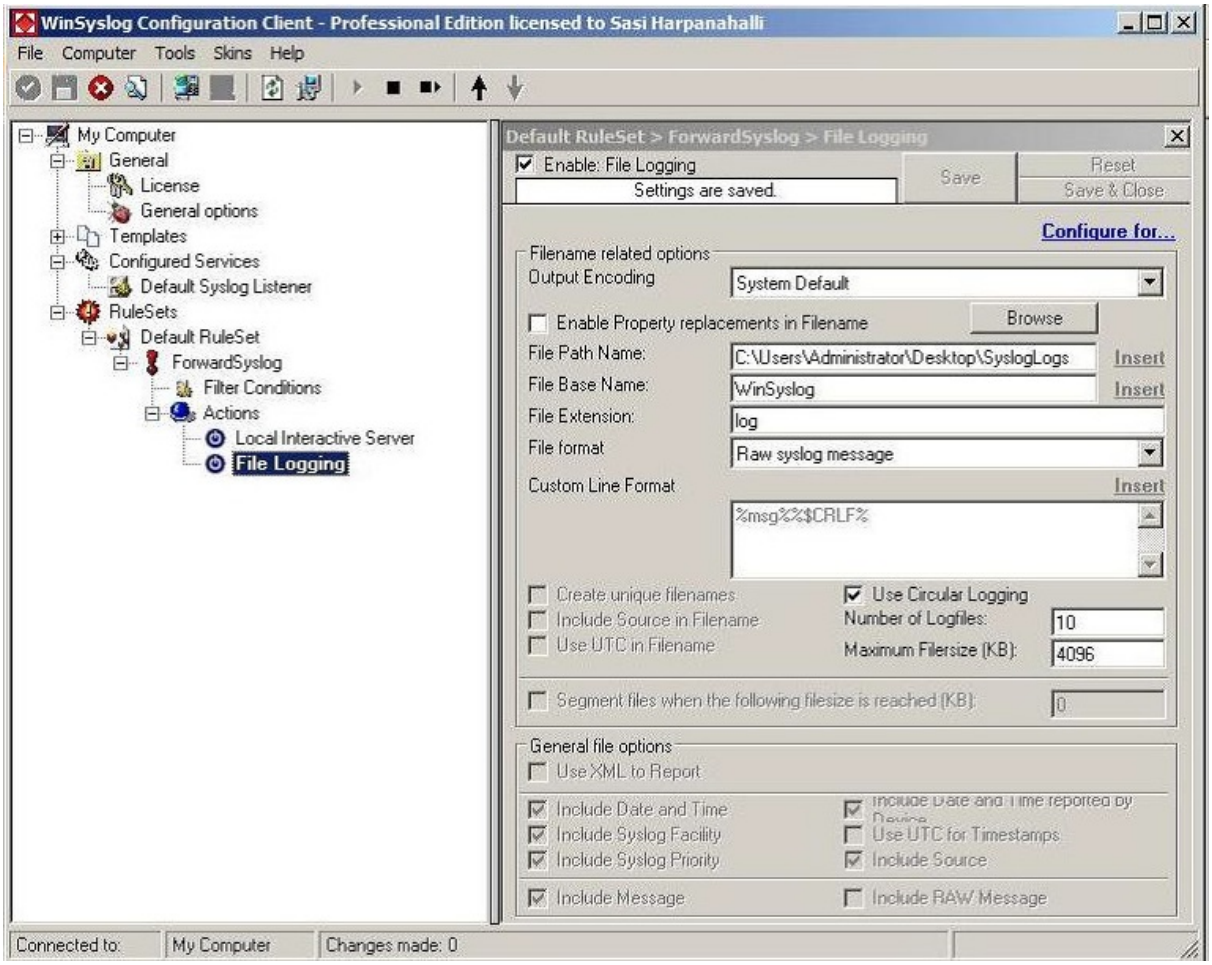


The Default RuleSet consists of Local Interactive Server and File Logging. In this example, the Syslog messages are sent to the Local Interactive Server (another application that comes with WinSyslog) so that the messages can be displayed in real time as they are written to the server.

Note:

This communication is to the localhost 192.0.2.7, therefore this communication does not leave the server.

10. In the following example, the server is configured to write the Syslog messages to a file on the local machine.



11. Use the options at the top of the screen to stop and then restart the Syslog server.

Completing the configuration

Perform the following actions to complete configuration:

1. Launch the interactive Syslog Viewer application on the WinSyslog Server PC.
2. Launch PuTTY and establish the SSH forwarder session:
   a. Login using the desired Security Administrator user – either the default one or the created user (in the preceding example).
   b. After logging on to the PuTTY, this session must be left alone as it is the forwarded for the RFC 3195 logs.
   c. Ensure that all power saving settings on the server are disabled, else the Tunnel is terminated if the server enters sleep or hibernation mode.
3. After the PuTTY session establishes the secure Syslog tunnel to the ERS switch, the interactive Syslog viewer displays Syslog messages from the ERS switch.

Switch hardening in Enhanced Secure Mode

This section provides configuration examples for hardening the switch when Enhanced Secure Mode is enabled.

Initial Login and Basic Configuration Tasks

Initial login

1. Connect to the switch using an RJ-45 to DB-9 or a DB-9 to RJ-45 adapter.
2. Login to the switch for the first time using the factory default username and password pair of *admin / password*.
3. At the initial login, you must change the initial security administrator account using a new username/password pair. By default the switch does not allow repeated characters or sequential characters in the new passwords.
4. Login using the newly defined username/password pair for the initial security administrator account.
5. At the first login for this newly created account you must change and confirm the password.

Basic configuration tasks

Telnet access is configurable and is enabled by default on switch. To enhance security on switch, you can disable telnet access.

1. Disable TELNET Server:

   ```
   Switch:(config)#no telnet-access
   ```

2. Disable Web Server:

   ```
   Switch:(config)#web-server disable
   ```

3. Enable SSH Server:

   ```
   Switch:(config)#ssh
   ```

4. Enable Serial Console Security. Set this parameter to drop console sessions when the serial console cable is physically disconnected. Re-authentication is required to gain access to the switch.

   ```
   Switch:(config)#serial-security enable
   ```

5. Configure the switch for MSTP mode.

   Multiple Spanning Tree Protocol mode (IEEE 802.1s) is the default operation mode on the ERS 4900/5900 switches. MSTP is the best STP operational mode for both Heterogeneous configurations in which the switch is interoperating with another vendor switch and Homogeneous solutions involving only Extreme Networks equipment.

   For more information about MSTP, see Configuring VLANs, Spanning Tree, and MultiLink Trunking on Ethernet Routing Switch 4900 and 5900 Series.

   To set the switch to use MSTP, enter the following command:

   ```
   Switch:(config)#spanning-tree mode mst
   ```

6. Save the running configuration to NVRAM:

```
Switch:(config)#copy config nvram
```

7. Power cycle the switch.
8. Verify the above configuration:

```
Switch:#show ipmgr

TELNET Access: Disabled
SNMP Access:   Disabled
WEB Access:    Disabled
SSH Access:    Enabled
TELNET IP List Access Control: Enabled
SNMP IP List Access Control:   Enabled
WEB IP List Access Control:    Enabled
SSH IP List Access Control:    Enabled
Allowed Source IP Address  Allowed Source Mask
-------------------------  ------------------
1  0.0.0.0                    0.0.0.0
2  255.255.255.255            255.255.255.255
3  255.255.255.255            255.255.255.255

Switch:#show serial-security

Serial security is enabled

Switch:#show spanning-tree mode

Current STP Operation Mode: MST
```

Configuring SSH

The following is an example of configuring SSH on switch.

1. Configure the idle session timeout to 10 minutes:

```
Switch:(config)#telnet-access inactive-timeout 10
```

2. Configure the login session timeout to 60 seconds. The login session timeout timer also controls the login session timeout for the serial console port.

```
Switch:(config)# ssh timeout 60
```

3. Configure the number of failed login retries:

```
Switch:(config)# ssh retries 3
```

4. Verify the above configuration:

```
Switch(config)#show ssh global
Active SSH Sessions     :  0
Version                 :  Version 2 only
Port                    :  22
Authentication Timeout  :  60
DSA Authentication      :  True
RSA Authentication      :  True
Password Authentication :  True
X.509v3 Authentication  :  True
X.509v3 Username Overwrite  : True
X.509v3 Strip Domain    :  True
X.509v3 Use-Domain      :  my.domain.com
Auth Retries            :  3
SSH Rekey               :  False
```

```
SSH Rekey-Interval      :  3600000
SSH Rekey-DataLimit     :  1
Auth Key TFTP Server    :  192.0.2.1
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys           :  Exist
RSA Host Keys           :  Exist
Enabled                 :  False
```

5. Configure the SSH access policy.

   Apply IP Manager access polices to SSH connections as Condition of Fielding. This command filters incoming IPv4 connections and permits SSH access only to addresses in the 192.0.2.2 subnet, further limit this filter to a specific IP address by using a 32 bit mask. The “1” parameter specifies the access list entry number for IPv4 addresses; for IPv4 the maximum number of IP Mgr access list entries is 50 (1-50). For IPv6 the maximum number of IP Mgr access list entries is 50 (51-100).

```
Switch:(config)#ipmgr ssh
Switch:(config)#ipmgr source ip 1 192.0.2.2 mask 255.255.255.0
Switch:(config)#ipmgr source ip 51 2092::45/64
```

6. Verify the above configuration.

```
Switch:(config)#show ipmgr ipv4

TELNET Access: Disabled
SNMP Access:   Disabled
WEB Access:    Disabled
SSH Access:    Enabled
TELNET IP List Access Control: Enabled
SNMP IP List Access Control:   Enabled
WEB IP List Access Control:    Enabled
SSH IP List Access Control:    Enabled
Allowed Source IP Address  Allowed Source Mask
-------------------------  ------------------
1  192.0.2.2                  255.255.255.0
2  255.255.255.255            255.255.255.255
3  255.255.255.255            255.255.255.255
Switch:(config)#show ipmgr ipv6

TELNET Access: Disabled
SNMP Access:   Disabled
WEB Access:    Disabled
SSH Access:    Enabled
TELNET IP List Access Control: Enabled
SNMP IP List Access Control:   Enabled
WEB IP List Access Control:    Enabled
SSH IP List Access Control:    Enabled
Allowed Source IPv6 Address
-------------------------------------------
51 2092::45/64
52 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
53 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
```

Configuring passwords

The following is an example of configuring password parameters.

1. Configure the global password aging interval:

```
Switch:(config)#password aging-time 90
```

2. Configure the password aging interval account value for an existing user:
```
Switch:(config)#password aging-time username security_adm 90
```
3. Configure the password change interval:
```
Switch:(config)#password change-interval 30
```
4. Configure the maximum number of passwords retained in history:
```
Switch:(config)#password password-history 3
```
5. Configure the password complexity:
   - Configure a minimum password length of 15 characters:
```
Switch:(config)#password min-length 15
```
   - Configure the password rule 2 2 2 2:
```
Switch:(config)#password complexity lower-case 2 numeric 2 special 2 upper-case 2
```
   - Enable the rejection of repeated characters in a password:
```
Switch:(config)#password check-repeated enable
```
   - Enable the rejection of sequential characters. The switch checks the following strings, uppercase letters included, in forward and reverse order: "abcdefghijklmnopqrstuvwxyz","01234567890", "qwertyuiop", "asdfghjkl", "zxcvbnm", "!@#$%^&*()")
```
Switch:(config)#password check-sequential enable
```
6. Configure the amount of delay time after 3 failed login attempts within one minute:
```
Switch:(config)#password delay-time 60
```
7. Configure the notification message to users encountering a login failure:
```
Switch:(config)#password login-failure-notification "Login failure"
```
8. Enable the switch to enforce a password change on first login for all new users:
```
Switch:(config)#password password-change-on-first-login enable
```
9. Restrict number of times a password can be changed in a day:
```
Switch:(config)#password password-change-rate-limiter 1
```
10. Configure the pre-expiry notification interval:
```
Switch:(config)#password notifications 30
```
11. Configure the allowed grace interval for post-expiration login:
```
Switch:(config)#password grace-period 3
```
12. Configure the number of allowed post-expiration logins:
```
Switch:(config)#password post-expiration-login 3
```
13. Enable internal password encryption:
```
Switch:(config)#password encryption-key aes-cbc
<Enter and confim encryption key>
```
14. Configure the number of days after which a disabled account due to inactivity timeout will be re-enabled:
```
Switch:(config)#password unlock-timer 7
```

15. Verify the configuration above. Enter a question mark after the command to display the permitted sub-commands.

```
Switch:#show password ?

Display password security restrictions
  aging-time                      Password validity period (in days)
  change-interval                 Display the password change interval
  check-repeated                  State of check-repeated-characters option
  check-sequential                State of check-sequential-characters option
  complexity                      Display password complexity rules settings
  delay-time                      Display the delay time after 3 failed login
                                  attempts within one minute
  grace-period                    Display the interval for post-expiration log
                                  in
  login-failure-notification      Display notification message to users
                                  encountering a login failure
  min-length                      Display the password minimum length
  notifications                   Display password expiration notifications
                                  intervals
  password-change-on-first-login  State of password-change-on-first-login
                                  option
  password-change-rate-limiter    Display number of times a password can pe
                                  changed in a day
  password-history                Number of passwords in history
  post-expiration-login           Display the number of post-expiration logins
  unlock-timer                    State of unlock-timer option
```

Customizing the login banner

The following is an example of customizing the login banner.

1. Configure the banner mode to custom and verify the setting:

```
Switch:(config)#banner custom
Switch:(config)#show banner

Current banner setting: CUSTOM
```

2. Configure the CUSTOM banner, line by line, entering up to 20 lines of text:

```
Switch:(config)#banner 1 "<Text for line 1>"
Switch:(config)#banner 2 "<Text for line 2>"
Switch:(config)#banner 3 "<Text for line 3>"
```

3. You can configure the switch to display a commonly used login banner from the Defense Switched Network (DSN) Security Technical Implementation Guide (STIG):

```
Switch:(config)#banner usg
"You are accessing a U.S. Government (USG) Information System (IS) that is
Provided for USG-authorized use only. By using this IS (which includes any device
attached to
this IS), you consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring, network
operations and defense, personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to
routine monitoring, interception, and search, and may be disclosed or used for any
USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to
protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or
```

```
CI investigative searching or monitoring of the content of privileged
communications,
or work product, related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such communications and work
product are private and confidential. See User Agreement for details

Enter Ctrl-Y to begin and acknowledge the above statements."
```

User account creation

The following is an example of creating user accounts for role based access control.

1. Display the available default roles that can be used for user account creation:

```
Switch:(config)#show role

Roles                           Groups                          Rights
------------------------------- ------------------------------- ------------
app_administrator               cli-basic-group                 show-config
                                system-cmds-group               show-only
security_administrator          cli-basic-group                 show-config
                                security-cmds-group             show-config
                                system-cmds-group               show-config
                                audit-cmds-group                show-config
system_administrator            cli-basic-group                 show-config
                                system-cmds-group               show-config
                                audit-cmds-group                show-only
emergency_administrator         cli-basic-group                 show-config
                                security-cmds-group             show-config
                                system-cmds-group               show-config
                                audit-cmds-group                show-config
```

2. Create an additional user account with an appropriate role and provide the user account with an initial password:

```
account with an initial password:
Switch:(config)#username add systemadmn role-name system_administrator password
```

3. Verify the account created:

```
Switch:(config)#show username

Lockout timeout: 60 min
Lockout retries: 5
Emergency account timeout: not set

Username:           systemadmn
-----------------------------------------
ntp authentication-key 100 type md5/sha1
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Verify the NTP key:
FED1(config)#sh ntp key
Key Id      Key                     Key Type
-----------------------------------------
100         ********                MD5
200         ********                SHA1
SSH access: Enabled
TELNET access: Enabled

Username:           security_adm
-----------------------------------------
Role name:          security_administrator
```

```
Enabled:            Yes
Password aging-time:  90 days
Lockout status: Available
Access-start-hour:  0
Access-stop-hour:   24
Inactive period:    360 days
Maximum number of sessions: 12
SSH access: Enabled
TELNET access: Enabled
```

4. Configure the duration of session lockout time for failed login attempts:

```
Switch:(config)#username lockout-time 1
```

5. Configure Number of retries in a session before a user gets locked:

```
Switch:(config)#username lockout-retries 5
```

6. Configure the emergency account timeout:

```
Switch:(config)#username emergency_account_timeout 30
```

7. Configure the per-user daily access interval:

```
Switch:(config)#username systemadmn daily-access-interval access-start-hour 9
access-stop-hour  18
```

8. Configure the per-user inactivity period after which the account will be disabled:

```
Switch:(config)#username systemadmn inactive-period 30
```

9. Configure the maximum number of concurrent sessions allowed per user account:

```
Switch:(config)#username systemadmn max-number-of-sessions 1
```

10. Enable or disable TELNET or SSH access for the user:

```
Switch:(config)#username systemadmn telnet-access disable
Switch:(config)#username systemadmn ssh-access enable
```

11. When needed, a security administrator can unlock a previously locked user account:

```
Switch:(config)#username systemadmn unlock
```

12. (Optional) A security administrator can change the password and assigned role for another user account already defined in the system:

```
Switch:(config)#username systemadmn password
Switch:(config)#username systemadmn role-name app_administrator
```

Configuring the out of band management port

The following is an example of configuring the Out of Band (OOB) management port. The switch can use the OOB management port only for management traffic.

1. Configure IPv4 network management.

   Assign the management IP address.

```
Switch:(config)#ip mgmt address 192.0.2.11 255.255.255.0
```

2. Assign the default gateway in order to manage the switch from remote subnets.

```
Switch:(config) #ip mgmt default-gateway 192.0.2.12
```

3. Verify the above configuration:

```
Switch:#show mgmt status
```

```
Unit Link Limit Shutdown Interval
---- ---- ----- ----------------
1    Up   7000  180

Switch:#show ip

Bootp/DHCP Mode: Disabled

                            Configured        In Use        Last BootP/DHCP
                           -------------- --------------- --------------------
Stack IP Address:          192.0.2.1                     0.0.0.0
Switch IP Address:         192.0.2.3                    0.0.0.0
Stack Subnet Mask:         255.255.255.0   255.255.255.0   0.0.0.0
Mgmt Stack IP Address:     192.0.2.11     192.0.2.11
Mgmt Switch IP Address:    0.0.0.0
Mgmt Subnet Mask:          255.255.255.0 255.255.255.0
Mgmt Def Gateway:          192.0.2.12     192.0.2.12
Default Gateway:           0.0.0.0
```

4. Configure IPv6 network management.

```
Switch:(config)#ipv6 enable
Switch:(config)#ipv6 mgmt interface
Switch:(config)#ipv6 mgmt address 2001:DB8:6:1200::2/55
Switch:(config)#ipv6 mgmt default gateway 2001:DB8:6:1200::1
```

5. Verify the above configuration:

```
Switch:#show ipv6 global
forwarding                     : disabled
default-hop-cnt                : 30
number-of-interfaces           : 0
number-of-tunnels              : 0
admin-status                   : enabled
icmp-error-interval            : 1000
icmp-redirect-msg              : disabled
icmp-unreach-msg               : disabled
icmp port-unreach              : enabled
icmp addr-unreach              : enabled
multicast-admin-status         : disabled
icmp-error-quota               : 50
block-multicast-replies        : disabled
autoconfig                     : disabled
slow-path-to-cpu               : disabled


Switch:#show ipv6 mgmt address

Mgmt Switch Address: ::/0
Mgmt Stack Address:  2001:DB8:6:1200::2/55

Switch:#show ipv6 mgmt default-gateway

Mgmt Default Gateway: 2001:DB8:6:1200::1
Status: Active
```

Configuring network management VLAN

The following is an example of configuring network management VLAN.

1. Configure IPv4 Network Management.

Create a single port VLAN different than VLAN 1. The example uses VLAN 50.

```
Switch:(config)#vlan create 50 name "Net Mgmt" type port
```

2. Configure this VLAN as the management VLAN and assign the management IP address:

```
Switch:(config)#vlan mgmt 50
Switch:(config)#ip address 192.0.2.1 255.255.255.0
```

3. Assign the VLAN to a data plane switch port (3/48) that is used solely for management traffic:

```
Switch:(config)#vlan members add 50 3/48
```

4. Assign the default gateway in order to manage the switch from remote subnets.

```
Switch:(config)#ip default-gateway 192.0.2.2
```

5. Verify the above configuration:

```
Switch:#show vlan

Id  Name                 Type     Protocol         PID      Active IVL/SVL Mgmt
--- -------------------- -------- ---------------- -------- ------ ------- ----
1   VLAN #1              Port     None             0x0000   Yes    IVL     No
        Port Members: NONE
50  Net Mgmt             Port     None             0x0000   Yes    IVL     Yes
        Port Members: 3/48
Total VLANs: 2


Switch:#show ip

Bootp/DHCP Mode: Disabled

                            Configured        In Use        Last BootP/DHCP
                           --------------- --------------- --------------------
Stack IP Address:          192.0.2.1   192.0.2.1   0.0.0.0
Switch IP Address:         192.0.2.3                     0.0.0.0
Stack Subnet Mask:         255.255.255.0   255.255.255.0   0.0.0.0
Mgmt Stack IP Address:     0.0.0.0
Mgmt Switch IP Address:    0.0.0.0
Mgmt Subnet Mask:          0.0.0.0
Mgmt Def Gateway:          0.0.0.0
Default Gateway:           192.0.2.2     192.0.2.2     0.0.0.0
```

6. Configure IPv6 Network Management:

```
Switch:(config)#ipv6 enable
Switch:(config)#interface vlan 50
Switch:(config-if)#ipv6 interface enable
Switch:(config-if)#exit
Switch:(config)#ipv6 address 2001:DB8::/32
Switch:(config)#ipv6 default gateway 2001:DB8::1
```

7. Verify the above configuration:

```
Switch:#show ipv6 global
forwarding                    : disabled
default-hop-cnt               : 30
number-of-interfaces          : 2
number-of-tunnels             : 0
admin-status                  : enabled
icmp-error-interval           : 1000
icmp-redirect-msg             : disabled
icmp-unreach-msg              : disabled
icmp port-unreach             : enabled
icmp addr-unreach             : enabled
multicast-admin-status        : disabled
```

```
icmp-error-quota               : 50
block-multicast-replies        : disabled
autoconfig                     : disabled
slow-path-to-cpu               : disabled


Switch:#show ipv6 address

Switch Address: ::/0
Stack Address:  2001:DB8::/32

Switch:#show ipv6 default-gateway

Default Gateway: 2001:DB8::1

Status: ActiveSta
```

Configuring NTP on switch

The following is an example of configuring the switch for NTP.

1. Configure the switch time source for NTP:

```
Switch:(config)#clock source ntp
Switch:(config)#ntp server 192.0.2.1
Switch:(config)#ntp
```

2. Verify the configuration above:

```
Switch:#show clock detail

System Clock time  :    THU OCT 06 11:09:04 2011
System Clock Source:    NTP
NTP time           :    2011-10-06 08:09:04 GMT
SNTP time           :    SNTP not synchronized.
SysUpTime           :    1 day, 20:13:05
Daylight saving recurring time is disabled
Daylight saving time is disabled
Time zone is set to 'itc', offset from UTC is 03:00

Switch:#show ntp

NTP client enabled : true
NTP polling interval : 15 minutes
Last NTP update:
latest update time : THU OCT 06 06:09:28 2011 itc
synchronized to : 192.0.2.1 (Stratum: 3)

Switch:#show ntp server

Server IP         Enabled   Auth      Key Id
-----------------------------------------------
10.100.107.10     true      false     1
```

3. Create the NTP authentication-key :

```
Switch:(config)#ntp authentication-key 1
Secret key: ****
Confirm secret key: ****
```

4. Verify the NTP key:

```
Switch:(config)#show ntp key
Key Id      SHA1 Key
```

```
-------------------------------------------
1           ********
```

5. Enable SHA1 authentication for the NTP server and assign the authentication key to the NTP server:

```
Switch:(config)#ntp server 192.0.2.2 auth-enable authentication-key 1
```

6. Verify the NTP server configuration:

```
Switch:#show ntp serv
Server IP         Enabled   Auth      Key Id
-----------------------------------------------
192.0.2.3         true      true      1
192.0.2.4         true      false     0
```

Configuring NTP on server

Use the following settings to configure NTP on a server. In this example Ubuntu 14.04.4 LTS is installed on server, with NTP package version *ntpd 4.2.6p5*.

1. Configure the ntp.conf file as follows:

```
keys /etc/ntp.keys
trustedkey 1
server 192.0.2.1      # local system clock
fudge 192.0.2.1 stratum 5
```

2. Configure the ntp.keys file as follows:

```
1 SHA1 myntpkey
```

- *1* indicates the index
- *SHA1* indicates the cryptographic algorithm
- *myntpkey* specifies the key string

```
2  MD5 myntpkey
```

- *2* indicates the index
- *MD5* indicates the cryptographic algorithm
- *myntpkey* specifies the key string

IPv6 ICMP Message Rate Limiting

The following is an example of configuring IPv6 ICMP Message Rate Limiting.

1. Configure the IPv6 ICMP error message interval. Enter a time value in milliseconds.

```
Switch:(config)#ipv6 icmp error-interval 1000
```

2. Configure the IPv6 ICMP error message quota. Enter a value for the number of packets.

```
Switch:(config)#ipv6 icmp error-quota 50
```

3. Verify the configuration above:

```
Switch:#show ipv6 global
```

```
forwarding                      : disabled
default-hop-cnt                 : 30
number-of-interfaces            : 2
number-of-tunnels               : 0
admin-status                    : enabled
icmp-error-interval             : 1000
icmp-redirect-msg               : disabled
icmp-unreach-msg                : disabled
icmp port-unreach               : enabled
icmp addr-unreach               : enabled
multicast-admin-status          : disabled
icmp-error-quota                : 50
block-multicast-replies         : disabled
autoconfig                      : disabled
slow-path-to-cpu                : disabled
```

SNMPv3

The following is an example of configuring the switch for SNMPv3.

1. When enabling snmp-server for the first time, the switch prompts you to change the default SNMPv1/v2c RO and RW community strings and to define a default SNMPv3 user with SHA authentication method and a preferred encryption protocol.

   Enable the SNMP server:

   ```
   Switch:(config)#snmp-server enable
   ```

2. Create an SNMP view to use for defining a secure SNMPv3 user:

   ```
   Switch:(config)#snmp-server view root 1.3 -1.3.6.1.4
   Switch:#show snmp-server view

   View Name                       ST RS View Spec(s)
   ------------------------------- -- -- --------------------------------------
   root                            NV AC +1.3
                                   NV AC -1.3.6.1.4
   ------------------------------- -- -- --------------------------------------
   nncli                           RO AC +1.3
                                   RO AC +1.0.8802.1.1.1
                                   RO AC +1.0.8802.1.1.2
                                   RO AC +1.0.8802.1.1.3
                                   RO AC +1.2.840.10006.300.43
   ------------------------------- -- -- --------------------------------------
   macsec                          NV AC +1.3
                                   NV AC +1.0.8802.1.1.3
   ------------------------------- -- -- --------------------------------------
   snmpv1Objs                      RO AC +1.3
                                   RO AC -1.3.6.1.6
                                   RO AC +1.0.8802.1.1.1
                                   RO AC +1.0.8802.1.1.2
                                   RO AC +1.0.8802.1.1.3
                                   RO AC +1.2.840.10006.300.43
                                   RO AC +1.3.6.1.6.3.10
                                   RO AC +1.3.6.1.6.3.12
                                   RO AC +1.3.6.1.6.3.13
                                   RO AC +1.3.6.1.6.3.1.1.4
                                   RO AC +1.3.6.1.6.3.1.1.5
   ------------------------------- -- -- --------------------------------------
   webSnmpObjs                     RO AC +1.3
                                   RO AC +1.0.8802.1.1.1
                                   RO AC +1.0.8802.1.1.2
   ```

```
                                RO AC +1.0.8802.1.1.3
                                RO AC +1.2.840.10006.300.43
-------------------------------- -- -- ------------------------------------
```

3. Create a secure SNMPv3 user for management use. This user will use SHA authentication with AES encryption and the previously defined SNMP view.

```
Switch:(config)#snmp-server user secureuser sha aes read-view root write-view root
notify-view root
Switch:#show snmp-server user

------------------------------------------------------------------------------
User Name:  initial
SNMP Engine ID:  Local
Authentication Protocol:  SHA
Privacy Protocol:  AES
Storage Type:  Non Volatile (NVRAM)
Status:  Active
Views for Unauthenticated Access:
    Read View:
    Write View:
    Notify View:
Views for Authenticated Access:
    Read View:
    Write View:
    Notify View:
Views for Authenticated and Encrypted Access:
    Read View:    snmpv1Objs
    Write View:   snmpv1Objs
    Notify View:  snmpv1Objs
------------------------------------------------------------------------------
User Name:  secureuser
SNMP Engine ID:  Local
Authentication Protocol:  SHA
Privacy Protocol:  AES
Storage Type:  Non Volatile (NVRAM)
Status:  Active
Views for Unauthenticated Access:
    Read View:
    Write View:
    Notify View:
Views for Authenticated Access:
    Read View:
    Write View:
    Notify View:
Views for Authenticated and Encrypted Access:
    Read View:    root
    Write View:   root
    Notify View:  root
------------------------------------------------------------------------------
```

4. Define an SNMPv3 trap receiver host to receive SNMP traps generated by the system. Traps are secured with both authentication and encryption.

```
Switch:(config)#snmp-server host 192.100.0.14 v3 auth-priv secureuser
```

5. Verify the above configuration.

```
Switch:#show snmp-server host

------------------------------------------------------------------------------
Notify Group: inform
  Type        : Inform
  Storage Type: Read-Only
  Status      : Active
------------------------------------------------------------------------------
```

```
Destination                             SNMP Security Community String
Address         Port   Timeout    Rtr Vers  Level     or User Name
--------------- ------ ---------- --- ---- -------- --------------------------
--------------------------------------------------------------------------------
Notify Group: s5AgTrpRcvr
  Type        : Trap
  Storage Type: Read-Only
  Status      : Active
--------------------------------------------------------------------------------
Destination                             SNMP Security Community String
Address         Port   Timeout    Rtr Vers  Level     or User Name
--------------- ------ ---------- --- ---- -------- --------------------------
--------------------------------------------------------------------------------
Notify Group: trap
  Type        : Trap
  Storage Type: Read-Only
  Status      : Active
--------------------------------------------------------------------------------
Destination                             SNMP Security Community String
Address         Port   Timeout    Rtr Vers  Level     or User Name
--------------- ------ ---------- --- ---- -------- --------------------------
192.100.0.14    162    1500       3   V3   AuthPriv secureuser


IPv6 Trap Destinations:

--------------------------------------------------------------------------------
Notify Group: inform
  Type        : Inform
  Storage Type: Read-Only
  Status      : Active

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

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

Assigning unused ports to Quarantine VLAN

As a best practice, assign all ports to a null VLAN. The “null” VLAN can be considered as the Quarantine VLAN, meaning that the ports have no VLAN assignment. This is the most secure setting.

To add ports to the null VLAN, simply remove them from the VLAN that they are currently configured for. Perform this procedure for all ports that are in VLAN 1, if any.

1. Verify the port VLANs assignment:

```
Switch:#show vlan
Id  Name                 Type     Protocol         PID      Active IVL/SVL Mgmt
--- -------------------- -------- ---------------- -------- ------ ------- ----
1   VLAN #1              Port     None             0x0000   Yes    IVL     No
        Port Members: 1/2-26,2/1-48,3/1-48
```

```
2   VLAN #50             Port     None             0x0000   Yes    IVL     Yes
        Port Members: 1/1
Total VLANs: 2
```

2. In this example VLAN #1 has some ports assigned. To assign them to the “null” VLAN you must remove them from VLAN #1 or from any other VLAN they are assigned to:

```
Switch:(config)#vlan members remove 1 1/2-26,2/1-48,3/1-48
Switch:#show vlan
Id  Name                 Type     Protocol         PID      Active IVL/SVL Mgmt
--- -------------------- -------- ---------------- -------- ------ ------- ----
1   VLAN #1              Port     None             0x0000   Yes    IVL     No
            Port Members: NONE
2   VLAN #50             Port     None             0x0000   Yes    IVL     Yes
            Port Members: 1/1
Total VLANs: 2
```

QoS configuration example

The following is an example of configuring QoS on switch.

By default the switch uses 2 priority queues. The switch supports up to 8 queues. The following is an example of changing the number of available queues for QoS.

1. Verify the default configuration, using 2 priority queues:

```
Switch:#show qos agent
QoS Operational Mode: Enabled
QoS NVRam Commit Delay: 10 seconds
QoS Current Queue Set: 2
QoS Next Boot Queue Set: 2
QoS Current Buffering: Large
QoS Next Boot Buffering: Large
QoS UBP Support Level: Disabled
QoS Default Statistics Tracking: Aggregate
QoS DoS Attack Prevention: Disabled
    Minimum TCP Header Length: 20
    Maximum IPv4 ICMP Length: 512
    Maximum IPv6 ICMP Length: 512
Auto QoS Mode: Disabled
Switch:#show qos queue-set 2

Set Queue        General        Bandwidth Bandwidth  Service  Size
ID   ID        Discipline          (%)    Allocation  Order  (Bytes)


___ _____ ____________________ _________ __________ _______ _______
2   1     Priority Queuing     100       Relative   1       180128
2   2     Priority Queuing     100       Relative   2       81952
```

2. Change the number of available queues for QoS to 6, or to the appropriate number of queues.

```
Switch:(config)#qos agent queue-set 6
```

3. Reboot the switch:

```
Switch:(config)#boot
```

4. Check the new queue-set in use and queue-set queues used:

```
Switch:#show qos agent
QoS Operational Mode: Enabled
QoS NVRam Commit Delay: 10 seconds
QoS Current Queue Set: 6
```

```
QoS Next Boot Queue Set: 6
QoS Current Buffering: Large
QoS Next Boot Buffering: Large
QoS UBP Support Level: Disabled
QoS Default Statistics Tracking: Aggregate
QoS DoS Attack Prevention: Disabled
    Minimum TCP Header Length: 20
    Maximum IPv4 ICMP Length: 512
    Maximum IPv6 ICMP Length: 512
Auto QoS Mode: Disabled
Switch:#show qos queue-set 6
Set Queue        General        Bandwidth Bandwidth  Service  Size
ID   ID        Discipline          (%)    Allocation  Order  (Bytes)

___ _____ ____________________ _________ __________ _______ _______
6   1     Priority Queuing     100       Relative   1       51168
6   2     Weighted Round Robin 52        Relative   2       49296
6   3     Weighted Round Robin 24        Relative   2       47216
6   4     Weighted Round Robin 14        Relative   2       43056
6   5     Weighted Round Robin 7         Relative   2       37440
6   6     Weighted Round Robin 3         Relative   2       34320
```

5. Configure 4 priority queues and trust for IPv4 DSCP and IPv6 Traffic Class values:
   - Configure queue set 4 and reboot:

     ```
     Switch:(config)#qos agent queue-set 4
     Switch:(config)#boot
     ```

   - Verify if the new queue-set is in use:

     ```
     Switch:#show qos agent
     QoS Operational Mode: Enabled
     QoS NVRam Commit Delay: 10 seconds
     QoS Current Queue Set: 4
     QoS Next Boot Queue Set: 4
     QoS Current Buffering: Large
     QoS Next Boot Buffering: Large
     QoS UBP Support Level: Disabled
     QoS Default Statistics Tracking: Aggregate
     QoS DoS Attack Prevention: Disabled
         Minimum TCP Header Length: 20
         Maximum IPv4 ICMP Length: 512
         Maximum IPv6 ICMP Length: 512
     Auto QoS Mode: Disabled
     ```

   - Configure QoS interface group for trusting IPv4 DSCP and IPv6 Traffic Class values, assign interface group to switch interfaces

     ```
     Switch:(config)#qos if-group name trust class trusted
     Switch:(config)#qos if-assign port 1/ALL,2/ALL,3/ALL,4/ALL name trust
     ```

   - Verify QoS interface group and interface assignment:

     ```
     Switch:#show qos if-group
            Role            Interface       Capabilities     Statistics   Storage
        Combination           Class                           Tracking     Type

     ____________________ _____________ ____________________ __________ ___________
     allQoSPolicyIfcs     Untrusted     Input 802, Input IP Aggregate  ReadOnly
     trust                Trusted       Input 802, Input IP Aggregate  NonVolatile
     $qosDisabledIfcs     Unrestricted  Input 802, Input IP Disabled   Other

     Switch:#show qos if-assign
     Unit Port IfIndex Role Combination Queue Set Capability  DAPP Support
     ____ ____ _______ ________________ _________ __________ ____________
     1    1    1       trust            4         Version 1,2 Yes
     1    2    2       trust            4         Version 1,2 Yes
     1    3    3       trust            4         Version 1,2 Yes
     ```

```
1    4    4       trust            4         Version 1,2 Yes
...
```

6. Queue custom egress maps and queues assignment for custom DSCP/Traffic Class values.
   - This example uses the following standard traffic pattern:
     - Voice - DSCP 49 & 15
     - Video - DSCP 39
     - Preferred Data - DSCP 11
     - Best Effort - DSCP 0
   - Assign each traffic pattern to a specific queue. In this example voice traffic with DSCP 15 must be re-marked as DSCP 45.
   - Change egressmap settings, map DSCP values to Layer 2 COS values:

```
Switch:(config)#qos egressmap ds 11 1p 1 dp low-drop ds-new 11
Switch:(config)#qos egressmap ds 15 1p 5 dp low-drop ds-new 45
Switch:(config)#qos egressmap ds 39 1p 4 dp low-drop ds-new 39
Switch:(config)#qos egressmap ds 49 1p 5 dp low-drop ds-new 49
```

   - Verify egressmap settings:

```
Switch:#show qos egressmap ds 0
DSCP 802.1p Priority Drop Precedence New DSCP       Name
____ _____________ _______________ ________ _________________
0    0             High Drop       0        Standard Service
Switch:#show qos egressmap ds 11
DSCP 802.1p Priority Drop Precedence New DSCP       Name
____ _____________ _______________ ________ _________________
11   1             Low Drop        11       Standard Service
Switch:#show qos egressmap ds 15
DSCP 802.1p Priority Drop Precedence New DSCP       Name
____ _____________ _______________ ________ _________________
15   5             Low Drop        45       Standard Service
Switch:#show qos egressmap ds 39
DSCP 802.1p Priority Drop Precedence New DSCP       Name
____ _____________ _______________ ________ _________________
39   4             Low Drop        39       Standard Service
Switch:#show qos egressmap ds 49
DSCP 802.1p Priority Drop Precedence New DSCP       Name
____ _____________ _______________ ________ _________________
49   5             Low Drop        49       Standard Service
```

   - Assign Layer 2 COS priorities to appropriate QoS queues. This examples assumes queue-set 4 configured above.

```
Switch:(config)#qos queue-set-assignment queue-set 4 1p 1 queue 3
Switch:(config)#qos queue-set-assignment queue-set 4 1p 4 queue 2
Switch:(config)#qos queue-set-assignment queue-set 4 1p 5 queue 1
```

   - Verify QoS queue-set assignment:

```
Switch:#show qos queue-set-assignment queue-set 4

Queue Set 4
802.1p Priority Queue
_______________ _____
0               4
1               3
2               4
3               4
4               2
```

```
5               1
6               1
7               2
```

7. Configure interface queue shapers for specific queues.
   - Configure queue shapers per uplink ports with desired rates for Voice, Video and Preferred data queues above. This example assumes the following requirements:
     - Voice queue - shaped at 2.49 Gbps
     - Video queue - shaped at 1.49 Gbps
     - Preferred data queue - shaped at 3.99 Gbps

```
Switch:(config)#interface Ethernet ALL
Switch:(config-if)#qos if-queue-shaper port 1/36,1/51,2/28,3/27,4/28 queue 1
shape-rate 2490000 shape-min-rate 0
Switch:(config-if)#qos if-queue-shaper port 1/36,1/51,2/28,3/27,4/28 queue 2
shape-rate 1490000 shape-min-rate 0
Switch:(config-if)#qos if-queue-shaper port 1/36,1/51,2/28,3/27,4/28 queue 3
shape-rate 3990000 shape-min-rate 0
Switch:(config-if)#exit
```

8. Verify overall QoS config.

```
Switch:#show run mod qos
! Embedded ASCII Configuration Generator Script
! Base model = Ethernet Routing Switch 5952GTS-PWR+
! Base Software version = v7.2.0.009
!Stack Base Unit = 1
! Stack info:
!Unit# Switch Model     Pluggable Pluggable Pluggable  Pluggable SW Version
!                         Port      Port      Port       Port
!----- ---------------- --------- --------- --------- ---------- ----------
!1     5952GTS-PWR+     (49) SX   (50) None (51) SR    (52) None v7.2.0.009
!2     5928GTS-PWR+     (25) None (26) SX   (27) None  (28) SR   v7.2.0.009
!3     5928GTS-PWR+     (25) None (26) None (27) SR    (28) None v7.2.0.009
!4     5928GTS-uPWR     (25) None (26) None (27) None  (28) SR   v7.2.0.009
!
! Displaying only parameters different to default
!================================================
enable
configure terminal
!
! *** QOS ***
!
qos if-group name trust class trusted
interface Ethernet ALL
qos if-queue-shaper port 1/36,1/51,2/28,3/27,4/28 queue 1 shape-rate 2490000 shape-
min-rate 0
qos if-queue-shaper port 1/36,1/51,2/28,3/27,4/28 queue 2 shape-rate 1490000 shape-
min-rate 0
qos if-queue-shaper port 1/36,1/51,2/28,3/27,4/28 queue 3 shape-rate 3990000 shape-
min-rate 0
exit
qos if-assign port 1/ALL,2/ALL,3/ALL,4/ALL name trust
!qos agent queue-set 4
qos egressmap ds 11 1p 1 dp low-drop ds-new 11
qos egressmap ds 15 1p 5 dp low-drop ds-new 45
qos egressmap ds 39 1p 4 dp low-drop ds-new 39
qos egressmap ds 49 1p 5 dp low-drop ds-new 49
qos queue-set-assignment queue-set 4 1p 1 queue 3
qos queue-set-assignment queue-set 4 1p 4 queue 2
qos queue-set-assignment queue-set 4 1p 5 queue 1
```

Glossary

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.
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.
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.
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.
CLI	Command Line Interface (CLI) is a text-based, common command line interface used for device configuration and management across Extreme Networks products.
CLI 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.
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)	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 Extreme Networks 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	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 for certain devices. For example, you can configure a higher priority for 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 Extreme Networks 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.
stack	Stackable Extreme Networks Ethernet Routing Switch 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 Extreme Networks 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/ Internet Protocol (TCP/IP)	Provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems—TCP/IP signifies the family of common Internet Protocols that define the Internet. Transmission Control Protcol 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.